

802.11ac Wireless Access Point Model WAC120

Reference Manual



August 2014 202-11353-01

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.

Compliance

For regulatory compliance information, visit http://www.netgear.com/about/regulatory.

See the regulatory compliance document before connecting the power supply.

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 Hardware Setup

System Requirements	6
Unpack Your Access Point	6
Front and Side View	7
LEDs and Buttons	7
Rear View	8
Label	9

Chapter 2 Initial Setup

Install the Access Point
Connect to the Access Point and Log In
Specify the Access Point Name and Location
Set the Time
Configure the Basic IP Settings 15
Set Up and Test Wireless Connectivity
Basic Wireless Settings 17
Wireless On-Off Schedule
Wireless Security Options 21
Wireless Security Profiles
MAC Authentication
Connect Stations to the Wireless Access Point
QoS Settings
Deploy the Access Point
Position Your Access Point

Chapter 3 Network Settings

Set Up an 802.1Q VLAN	33
Advanced Wireless Settings.	34
Advanced QoS Settings	37
Wireless Bridging and Repeating.	39
Wireless Point-to-Point Bridge Mode	41
Wireless Point-to-Multi-Point Bridge Mode	43
Client Mode	46

Chapter 4 Manage the Access Point

Change the admin Password	49
Upgrade the Firmware	49
Manage the Configuration File	51

	Back Up the Configuration File	5	1
	Restore the Configuration File	5	1
	Restore the Factory Default Settings	5	2
En	able a Syslog Server	5	3

Chapter 5 Monitoring

View System Information.	56
View Available Wireless Stations.	57
Activity Log	58
View Network Traffic Statistics	59

Chapter 6 Troubleshooting and Debugging

Troubleshooting with the LEDs	. 62
All LEDs Are Off	. 62
LAN LED Is Off	. 62
WLAN LED Is Off.	. 62
Cannot Connect to the Access Point to Configure It	. 63
Wireless Access to the Network	. 63
Time-Out Error for URL or IP Address	. 63

Appendix A Supplemental Information

Factory Settings	. 66
Technical Specifications	. 70

Hardware Setup

1

This chapter covers the following topics:

- System Requirements
- Unpack Your Access Point
- Front and Side View
- Rear View

For more information about the topics covered in this manual, visit the support website at *http://support.netgear.com*.

Firmware updates with new features and bug fixes are made available from time to time at *http://downloadcenter.netgear.com*. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this guide, you might need to update your firmware.

System Requirements

Before installing the access point, make sure that your system includes the following:

- A 10/100/1000 Mbps local area network device such as a hub or switch
- The Category 5 UTP straight-through Ethernet cable with RJ-45 connector included in the package, or one like it
- A 100–120 V, 50–60 Hz AC power source
- A web browser for configuration
- At least one computer with the TCP/IP protocol installed
- 802.11b/g-compliant or 802.11b/g-compliant devices

Unpack Your Access Point

Your package contains the following items.



Figure 1. Package contents

Your box contains the following items:

- 802.11ac Wireless Access Point Model WAC120
- 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.

Front and Side View



The status LEDs and icons on the front and side panels are shown in the following figure.

Figure 2. Front and side view

LEDs and Buttons

The LEDs on the wireless access point light to indicate wireless access point activity:

LED	Description		
Power	 Off. Power is off. Green. Power in on. Amber. A self-test is running. During startup the LED is amber, then blinking green before turning steady green after 45 seconds. If the LED is amber or continues blinking green after one minute, a system fault exists. 		
Activity	 Off. No Ethernet traffic is detected. Green or blinking green. Ethernet traffic is detected. 		

Table 1. LEDs (continued)

LED	Description			
LAN	 Off. No link is detected. Green. A 1000 Mbps link is detected. Amber. A 100 Mbps or 10 Mbps link is detected. 			
WiFi	 Off. Both the 2.4G and 5G radios are off. Green. The 2.4G, 5G, or both radios are ready. Blinking green. Wireless activity of 2.4G or 5G is detected. Slow blinking green. WPS is enabled. 			

The WiFi and WPS buttons toggle the WiFi and WPS functions on and off, as follows:

- WiFi On/Off button. Pressing and holding this button for two seconds turns the 2.4 GHz and 5 GHz wireless radios on or off. If the WiFi LED is lit, the wireless radios are on. If this LED is off, the wireless radios are 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 slowly, green for three seconds, then off for three seconds, when the access point is trying to add the wireless device or computer.

Rear View

The buttons and connections on the back panel are shown in the following figure.



Figure 3. Rear view

Pressing the **Reset** button restores the factory settings. See *Factory Settings* on page 66.

Label

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

Default access information



Figure 4. The label shows unique information about your router

Initial Setup

2

This chapter covers the following topics:

- Install the Access Point
- Connect to the Access Point and Log In
- Specify the Access Point Name and Location
- Set the Time
- Configure the Basic IP Settings
- Set Up and Test Wireless Connectivity
- QoS Settings
- Deploy the Access Point

Install the Access Point

Make sure that your Internet service is active before you install your access point.

> To install your access point:

1. Prepare your network.



Make sure that your modem is cabled only to the wall jack for your Internet service.

2. Connect your devices.



- **a.** Plug in, then turn on your gateway or modem.
- **b.** With an Ethernet cable, connect your gateway or modem to a network switch.
- **c.** With the Ethernet cable that came with the access point, connect the network switch to the LAN port on your access point.

- 3. Add power to the access point:

- **a.** Connect the power adapter to the access point and plug the power adapter into an outlet.
- **b.** Wait for the Power LED on the front panel to light amber and turn green.

If no LEDs are lit, press the **Power On/Off** button on the rear panel of the access point.



4. Connect a computer.

Connect to the Access Point and Log In

You can connect to the access point's web management interface to view or change its LAN and wireless access settings.

> To connect to the access point:

1. Configure a computer with a static IP address of 192.168.0.210 and a subnet mask of 255.255.255.0.

For help configuring a static IP address on your computer, check the instructions or online help that came with that computer.

- 2. Connect the Ethernet cable to the computer.
- 3. Connect the other end of the Ethernet cable to the LAN port on the access point.
- 4. Connect the power adapter to the access point and plug the power adapter into a power outlet.
- 5. Press the On/Off button on the access point.
- 6. On the computer that is connected to the access point, enter http://192.168.0.100 in the address field of a browser.

A login screen displays.

7. Enter admin for the user name and password for the password.

The web management interface of the access point displays.

NETGEA	R'	WAC120 Product Day In Workson AC Assess Pro	
Testen IP No	where her artic Wreeless finds	Laport .	
	General	197.7WA 2	
	General		
Advanced	Access Point Name Country / Region	netgesc104480	

Specify the Access Point Name and Location

You must use a computer that is configured with a static IP address of 192.168.0.210 and a subnet mask of 255.255.255.0. During initial setup, use a wired Ethernet connection from the computer to the access point.

> To specify the access point name and location:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA Confectation	R' Notificities Habitmenter	Separat		WAC120 Perferin Duel Band Workson AC Assessed Fact
Tables 2P Mir	nless Secondy Wreless Bridg	in i wina		
-	General			
a These	General			
Advanced	Accume Point Name Country / Region	netgear234480 posied Ittatee		

4. In the Access Point Name field, type the access point name.

This unique name is the access point NetBIOS name. The access point name is printed on the product label of the access point. The default is netgearxxxxx, where xxxxxx represents the last 6 digits of the access point MAC address. You can replace the default name with a unique name up to 15 characters long.

5. From the Country/Region list, select the region where the access point is located.

In the United States this setting cannot be changed. If your country or region is not listed, check with NETGEAR support for the correct selection.

6. Click the Apply button.

Your settings are saved.

Set the Time

You must use a computer that is configured with a static IP address of 192.168.0.210 and a subnet mask of 255.255.255.0. During initial setup, use a wired Ethernet connection from the computer to the access point.

- > To set the time:
 - 1. Launch a web browser on the computer that is connected to the access point.
 - 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R'	WAC120 Periodic Dual Band Western AC Assess Part	
Configuration	Persitaring Paintmann	Sapport	Second Street Street Law 2.
Tester 1P We	eless firearity Wereless firsty	e : wes	
-	General		
	General		
Advanced	Access Point Barnel	respectivelity	
	Country / Region	poined States (w)	

4. Select Configuration > System > Basic > Time.

Configuration	Hastoling Nationalis	mappet	(m
System (av) min	efteen Security Mindees Brad	e 1895	
- Rents Inc.	Time		
* Cerend	Time Settings		
Advanced	Tome Jone Carrowi Tome BTF Cloud Use Caston HTP Server Heatmans / JF Address	ISA-Perfe Tue Jan ID (A 03-05 PPT 1815 # Analos © Double D	

- 5. Adjust the following fields:
 - **Time Zone**. From the list, select the local time zone for your access point. The default is USA-Pacific. The access point gets the current time from the connecting computer.
 - **NTP Client**. Enable the NTP client to synchronize the time of the access point with an NTP server. The **Enable** radio button is selected by default.

Note: You need an Internet connection to get the current time using an NTP client.

- Use Custom NTP Server. Select this check box if you use a custom NTP server. The check box is cleared by default.
- **Hostname / IP Address**. Enter the host name or the IP address of the custom NTP server. The default is time-b.netgear.com.
- 6. Click the **Apply** button.

Your settings are saved.

Configure the Basic IP Settings

The default settings work in most cases. However, if your access point is part of a more complex LAN network, modify these settings to meet the requirements of your network.

You must use a computer that is configured with a static IP address of 192.168.0.210 and a subnet mask of 255.255.255.0. During initial setup, use a wired Ethernet connection from the computer to the access point.

> To configure the basic IP settings:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R'		WAC120 Products Dual Bread
Configuration	Persilaring Paintenance	Sapport	Second Second Second
Section (10) and	niesa Secarity Wreless firsty	e : wes	
1 Marca 1	General		
a second	Cetural		
Advanced	Accuse Point Barne Country / Region	retgen 134482 (m)	

4. Select Configuration > IP.

The IP Settings screen displays.

Configuration Handburg Hainburgers S	Septert	(cuun)
System (Wenters Security Wenters Bridge	Here:	
IP Settings		
1P Settlege	10	
DHCP Cheat	C traite # thatis	
3P Address	198.000.0.100	
1P Subrot Have	211.215.288.0	
Befault Cateway		
Primary 2665 Server		
Amoundary DRS Servey		
Network Integrity Check	(D)	

- **5.** If necessary, specify the following settings:
 - DHCP Client. By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If your LAN includes a DHCP server and you enable DHCP, the access point gets its IP address, subnet mask, and default gateway settings automatically from the DHCP server on your network when you connect the access point to your LAN.
 - **IP Address**. The IP address of your access point. The default IP address is 192.168.0.100. To change it, enter an unused IP address from the address range used on your LAN, or enable DHCP.
 - **IP Subnet Mask**. The access point calculates the subnet mask based on the IP address that you assign. Otherwise, you can use 255.255.255.0 (the default) as the subnet mask.
 - **Default Gateway**. 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 access point is connected. The default is 0.0.0.0.
 - **Primary DNS Server**. The IP address for the primary Domain Name Server used by stations on your LAN. The default is 0.0.0.0.
 - Secondary DNS Server. The IP address for the secondary Domain Name Server used by stations on your LAN. The default is 0.0.0.0.
- 6. Click the Apply button.

