



Dual-Band Wireless AC Access Point

User Manual

Models WAC720 and WAC730

March 2018
202-11624-06

350 E. Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for purchasing this NETGEAR product. You can visit www.netgear.com/support to register your product, get help, access the latest downloads and user manuals, and join our community. We recommend that you use only official NETGEAR support resources.

Conformity

For the current EU Declaration of Conformity, visit http://kb.netgear.com/app/answers/detail/a_id/11621.

Compliance

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

See the regulatory compliance document before connecting the power supply.

Trademarks

© NETGEAR, Inc., NETGEAR, and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Revision History

Publication Part Number	Publish Date	Comments
202-11624-06	March 2018	<p>Changed the product name and published the manual in a new format.</p> <p>Revised <i>Specify Captive Portal Profile Settings and Enable the Captive Portal Instance</i> on page 121.</p> <p>Added <i>Set Up Facebook Wi-Fi for a Captive Portal Profile</i> on page 124.</p>
202-11624-05	April 2017	<p>Made the following changes to provide information about new and enhanced features:</p> <p>Revised <i>Disable Business Central Mode for a Standalone Access Point</i> on page 19.</p> <p>Revised <i>Configure and Enable WiFi Security Profiles</i> on page 39.</p> <p>Added <i>Manage MAC Address Filter Profiles in the Local MAC Address Database</i> on page 50.</p> <p>Revised <i>Enable Rogue AP Detection and Monitor Rogue APs</i> on page 53.</p> <p>Revised <i>Schedule the WiFi Radios to Be Turned Off</i> on page 57.</p> <p>Revised <i>Monitor WiFi Clients</i> on page 83.</p> <p>Revised <i>Configure Advanced WiFi Settings</i> on page 106.</p> <p>Revised <i>Manage Captive Portals</i> on page 120.</p> <p>Added <i>Configure the Access Point in Business Central Mode</i> on page 143.</p> <p>Changed cloud mode to Business Central mode throughout the manual.</p> <p>Updated various figures throughout the manual.</p>

Dual-Band Wireless AC Access Point WAC720 and WAC730 User Manual

Publication Part Number	Publish Date	Comments
202-11624-04	March 2016	<p>Revised <i>Mount the Access Point</i> on page 30 to show the changes to the access point mounting bracket.</p> <p>Changed firmware version 3.5.4.0 to version 3.5.6.0 (see <i>Log In to the Access Point</i> on page 16 and <i>Disable Business Central Mode for a Standalone Access Point</i> on page 19).</p>
202-11624-03	March 2016	<p>Major revision with the following major changes:</p> <p>Revised <i>Log In to the Access Point</i> on page 16.</p> <p>Added <i>Disable Business Central Mode for a Standalone Access Point</i> on page 19.</p> <p>Added <i>View Dashboard Information</i> on page 80.</p> <p>Revised <i>Configure and Enable WiFi Security Profiles</i> on page 39.</p> <p>Added <i>Configure Load Balancing</i> on page 118.</p> <p>Revised <i>Set Up, Manage, and Monitor Ensembles</i> on page 87.</p> <p>Revised <i>Manage Captive Portals</i> on page 120.</p> <p>Removed the legacy 802.1x security option (RADIUS security option).</p> <p>Removed the WPA and WPA-PSK (TKIP) security options.</p> <p>In addition, made many minor changes plus the following nontechnical changes:</p> <p>Increased the quality of all screen shots.</p> <p>Replaced many screen shots.</p> <p>Converted all procedures to standalone procedures.</p> <p>Changed the name of the manual from Reference Manual to User Manual.</p>
202-11624-02	February 2016	Revised <i>Configure WiFi Bridging</i> on page 132.
202-11624-01	December 2015	Revised <i>Mount the Access Point</i> on page 30.
202-11607-01	October 2015	First publication.

Contents

Chapter 1 Introduction and Hardware Overview

Unpack Your Access Point.....	9
Top Panel.....	9
Rear Panel.....	10
Access Point Label.....	11

Chapter 2 Initial Setup

What You Need Before You Begin.....	13
System Requirements.....	13
WiFi Equipment Placement and Range Guidelines.....	13
Ethernet Cabling Requirements.....	14
LAN Configuration Requirements.....	14
Hardware Requirements for Computers on Your LAN.....	14
Operating Frequency Guidelines.....	14
Requirements for Entering IP Addresses.....	14
IPv4.....	14
IPv6.....	15
Install and Configure the Access Point.....	15
Connect the Access Point to a Computer.....	15
Log In to the Access Point.....	16
Log In to the Access Point When It Is Directly Connected to Your Computer...17	
Log In to the Access Point When It Is Connected to a Network With a DHCP Server.....	18
Local Browser Interface.....	18
Disable Business Central Mode for a Standalone Access Point.....	19
Configure Basic General System Settings.....	20
Configure Time Settings.....	22
Configure the IPv4 Settings.....	23
Configure the Basic WiFi Settings.....	24
Configure 802.11bg/ng/bgn WiFi Settings.....	24
Configure 802.11a/a-na-ac WiFi Settings.....	27
Test Basic WiFi Connectivity.....	29
Mount the Access Point.....	30
Package Content of the Ceiling and Wall Installation Kit.....	30
Mount the Access Point to a Drop Ceiling.....	30
Mount the Access Point to a Wall.....	33

Chapter 3 Configure the WiFi Features and Security

WiFi Data Security Options.....	37
WiFi Security Profiles.....	38
Configure and Enable WiFi Security Profiles.....	39
About WPA2-PSK and WPA-PSK & WPA2-PSK.....	46

About WPA2 With RADIUS and WPA & WPA2 With RADIUS.....	47
Change the QoS Policy for a WiFi Security Profile.....	47
Configure RADIUS Server Settings.....	48
Manage MAC Address Filter Profiles in the Local MAC Address Database.....	50
Add a MAC Address Filter Profile.....	51
Modify a MAC Address Filter Profile.....	52
Delete a MAC Address Filter Profile.....	53
Enable Rogue AP Detection and Monitor Rogue APs.....	53
Enable Rogue AP Detection.....	54
Monitor Rogue APs.....	55
Monitor Known APs.....	56
Schedule the WiFi Radios to Be Turned Off.....	57
Configure Basic WiFi Quality of Service.....	59

Chapter 4 Manage and Monitor the Access Point

Enable Remote Management.....	62
SNMP Management.....	62
Secure Shell and Telnet Management.....	63
Manage the Access Point over a Telnet Connection.....	64
Upgrade the Access Point Firmware.....	65
Upgrade the Firmware Over a Web Browser.....	65
Upgrade the Firmware Over a TFTP Server.....	66
Manage the Configuration File or Reset to Factory Defaults.....	67
Save the Configuration.....	68
Restore the Configuration.....	68
Restore the Access Point to the Factory Default Settings.....	69
Use the Local Browser Interface to Restore Factory Default Settings.....	70
Use the Reset Button to Restore Factory Default Settings.....	70
Reboot the Access Point Without Restoring the Default Configuration.....	71
Change the Administrator Password.....	72
Manage User Accounts.....	73
Add a New User Account.....	73
Change the Name for a User Account.....	74
Change the Privilege for a User Account.....	75
Reset the Password for a User Account.....	75
Delete a User Account.....	76
Enable the Syslog Server.....	76
Monitor the Access Point.....	77
View System Information.....	78
View Dashboard Information.....	80
View the Standalone Dashboard.....	80
View the Ensemble Dashboard.....	81
Monitor WiFi Clients.....	83
View the Activity Logs.....	85
View the Traffic Statistics.....	86
Set Up, Manage, and Monitor Ensembles.....	87
Configure Enable Ensemble Mode.....	88
Manage an Ensemble.....	88

Specify an Ensemble Management IP Address.....	89
Configure Ensemble Security With a Passphrase.....	89
Specify an Ensemble's Channel Assignment Settings.....	90
Manage Automatic Channel Assignment for an Ensemble.....	91
Upgrade the Firmware of Ensemble Members From a Downloaded Firmware File.....	93
Upgrade the Firmware of Ensemble Members Over a TFTP Server.....	95
Monitor an Ensemble.....	96
Monitor the Status of the Ensemble.....	96
Monitor the Devices Connected to the Ensemble.....	97
Monitor the Access Points and Networks Neighboring the Ensemble.....	98

Chapter 5 Configure Advanced Network and WiFi Features

Configure IPv6 Settings.....	101
Configure Spanning Tree Protocol, 802.1Q VLAN, and Link Layer Discovery Protocol.....	102
Configure STP and VLANs.....	102
Configure Ethernet LLDP.....	104
Configure Bonjour.....	105
Configure Advanced WiFi Settings.....	106
Configure Advanced Quality of Service Settings.....	109
Configure and Manage Quality of Service Policies.....	112
Configure a New QoS Policy.....	112
Modify a QoS Policy.....	117
Delete a QoS Policy.....	118
Configure Load Balancing.....	118
Manage Captive Portals.....	120
Enable the Access Point to Register With Facebook.....	121
Specify Captive Portal Profile Settings and Enable the Captive Portal Instance.....	121
Set Up Facebook Wi-Fi for a Captive Portal Profile.....	124
Add User Accounts to the Local Database for Captive Portal Access.....	126
Upload a Custom Logo.....	128
Configure a Default or Custom Captive Portal Splash Page.....	129
Enable the Global Captive Portal Mode.....	131
Configure WiFi Bridging.....	132
Point-to-Point Bridge and Point-to-Multipoint Bridge.....	132
Configure a WiFi Bridge.....	133

Chapter 6 Troubleshooting

Troubleshoot the Basic Functions.....	137
Verify the Correct Sequence of Events at Startup.....	137
No LEDs Are Lit on the Access Point.....	137
The Active LED or the LAN LED Is Not Lit.....	138
The WLAN LED Does Not Light.....	138
You Cannot Access the Internet or the LAN From a WiFi Computer.....	138
You Cannot Configure the Access Point From a Browser.....	139
When You Enter a URL or IP Address a Time-Out Error Occurs.....	140
Troubleshoot a TCP/IP Network Using the Ping Utility.....	140

Test the LAN Path to Your Access Point.....	140
Test the Path from Your Computer to a Remote Device.....	141
Problems With Date and Time.....	141
Use the Packet Capture Tool.....	142

Appendix A Configure the Access Point in Business Central Mode

Enable Business Central Mode.....	144
Configure the IP and 802.1Q VLAN Settings in Business Central Mode.....	145
Reboot the Access Point in Business Central Mode.....	146
Reset the Access Point in Business Central Mode to Factory Default Settings..	147
Upgrade Access Point Firmware in Business Central Mode.....	148
Configure MAC Authentication in Business Central Mode.....	148
Add a MAC Address Filter Profile on an Access Point in Business Central Mode.....	149
Assign a MAC Address Filter Profile on an Access Point in Business Central Mode.....	151
Modify a MAC Address Filter Profile on an Access Point in Business Central Mode.....	153
Delete a MAC Address Filter Profile on an Access Point in Business Central Mode.....	154
Monitor the Access Point in Business Central Mode.....	154
View the Activity Logs of an Access Point in Business Central Mode.....	155
View Basic Information About the Access Point In Business Central Mode...	156

Appendix B Supplemental Information

Technical Specifications.....	158
Factory Default Settings.....	161

Introduction and Hardware Overview

1

This user manual describes how you can manage the NETGEAR Dual-Band Wireless AC Access Point models WAC720 and WAC730 by using the local browser-based management interface, in this manual referred to as the local browser interface.

The essential differences between the two models are the maximum theoretical WiFi throughput and the number of supported optional dual-band antennas:

- **Model WAC720.** This model can support two optional dual-band antennas. The maximum theoretical WiFi throughput is 300 Mbps in the 2.4 GHz band and 867 Mbps in the 5 GHz band
- **Model WAC730.** This model can support three optional dual-band antennas. The maximum theoretical WiFi throughput is 450 Mbps in the 2.4 GHz band and 1300 Mbps in the 5 GHz band

This chapter includes the following sections:

- *Unpack Your Access Point*
- *Top Panel*
- *Rear Panel*
- *Access Point Label*

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

Note Firmware updates with new features and bug fixes are made available from time to time at 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.

Note In this manual, *WiFi* and *wireless* are interchangeable terms.

Unpack Your Access Point

Your package contains the following items:

- ProSAFE Dual-Band Wireless AC Access Point
- Straight-through Category 5 Ethernet cable
- Ceiling and wall installation kit
- Installation guide

Contact your reseller or customer support in your area if any parts are missing or damaged.

Visit the NETGEAR website at support.netgear.com/general/contact/default.aspx for the telephone number of customer support in your area.

Top Panel






The following figure shows the LEDs on the top panel.



Figure 1. Top panel

The following table describes the LEDs on the top panel.

Table 1. Top panel LEDs

Item	LED	Description		
1		Power/Test	Off	Power is off.
			On (green)	Power is on.
			Amber, then blinking green	A self-test is running or firmware is being loaded. During startup, the LED is first steady amber, then goes off, and then blinks green before turning steady green after about 45 seconds. If after one minute the LED remains amber or continues to blink green, it indicates a system fault.
2		Active	Off	No Ethernet traffic is detected, or no link is detected.
			On or blinking (green)	Ethernet traffic is detected.
3		LAN	Off	A 10 Mbps or no link is detected on LAN port.
			Amber	A 100 Mbps link is detected on LAN port.
			Green	A 1000 Mbps link is detected on LAN port.
4		2.4 GHz WLAN	Off	The WiFi 802.11b/g/n (2.4 GHz) LAN is not ready, or no WiFi activity is detected.
			On or blinking (green)	The WiFi 802.11b/g/n (2.4 GHz) LAN is ready, or WiFi activity is detected.
5		5 GHz WLAN	Off	The WiFi 802.11n/a (5 GHz) LAN is not ready, or no WiFi activity is detected.
			On or blinking (green)	The WiFi 802.11n/a (5 GHz) LAN is ready, or WiFi activity is detected.

Rear Panel

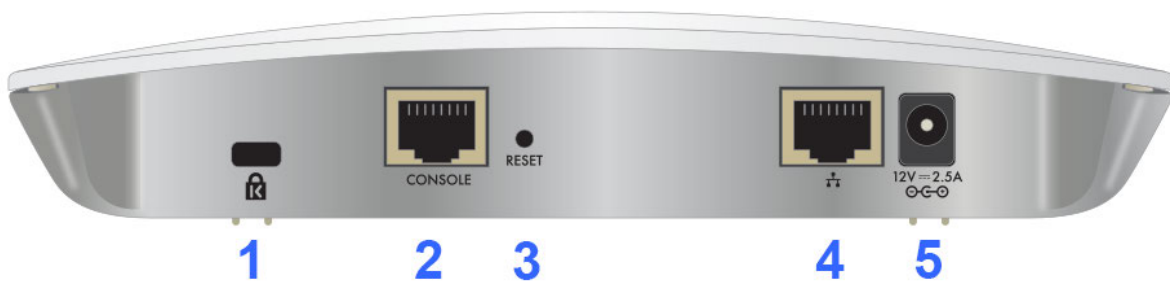


Figure 2. Rear panel

Dual-Band Wireless AC Access Point WAC720 and WAC730 User Manual

The rear panel components of the access point, from left to right, are described in the following list:

1. Cable security lock receptacle for an optional lock.
2. Console port for connecting to an optional console terminal. The port provides an RJ-45 connector and supports the following settings: 115200 K default baud rate, 8 data bits, no (N) parity bit, and one (1) stop bit.
3. Factory default **Reset** button. Using a sharp object, press and hold this button for about five seconds to reset the access point to factory defaults settings. All configuration settings are lost, and the default password is restored. For more information, see [Restore the Access Point to the Factory Default Settings](#) on page 69.
4. 10/100/1000BASE-T Gigabit Ethernet (RJ-45) port with Auto Uplink (Auto MDI-X) and support for IEEE 802.3af Power over Ethernet (PoE) for connection to a switch or router that can provide PoE.
5. Power socket for an optional 12 VDC, 2.5A power adapter.

Note The WAC720 access point can support up to two optional 2.4 GHz/5 GHz dual-band antennas. The WAC730 access point can support up to three optional 2.4 GHz/5 GHz dual-band antennas.

Access Point Label

The access point label on the bottom of the access point's enclosure displays factory default settings, regulatory compliance, and other information.



Figure 3. Label model WAC720



Figure 4. Label model WAC730

This chapter includes the following sections:

- *What You Need Before You Begin*
- *Install and Configure the Access Point*
- *Connect the Access Point to a Computer*
- *Log In to the Access Point*
- *Disable Business Central Mode for a Standalone Access Point*
- *Configure Basic General System Settings*
- *Configure Time Settings*
- *Configure the IPv4 Settings*
- *Configure the Basic WiFi Settings*
- *Test Basic WiFi Connectivity*
- *Mount the Access Point*

What You Need Before You Begin

You must consider the following guidelines and requirements before you can set up your access point.

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 PoE switch or a 12V, 2.5 A, DC power source
- A web browser for configuration
- At least one computer with the TCP/IP protocol installed
- 802.11bg/ng/bgn-compliant or 802.11a/a-na-ac-compliant devices

WiFi Equipment Placement and Range Guidelines

The range of your WiFi connection can vary significantly based on the location of the access point. The latency, data throughput performance, and power consumption of WiFi devices also vary depending on your configuration choices.

Note Failure to follow these guidelines can result in significant performance degradation or inability to connect over WiFi to the access point. For complete performance specifications, see *Supplemental Information* on page 157.

Note Before you position and mount the access point at its permanent position, first configure the access point and test the computers on your LAN for WiFi connectivity as described in this chapter.

For best results, place your access point according to the following general guidelines:

- Near the center of the area in which the WiFi devices will operate.
- In an elevated location such as a high shelf where the WiFi devices are in a line-of-sight (even if through walls).
- Away from sources of interference, such as computers, microwaves ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces or water.
- Placing an external antenna in a vertical position provides best side-to-side coverage. Placing an external antenna in a horizontal position provides best up-and-down coverage. (An external antenna does not come standard with the access point.)

If you are using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is five channels (for example, use Channels 1 and 6, or 6 and 11, or 1 and 11).

The time it takes to establish a WiFi connection can vary depending on both your security settings and placement.

Ethernet Cabling Requirements

The access point connects to your LAN using twisted-pair Category 5 Ethernet cable with RJ-45 connectors.