Your settings are saved.

If you changed the subnet of the LAN IP address, you are disconnected from the access point user interface. To reconnect, reconfigure your computer with a static IP address within the new LAN IP subnet.

Set Up and Test Wireless Connectivity

This section covers the following topics:

- Basic Wireless Settings
- Wireless On-Off Schedule
- Wireless Security Options
- Wireless Security Profiles
- MAC Authentication
- Connect Stations to the Wireless Access Point

You must use a computer that is configured with a static IP address of 192.168.0.210 and a subnet mask of 255.255.255.0. During initial setup, use a wired Ethernet connection from the computer to the access point.

Basic Wireless Settings

- > To configure the basic wireless settings:
 - 1. Launch a web browser on the computer that is connected to the access point.
 - 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R		WAC120 Parliety Dual Band Workson AC Assesse Taget
Configuration	Residentes Relationers	Sapport	Second Se
States 27 201	niena Socarity Wereless Bridy	e: 1 WPS	
-	General		
	General	-	
Advanced	Accuse Point Name Country / Region	Pergenet294930 (m)	

- 4. Select Configuration > System.
- 5. Verify that the correct country or region is selected.
- 6. If you changed the setting, click the **Apply** button.

Your settings are saved.

7. Select Configuration > Wireless.

A dama	Wireless Settings		
T- photomer (1- 147	Windows Selfings	*	
- Quit Sattrage Advanced	NULIN/NU/NET NELINIAUN		
	Wireless Hode Lars Radio (b) Mireless Network Name (2010) RF Switch Status Wireless (b)-Off Status	3.450he Rawel C Line C Line, * Sing?" R Networks, sing	
	Breadcast Wireless Helesch Nesse (1922) Channel / Frequency	R Tala () Bala (After ())	
	Channel Width	30 HP4 (m)	
	Gaard Intervel Datput Power	Auto II	

Change any of the default settings that you want to change.

- 8. Select a Wireless Mode radio button:
 - **11b**. All 802.11b wireless stations can be used. (The 802.11g wireless stations can still be used if they can operate in 802.11b mode.)
 - **11bg**. Both 802.11b and 802.11g wireless stations can be used.
 - **11ng**. All 11b, 11g, and 11ng wireless stations can be used. This is the default. If you select this option, then two additional lists, **Channel Width** and **Guard Interval**, display.
 - **Note:** If you select a wireless mode option and other settings on this screen are disabled, then you must select the **Turn Radio On** check box to enable options on this screen.
- 9. Select the Turn Radio On check box.

This check box is selected 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. The following information displays:

- **RF Switch Status**. This field displays the status of the hardware RF switch that is available on the access point. When the RF switch is enabled, this field shows ON in green. When the RF switch is disabled, it shows OFF in red and users cannot change any wireless parameter.
- Wireless On-Off Status. This field displays the status of the Wireless On-Off feature. When this feature is enabled, this field shows ON in green and users cannot change the radio status. When this feature is disabled, it shows OFF in red.

For information about how to turn the wireless radio on and off according to a schedule, see *Wireless On-Off Schedule* on page 20.

10. Enter a wireless network name in the Wireless Network Name (SSID) field.

This is the name of your wireless network. It is set to the default name of NETGEAR_11a for 802.11a/n devices and NETGEAR_11ng for 802.11b/g/n devices.

- **Note:** The SSID of any wireless client must match the SSID you configured in the access point. If they do not match, you cannot get a wireless connection.
- 11. Select the Broadcast Wireless Network Name (SSID) Yes radio button.

If you disable broadcast of the SSID, only devices that use 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. By default, the **Yes** radio button is selected.

12. Ensure that the **Auto** is selected in the **Channel / Frequency** list. This feature selects a channel that ensures the least interference.

You do not need to change the wireless channel unless you notice interference 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 access point.

The wireless channel in use can be from 1 to 11 for the United States and Canada, or 1 to 13 for Europe and Australia. The default is Auto.

Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is the best. If you select the **Auto** channel option, the access point automatically picks the channel with the least interference. When selecting or changing channels, bear these points in mind:

- Access points use a fixed channel. You can select the channel used. This allows you to select a channel that provides the least interference and best performance. In the United States and Canada, 11 channels are available.
- If you are using multiple access points, it is better if adjacent access points use different channels to reduce interference. NETGEAR recommends channel spacing between adjacent access points of 5 channels (for example, use Channels 1 and 6, or 6 and 11).
- Wireless stations usually 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 happen only when the access points use the same SSID.
- **Note:** If you want to use wireless bridging and repeating, you must select a specific channel for your network. For more information, see *Wireless Bridging and Repeating* on page 39.

13. From the list, select the MCS Index/Data Rate.

You can select the transmit data rate of the wireless network. Depending on the band selected, the set of rates varies. (When the auto channel is enabled in the 802.11ng mode, then the default channel width mode is 20 MHz. In this case, you cannot modify this parameter unless you change to a static channel.) For the possible supported data rates, see *Technical Specifications* on page 70.

14. From the list, select the Channel Width.

Select the available channel width of the access point. A wider channel improves the performance, but some legacy devices can operate only on either 20 MHz or 40 MHz. The following channel width options are available:

- **20 MHz**. This is the static, legacy mode. It gives the least throughput.
- **40 MHz**. This is the static, high-throughput mode. Legacy clients cannot connect in this mode.
- **80 MHz**. This setting is available for the 5 GHz band only.
- **20/40 MHz**. This is the dynamic compatibility mode. Legacy clients can connect to 20 MHz and 11n clients can connect to 40 MHz.
- 20/40/80 MHz. This setting is available for the 5 GHz band only.

15. From the list, select the **Guard Interval**.

The guard interval protects from interference from other transmissions. The default is Auto.

16. From the list, select the **Output Power**.

This is the transmit power of the access point. The options are Full, Half, Quarter, Eighth, and Minimum. Decrease the transmit power if two or more access points are close together and use the same channel frequency. The default is Full. The transmit power might vary depending on the local regulatory regulations.

17. Click the **Apply** button.

Your settings are saved.

18. Configure and test your remaining wireless clients for wireless connectivity.

Check that they are connected wirelessly and can obtain an IP address by DHCP from the access point. Then you can configure the wireless security.

Wireless On-Off Schedule

If you do not want the wireless radio on all the time, you can turn the wireless radio on and off according to a schedule.

> To configure the wireless on-off schedule:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R' Relations	Gapanet	WAC120 Profeste Dual Band Workson AC Assess Part
Testen (17) and	nlana Sanardy Weeless Bruh	at 1 week	
a there	General		
Advanced	Accuse Point Name Country / Region	retgenrith+Hit	

4. Select Configuration > Wireless > Basic > Wireless On-Off.

Configuration (1	bailturing Holatomator	Support	(
Appleon IP (Rivela	B BecarRy Workins Brid	e l'arra	
	Wireless On-Off		
* thi sidel beforge	Windows On Off	*	
· (just their up)	Wheeless Do-Dff	Cox # or	
Advented	state off schedule	5555555	
	Rada ON Tone	T I DE INT	
	Rada-Off Time	THE COLUMN TWO	

5. To enable the wireless on-off schedule, select the Wireless On-Off **On** radio button.

To disable the schedule, select the **Off** radio button.

- 6. To select the days of the week when you want the wireless radio to be off, select the Radio off schedule check boxes that correspond to those radio-off days.
- 7. To select the time of day when the wireless radio is to turn on, in the **Radio ON Time** field, enter the hour and minute.
- 8. To select the time of day when the wireless radio is to turn off, in the **Radio OFF Time** field, enter the hour and minute.
- 9. Click the **Apply** button.

Your settings are saved.

Wireless Security Options

Anyone with a compatible wireless adapter can receive your wireless data transmissions well beyond your walls. For this reason, use the security features of your wireless equipment. The access point provides highly effective security features, which are covered in detail in this chapter. Deploy the security features appropriate for your needs.

You can enhance the security of your wireless network in several ways:

- Use the WPA2 or WPA security option. A security option is the type of security protocol applied to your wireless network. The security protocol encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. Several types of encryption are available: Wi-Fi Protected Access II (WPA2), WPA, and Wired Equivalent Privacy (WEP).
 - WPA2 is the latest and most secure. NETGEAR recommends that you use this option if your equipment supports it.

- WEP and TKIP provide only legacy (slower) rates of operation. NETGEAR recommends AES encryption so that you can use the 11n rates and speed.

For more information, see Wireless Security Profiles on page 22.

- Connect stations manually. When you initiate a WPS connection, you provide a short window of two minutes for a WPS-capable wireless client to join your network. Once the connection is made, the intruder can learn your wireless security settings and rejoin your network at a later time. For more information, see *Connect Stations to the Wireless Access Point* on page 26.
- Keep watch over your wireless network. Regularly monitor the wireless stations that are allowed to connect to your access point and make sure that all of them are legitimate. For more information, see *View Available Wireless Stations* on page 57.
- **Change the login password regularly**. When you use the default login password, an intruder can more easily figure out how to log in to the management interface of the access point and change the settings. For more information, see *Change the admin Password* on page 49.

Note: For additional wireless security, you can change the default network key regularly. But whenever you change the network key, you must reconnect all of the wireless devices. For more information, see *Wireless Security Profiles* on page 22.

- **Turn off the wireless radio**. During the hours when your offices are closed, turn off the wireless radio. For more information, see *Wireless On-Off Schedule* on page 20.
- **Turn off the broadcast of the wireless network name (SSID)**. If you disable broadcast of the SSID, only devices that use 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. For more information, see *Wireless Security Profiles* on page 22.
- **Restrict access based on MAC address**. You can restrict access to only trusted computers so that unknown computers cannot connect wirelessly to the access point. MAC address filtering adds an obstacle against unwanted access to your network. For more information, see *MAC Authentication* on page 24.

Wireless Security Profiles

Details of each wireless network are contained in a security profile. You can edit up to eight security profiles for each SSID. Each security profile contains the following information:

- **Profile name**. This is the unique profile name. This value can be up to 32 alphanumeric characters.
- **SSID**. This is the current SSID associated with this profile.
- **Security**. This is the current security standard, such as WPA-PSK, associated with the profile.

> To edit the security profile settings:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA Configuration	R'	Separe	WAC120 Products David Band Woolcon AC Acatel Part
States 27 300	nless / Secondy / Weeksa Bedg	e i wes	
-	General		
a these	General		
Advanced	Accuse Point Harse Country / Region	retges 134410	

4. Select Configuration > Security.

Configuration	Nuclturing Nationance Support	(14==1)
System IP Store	line (Martine) Workers Bridge (1875	
Advanced	Profile Settings Profile Settings	
	NELECTION OF SECTION O	

For initial configuration and testing, the **Security** field for Profile 1 (the default profile) is set to Open System and the SSID is set to NETGEAR_11ng (for information about how to configure a profile, see *Basic Wireless Settings* on page 17).

- **Note:** The SSID of any wireless client must match the SSID you configured in the access point. If they do not match, you cannot get a wireless connection.
- 5. Select the profile that you want to change and click the **Edit** button.

Configuration	Hondoring Hairdenores Support	0	
System 1971 March	ene / Gecurity Windows Bridge 1995		
-	Edit Security Profile		
Advanced	Profile Defaition		
	Weekse Kelwerk Rame (NSD) Droadcart Weekse Vetwork Rame (Authoritistism Settings	infidint_ling salid) € tes ○ tes	
	Network Authoritication Data Encryption 1974 Pape 1974 Paraphrane (Network Key) 1974 Pist Works Chart Security Separation	ering-Atter. (v) Atts (v) Pipe (* Pessphreen Deatter(+)	

The fields that display depend on the settings.

- 6. To change the wireless network name, in the Wireless Network Name (SSID) field, enter the new wireless network name.
- To broadcast the wireless network name, select the Broadcast Wireless Network Name (SSID) Yes radio button.
- 8. In the **Network Authentication** list, select the authentication type:
 - **Open System**. This selection can be used with WEP encryption or no encryption.
 - **WPA2-PSK**. Select this option only if all clients support WPA2. If you select this option, you must use AES and 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 you select this option, you must use TKIP + AES encryption and enter the WPA passphrase (network key).
- 9. In the **Data Encryption** list, select the data encryption type.

The options available for data encryption depend on the the option you select in the **Network Authentication** list.

- None. No encryption is used.
- **64 bits WEP**. Standard WEP encryption, 40/64-bit encryption is used.
- **128 bits WEP**. Standard WEP encryption, 104/128-bit encryption is used.
- **152 bits WEP**. Proprietary mode, works only with other wireless devices that support this mode is used.
- **AES**. This is the standard encryption method for WPA2. Some clients support AES with WPA, but this access point does not.
- **TKIP + AES**. 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.
- **10.** In the **Wireless Client Security Separation** list, specify if you want the associated wireless clients to be able to communicate with each other.

If you select **Enable**, the associated wireless clients cannot communicate with each other. This feature is intended for hotspots and other public access situations.

11. Click the **Apply** button.

Your settings are saved.

MAC Authentication

For an additional layer of security, you can allow only trusted stations to interact with the access point.

- > To configure MAC authentication:
 - 1. Launch a web browser on the computer that is connected to the access point.

Enter http://192.168.0.100 in the address field of the browser.
 A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEAR			WAC120
Configuration	Notarity Haistmann	Contraction of House, 1.	
States 27 340	nless Secondy Weekess Bridg	e 1 WPS	
-	General		
a Tana	General		
Advanced	Accume Point Harne Country / Region	retgenet34480 Jonied States (=)	

4. Select Configuration > Security > Advanced > MAC Authentication.

Profile Sollings	MAC Authentication	
and and a set of the	HAC industrialise	
a frances and	911.115/bg/vg ⁻¹ 882.216/inf m ⁻¹	
	Term Access Lastred De	
	Relact Access Castrol Dalakase Land MhC Address Catalogs	
	PAL Address	
	1 10 FD RD 40 A0-04	

- 5. To enable MAC authentication, select the **Turn Access Control On** check box.
- 6. Select a database from the Select Access Control Database list.

The access point uses the local MAC address table for access control.

The Trusted Wireless Stations list displays the trusted wireless stations.

- 7. To add a station to the Trusted Wireless Stations list, enter its MAC access in the **MAC** Address field and click the Add button.
- 8. To delete a station from the Trusted Wireless Stations list, select the station that you want to delete and click the **Delete** button.
- **9.** To view the available wireless stations in the area, select check box in the Available Wireless Stations list and click the **Refresh** button.

The wireless stations in the area display.

10. To add an available wireless station to the Trusted Wireless Stations list, select the station that you want to add and click the **Move** button.

The wireless station displays on the Trusted Wireless Stations list.

11. Click the **Apply** button.

Your settings are saved.

Connect Stations to the Wireless Access Point

Connect wireless devices such as desktops, laptops, smartphones, and tablets to your access point. You can connect these WiFi devices either manually or using the WPS (Wi-Fi Protected Setup) method.

Manual Method

- > To connect WiFi devices manually to your access point:
 - 1. From your wireless device, view the available wireless networks.

For more information, see the manual that came with your device.

2. From the list of available wireless networks, select the wireless network name (SSID) of the access point.

The SSID is printed on the product label.

3. From your wireless device, initiate a wireless connection.

For more information, see the manual that came with your device.

4. When prompted by your wireless device, enter the wireless network key (password) of the access point.

The password is printed on the product label.

5. From the screen of your wireless device, click the appropriate button to continue the connection procedure.

You are connected wirelessly to the access point.

6. Repeat *Step 1* through *Step 5* for each wireless device that you want to connect to the access point.

Wi-Fi Protected Setup Method

Wi-Fi Protected Setup (WPS) is a standard for easily adding computers and other devices to a wireless network while maintaining security. To use WPS, make sure that all wireless devices to be connected to the network are Wi-Fi certified and support WPS.

For the access point, WPS is disabled by default. When WPS is enabled, you decide which security settings to use when WPS connects wireless clients with the access point.

- Use a wireless client's security settings. A wireless client configures the SSID and wireless security settings of the access point by using the access point's 8-digit wireless PIN that is on the label and WPS Settings screen. With this approach, users must make sure that all wireless clients on the network use the same security settings.
- Use the access point's security settings. The access point configures the SSID and wireless settings of the wireless clients. This approach ensures that each wireless client's security settings match the security settings of the access point.

To enable WPS, MAC authentication must be in its default state of disabled. For more information, see *MAC Authentication* on page 24.

> To configure WPS:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R'	WAC120 Protein Dual Band Western AC America Port	
System (20) and	nless / Secondy / Weeksa Bridg	e i wrs	
1.100	General	No. of Concession, Name	
Advanced	Accuse Point Name Country / Regim	retgear234482	

4. Select Configuration > WPS.

findipatentian (Hostoring Haldmanut	Inspect	
System 11P Mindle	ive i Secondar i Minelene Br	Mar Emmi	
Add 1075 Chest	WPS Settings		
	sars Ar's Pak	C Busin # Dualin Incontin Deaths APs 938 Keep Conting Workers Settings	

5. To enable WPS, select the WPS **Enable** radio button.

WPS is enabled.

6. To disable the access point's PIN, select the **Disable AP's PIN** check box.

The wireless client cannot use the access point's PIN to connect to the access point.

7. To keep the existing access point's wireless settings when a wireless client uses WPS to connect to the access point, select the **Keep Existing Wireless Settings** check box.

Whether you use the access point's PIN or wireless client's PIN to initiate the connection, the access point's preconnection wireless settings stay the same. The client's wireless settings change to the access point's wireless settings after the connection.

8. Click the **Apply** button.

Your settings are saved.

- > To connect WiFi devices to your access point with WPS:
 - 1. Launch a web browser on the computer that is connected to the access point.
 - 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEAR'			WAC120 Protector Dural Band Windows CA Annual Part
Configuration Residenting Relationseen Support			No. 1. The State of S
States 35 860	nless Secondy Weekees Bridy	e i wes	
1	General		
	General		
Advanced	Accuse Point Name Country / Region	netgeneritie48th posted States (m)	

4. Select Configuration > WPS > Add WPS Client.

therigeration	Saituring Haldhouse Support	
System P wirele	ve Security Workey Indge 600	
MPS Settings	Add WPS Client	
	New and many way to connect to His Winglass Access Paint ina WWI Prefected Debug (WWI)	
	de antralises closest fusit les supgestes WHS Particulates les services du cana Une anisant les settés Par riteurs tra sums Veille anachieut Winderse deures (Ferreiri, Ellesses Antralis Films, aux menues) autris généries et provi establises clisent les antralises du cana advantitair é supporte dus 2015 functions. El proce antraleses durant durant provi fuer attriffs functions and advantitair et supporte dus 2015 functions. El proce antraleses durant durant menues durant durant durant durant menues du canadagent dura 2015 functions.	
	Ited	

- 5. Click the **Next** button.
- 6. Select one of the following radio buttons:
 - Push Button (recommended). Click the 👩 button.

Configuration	Numbering Meditionation Topparty	(append)
WPS Settings	Add WPS Client	
	Notes & a Tartag Hallowit P music instrume(Naccommendad) Tara etter andres preser the finale function physically and the annexes point an preser the final physical final function (). Preserve and the instrumental bioartification framework)	

Within two minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.

• **PIN Number**. Select the **PIN Number** radio button and enter the wireless client's security PIN in the field that displays. Click the **Next** button.



Within two minutes, go to the wireless device and use its WPS software to join the network without entering a password. For more information, see the manual that came with your device.

The access point attempts to add the WPS-capable wireless device. The WiFi LED on the access point blinks slowly, green for three seconds, then off for three seconds. The WiFi LED on the access point blinks green when the computer or WiFi device connects to your access point and the access point WPS screen displays a confirmation message.

7. Repeat Step 6 for each wireless device that you want to connect to the access point.

QoS Settings

Wireless Multimedia (WMM) is a subset of the 802.11e standard. WMM allows wireless traffic to receive a range of priorities, depending on the type of data. Time-dependent information, such as video or audio, receives a higher priority than normal traffic. For WMM to function correctly, wireless clients must support WMM. Wi-Fi Multimedia (WMM) is enabled by default in the access point.

You must use a computer that is configured with a static IP address of 192.168.0.210 and a subnet mask of 255.255.255.0. During initial setup, use a wired Ethernet connection from the computer to the access point.

> To change the QoS settings:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R'	Capacity .	WAC120 Petition Dual Band Western AC Assessment Part
Netwood (19 Workers Records Wreless Knige WPS			
-	General		
a these	General		
Advanced	Accuse Point Name Country / Region	retgen:134430	

4. Select Configuration > Wireless > Basic > QoS Settings.

Configuration	Carlignetive Numbering Hamisterates Support		
Numbers 1 art million	Becarity Mindon Bollan (1979		
Perr	Qo5 Settings		
· Women Stational	Qas Settings		
Advanced	#81.116/bg/mg7 [#81.116/m/m/7		
	Enable W-Fi Haltowalia (WHH) # Enable C Daubie BHH Passensave # Enable C Daubie		

- 5. Select the Enable Wi-Fi Multimedia (WMM) Enable or Disable radio button.
- 6. Select the WMM Powersave Enable or Disable radio button.
- 7. Click the **Apply** button.

Your settings are saved.

Deploy the Access Point

Before mounting the access point in a high location, first set up and test the access point to verify wireless network connectivity.

By default, the DHCP client is disabled in the access point. If your network uses dynamic IP addresses, you must change this setting. To connect to the access point after the DHCP server on your network assigns it a new IP address, enter the access point name in your web browser. The default name is netgearxxxxx, where xxxxx represents the last 6 bytes of the MAC address. The default name is printed on the product label.

> To deploy the access point:

1. Disconnect the access point from the computer that you used to configure it, and put the access point where it will be deployed.