LAN Configuration Requirements

For the initial configuration of your access point, you must connect a computer to the access point.

Hardware Requirements for Computers on Your LAN

To connect to the access point on your network, your WiFi device must support 802.11b, 802.11g, 802.11n, 802.11a, or 802.11ac. If your computer does not include an internal WiFi adapter, we recommend using the NETGEAR A6210 WiFi USB Adapter.

Operating Frequency Guidelines

You do not need to change the operating frequency (channel) unless you notice interference problems or you place the access point near another access point. If you do change the operating frequency, observe the following guidelines:

- Access points use a fixed channel. You can select a channel that provides the least interference and best performance. In the United States and Canada, 11 channels are available.
- If you use multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is five channels (for example, use Channels 1 and 6, or 6 and 11).
- In infrastructure mode (which is the default mode for the access point), WiFi stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This is possible only if the access points use the same SSID.

Requirements for Entering IP Addresses

IP addresses assigned to the access points must follow the following requirements for IPv4 and IPv6 addresses.

IPv4

The fourth octet of an IP address must be between 0 and 255 (both inclusive). This requirement applies to any IP address that you enter on the access point's local browser interface.

IPv6

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. Any four-digit group of zeroes within an IPv6 address can be reduced to a single zero or altogether omitted.

The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

Install and Configure the Access Point

Install and configure your access point in the order of the following sections:

1. *Connect the Access Point to a Computer* on page 15
2. *Log In to the Access Point* on page 16
3. *Disable Business Central Mode for a Standalone Access Point* on page 19
4. *Configure Basic General System Settings* on page 20
5. *Configure Time Settings* on page 22
6. *Configure the IPv4 Settings* on page 23
7. *Configure the Basic WiFi Settings* on page 24

Before installing the access point, make sure that your Ethernet network functions. After you connect the access point to the Ethernet network, computers that support 802.11b/g/a/n/ac are able to communicate with the Ethernet network.

For this to work correctly, verify that you meet all the system requirements, shown in *What You Need Before You Begin* on page 13.

Connect the Access Point to a Computer

Tip Before you place the access point in an elevated position that is difficult to reach, first set up and test the access point to verify WiFi network connectivity.






► To set up the access point:

1. Unpack the box and verify the contents.
2. Prepare a computer with an Ethernet adapter.
If this computer is already part of your network, record its TCP/IP configuration settings. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 as the subnet mask.
3. Connect an Ethernet cable from the access point to the computer.
4. Securely insert the other end of the cable into the access point's Ethernet port.
5. Turn on your computer.

- Connect the access point to a PoE switch or power adapter.

Tip The access point supports Power over Ethernet (PoE) with power redundancy. If you are using a switch that provides PoE, you do not need to use a power adapter to power the access point. Using PoE can be especially convenient when the access point is installed in a high location far away from a power outlet.

- Verify that the LEDs functions as indicated in the following table:

LED	Description
	Power/Test LED. The Power/Test LED blinks when the access point is first turned on. (To be exact, during startup, the LED is first steady amber, then goes off, and then blinks green.) After about 45 seconds, the LED stays lit (steady green). If after one minute the Power/Test LED is not lit or is still blinking, check the connections and see if the power outlet is controlled by a wall switch that is turned off.
	Active LED. The Active LED is lit or blinks green when Ethernet traffic is detected.
	LAN LED. The LAN LED indicates the LAN speed for LAN port 1: green for 1000 Mbps, amber for 100 Mbps, and no light for 10 Mbps. If the LAN LED is not lit, make sure that the Ethernet cable is securely attached at both ends.
2.4 GHz 	2.4 GHz WLAN LED. The 2.4 GHz WLAN LED is lit or blinks green when the WiFi LAN (WLAN) is ready.
5 GHz 	5 GHz WLAN LED. The 5 GHz WLAN LED is lit or blinks green when the WiFi LAN (WLAN) is ready.

Log In to the Access Point

The default IP address of your access point is 192.168.0.100.

By default, the access point functions as a DHCP client. If the access point is installed in a network that includes a DHCP server, the IP address of the access point is issued by the DHCP server. You can find the IP address of the access point by accessing the DHCP server or by using an IP address scanner utility. (Free IP address scanner utilities are available online.)

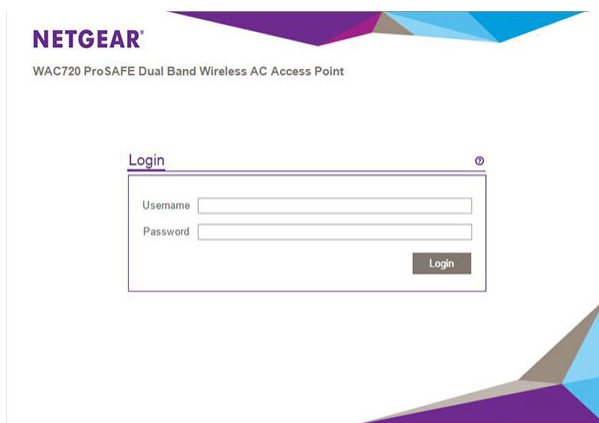
If you must configure the access point with a static IPv4 address, see the steps in [Log In to the Access Point When It Is Directly Connected to Your Computer](#) on page 17 and [Configure the IPv4 Settings](#) on page 23.

Note When the access point runs firmware version 3.5.6.0 or a later version, by default, the access point is enabled for the cloud (that is, Business Central mode is enabled) and operates with a limited local browser interface (only the Configuration and Monitoring menu tabs display).

Log In to the Access Point When It Is Directly Connected to Your Computer

► **To log in to the access point when it is directly connected to your computer:**

1. Change the IP address of your computer to an IP address in the 192.168.0.x subnet, which is the subnet in which the access point's default IP address is located.
2. For example, change the computer's IP address to 192.168.0.210.
3. Connect your computer to the access point with an Ethernet cable.
4. Open a web browser on your computer.
5. In the address bar, enter **http://192.168.0.100**.
192.168.0.100 is the default IP address of the access point.

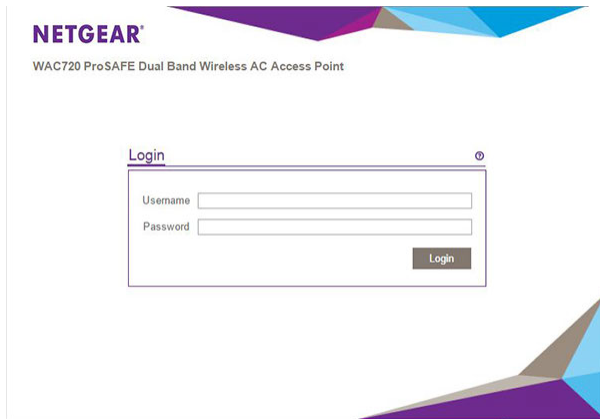


6. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
7. Click the **Login** button.
The web browser displays the General page under the **Configuration** tab. If you are using the access point as a standalone access point or as an access point with a wireless controller, you must disable Business Central mode (see [Disable Business Central Mode for a Standalone Access Point](#) on page 19).
After you disable Business Central mode and you log in to the access point, the web browser displays the Dashboard page under the **Monitoring** tab of the main menu. For more information, see [View Dashboard Information](#) on page 80.

Log In to the Access Point When It Is Connected to a Network With a DHCP Server

► To log in to the access point when it is connected to a network with a DHCP server.

1. Open a web browser from a computer that is connected to the same network as the access point.
2. In the address bar, enter the network IP address of the access point.
You can find the IP address of the access point by accessing the DHCP server or by using an IP address scanner utility. (Free IP address scanner utilities are available online.)



3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Click the **Login** button.
The web browser displays the General page under the **Configuration** tab. If you are using the access point as a standalone access point or as an access point with a wireless controller, you must disable Business Central mode (see [Disable Business Central Mode for a Standalone Access Point](#) on page 19).
After you disable Business Central mode and you log in to the access point, the web browser displays the Dashboard page under the **Monitoring** tab of the main menu. For more information, see [View Dashboard Information](#) on page 80.

Local Browser Interface

The navigation tabs across the top of the pages of the local browser interface provide access to all the configuration functions of the access point and remain constant. The menu items in the blue bar change according to the navigation tab that is selected.

The top right corner of all pages that allow you to make configuration changes show the **Apply** and **Cancel** buttons, and on several pages the **Edit** button.

These buttons provide the following functions:

- **Edit.** Allows you to edit the existing configuration.
- **Cancel.** Cancels all configuration changes that you made on the page.
- **Apply.** Saves and applies all configuration changes that you made on the page.

Disable Business Central Mode for a Standalone Access Point

When the access point runs firmware version 3.5.6.0 or a later version, by default, Business Central mode (also referred to as cloud mode) is enabled for the access point and the local browser interface is a restricted interface that shows only the **Configuration** and **Monitoring** menu tabs with limited configuration options.

If you are using the access point as a standalone access point or as an access point with a wireless controller, you must disable Business Central mode.

For information about configuring the access point in Business Central mode, see [Configure the Access Point in Business Central Mode](#) on page 143.