The best location is elevated, such as on a wall or ceiling 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. Connect an Ethernet cable from your access point to a LAN port on your router, switch, or hub.
- 3. Connect the power adapter to the wireless access point, and plug the power adapter into a power outlet. The Power and LAN LEDs light, and the WLAN LED blinks.

Position Your Access Point

The access point lets you access your network 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.

Additionally, other wireless access points in and around your location might affect your access point's signal. Wireless access points are access points, repeaters, WiFi range extenders, or any other device that emits a wireless signal for network access.

Position your access point according to the following guidelines

- Place your access point near the center of the area where your computers and other devices operate and within line of sight to your wireless devices.
- Make sure that the access point is within reach of an AC power outlet and near Ethernet cables for wired computers.
- Place the access point in an elevated location, minimizing the number walls and ceilings between the access point and your other devices.
- Place the access point away from electrical devices such as these:
 - Ceiling fans
 - Home security systems
 - Microwaves
 - Computers
 - Base of a cordless phone
 - 2.4 GHz cordless phone
- Place the access point away from large metal surfaces, large glass surfaces, insulated walls, and items such as these:
 - Solid metal doors
 - Aluminum studs
 - Fish tanks
 - Mirrors
 - Brick
 - Concrete
- (Optional) If you use adjacent access points, use different radio frequency channels to reduce interference.

Network Settings



This chapter covers the following topics:

- Set Up an 802.1Q VLAN
- Advanced Wireless Settings
- Advanced QoS Settings
- Wireless Bridging and Repeating

Set Up an 802.1Q VLAN

A Spanning Tree Protocol provides network traffic optimization in locations where multiple access points are present. The 802.1Q VLAN protocol on the access point separates traffic logically on the same physical network. The following choices are available:

 Untagged VLAN. You can allow one VLAN to be configured as an untagged VLAN. When the access point sends frames associated with the untagged VLAN out from the Ethernet LAN interface, these frames are untagged. When the access point receives untagged traffic from the Ethernet LAN interface, these frames are assigned to the untagged VLAN. Otherwise, the access point tags all outgoing Ethernet LAN frames and accepts only incoming frames that are tagged with known VLAN IDs.

Note: You lose IP connectivity when the hubs and switches on your network are not yet configured with the corresponding VLANs. Use untagged VLANs only when the hubs and switches on your LAN support the 802.1Q VLAN standard. Change the default untagged VLAN value only when the hubs and switches on your LAN support the 802.1Q VLAN standard.

Management VLAN. Use management VLANs to manage Telnet, SNMP, and HTTP traffic to and from the access point. Frames belonging to the management VLAN are not given any 802.1Q header when sent over the trunk. When a port is in a single VLAN, the port can remain untagged. But when the port must be a member of multiple VLANs, the port must be tagged.

> To set up an 802.1Q VLAN:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEAR			WAC120 Products David Band
Configuration System (P) Were	Neillering Heilelenanne dens Security Directors finds	Territor Constants	
-	General	1	
a then	General		
Advanced	Accume Point Name Country / Region	panied States	

4. Select Configuration > System > Advanced > General.

Configuration	Mechaning Malafonance	Baggaort	
enteren (189 60a	referes Norsetty Ministers Bridge	I WPS	
Part.	General Spanning True Protocol		
1 Sump	Spanning Tree Protocol	O statie · · · · · · · ·	
	HILLO YLAR		
	Contagged VLAN Management VLAN	1	

- 5. Select the Spanning Tree Protocol **Enable** or **Disable** radio button.
- 6. To require all VLANs to be configured as tagged VLANs, clear the **Untagged VLAN** check box.
- 7. To change the untagged VLAN value, enter the new value in the Untagged VLAN field.
- 8. To change the number of management VLANs, enter the new value in the **Management VLAN** field.
- 9. Click the Apply button.

Your settings are saved.

Advanced Wireless Settings

The default wireless LAN parameters usually work well. However, you can use these settings to fine-tune the overall performance of your access point for your environment.

> To configure advanced wireless settings:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R'		WAC120 Period Durit Band Weighter AC Annuel Page
Configuration	Persitaring Perintenance	Second Se	
Tenten 20 1000	eless. Secondy Weeless Bridg	e : With	
-	General		
a second second	Cetural		
Advanced	Accuse Point Barne Country / Region	netges:334485	

4. To configure the advanced wireless settings for the 2.4 GHz band, select Configuration > Wireless > Advanced > Wireless Settings > 802.11b/bg/ng.

	Contraction of the second s				
	Wirdess Settings				
	Window Settings		191		
bett-un .	BULLIN/NA/NET BULLIN/NA/N	80			
	878 Threadadd (0-2387)	zast-			
	Pregnostation Length (258-2346)	2348			
	Beacon Interval (100-1999)	395			
	Apprepation Length (1024-65535)	65525			
	AMPDU	· paste C blaste			
	BIFS Transmusen	C tratte # Livelite			
	DTIM Interval (3-2553	3			
	Preamble Type	* Auto Chang			
	892.116	2			
	Nov. Windees Clients	.84			
	Rand Meering to SQNs	Canadra R Disattle			
	Bast Threakold 2.4GHz	IN.			
	Reat Threahold SGHz	21			

- 5. To change the default settings, enter the appropriate information in the following fields:
 - **RTS Threshold (0–2347)**. Request to Send threshold. The packet size that is used to determine if the station should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) mechanism for packet transmission.
 - With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet until the silence period ends.
 - With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

The default is 2347.

- Fragmentation Length (256–2346). This is the maximum packet size. Packets larger than the size specified in this field are fragmented. The Fragmentation Length value must be larger than the RTS Threshold value. The default is 2346.
- **Beacon Interval (100–1000)**. The time interval between 100 ms and 1000 ms for each beacon transmission, which allows the access point to synchronize the wireless network. The default is 100.
- Aggregation Length (1024 65535). The aggregation length defines the size of aggregated packets. Larger aggregation lengths can sometimes lead to better network performance. The default is 65535.
- **AMPDU**. Aggregated MAC Protocol data unit. Aggregates several MAC frames into a single large frame to achieve higher throughput. The default is enabled.
- **RIFS Transmission.** Reduced interframe space. RIFS transmissions are shorter than other interframe spaces, and if this feature is enabled, the access point allows transmission of successive frames at different transmit powers. The default is disabled.
- **DTIM Interval (1-255)**. The delivery traffic indication message. Specifies the data beacon rate between 1 and 255. The default is 3.

- **Preamble Type**. A long transmit preamble can provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance. The Auto setting automatically handles both long and short preambles. The default is Auto.
- **802.11d.** Select this check box to include support for additional regulatory domains that are not in the current standard.
- **Max. Wireless Clients**. The maximum number of wireless clients that can connect to the access point at one time. The default is 128 per radio.
- **Band Steering to 5GHz**. Band steering identifies the wireless devices that are capable of operating in both the 2.4 GHz and 5 GHz bands. The access point responds to these devices only on the 5 GHz band and allows the dual-band-capable client to connect to the 5 GHz band rather than the 2.4 GHz band, since more channels and bandwidth are available on the 5 GHz band and using this band causes less interference for users.
- **Rssi Threshold 2.4GHz**. The minimum RSSI threshold that a client must use to connect to a 2.4 GHz access point.
- **Rssi Threshold 5GHz**. The minimum RSSI threshold that a client must use to connect to a 5 GHz access point.
- To configure the advanced wireless settings for the 5 GHz band, select Configuration > Wireless > Advanced > Wireless Settings > 802.11a/ag/na.

Coeffiguration	tooloring Habiteenen Separt		and the second s
nyahan (ar) Maah	an Theorem Theorem Bredge 1 were		
Res.	Wireless Settings Wireless Settings		
(Qui Satea)	AUE 3 44.7mg, mg ²⁰ AUE 3 44.7mg, mg ²⁰ AUS 114/3mg/au AUS 114	2047 2040 100	
	UTIN Internet (1-255) Has. Mareless Chests		

- 7. To change the default settings, enter the appropriate information in the following fields:
 - **RTS Threshold (0–2347)**. Request to Send threshold. The packet size that is used to determine if the station should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) mechanism for packet transmission.
 - With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet until the silence period ends.
 - With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

The default is 2347.

• Fragmentation Length (256–2346). This is the maximum packet size. Packets larger than the size specified in this field are fragmented. The Fragmentation Length value must be larger than the RTS Threshold value. The default is 2346.
- **Beacon Interval (100–1000)**. The time interval between 100 ms and 1000 ms for each beacon transmission, which allows the access point to synchronize the wireless network. The default is 100.
- **DTIM Interval (1-255)**. The delivery traffic indication message. Specifies the data beacon rate between 1 and 255. The default is 3.
- **Max. Wireless Clients**. The maximum number of wireless clients that can connect to the access point at one time. The default is 128 per radio.
- 8. Click the **Apply** button.

Your settings are saved.

Advanced QoS Settings

Wi-Fi Multimedia (WMM) is a subset of the 802.11e standard. WMM allows wireless traffic to receive a range of priorities, depending on the type of data. Time-dependent information, such as video or audio, receive a higher priority than normal traffic. For WMM to function correctly, wireless stations and clients must support WMM.

For most networks, the default QoS (Quality of Service) queue settings work well. You can specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic, like VoIP, and other types of audio, video, and streaming media, as well as traditional IP data.

The queues defined for types of data transmitted from access point to station and from station to access point are as follows:

- **Data 3 (Voice)**. Highest-priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- **Data 2 (Video)**. Highest-priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
- **Data 1 (Background)**. Lowest-priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
- **Data 0 (best effort)**. Medium-priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.

> To configure advanced QoS settings:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

NETGEA Configuration	R'	Sapanet		WAC120 Packets Dual Band Workers AC Annual Pack
Tables 27 100	eless Secondy Weeksa Bridg	e 1 wes		
1	General			
a these	General			
Advanced	Accuse Point Name Country / Region	netgear2344820 provid 20ates	-	

4. Select Configuration > Wireless > Advanced > QoS Settings.

Configuration 1	hamberbeg Malatenance	Report	
and and the state	and descartly . Wiredows fro	fan WTS	
less:	QoS Settings		
• Western Dertruge	Quis Settlings		
and see all	853.135/bs/vs ^{TC} 8	RD (Contraction 17	
	AP EDCA parameters		
	Queses	AITS mellin mellax Non Bent	
	Colo C (Sect Effort)	TRANSFER TO THE TRANSFER	
	Date 1 (Binchgenerid)	7 12 + 1022+ 0	
	Telle 2 (Video)	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
	Deta 3 (Volce)	1100 3.0 W 7.0 W 1101	
	Station EDCA periorette	13	
	Question	AIFS with with 100P Link	
	Data D (Best Effort)	2 11 12 12 12 12 1002 m 1	
	Tidle 1 (Beckground)	P 118 w 1222 w 8	
	Deta 3 (Video)		
	Deta 3 (Volca)	3 9 w 7 w 15%	

The QoS Setting fields are the same for the 2.4 GHz and 5 GHz bands.

5. To change the default settings of the access point EDCA settings, enter the appropriate information in the AP EDCA parameters fields.

The following access point Enhanced Distributed Channel Access (EDCA) parameters affect traffic flowing from the access point to the client station:

- **AIFS**. The Arbitration Inter-Frame Spacing (AIFS) interval specifies, in milliseconds, the wait time between data frames. Higher AIFS values mean higher priority to that queue. Valid values for AIFS are 1 through 255.
- **CwMin**. The minimum contention window (CwMin) value specifies the upper limit (in milliseconds) of a range from which the initial random back-off wait time is determined. Decreasing this value increases the priority of the queue. The value for CwMin must be lower than the value for CwMax. Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1024.
- **CwMax**. The maximum contention window (CwMax) value specifies (in milliseconds) the upper limit for the doubling of the random back-off value. Decreasing this value increases the priority of the queue. The value for CwMax must be higher than the value for CwMin. Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1024.
- **Max. Burst**. (access point only) The maximum burst value specifies (in milliseconds) the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information.

Decreasing this value increases the priority of the queue. Valid values for maximum burst length are 0.0 through 999.9.

6. To change the default settings of the station EDCA settings, enter the appropriate information in the Station EDCA parameters fields.

The following station Enhanced Distributed Channel Access (EDCA) parameters affect traffic flowing from the client station to the access point:

- **AIFS**. The Arbitration Inter-Frame Spacing (AIFS) interval specifies, in milliseconds, the wait time between data frames. Higher AIFS values means higher priority to that queue. Valid values for AIFS are 1 through 255.
- **CwMin**. The minimum contention window (CwMin) value specifies the upper limit (in milliseconds) of a range from which the initial random back-off wait time is determined. Decreasing this value increases the priority of the queue. The value for CwMin must be lower than the value for CwMax. Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1024.
- **CwMax**. The maximum contention window (CwMax) value specifies (in milliseconds) the upper limit for the doubling of the random back-off value. Decreasing this value increases the priority of the queue. The value for CwMax must be higher than the value for CwMin. Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1024.
- **TXOP Limit**. The transmission opportunity (TXOP) is an interval of time (in milliseconds) when a client station can initiate transmissions on the wireless medium (WM). Decreasing this value increases the priority of the queue. Valid values for maximum burst length are 0.0 through 999.9.
- 7. Click the **Apply** button.

Your settings are saved.

Wireless Bridging and Repeating

You can use the access point as a component to build large bridged wireless networks. The following modes are available:

• **Wireless point-to-point bridge mode**. The access point communicates with one other bridge-mode wireless station. You can associate wireless clients with this access point.



AP1 and AP2 in point-to-point bridge mode with each other

Figure 5. Point-to-point bridge mode

For more information, see *Wireless Point-to-Point Bridge Mode* on page 41.

• Wireless point-to-multi-point bridge mode. The access point serves as the base station for a group of bridge-mode wireless stations. You can associate wireless clients with this access point.



AP2 (base station) in point-to-multi-point bridge mode AP1 and AP3 in point-to-point bridge mode with AP2

Figure 6. Point-to-multi-point-bridge mode

For more information, see *Wireless Point-to-Multi-Point Bridge Mode* on page 43.

The other bridge-mode wireless stations in the network must be set to point-to-point bridge mode and use the MAC address of the base station access point. They send all traffic to the base station rather than communicating directly with each other. For more information, see *Wireless Point-to-Point Bridge Mode* on page 41.

• **Client mode**. The access point operates as a client bridge only and sends all traffic to the remote access point or peer device. Use client mode to extend the local area network to those clients that are not connected wirelessly. Client mode supports MAC cloning. For more information, see *Client Mode* on page 46.

Wireless Point-to-Point Bridge Mode

Coordinate the following information ahead of time for each access point:

- **MAC addresses**. You must know the MAC address of each access point in the bridge network. You can use the 2.4 GHz or 5 GHz band for the wireless bridge, but the 2.4 GHz and 5 GHz bands of each access point use a unique MAC address.
- Authentication settings. You must specify the same wireless authentication settings for each access point in the bridge network. Each access point must use the same ESSID, channel, authentication mode, if any, and security settings.

- LAN address range. Each access point must be configured to operate in the same LAN network address range as the LAN devices.
- **DHCP**. If you are using DHCP, all access points must be set to obtain an IP address automatically. See *Configure the Basic IP Settings* on page 15.

When the wireless bridge is completed, a computer on either LAN segment can connect to the Internet and share files and printers with any other computers or servers connected to LAN Segment 1 or LAN Segment 2.

> To configure a point-to-point wireless bridge between two access points:

- 1. Launch a web browser on the computer that is connected to the first access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R'		WAC120
Configuration	Perilaring Paintenance	Sapport	[Januar] -
Testan 20 100	eless Secondy Weeless Bridg	e 1 WPS	
-	General		
	General		
Advanced	Accume Point Harme Country / Region	retgesc104480 poiled Baster (m)	

4. Select Configuration > Wireless Bridge.

Spatian 10 With	store Security musicial project with			
	Bridging			
	HELLIN/Harver ^{an} MELLIN/Harver	Cl. (14)(14040-11)		
	* Weeksa Punt to Punt Bridge Bratte Weekse Cont Association	Minutese Front to Half- Front Bridge	there	
	F 1 DETERATION	Descentry Down Rostern	featle	

- 5. Select the band that you want to use for the bridge:
 - To set up the bridge on the 2.4 GHz band, click the **802.11b/bg/ng** tab.
 - To set up the bridge on the 5 GHz band, click the **802.11a/ag/na** tab.
- 6. Select the Enable Wireless Bridging check box.
- 7. Select the **Wireless Point-to-Point Bridge** radio button.
- 8. To enable wireless client association, select the **Enable Wireless Client Association** check box.

9. Click the **Edit** button.

tantipaiation	Hamilton Haltreneter	Sapport		- a the C Lange
System 1PT V	Edit Security Profile	NTS.		
	Profile Definition		00	
	Posilie Harre Reserve HAC Address	HETERAR HEG-1		
	Auffantikation Settings		-	
	Network Authoritication Data Exception	Gast Svider(=) Rome (=)		

- **10.** In the **Remote MAC Address** field, enter the MAC address of the other access point.
- **11.** Under Authentication Settings, specify the authentication settings for your bridge network.
- **12.** Click the **Apply** button.

Your settings are saved.

- **13.** Configure and verify the following parameters for the access point:
 - Verify that both access points are configured to operate in the same LAN network address range as the LAN devices.
 - Verify that both access points use the same ESSID, channel, authentication mode, if any, and security settings.
- 14. Repeat Step 1 through Step 13 for the second access point.
- **15.** Verify connectivity across LAN 1 and LAN 2.

A computer on either LAN segment can connect to the Internet and share files and printers with any other computers or servers connected to LAN Segment 1 or LAN Segment 2.

Wireless Point-to-Multi-Point Bridge Mode

In a multi-point wireless bridge, one of the wireless stations is designated as the base station and configured in wireless point-to-multi-point bridge mode. All of the other access points in the wireless bridge are configured in wireless point-to-point bridge mode. You can connect up to four access points to the base station access point.

Coordinate the following information ahead of time for each access point:

- **Base station**. Select the access point that serves as the base station. The other access points in the wireless bridge network must use the MAC address of the base station.
- **MAC addresses**. You must know the MAC address of each access point in the bridge network. You can use the 2.4 GHz or 5 GHz band for the wireless bridge, but the 2.4 GHz and 5 GHz bands of each access point use a unique MAC address.
- Authentication settings. You must specify the same wireless authentication settings for each access point in the bridge network. Each access point must use the same ESSID, channel, authentication mode, if any, and security settings.
- LAN address range. Each access point must be configured to operate in the same LAN network address range as the LAN devices.

• **DHCP**. If you are using DHCP, all access points must be set to obtain an IP address automatically. For more information, see *Configure the Basic IP Settings* on page 15.

When the wireless bridge is completed, a computer on either LAN segment can connect to the Internet and share files and printers with any other computers or servers connected to LAN Segment 1 or LAN Segment 2.

You can extend this multi-point bridging by adding additional access points configured in point-to-point bridge mode for each additional LAN segment. You can also extend the range of the wireless network with NETGEAR wireless antenna accessories.

> To configure a point-to-multi-point wireless base station:

- 1. For the first access point (AP 1) on LAN Segment 1, launch a web browser on a computer that is connected to the access point.
- 1. On the base station access point, launch a web browser on the computer that is connected to it.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R		WAC120 Frederic Dual Band Workson AC America Paper
Configuration	Participant Participant		
	General	5/5W62	
	General		
Advanced	Accume Point Harne Country / Region	(respensit)///kb / (poiled thefee (=)	

4. Select Configuration > Wireless Bridge.

Configuration	Northaring Malatonees Support			
Systems 10 Words	na Security Withdate Brough 1978			
	Bridging Bridging			
	MILLIN/MA/WW ^{III} MILLIN/MA/W Enable Western Bridging Local NAC Address	C. C. C. C		
	P Weeksa Post-ta-Post Bedge Bratte Weekse Cort Association	Mindata Road to Halti Hand Bridge	ther	
	T BETERAL	Deen Refer	featle	

- 5. Select the band that you want to use for the bridge:
 - To set up the bridge on the 2.4 GHz band, click the **802.11b/bg/ng** tab.
 - To set up the bridge on the 5 GHz band, click the **802.11a/ag/na** tab.
- 6. Select the Enable Wireless Bridging check box.

7. Select the Wireless Point-to-Multi-Point Bridge radio button.

Bridging		
Bridging		
802.135/6g/sg? 802.135	Contract To Contra	
Enable Weekee Bridging Local MAC Abbrevs	2 C4/04/18/40-50-01	
O Window Port to Front Stale	* Workers Parel to Park Parel Ander	Cithest
Inable Wisless Glant Association		
a Profile Rame	Socarity	tashte
# 1 NETOKAR-WER-1	Open System	12
's writinte when a	Spars Bullery	0
C 5 MITODAR-WEIR-S	Ourse Busines	10.11
I A MILLION AND A	Court Burbary	

- 8. To enable wireless client association, select the **Enable Wireless Client Association** check box.
- 9. Select the radio button for the first access point that you want to connect to the base station and click the **Edit** button.

tantipaistan a	taliting Makemann 3	hipport	and the second second
	Edit Security Profile		
	Prefile Defielden		
	Postle Barre Scente HAC Address	NETUEAR HOS-1	
	Autombiation Solliege		
	Network Authoritication Data Encryption	Oper Sviter(a) Baies a	

- **10.** In the **Remote MAC Address** field, enter the MAC address of the other access point.
- **11.** Under Authentication Settings, specify the authentication settings for your bridge network.
- **12.** Click the **Apply** button.

Your settings are saved.

- **13.** Select the radio button for the next access point that you want to connect to the base station and click the **Edit** button. Repeat *Step 10* through *Step 12* for this next access point.
- **14.** Repeat *Step 13* for each of the remaining access points that you want to connect to the base station.

You can specify up to four access points that connect to the base station access point.