► To disable Business Central mode:

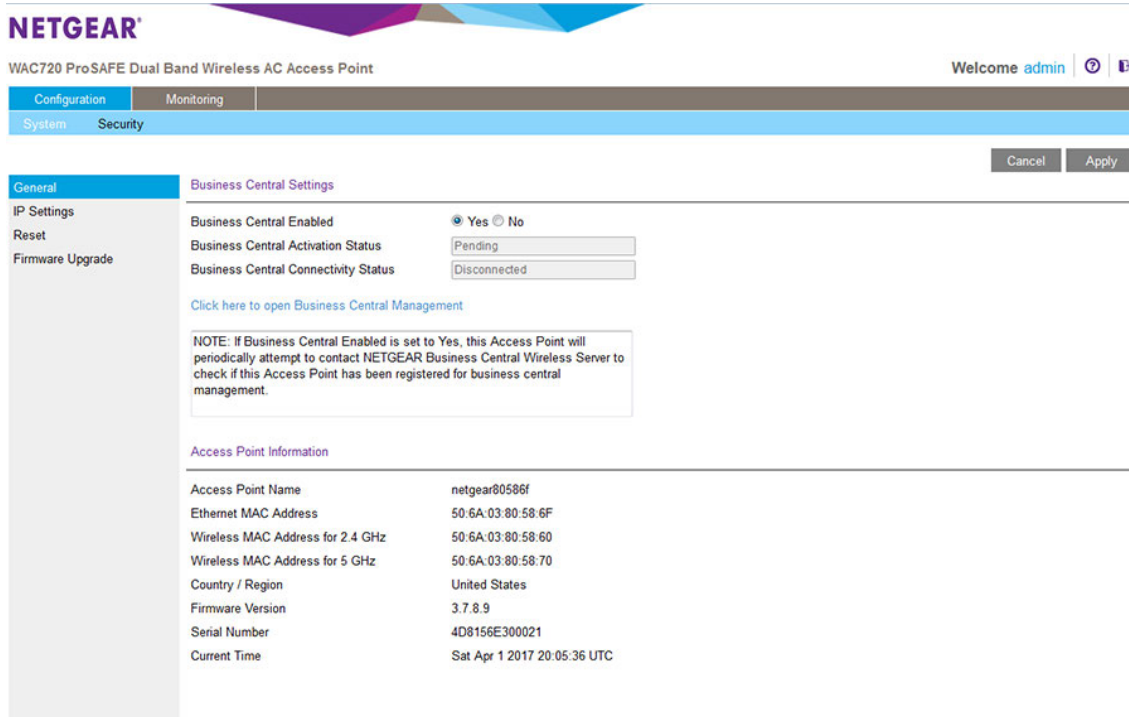
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.

For more information, see [Log In to the Access Point](#) on page 16.

2. In the address bar, enter the IP address of the access point.
A login window opens.

3. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.



4. Select the Business Central Enabled **No** radio button.

5. Click the **Apply** button.

The access point restarts with factory default settings but retains its IP configuration and management VLAN.

The access point is now ready for standalone operation with a full local browser interface.

Configure Basic General System Settings

► To configure basic system settings:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.

For more information, see [Log In to the Access Point](#) on page 16.

2. In the address bar, enter the IP address of the access point.

A login window opens.

3. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Configuration > System > Basic > General**.

Dual-Band Wireless AC Access Point WAC720 and WAC730 User Manual

NETGEAR

WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration Monitoring Maintenance Support

System IP Wireless Security Wireless Bridge Ensemble Captive Portal

Cancel Apply

Basic General

General

Access Point Name netgear0586f

Country / Region US - United States

Business Central Settings

Business Central Enabled Yes No

Business Central Activation Status Pending

Business Central Connectivity Status Disconnected

[Click here to open Business Central Management](#)

NOTE: If Business Central Enabled is set to Yes, this Access Point will periodically attempt to contact NETGEAR Business Central Wireless Server to check if this Access Point has been registered for business central management.

- Configure the settings as described in the following table.

Setting	Description
Access Point Name	This unique name is the access point NetBIOS name. The name is printed on the access point label. The default is netgearxxxxxx, in which 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. The access point name can be retrieved through SNMP.
Country / Region	<p>From the Country / Region menu, select the country where the access point is installed.</p> <hr/> <p>Note Make sure that the country is set to the location where the device is operating. You are responsible for complying with the local, regional, and national regulations that are set for channels, power levels, and frequency ranges.</p> <hr/> <p>Note It might not be legal to operate this access point in a region other than one of those identified in this field.</p> <hr/>

Note For information about the Business Central settings and about enabling Business Central mode, see *Configure the Access Point in Business Central Mode* on page 143.

- Click the **Apply** button.
Your settings are saved.

Configure Time Settings

► To configure time settings:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > Basic > Time**.

The screenshot shows the NETGEAR configuration interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The user is logged in as 'admin'. The navigation menu includes Configuration, Monitoring, Maintenance, and Support. Under Configuration, there are tabs for System, IP, Wireless, Security, Wireless Bridge, Ensemble, and Captive Portal. The 'Basic' section is expanded to show 'Time' settings. The 'Time' settings include: Time Zone (USA (Pacific)), Current Time (Fri Dec 31 1999 12:14:09 PST), NTP Client (radio buttons for Enable and Disable, with Enable selected), Use Custom NTP Server (checkbox), and Hostname / IP Address (time-b.netgear.com). There are 'Cancel' and 'Apply' buttons at the bottom right.

5. Configure the settings as described in the following table.

Setting	Description	
Time Zone	Select the time zone to match your location.	
Current Time	This is a nonconfigurable field that displays the current date and time.	
NTP Client	Enable the Network Time Protocol (NTP) client to synchronize the time of the access point with an NTP server. By default the Enable radio button is selected.	
Use Custom NTP Server	Select this check box if you want to use a custom NTP server. You need an Internet connection to use an NTP server that is not on your local network.	
	<table border="1"> <tr> <td>Hostname / IP Address</td> <td>Enter the host name or IP address of the custom NTP server. The default is time-b.netgear.com. If you use a host name, make sure that you configured a DNS server.</td> </tr> </table>	Hostname / IP Address
Hostname / IP Address	Enter the host name or IP address of the custom NTP server. The default is time-b.netgear.com. If you use a host name, make sure that you configured a DNS server.	

6. Click the **Apply** button.
Your settings are saved.

Configure the IPv4 Settings

Note For information about how to configure the IPv6 settings, see [Configure IPv6 Settings](#) on page 101.



WARNING:

If you enable the DHCP client, the IP address of the access point changes when you click the Apply button, causing you to lose your connection to the access point. You must use the new IP address to reconnect to the access point.

Tip If you enable the DHCP client on the access point, you can discover the new IP address of the access point by accessing the DHCP server on your LAN, or by using a network IP address scanner utility.

► **To configure the IPv4 settings:**

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > IP > IP Settings**.

The screenshot shows the Netgear web interface for the WAC720 ProSAFE Dual Band Wireless AC Access Point. The user is logged in as 'admin'. The navigation menu is expanded to show 'IP Settings'. The 'IP Settings' page has a sidebar with 'IP Settings' and 'IPv6 Settings'. The main content area shows the following settings:

DHCP Client	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Address	<input type="text" value="192.168.0.100"/>
IP Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text"/>
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
Network Integrity Check	<input type="checkbox"/>

5. Configure the IPv4 settings as described in the following table.

Setting	Description
DHCP Client	By default, the Dynamic Host Configuration Protocol (DHCP) client is enabled. The access point receives 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	Enter the IP address of your access point. The default IP address is 192.168.0.100. To change the address, enter an unused IP address from the address range used on your LAN, or enable DHCP the server.
IP Subnet Mask	Enter the network number portion of an IP address. Unless you are implementing subnetting, enter 255.255.0.0 as the subnet mask.
Default Gateway	Enter the IP address of the ISP gateway to which the access point connects.
Primary DNS Server	Enter the IP address of the primary and secondary DNS servers. A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your access point during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually in this field.
Secondary DNS Server	
Network Integrity Check	Select this check box to validate that the upstream link is active before allowing WiFi associations. Ensure that the default gateway is configured.

6. Click the **Apply** button.

Your settings are saved.

If you changed the IP address settings and want to log in to the access point again, you must use the new IP address of the access point.

Configure the Basic WiFi Settings

For proper compliance and compatibility between similar products in your coverage area, you must configure the 802.11bg/ng/bgn and 802.11a/a-na-ac settings correctly, including the operating channel and country. You also must configure the basic WiFi network settings so that WiFi devices can connect to your network. For other WiFi features, including WiFi security, see *Configure the WiFi Features and Security* on page 36.



WARNING:

If you configure the access point from a WiFi computer and you change the access point's SSID, channel, or WiFi security settings, you lose your WiFi connection when you click the Apply button. You then must change the WiFi settings of your computer to match the access point's new settings.

Configure 802.11bg/ng/bgn WiFi Settings

► **To configure the 802.11bg/ng/bgn WiFi settings:**

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.

For more information, see *Log In to the Access Point* on page 16.

2. In the address bar, enter the IP address of the access point.

A login window opens.

Dual-Band Wireless AC Access Point WAC720 and WAC730 User Manual

3. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

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

The screenshot shows the configuration page for the 2.4 GHz band. The 'Turn Radio On' checkbox is checked. The 'Wireless Network Name (SSID)' is 'NETGEAR_11ng'. The 'Broadcast Wireless Network Name (SSID)' is 'Yes'. The 'Channel / Frequency' is 'Auto', 'MCS Index / Data Rate' is 'Best', 'Channel Width' is '20 MHz', and 'Guard Interval' is 'Auto'. The 'Output Power' is 'Full'. The 'Wireless Scheduling Status' is 'Disabled'. The 5 GHz band settings are also visible below, with 'Turn Radio On' checked and 'Wireless Scheduling Status' disabled.

Select the WiFi mode in the 2.4 GHz band:

- **11bg**. 802.11b-compliant devices and 802.11g-compliant devices can connect to the access point.
- **11ng**. 802.11n-compliant devices and 802.11g-compliant devices can connect to the access point
- **11bgn**. This is the default setting. 802.11b-compliant devices, 802.11n-compliant devices and 802.11g-compliant devices can connect to the access point. If you keep the default setting, go to step 8.

When you change the WiFi mode, the Turn Radio On check box is automatically cleared, and all fields, buttons, and menus on the page are masked out.

5. Turn on the radio by selecting the **Turn Radio On** check box.

A pop-up window opens.

Note Under normal conditions, you want the radio to be turned on. Turning off the radio disables access through the access point, which can be helpful for configuration, network tuning, or troubleshooting activities.

6. Click the **OK** button to confirm the change of WiFi mode.

The change does not take effect until you click the **Apply** button after you complete the WiFi configuration.

Initial Setup

Dual-Band Wireless AC Access Point WAC720 and WAC730 User Manual

7. Specify the remaining WiFi settings as described the following table.

Setting	Descriptions	
Wireless Network Name (SSID)	Enter a 32-character (maximum) service set identifier (SSID); the characters are case-sensitive. The default is NETGEAR_11ng. The SSID assigned to a WiFi device must match the access point's SSID for the WiFi device to communicate with the access point. If the SSIDs do not match, you do not get a WiFi connection to the access point.	
Broadcast Wireless Network Name (SSID)	Select the Yes radio button to enable the access point to broadcast its SSID, allowing WiFi stations with a null (blank) SSID to adopt the access point's SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button.	
Channel / Frequency	<p>From the menu, select the channel that you want to use for your WiFi LAN. The available WiFi channels and frequencies depend on the country and WiFi mode. The default setting is Auto, which enables the access point to automatically select the most suitable channel.</p> <p>However, you do not need to change the WiFi channel unless you experience interference (indicated by lost connections or slow data transfers). If this happens, you might want to experiment with different channels to see which is the best. For more information, see Operating Frequency Guidelines on page 14.</p> <p>For more information about available channels and frequencies, see Technical Specifications on page 158.</p> <p>If the access point is a member of an ensemble for which automatic channel assignment is enabled (see Manage Automatic Channel Assignment for an Ensemble on page 91), Auto is not available as a selection from the Channel / Frequency menu.</p>	
11ng and 11bgn modes only (For most networks, the default settings work fine.)	MCS Index / Data Rate	From the menu, select a Modulation and Coding Scheme (MCS) index and transmit data rate for the WiFi network. The default setting is Best. For a list of all options that you can select from in 11ng and 11bgn modes, see Factory Default Settings on page 161.
	Channel Width	From the menu, select a channel width. The options are 20 MHz and 40 MHz . The default is 40 MHz.
	Guard Interval	From the menu, select the guard interval to protect transmissions from interference. The default is Auto, or you can select Long - 800 ns . Some legacy devices can operate only with a long guard interval.
11bg modes only	Data Rate	From the menu, select the transmit data rate of the WiFi network. The default setting is Best. For a list of all options that you can select from in 11bg mode, see Factory Default Settings on page 161.
Output Power	<p>From the menu, select the transmission power of the access point: Full, Half, Quarter, Eighth, Minimum. The default is Full.</p> <p>Increasing the power improves performance, but if two or more access points are operating in the same area and on the same channel, interference can occur.</p> <p>Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.</p>	

8. Click the **Apply** button.
Your settings are saved.

Note For information about how to configure advanced WiFi settings, see [Configure Advanced WiFi Settings](#) on page 106.

Configure 802.11a/a-na-ac WiFi Settings

► To configure the 802.11a/a-na-ac WiFi settings:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Wireless > Basic > Wireless Settings**.

NETGEAR

WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration | Monitoring | Maintenance | Support

System | IP | Wireless | Security | Wireless Bridge | Ensemble | Captive Portal

Cancel | Apply

Basic

Wireless Settings - 802.11 b/g/ng/bgn

Wireless Mode: 2.4 GHz Band | 11bg | 11ng | 11bgn

Turn Radio On:

Wireless Network Name (SSID): NETGEAR_11ng

Broadcast Wireless Network Name (SSID): Yes No

Channel / Frequency: Auto

MCS Index / Data Rate: Best

Channel Width: 20 MHz

Guard Interval: Auto

Output Power: Full

Wireless Settings - 802.11 a/a-na-ac

Wireless Mode: 5 GHz Band | 11a | 11a-na-ac

Turn Radio On:

Wireless Network Name (SSID): NETGEAR_11ac

Broadcast Wireless Network Name (SSID): Yes No

Channel / Frequency: Auto

MCS Index / Data Rate: Best

Channel Width: 80 MHz

Guard Interval: Auto

Output Power: Full

Wireless Settings - AP

Wireless Scheduling Status: Disabled

5. Select the WiFi mode in the 5 GHz band:
 - **11a**. 802.11n-compliant devices can connect to the access point because they are backward compatible.
 - **11a-na-ac**. This is the default setting. If you keep the default setting, go to step 8.

When you change the WiFi mode, the **Turn Radio On** check box is automatically cleared, and all fields, buttons, and menus on the page are masked out.

6. Turn on the radio by selecting the **Turn Radio On** check box.
A pop-up window opens.

Note Under normal conditions, you want the radio to be turned on. Turning off the radio disables access through the access point, which can be helpful for configuration, network tuning, or troubleshooting activities.

7. Click the **OK** button to confirm the change of WiFi mode.
The change does not take effect until you click the **Apply** button after you complete the WiFi configuration.
8. Specify the remaining WiFi settings as described the following table.

Setting	Descriptions	
Wireless Network Name (SSID)	Enter a 32-character (maximum) service set identifier (SSID); the characters are case-sensitive. The default is NETGEAR_11ac. The SSID assigned to a WiFi device must match the access point's SSID for the WiFi device to communicate with the access point. If the SSIDs do not match, you do not get a WiFi connection to the access point.	
Broadcast Wireless Network Name (SSID)	Select the Yes radio button to enable the access point to broadcast its SSID, allowing WiFi stations with a null (blank) SSID to adopt the access point's SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button.	
Channel / Frequency	<p>From the menu, select the channel that you want to use for your WiFi LAN. The available WiFi channels and frequencies depend on the country and WiFi mode. The default setting is Auto, which enables the access point to automatically select the most suitable channel.</p> <p>However, you do not need to change the WiFi channel unless you experience interference (indicated by lost connections or slow data transfers). If this happens, you might want to experiment with different channels to see which is the best. For more information, see Operating Frequency Guidelines on page 14.</p> <p>For more information about available channels and frequencies, see Technical Specifications on page 158.</p> <p>If the access point is a member of an ensemble for which automatic channel assignment is enabled (see Manage Automatic Channel Assignment for an Ensemble on page 91), Auto is not available as a selection from the Channel / Frequency menu.</p>	
11a-na-ac mode only (For most networks, the default settings work fine.)	MCS Index / Data Rate	From the menu, select a Modulation and Coding Scheme (MCS) index and transmit data rate for the WiFi network. The default setting is Best. For a list of all options that you can select from in 11a-na-ac mode, see Factory Default Settings on page 161.
	Channel Width	From the menu, select a channel width. The options are 20 MHz , 40 MHz , and 80 MHz . The default is 80 MHz.
	Guard Interval	From the menu, select the guard interval to protect transmissions from interference. The default is Auto, or you can select Long - 800 ns . Some legacy devices can operate only with a long guard interval.

(Continued)

Setting	Descriptions	
11a mode only	Data Rate	From the menu, select the transmit data rate of the WiFi network. The default setting is Best. For a list of all options that you can select from in 11a mode, see <i>Factory Default Settings</i> on page 161.
Output Power	<p>From the menu, select the transmission power of the access point: Full, Half, Quarter, Eighth, Minimum. The default is Full.</p> <p>Increasing the power improves performance, but if two or more access points are operating in the same area and on the same channel, interference can occur.</p> <p>Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.</p>	

- Click the **Apply** button.
Your settings are saved.

Note For information about how to configure advanced WiFi settings, see *Configure Advanced WiFi Settings* on page 106.

Test Basic WiFi Connectivity

After you configure the access point, make sure that WiFi devices can connect to the access point before you position and mount the access point at its permanent position.

► To test for WiFi connectivity:

- Configure your WiFi devices so that they can connect to a WiFi network that you configured on the access point.
- Verify that your WiFi devices acquired a WiFi link to the access point.
- Verify network connectivity by using a browser to connect to the Internet, or check for file and printer access on your network.

Note If you experience trouble connecting to the access point, see *Troubleshooting* on page 136.

We recommend that you complete the following tasks before you deploy the access point in your network:

- Configure WiFi security and other WiFi features as described in *Configure the WiFi Features and Security* on page 36.
- Configure any additional features that you might need as described in *Manage and Monitor the Access Point* on page 61, and *Configure Advanced Network and WiFi Features* on page 100.