- **15.** For each access point that you want to allow to connect to the base station access point, select its **Enable** check box.
- **16.** Click the **Apply** button.

Your settings are saved.

17. Configure each access point that is to connect to the base station access point in wireless point-to-point bridge mode.

For more information, see *Wireless Point-to-Point Bridge Mode* on page 41.

18. Verify the following parameters for all access points:

- Only the base station access point is configured in wireless point-to-multi-point bridge mode and all the other access points are in wireless point-to-point bridge mode.
- For all point-to-point access point, the MAC address of the base station access point must be specified in their **Remote AP MAC Address** fields.
- All access points are configured to operate in the same LAN network address range as the LAN devices.
- All access points use the same SSID, channel, authentication mode, if any, and encryption.
- If you are using DHCP, all the access points must be set to obtain an IP address automatically. For more information, see *Configure the Basic IP Settings* on page 15.
- **19.** Verify connectivity across the LANs:
 - A computer on any LAN segment can connect to the Internet and share files and printers with any other computers or servers connected to any of the other LAN segments.
 - The wireless stations that you enable can connect to the access points. If you require wireless stations to access any LAN segment, you can add additional access points configured in wireless bridge mode to any LAN segment.

Client Mode

In client mode, the access point operates as a client bridge only and sends traffic to the selected remote access point or peer device.

> To configure the access point for client mode:

- 1. Launch a web browser on a computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R'		WAC120 Probability Durit Bund Workson AC Appendix Party
Patient IP Mer	dess fee artly Wreless finds	e : wes	
T Date	General		
Advance#	Accume Point Harnel Country / Region	retgen:134455	

4. Select Configuration > Wireless Bridge.

-	Bridging				
	Artiging				
	(and the factor for the second				
	Contractor of the second second	FM			
	Exable Wordson Bridging				
	Local MAC Address	C4/04/(5)4D-65/01			
	* Weekss Post-to-Post Bodys	Mindate Post in Halt-Ford Indge	a Sines		
	Brable Wreters Clark Association	10			
	# Profile Name	Security	Teable		
	F I INTERATORI	Down Rotert	11.24		
	The second				

- 5. Select the band that you want to use for the bridge:
 - To set up the bridge on the 2.4 GHz band, click the **802.11b/bg/ng** tab.
 - To set up the bridge on the 5 GHz band, click the **802.11a/ag/na** tab.
- 6. Select the Enable Wireless Bridging check box.
- 7. Select the **Client** radio button.

Configuration (1)	mitstag Malateased Inquest	14.000
System 27 Musless	a Security Dimeter Birthis 1 With	
Langes.	Bridging	
	Aridging	
	853.116/bg/vg * MELTINIAN *	
	Frukte Weetens Bridging St. Lacal PAC Address Condected St. Co. Sector 2010 Ct.	
	C Weakee Point to Point Bridge C Washess Point to Note Point Bridge # Cheek	
	NAC Clove C Brukke # Studies	

8. Enable the MAC clone feature.

The **Disable** radio button is selected by default. If you enable the MAC clone feature, enter the MAC clone address.

9. Click the **Apply** button.

Your settings are saved.

Manage the Access Point



This chapter covers the following topics:

- Change the admin Password
- Upgrade the Firmware
- Manage the Configuration File
- Enable a Syslog Server

Change the admin Password

The default password for admin is **password**. NETGEAR recommends that you change this to a more secure password.

> To change the admin password:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is admin and the default password is password.

The General screen displays.

NETGEA	R'			W	AC120
Configuration	Notificing - Haidingers	Sapport		2030/02/223	There is
Testen 2P We	elesa Secarity Wreless Bridg	in 1.WPV			
-	General				-
	General				
Advanced	Accume Point Harne Country / Region	netgewr234480 posied theter	i		

4. Select Maintenance > Password > Change Password.

Gellanding Hostoring Hidelensers	Samuel	()
Parameter I descent i reportedan		
Change Pasaword		
Charge Pessererd	-	
Correct Passarded		
Rev Password Repeat Rev Password		
Rastore Delaalt Personne	O 164 ₩ 560	

- 5. Type the password in the **Current Password** field.
- 6. Type the new password in the New Password field and in the Repeat New Password field.
- 7. To restore the default password, select the Restore Default Password Yes radio button.
- 8. Click the **Apply** button.

Your settings are saved.

Upgrade the Firmware

The firmware is stored in flash memory and can be updated as NETGEAR releases new firmware. You can download upgrade files from the NETGEAR website. If the upgrade file is compressed (.zip file), you must first extract the image (.rmt) file before sending it to the access point. You can send the upgrade file using your browser.

Note: The web browser must support HTTP uploads.

You cannot perform the software upgrade from a computer that is connected to the access point wirelessly. You must use a computer that is connected with an Ethernet cable.



WARNING:

When uploading firmware to the access point, do not interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload might fail, corrupt the software, and render the access point inoperable.

> To upgrade the firmware:

1. Download the new software file from the NETGEAR website, save it to your hard disk, and unzip it.

Visit http://www.netgear.com.

- 2. Launch a web browser on the computer that is connected to the access point.
- 3. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

4. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R		WAC120 Probate Dural Band Western AC Annuel Part
Configuration	Periliring Pickinson	North Contraction of Street St	
Statute 20 Mar	dess. Secondy Wreless Bridg	e: 1 WPN	
-	General		
	General		
Advanced	Accuse Point Name Country / Region	retgescittetitt	

5. Select Maintenance > Upgrade > Firmware Upgrade.

Configuration	toutoring Malatena	and Segment	
Ferrenteret 1 Separat 116	leger distant		
	Firmware Upgrad	e .	
Bachigo Sietlange	Firmune Stegrad		*
Bostore Settings	Select Nix	Brown Pro Pin polastad.	

- 6. Click the Browse button and browse to the location of the image (.rmgs) upgrade file.
- 7. Click the Apply button.

When the upload is completed, your access point automatically restarts. The upgrade process typically takes at least three minutes.

Manage the Configuration File

The access point settings are stored in the access point in a configuration file. This file can be saved (backed up) or restored.

Back Up the Configuration File

- > To back up the access point settings in a configuration file:
 - 1. Launch a web browser on the computer that is connected to the access point.
 - 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEAR'					WAC120 Particity Dual Band Workson AC Auston Part
	General				
of Tares	General				
Advanced	Accuse Point Barne Country / Begion	retgescittetist project theter	í		

4. Select Maintenance > Upgrade > Backup Settings.

Cashgoontine #	Instantes Malatematics Seguet	(+=+)
Personnel Beart 1		
Fermates	Backup Settings	
Degrade	Buckup Settings	
Resilve buildage	Rachus a copy of the correct settings to a bla (Milliff)	

5. Click the **Backup** button.

Your browser extracts the configuration file from the access point and prompts you for a location on your computer to store the file.

6. Give the file a meaningful name, such as WAC120.cfg, and click the Save button.

Restore the Configuration File

- > To restore the access point settings from a saved configuration file:
 - 1. Launch a web browser on the computer that is connected to the access point.
 - 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R'	WAC120	
Configuration	Persiliarity Pickelmann	Second Frank L	
Testine 2P We	eless firearity Wereless first	e - wes	
1000	General		
1.100	General	-	
Advanced	Access Point Name	(retges:2344b) /	
	Country / Region	_ lating liters [-	

4. Select Maintenance > Upgrade > Restore Defaults.

Configuration 4	finition Haldesonia Support	()
Property in Resett 111		
Fireware	Restore Settings	
tingrada. Rector Settings	Reduce Settings	
The second designed	Restore seved attlings from a file Bernel. In the principal	

5. Click the **Browse** button.

You are prompted to select a file where you previously saved configuration settings.

- 6. Select the file.
- 7. Click the **Restore** button.

The file uploads and the access point reboots.

Restore the Factory Default Settings

You can restore the access point to the factory default settings using the **Restore Defaults** menu selection, or by using the **Reset** button.

> To restore the factory settings:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

NETGEA	R' Halatanana	Saparr	WAC120 Products David Band Woolston AC Assessed Parts
Station 20 100	niesa Sacarity Wreless Bridg	e i wes	
a time	General		
Advanced	Accuse Point Barne Country / Begins	relgescionist protection	

4. Select Maintenance > Reset > Restore Defaults.

(indigeneities) [Munikering Habringerin Support		(Amount)
Processing Marries	The second s		
Radoust AF	Restore Defaults Restore Defaults	1	
	Restore to factory delayst settings 😳 760 🖷 80		

- 5. Select the **Yes** radio button.
- 6. Click the Apply button.

The access point password is password, the access point DHCP client is disabled, the default LAN IP address is 192.168.0.100, and the access point name is reset to the name printed on the product label.

Enable a Syslog Server

You can enable the syslog option if your LAN includes a syslog server.

- > To enable a syslog server:
 - 1. Launch a web browser on the computer that is connected to the access point.
 - 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is admin and the default password is password.

The General screen displays.

Confectation	Restoring Finishments	Sapart	WAC120 Analytic New York
Tables 20 Mar	dess fer anty Wreless find General	te ; mai	
	General		
Advancell	Access Point Barbo Country / Begion	retgescionthis	

4. Select Configuration > System > Advanced > SysLog.

Carligeration	Minibering Mainference 3	superint to the second s	
SAMERICAR MAN	elese Security Window Bridge	AT5.	
1	Syslog Syslog Settings		
County of	Exable Syring Byolog Server IP Address Port Namber	344	

- 5. If your LAN includes a syslog server, select the **Enable Syslog** check box.
- 6. In the Syslog Server IP Address field, type the IP address of your syslog server.

The access point sends all the syslog files to the specified IP address if the syslog option is enabled. The default is 0.0.0.0.

7. In the **Port Number** field, type the port number that your syslog server is configured to use.

The default port number is 514.

8. Click the **Apply** button.

Your settings are saved.

Monitoring

5

This chapter covers the following topics:

- View System Information
- View Available Wireless Stations
- Activity Log
- View Network Traffic Statistics

View System Information

You can view a summary of the current access point configuration settings, including current IP settings and current wireless settings. This information is read-only, so any changes must be made on other screens.

> To view system information:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

The user name is **admin** and the default password is **password**.

The General screen displays.

NETGEA	R'		WAC120 Packade David Band Western AC Automoti Part
Configuration	Perilarian Paintenane	Exposit	Scott Condition
Tenter 2P Mer	desa Secarity Wredesa Bridg	a lawas	
1000	General		
	General		
Advancell	Accum Point Barni Country / Region	retgesct34480	

4. Select Monitoring > System.

System		
Access Food Information	10	
Assess Paul Same	hergee(224102)	
Ethnited MAC Address	C4-84-19-401-00 08	
Workess HAC Address for 2 4044	CR 94 18 AD AD AD	
Wireless MAC Address for SSHz	C8-84-18-40-60-18	
Hand Steering to Nillia	Distribut	
Country / Regism	United States	
Firmmanian Version	WACLE VED.	
Sanial Number	BURT AT BRANCES.	
Earrow Taxes	and Dec 31 18:43:44 MSF 2988	
Carrow Med Indlings		
IPud Address	192 388.0.108	
Statement Manufe	215-201-208.8	
Belauft Catestry		
DHOP Chest	Disetteri	

The following access point information displays:

- Access Point Name. The NetBIOS name. The default name can be changed.
- Ethernet MAC Address. The MAC address of the access point's Ethernet port.
- Wireless MAC Address for 2.4 GHz. The MAC address of the access point's 2.4 GHz wireless port.