After you complete the configuration of the access point, you can reconfigure the computer that you used for this process back to its original TCP/IP settings.

Mount the Access Point

The following sections explain how to mount your access point. We recommend that you review the information in *WiFi Equipment Placement and Range Guidelines* on page 13 before you mount the access point at its permanent position.

- *Package Content of the Ceiling and Wall Installation Kit* on page 30
- *Mount the Access Point to a Drop Ceiling* on page 30
- *Mount the Access Point to a Wall* on page 33

Package Content of the Ceiling and Wall Installation Kit

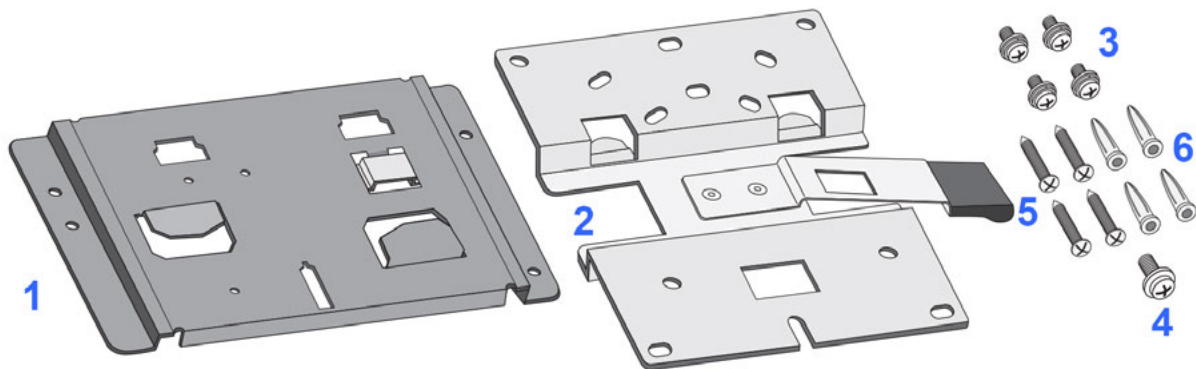


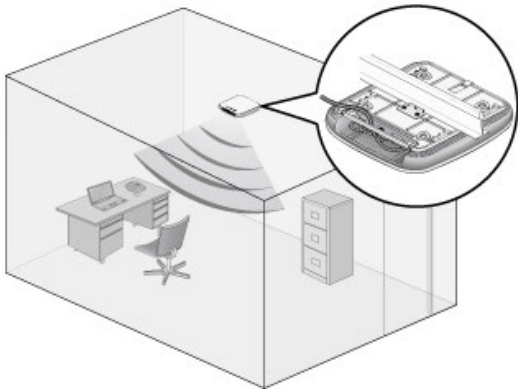
Figure 5. Ceiling and wall installation kit

The ceiling and wall installation kit contains the following components:

1. One access point mounting bracket
2. One wall mounting bracket
3. Four mounting screws with integrated washers for the access point mounting bracket
4. One T-bar screw for the access point mounting bracket
5. Four wall screws for the wall mounting bracket
6. Four wall anchors for the wall mounting bracket

Mount the Access Point to a Drop Ceiling

The best location for ceiling installation is at the center of your WiFi coverage area, and within line of sight of all mobile devices. Make sure that the top (the dome side) of the access point is directed toward the users and not the ceiling. Do not place the access point in a false ceiling space facing up.



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

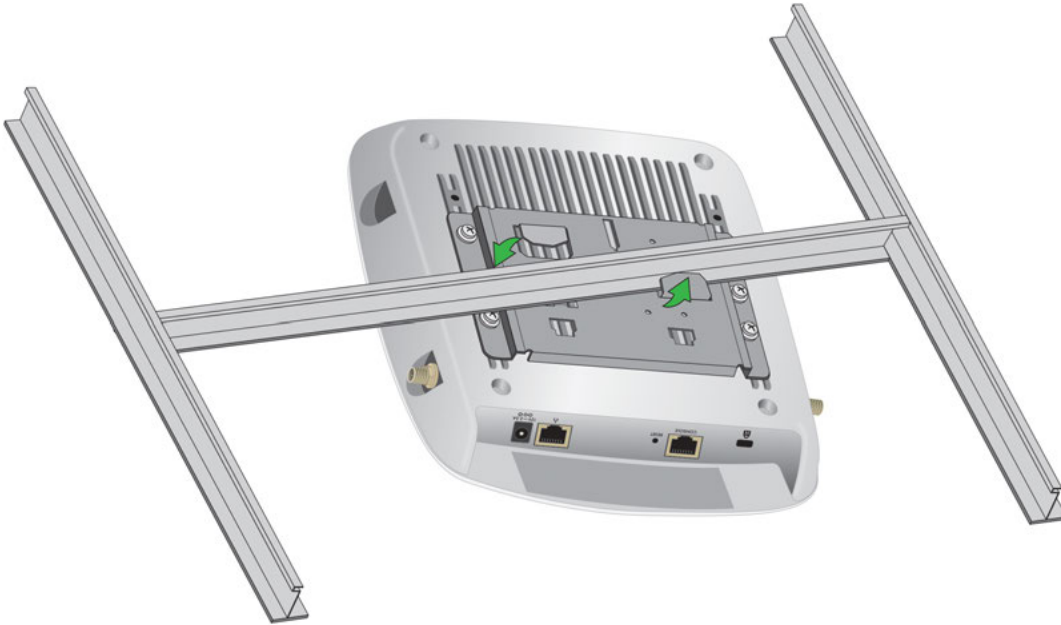
If you are mounting the access point on a hard ceiling, use the wall installation instructions.

▶ To mount the access point to a drop ceiling:

1. Locate the access point mounting bracket, four mounting screws, and T-bar screw in the product package.
2. Attach the access point mounting bracket to the access point using the four mounting screws.



3. Place the access point so that the ceiling rail is between the two tabs on the access point mounting bracket.



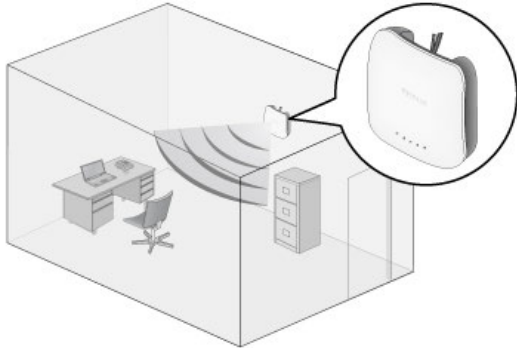
4. Twist the access point to hang it from the ceiling rail.



5. Secure the access point to the ceiling rail using the T-bar screw.

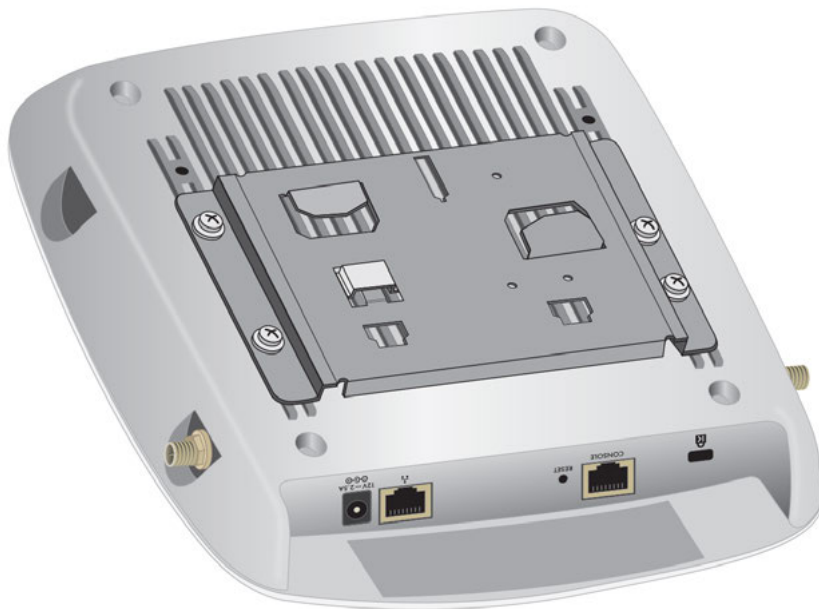
Mount the Access Point to a Wall

The best location for wall installation is at the center of your WiFi coverage area, and within line of sight of all mobile devices. Make sure that the top (the dome side) of the access point is directed toward the users and not the wall.