- Wireless MAC Address for 5 GHz. The MAC address of the access point's 5 GHz wireless port.
- **Band Steering**. Indicates whether band steering is enabled or disabled.
- **Country/Region**. The domain or region for which the access point is licensed for use. It might not be legal to operate this access point in a region other than one of those identified in this field.
- Firmware Version. The version of the firmware currently installed.
- Serial Number. The serial number of the device.
- Current Time. The time setting for the access point.

The following current IPv4 settings information displays:

- IP Address. The IP address of the access point.
- Subnet Mask. The subnet mask for the access point.
- **Default Gateway**. The default gateway for the access point communication.
- **DHCP Client**. Enabled indicates that the current IP address was obtained from a DHCP server on your network. Disabled indicates a static IP configuration.

The following current wireless settings for each wireless band display:

- **Operating Mode**. Identifies the 802.11 operating mode of the access point.
 - Access Point
 - Point-to-Point Bridge
 - Point-to-Point Bridge with Access Point
 - Multi-Point Bridge
- Channel / Frequency. Identifies the channel that the wireless port is using.

View Available Wireless Stations

You can view all IP devices associated with this access point in the wireless network defined by the wireless network name (SSID). If your network includes more than one access point sharing the same SSID, remember that you can view only the wireless stations associated with this access point.

> To view the Available Wireless Stations list:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

NETGEA	R	WAC120 Probate Dural Read	
Configuration	Perilaring Paintenance	Second Street Provide Street S	
States 30 Mar	dess. Secondy Weekess Bridg	el-wes	
-	General		11
a Tana	Getated		
Advanced	Accuse Point Name Country / Region	retgenet34482	

4. Select Monitoring > Wireless Stations.

Confidentian (1)	Authoring Maintenance Seguet	-
Surviva I Openhius M	atom / Lags & Stateme	
The second second	Wireless Stations	
	Available Wheeless Stations (#03.13mg)	
	MAC Address #5500 SSID Chassel Note State Type AD Hole States	
	Available Workson Stations (802.11ac)	
	HAC Address 19500 SSID Channel Nate State Type AID Hode States	

You can view the MAC address, IP address, BSSID, SSID, channel rate, state, type, AID, mode, and status (whether the station is allowed to communicate with the access point).

- 5. To update the list, click the **Refresh** button.
 - **Note:** If the access point reboots, the wireless station information does not display until the access point rediscovers the devices. To force the access point to look for associated devices, click the **Refresh** button.

Activity Log

You can view a log of the access point system activity.

> To display the activity log:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.

A login prompt displays.

3. Enter the user name and password.

NETGEA	R'		WAC120
Configuration	Persilarity Painteness	Sapport	Second French Bernin L.
Section 20 100	eless for setty Wereless firsty	e 1 WPS	
-	General		
	General		
Advanced	Accume Point Name Country / Region	retgesch344bb /	

4. Select Monitoring > Logs.

The Logs screen displays:

rates - Wantess	Nostoring Malalamana Engent	1440
-	Logs	
	Ings Esc El 10120128 Norresl: cl ath veg det parmai TBF parma ndaupport - Dec El 10120128 Norresl: TBER: Cl_thra_dot_id: per 505s	
	Dec 21 16:10:12 Messel: 2006; ees spec for pers Midestil (44:14) Dec 21 16:10:20 Messel: Setting Your parame = 16, value = 3 Dec 21 16:10:10 Messel: Fetting Your (14:10:13) Mail Dec10 Messel: Your 2017 Dec 31 16:10:10 Messel: PRLOD: [3:81:120] Mail Dec10 Messel: Your 2010	
	Der 31 10/10/104 Berreil (WECO) 11/(0.00) WAL DESID B MOOD INJUE Des 31 10/10/01 Berreil (WECO) 10/00000 BAL DESID BE MOOD INJUE Des 31 10/10/11/ Berreil (WECO) 10/10/01 BAL DESID BE MOOD INJUE Des 31 10/10/11/ Berreil (WECO) 10/10/01 WAL DESID BE MOOD INJUE	
	Dec 21 24197100 Bestell WELDS: 22912513 Well 18820 WELDS: 10.000 TRIDER Dec 51 14107108 Bernell WELDS: 12120003 Well Bell 19700 TRIDER -	

- 5. To update the display, click the **Refresh** button.
- 6. To clear the log content, click **Clear** button.

To save the log contents in a file on your computer or to save the file to a disk drive, click the **Save As** button. The log contents file is saved.

View Network Traffic Statistics

You can view information for both wired (LAN) and wireless (WLAN) interface network traffic.

> To view the network traffic statistics:

- 1. Launch a web browser on the computer that is connected to the access point.
- 2. Enter http://192.168.0.100 in the address field of the browser.
 - A login prompt displays.
- 3. Enter the user name and password.

NETGEA	R			WAC120
Configuration	Configuration Membering Maintenant Superit			(parties)
Statute 27 1844	niena Socarity Wereless Bridg	er i WPS		
-	General			-
	General			
Advanced	Accuse Point Harse Country / Region	retges:234482		

4. Select Monitoring > Statistics.

Configurations Residenting Relation	-	lappedt	L manufer
etters Mirelans Matters Loge Matter	Q2 -		
Statistics			
Wived Ethernet			
Provident State	I Tree	detail the second s	
Packets \$1200	Past		
Byles mirest	-	ei - 5	
Wiveless 802.11	**	12 - R	
	Recei	d Transmitted	
Unicast Packets		401	
Breakcest Packets		1 M	
Bulliout Packets		1	
Total Packets		430	
Total Bytes		setts	
Window BDJ.1.5	M		
Reserves and the second	Recut	at Transmitted	
Unicest Packets	18,000	84	
Breedcast Packats	+	234	
and the second se		They'	

The following information is displayed:

- **Packets**. The number of packets sent and received on the Ethernet port since the access point was restarted.
- **Bytes**. The number of bytes sent and received on the Ethernet port since the access point was restarted.
- **Unicast Packets**. The unicast packets sent and received since the access point was restarted, shown separately for the 2.4 GHz and 5 GHz bands.
- **Broadcast Packets**. The broadcast packets sent and received since the access point was restarted, shown separately for the 2.4 GHz and 5 GHz bands.
- **Multicast Packets**. The multicast packets sent and received since the access point was restarted, shown separately for the 2.4 GHz and 5 GHz bands.
- **Total Packets**. The wireless packets sent and received since the access point was restarted, shown separately for the 2.4 GHz and 5 GHz bands.
- **Total Bytes**. The wireless bytes sent and received since the access point was restarted, shown separately for the 2.4 GHz and 5 GHz bands.
- **802.11ng Radio**. The number of associated clients on the 2.4 GHz band.
- **802.11ac Radio**. The number of associated clients on the 5 GHz band.
- 5. To update the statistics information for each interface, click the **Refresh** button.

Troubleshooting and Debugging

6

This chapter covers the following topics:

- Troubleshooting with the LEDs
- Cannot Connect to the Access Point to Configure It
- Wireless Access to the Network
- Time-Out Error for URL or IP Address

Note: For up-to-date WAC120 installation details and troubleshooting guidance, visit *http://support.netgear.com*.

Troubleshooting with the LEDs

Use the LEDs to verify that the access point is working properly.

All LEDs Are Off

It takes a few seconds for the Power LED to light. Wait a minute and check the Power LED on the access point.

If the access point is not receiving power, do the following:

- Make sure that the power cord is connected to the access point.
- Make sure that the power adapter is connected to a functioning power outlet. If it is in a power strip, make sure that the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet.
- Make sure that you are using the correct NETGEAR power adapter supplied with your access point.

LAN LED Is Off

A hardware connection problem occurred. Check these items:

- Make sure that the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router). A switch, hub, or router must be installed between the access point and the Ethernet LAN or broadband modem.
- Make sure that the connected device is turned on.
- Make sure that the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device includes Auto Uplink[™] (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

WLAN LED Is Off

Either the wireless radio is turned off (see *Basic Wireless Settings* on page 17) or the access point antennas are not working.

- If the WLAN LED stays off when the wireless radio is on, disconnect the adapter from its power source, and then plug it in again.
- Make sure that the antennas are securely connected to the access point.
- Contact NETGEAR technical support if the WLAN LED remains off.

Cannot Connect to the Access Point to Configure It

Check these items:

- The access point is installed correctly, LAN connections are OK, and the access point is powered on. Check that the LAN port LED is green to verify that the Ethernet connection is OK.
- The default configuration of the access point is for a static IP address of 192.168.0.100 and a subnet mask of 255.255.255.0 with DHCP disabled. Make sure that your network configuration settings are correct.
- If you are using the NetBIOS name of the access point to connect, ensure that your computer and the access point are on the same network segment or that there is a WINS server on your network.
- If your computer is set to obtain an IP address automatically (DHCP client), restart it.
- If your computer uses a fixed (static) IP address, ensure that it is using an IP address in the range of the access point. The default IP address is 192.168.0.100, and the default subnet mask is 255.255.255.0.

Wireless Access to the Network

If you cannot connect wirelessly, the wireless radio might be turned off (see *Basic Wireless Settings* on page 17) or a configuration problem might exist. For a configuration problem, check these items:

- If you did not restart the computer with the wireless adapter so that the TCP/IP changes took effect, restart the computer.
- The computer with the wireless adapter might not be configured with the correct TCP/IP settings to communicate with the network.

Restart the computer 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 (DHCP client).

• The access point's 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 URL or IP Address

A number of things could be causing this. Try the following troubleshooting steps:

- Check whether other computers on the network work without errors. If they do, ensure that your computer's TCP/IP settings are correct. If you are using a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP 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 or cable modem, and so on) to make sure that it is working correctly.
- Try again.

Supplemental Information



This appendix covers the following topics:

- Factory Settings
- Technical Specifications

Factory 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 router for at least seven seconds. The access point resets and returns to the factory configuration settings shown in the following table.