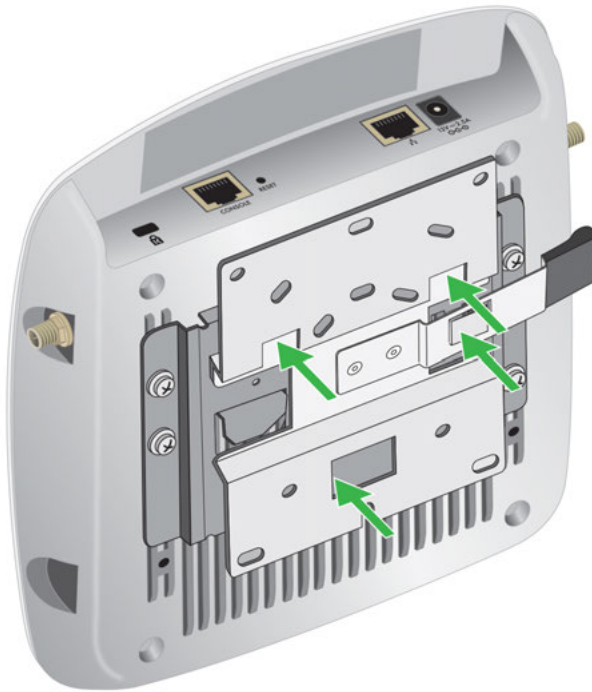


► To mount the access point to a wall:

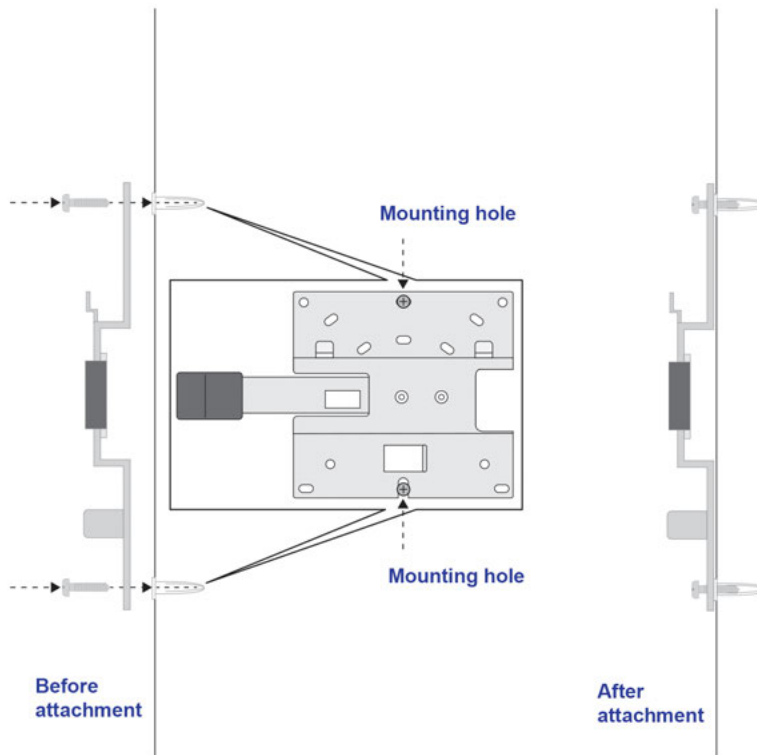
1. Locate the wall mounting bracket, access point bracket, four mounting screws, and wall anchors and screws in the product package.
2. Place the wall mounting bracket on the wall where you want to mount the access point.
3. Mark the wall where the two mounting holes are (see the figure in step 6).
4. Attach the access point mounting bracket to the access point using the four mounting screws as shown.



5. So you can see how the brackets fit together, attach the wall mounting bracket to the access point mounting bracket as shown in the following figure. The three hooks on the wall mounting bracket fit into the three holes on the access point mounting bracket. The handle on the wall mounting bracket also fits into a hole on the access point bracket. Release the wall mounting bracket by moving the handle.

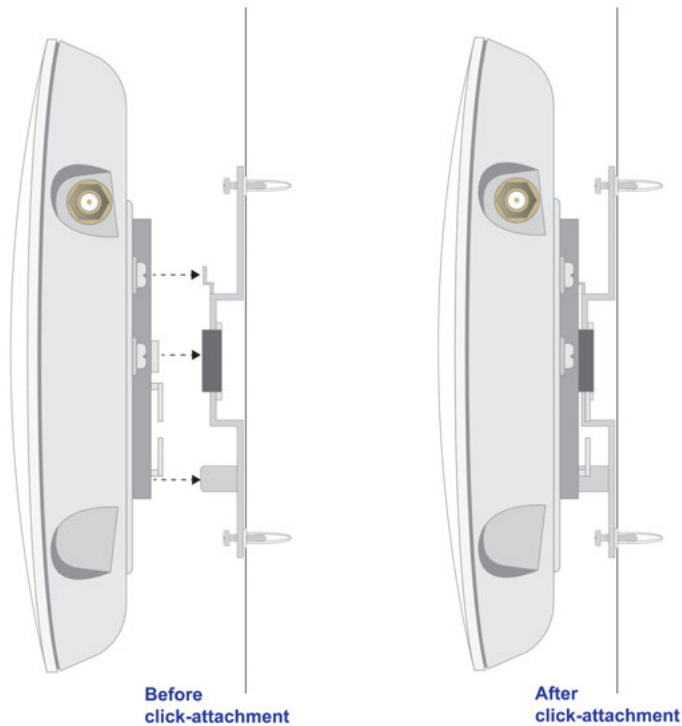


6. Using the wall anchors and screws, attach the wall mounting bracket to the wall where you previously marked. The following figures show a side view of the wall. The left figure includes a schematic view of the wall mounting bracket.



Note Although the product package includes four wall anchors and screws, two screws are sufficient to attach the wall mounting bracket as shown in the previous figure. However, if you prefer, you can use four screws and insert them through the mounting holes in the corners of the wall mounting bracket.

7. Align the three holes on the access point bracket with the three hooks on the wall mounting bracket and slide the access point down until it click-attaches to the wall mounting bracket and is secured. The following figures show a side view of the wall.



Configure the WiFi Features and Security 3

This chapter describes how to configure the WiFi features of the access point.

The chapter includes the following sections:

- *WiFi Data Security Options*
- *WiFi Security Profiles*
- *Configure RADIUS Server Settings*
- *Manage MAC Address Filter Profiles in the Local MAC Address Database*
- *Enable Rogue AP Detection and Monitor Rogue APs*
- *Schedule the WiFi Radios to Be Turned Off*
- *Configure Basic WiFi Quality of Service*

Before you set up WiFi security and additional WiFi features that are described in this chapter, connect the access point, get the Internet connection working, and configure the 802.11bg/ng/bgn and 802.11a/a-na-ac WiFi settings as described in *Initial Setup* on page 12. The access point functions with an Ethernet LAN connection. Make sure that you verify WiFi connectivity before you set up WiFi security and additional WiFi features.

Note If you are configuring the access point from a WiFi computer and you change the access point's SSID, channel, or WiFi security settings, you lose your WiFi connection when you save the settings. You must then change the WiFi settings of your computer to match the access point's new settings.

WiFi Data Security Options

Indoors, computers can connect over 802.11ac WiFi networks at a maximum range of 300 feet. Typically, an access point inside a building works best with devices within a 100-foot radius. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your WiFi data transmissions can extend beyond your walls and can be received by anyone with a compatible WiFi device. For this reason, use the security features of your WiFi equipment. The access point provides highly effective security features that are covered in detail in this chapter. Deploy the security features appropriate to your needs.

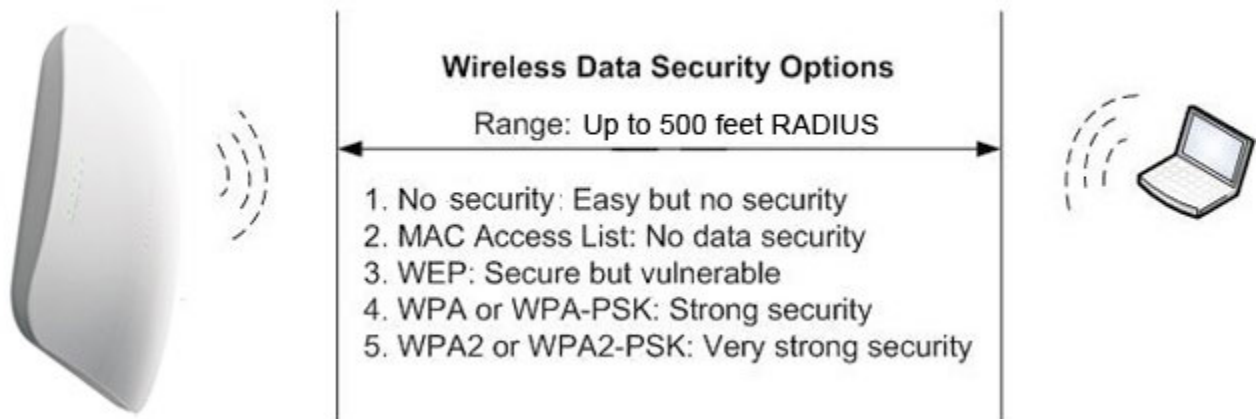


Figure 6. WiFi data security examples

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

- **Use multiple BSSIDs combined with VLANs.** You can configure combinations of VLANs and BSSIDs (security profiles) with stronger or less restrictive access security according to your requirements. For example, visitors could be given WiFi Internet access but be excluded from any access to your internal network. For information about how to configure BSSIDs, see [Configure and Enable WiFi Security Profiles](#) on page 39.
- **Restrict access based on MAC address.** You can allow only trusted devices to connect so that unknown devices cannot connect over the WiFi to the access point. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the WiFi link is fully exposed. For information about how to restrict access by MAC address, see [Manage MAC Address Filter Profiles in the Local MAC Address Database](#) on page 50.
- **Turn off the broadcast of the WiFi network name (SSID).** If you disable broadcast of the SSID, only devices with the correct SSID can connect. This nullifies the WiFi network discovery feature of some products, such as Windows XP, but the data is still exposed. For information about how to turn off broadcast of the SSID, see [Configure and Enable WiFi Security Profiles](#) on page 39.
- **WPA2-PSK (AES).** Wi-Fi Protected Access version 2 (WPA2) provides the most reliable security with Advanced Encryption Standard (AES) encryption. This very strong authentication along with dynamic per-frame rekeying of WPA2 makes it virtually impossible to compromise. You can also use a combination of Temporal Key Integrity Protocol (TKIP) and AES encryption. WPA2-PSK uses a pre-shared key (PSK) for authentication. For more information, see [Configure and Enable WiFi Security Profiles](#) on page 39 and [About WPA2-PSK and WPA-PSK & WPA2-PSK](#) on page 46.