Table 2.	Factory	default	settings
----------	---------	---------	----------

Feature		Description	
Login	for Management and Configuration		
	LAN IPv4 management address	192.168.0.100	
	Subnet mask for IPv4 management address	255.255.255.0	
	Required static IPv4 address for management computer	192.168.0.210 and 255.255.255.0	
	User name (case-sensitive) for login	admin	
	Login password (case-sensitive) for login	password	
LAN a	nd Management Features		
	DHCPv4 client	Disabled	
	Untagged VLAN	Enabled, VLAN ID 1	
	Management VLAN	VLAN ID 1	
	Syslog	Disabled	
	Spanning Tree Protocol (STP)	Disabled	
	Time zone	USA-Pacific	
	NTP client	Enabled	
	Custom NTP server	Disabled	
	Port speed	10/100/1000	
	Ethernet MAC address	See product label	
Radio	Radio and Wireless Settings		
	Operating mode	Access point, infrastructure mode	
	Wireless access point name	netgearxxxxx, where xxxxx are the last 6 digits of the wireless access point MAC address	
	Country and region	Varies by region	
	Wireless communication	2.4 GHz radio enabled 5 GHz radio enabled	

Featur	e	Description	
	Wireless modes	11ng 11ac	
	Wireless network names (SSIDs)	NETGEAR_11ng NETGEAR_11ac	
	Broadcast network names (SSIDs)	Enabled	
	Radio frequency channels	11ng: Auto 11ac: Auto	
	MCS index/data rate (transmission speed)	Best Note: Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual 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.	
	Channel width	11ng: 20 MHz 11ac: Dynamic 20/40/80 MHz	
	Guard interval	Auto	
	Output power	Full	
	Wireless on/off (radio scheduling)	Disabled	
	RTS threshold	2347	
	Fragmentation length	2346	
	Beacon interval	100	
	Aggregation length	65535	
	A-MPDU	Enabled	
	RIFS transmission	Disabled	
	DTIM interval	3	
	Preamble type	Auto	
	802.11d	Enabled	
	Client isolation	Disabled	
	Maximum wireless clients	64	
	Wi-Fi Multimedia (WMM)	Enabled	
	WMM powersave	Enabled	

 Table 2. Factory default settings (continued)

eature	Description	
AP EDCA parameters (QoS settings)	 AIFS. The Arbitration Inter-Frame Spacing (AIFS) interval specifies, in milliseconds, the wait time between data frames. Higher AIFS values mean higher priority to that queue. Valid values for AIFS are 1 through 255. CwMin. The minimum contention window (CwMin) value specifies the upper limit (in milliseconds) of a range from which the initial random back-off wait time is determined. Decreasing this value increases the priority of the queue. The value for CwMin must be lower than the value for CwMax. Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1024. CwMax. The maximum contention window (CwMax) value specifies (in milliseconds) the upper limit for the doubling of the random back-off value. Decreasing this value increases the priority of the queue. The value for CwMax must be higher than the value for CwMin. Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1024. Max. Burst. (access point only) The maximum burst value specifies (in milliseconds) the wireless network. A packet burst is a collection of multiple frames transmitted without header information. Decreasing this value increases the priority of the queue. Valid values for maximum burst length are 0.0 through 999.9. 	
Station EDCA parameters (QoS settings)	 AIFS. The Arbitration Inter-Frame Spacing (AIFS) interval specifies, in milliseconds, the wait time between data frames. Higher AIFS values means higher priority to that queue. Valid values for AIFS are 1 through 255. CwMin. The minimum contention window (CwMin) value specifies the upper limit (in milliseconds) of a range from which the initial random back-off wait time is determined. Decreasing this value increases the priority of the queue. The value for CwMin must be lower than the value for CwMax. Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1024. CwMax. The maximum contention window (CwMax) value specifies (in milliseconds) the upper limit for the doubling of the random back-off value. Decreasing this value increases the priority of the queue. The value for CwMax must be higher than the value for CwMin. Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1024. TXOP Limit. The transmission opportunity (TXOP) is an interval of time (in milliseconds) when a client station can initiate transmissions on the wireless medium (WM). Decreasing this value increases the priority of the queue. Valid values for maximum burst length are 0.0 through 999.9. 	
Wireless bridging	Disabled	

 Table 2. Factory default settings (continued)

Table 2.	Factory	default settings	(continued)
----------	---------	------------------	-------------

Feature		Description		
Defau	Default Wireless Profile and Profile Security			
	Profile name	NETGEAR		
	Wireless network names (SSIDs)	NETGEAR_11ng NETGEAR_11ac		
	Broadcast wireless network names (SSIDs)	Enabled		
	Network authentication	Open system (no authentication)		
	Data encryption	None		
	Wireless client security separation	Disabled		

Technical Specifications

Table 3. WAC120 access point specifications

Feature	Description		
802.11b/bg/ng Wireless Specifications			
802.11b data rates	1, 2, 5.5, and 11 Mbps, and auto-rate capable		
802.11bg data rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps, and auto-rate capable		
802.11ng MCS index and data rates	Data rates for a 20 MHz channel width and an automatic guard interval: 0 / 7.2 Mbps, 1 / 14.4 Mbps, 2 / 21.7 Mbps, 3 / 28.9 Mbps, 4 / 43.3 Mbps, 5 / 57.8 Mbps, 6 / 65 Mbps, 7 / 72.2 Mbps, 8 / 14.44 Mbps, 9 / 28.88 Mbps, 10 / 43.33 Mbps, 11 / 57.77 Mbps, 12 / 86.66 Mbps, 13 / 115.56 Mbps, 14 / 130 Mbps, 15 / 144.44 Mbps, and auto-rate capable		
	Data rates for a 20 MHz channel width and a long guard interval (800 ms): 0 / 6.5 Mbps, 1 / 13 Mbps, 2 / 19.5 Mbps, 3 / 26 Mbps, 4 / 39 Mbps, 5 / 52 Mbps, 6 / 58.5 Mbps, 7 / 65 Mbps, 8 / 13 Mbps, 9 / 26 Mbps, 10 / 39 Mbps, 11 / 52 Mbps, 12 / 78 Mbps, 13 / 104 Mbps, 14 / 117 Mbps, 15 / 130 Mbps, and auto-rate capable		
	Data rates for a 40 MHz channel width and an automatic guard interval: 0 / 15 Mbps, 1 / 30 Mbps, 2 / 45 Mbps, 3 / 60 Mbps, 4 / 90 Mbps, 5 / 120 Mbps, 6 / 135 Mbps, 7 / 150 Mbps, 8 / 30 Mbps, 9 / 60 Mbps, 10 / 90 Mbps, 11 / 120 Mbps, 12 / 180 Mbps, 13 / 240 Mbps, 14 / 270 Mbps, 15 / 300 Mbps, and auto-rate capable		
	Data rates for a 40 MHz channel width and a long guard interval (800 ms): 0 / 13.5 Mbps, 1 / 27 Mbps, 2 / 40.5 Mbps, 3 / 54 Mbps, 4 / 81 Mbps, 5 / 108 Mbps, 6 / 121.5 Mbps, 7 / 135 Mbps, 8 / 27 Mbps, 9 / 54 Mbps, 10 / 81 Mbps, 11 / 108 Mbps, 12 / 162 Mbps, 13 / 216 Mbps, 14 / 243 Mbps, 15 / 270 Mbps, and auto-rate capable		
802.11b/bg/ng operating frequencies	 2.412–2.462 GHz (US) 2.457–2.462 GHz (Spain) 2.410–2.484 GHz (Japan 11b) 2.410–2.472 GHz (Japan 11ng) 2.457–2.472 GHz (France) 2.412–2.472 GHz (Europe ETSI) 2.412–2.472 GHz (China) 		
802.11 b/bg/ng encryption	 64-bit, 128-bit, and 52-bit WEP AES TKIP 		
802.11a/na/ac Wireless Specifications			
802.11a data rates	6, 9, 12, 18, 24, 36, 48, 54 Mbps, and auto-rate capable		

Feature	Description		
802.11na data rates	Data rates for a 20 MHz channel width and an automatic guard interval: 0 / 14.4 Mbps, 1 / 28.9 Mbps, 2 / 43.3 Mbps, 3 / 57.8 Mbps, 4 / 86.7 Mbps, 5 / 115.6 Mbps, 7 / 144.4 Mbps, 8 / 173.4 Mbps, and auto-rate capable		
	Data rates for a 20 MHz channel width and a long guard interval (800 ms): 0 / 13.0 Mbps, 1 / 26.0 Mbps, 2 / 39.0 Mbps, 3 / 52.0 Mbps, 4 / 78.0 Mbps, 5 / 104.0 Mbps, 6 / 117.0 Mbps, 7 / 130.0 Mbps, 8 / 156.0 Mbps, and auto-rate capable		
	Data rates for a 40 MHz channel width and an automatic guard interval: 0 / 30.0 Mbps, 1 / 60.0 Mbps, 2 / 90.0 Mbps, 3 / 120.0 Mbps, 4 / 150.0 Mbps, 5 / 180.0 Mbps, 6 / 210.0 Mbps, 7 / 240.0 Mbps, 8 / 270.0 Mbps, 9 / 300.0 Mbps, 10 / 330.0 Mbps, 11 / 370.0 Mbps, 12 / 400.0 Mbps and auto-rate capable		
	Data rates for a 40 MHz channel width and a long guard interval (800 ms): 0 / 27.0 Mbps, 1 / 54.0 Mbps, 2 / 81.0 Mbps, 3 / 108.0 Mbps, 4 / 162.0 Mbps, 5 / 216.0 Mbps, 6 / 243.0 Mbps, 7 / 270.0 Mbps, 8/ 324.0 Mbps, 9 / 360.0 Mbps, and auto-rate capable		
	Data rates for a 80 MHz channel width and an automatic guard interval: 0 / 65.0 Mbps, 1 / 130.0 Mbps, 2 / 195.0 Mbps, 3 / 260.0 Mbps, 4 / 390.0 Mbps, 5 / 520.0 Mbps, 6 / 585.0 Mbps, 7 / 650.0 Mbps, 8 / 780.0 Mbps, 9 / 866.7 Mbps, and auto-rate capable		
	Data rates for a 80 MHz channel width and a long guard interval (800 ms): 0 / 58.5 Mbps, 1 / 117.0 Mbps, 2 / 175.5 Mbps, 3 / 234.0 Mbps, 4 / 351.0 Mbps, 5 / 468.0 Mbps, 6 / 526.5 Mbps, 7 / 585.0 Mbps, 8 / 702.0 Mbps, 9 / 780.0 Mbps, and auto-rate capable		
802.11a/na operating frequencies	 5.180–5.240 GHz (US, lower frequencies) 5.260–5.320 GHz (US, middle frequencies) 5.180–5240 GHz (CE [EU], lower frequencies) 5.260–5.320 GHz (CE [EU], middle frequencies) 5.500–5.680 GHz (CE [EU], upper frequencies) 		
802.11 a/na encryption	 64-bit, 128-bit, and 52-bit WEP AES TKIP 		
Management and Other Specifications			
Maximum clients	Limited by the amount of wireless network traffic generated by each node; a maximum of 64 clients is supported.		
Status LEDs	 Power LED Activity LED LAN LED WiFi LED 		
Electrical and Physical Specifications			
Power adapter	12 VDC, 1A; plug is localized to country of sale		

 Table 3. (continued)WAC120 access point specifications (continued)

Feature	Description
Physical specifications	 Dimensions (h x w x d): 178.6 x 169.4 x 57 mm (7.0 x 6.7 x 2.24 in.) Weight: 322g (0.71 lb)
Environmental specifications	Operating temperature: 0 to 50°C (32 to 122°F) Operating humidity: 10–90%
Electromagnetic compliance	 FCC Part 15 SubPart B FCC Part 15 SubPart C FCC Part 15 SubPart E CE C-TICK

 Table 3. (continued)WAC120 access point specifications (continued)