- **WPA2 with RADIUS.** Wi-Fi Protected Access version 2 (WPA2) with a RADIUS server provides the most reliable security with Advanced Encryption Standard (AES) encryption. This very strong authentication along with dynamic per-frame rekeying of WPA2 makes it virtually impossible to compromise.
WPA2 uses RADIUS-based 802.1x authentication. For more information, see [Configure and Enable WiFi Security Profiles](#) on page 39. and [About WPA2 With RADIUS and WPA & WPA2 With RADIUS](#) on page 47
- **WPA-PSK & WPA2-PSK mixed mode.** This mode provides reliable security for both WPA-PSK and WPA2-PSK clients. Encryption is supported with the TKIP + AES mode.
WPA-PSK & WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see [Configure and Enable WiFi Security Profiles](#) on page 39 and [About WPA2-PSK and WPA-PSK & WPA2-PSK](#) on page 46.
- **WPA & WPA2 mixed mode with RADIUS.** This mode provides reliable security for both WPA and WPA2 clients and a RADIUS server. Encryption is supported with the TKIP + AES mode.
WPA & WPA2 uses RADIUS-based 802.1x authentication. For more information, see [Configure and Enable WiFi Security Profiles](#) on page 39 and [About WPA2 With RADIUS and WPA & WPA2 With RADIUS](#) on page 47.

WiFi Security Profiles

WiFi security profiles, simply referred to as security profiles, let you configure unique security settings for each SSID on each radio of the access point. For each radio, the access point supports up to 8 WiFi security profiles (BSSIDs). That means that you can configure 16 security profiles with custom settings (see [Configure and Enable WiFi Security Profiles](#) on page 39).

To set up a security profile, select its network authentication type, data encryption, WiFi client security separation, and VLAN ID:

- **Network authentication.** The access point is set by default as an open system with no authentication. When you configure network authentication, bear in mind that some legacy WiFi devices do not support WPA2. If your network includes computers with legacy WiFi devices, configure WPA & WPA2 mixed mode.
For information about the types of network authentication that the access point supports, see [Configure and Enable WiFi Security Profiles](#) on page 39.
- **Data encryption.** Select the data encryption that you want to use. The available options depend on the network authentication setting (otherwise, data encryption is disabled by default). The data encryption settings are explained in [Configure and Enable WiFi Security Profiles](#) on page 39.
- **WiFi client security separation.** If this feature is enabled, the associated WiFi clients (using the same SSID) are not able to communicate with each other. This feature is useful for hotspots and other public access situations. By default, WiFi client separation is disabled. For more information, see [Configure and Enable WiFi Security Profiles](#) on page 39.
- **VLAN ID.** If this feature is enabled and if the network devices (hubs and switches) on your LAN support the VLAN (802.1Q) standard, the default VLAN ID for the access point is associated with each profile. The default VLAN ID must match the IDs that are used by the other network devices. For more information, see [Configure and Enable WiFi Security Profiles](#) on page 39.

Some concepts and guidelines regarding the SSID are explained in the following list:

- A basic service set (BSS) is a group of WiFi stations and a single access point, all using the same security profile or service set identifier (BSSID). The actual identifier in the BSSID is the MAC address of the WiFi radio. (A WiFi radio can be assigned multiple MAC addresses, one for each security profile.)
- An extended service set (ESS) is a group of WiFi stations and multiple access points, all using the same identifier (ESSID).
- Different access points within an ESS can use different channels. To reduce interference, specify that adjacent access points use different channels.
- Roaming is the ability of WiFi stations to connect over WiFi when they physically move from one BSS to another one within the same ESS. The WiFi station automatically changes to the access point with the least interference or best performance.

Configure and Enable WiFi Security Profiles

The access point support 16 WiFi security profiles, 8 on each radio.

A WiFi security profile defines the following characteristics for an individual WiFi network:

- **Profile Definition.** Lets you specify the profile name, WiFi network name (SSID), whether the SSID is broadcast, band steering, RSSI threshold, MAC authentication, 802.11K radio resource management (RRM), and WiFi client separation of the WiFi network.
- **Wireless Scheduling.** Lets you specify an on and off schedule for broadcast of the WiFi network. (For information about on and off scheduling of a radio, which affects all WiFi networks on the radio, see [Schedule the WiFi Radios to Be Turned Off](#) on page 57.)
- **Authentication Settings.** Lets you specify the network authentication, data encryption, and VLAN ID of the WiFi network.
- **QoS Policies.** Lets you specify the QoS policy and bandwidth limit of the WiFi network.
- **Captive Portal.** Lets you assign a captive portal profile to the WiFi network.

To configure and enable a WiFi security profile, you must enable the associated radio:

- For 802.11bg/ng/bgn modes, the 2.4 GHz radio must be enabled (see [Configure 802.11bg/ng/bgn WiFi Settings](#) on page 24).
- For 802.11a/a-na-ac modes, the 5 GHz radio must be enabled. (see [Configure 802.11a/a-na-ac WiFi Settings](#) on page 27).

Both radios can function concurrently and both radios are enabled by default.

► To configure and enable a WiFi security profile:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.

Dual-Band Wireless AC Access Point WAC720 and WAC730 User Manual

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Configuration > Security > Profile Settings**.

The Profile Settings page for the 802.11bg/ng/bgn and 802.11a/a-na-ac modes shows eight WiFi security profiles for each mode. (If the 2.4 GHz radio is disabled, the Enable column is masked out.)

The screenshot shows the NETGEAR web interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The user is logged in as 'admin'. The navigation menu includes Configuration, Monitoring, Maintenance, and Support. The 'Security' tab is selected, showing 'Profile Settings' for two radio bands: 802.11bg/ng/bgn and 802.11a/a-na-ac. Each band has a table of eight security profiles. The first profile (NETGEAR) is always enabled. The other profiles have their 'Enable' checkboxes unchecked. The 'WMF-Enable' checkboxes are also unchecked.

#	Profile Name	SSID	Security	VLAN	Enable	WMF-Enable
0	NETGEAR	NETGEAR_11ng	Open System	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1	NETGEAR-1	NETGEAR_11ng-1	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
2	NETGEAR-2	NETGEAR_11ng-2	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
3	NETGEAR-3	NETGEAR_11ng-3	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
4	NETGEAR-4	NETGEAR_11ng-4	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
5	NETGEAR-5	NETGEAR_11ng-5	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
6	NETGEAR-6	NETGEAR_11ng-6	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
7	NETGEAR-7	NETGEAR_11ng-7	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>

#	Profile Name	SSID	Security	VLAN	Enable	WMF-Enable
0	NETGEAR	NETGEAR_11ac	Open System	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1	NETGEAR-1	NETGEAR_11ac-1	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
2	NETGEAR-2	NETGEAR_11ac-2	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
3	NETGEAR-3	NETGEAR_11ac-3	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
4	NETGEAR-4	NETGEAR_11ac-4	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
5	NETGEAR-5	NETGEAR_11ac-5	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
6	NETGEAR-6	NETGEAR_11ac-6	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
7	NETGEAR-7	NETGEAR_11ac-7	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>

The following table explains the fields of the Profile Settings page.

Setting	Description
Profile Name	The unique name of the security profile that makes it easy to recognize the profile.
SSID	The WiFi network name (SSID) for the security profile.
Security	The configured WiFi authentication method for the security profile.
VLAN	The default VLAN ID that is associated with the security profile.
Enable	The check box that specifies whether the security profile is enabled. If you select the check box and click the Apply button, the security profile is enabled. You cannot disable security profile #0 (NETGEAR) for either radio band. To disable this security profile, turn off the radio for the radio band (see Configure 802.11bg/ng/bgn WiFi Settings on page 24 and Configure 802.11a/a-na-ac WiFi Settings on page 27).
WMF-Enable	The check box that specifies whether Wireless Multicast Forwarding (WMF) is enabled. If you select the check box and click the Apply button, WMF is enabled. WMF is required for applications that use multicasting, such as VLC streaming applications. When WMF is enabled, the access point converts multicast traffic to unicast traffic. WMF improves the overall performance because the access points transmits data according to the capability of each WiFi client.

5. To configure a WiFi security profile, select the corresponding radio button to the left of the WiFi security profile.

Configure the WiFi Features and Security

6. Click the **Edit** button.

The Edit Security Profile page displays. This page contains five sections that are described in detail in the following steps:

- **Profile Definition.** See step 7.
- **Wireless Scheduling.** See step 8.
- **Authentication Settings.** See step 9.
- **QoS Policies.** See step 10.
- **Captive Portal.** See step 11.

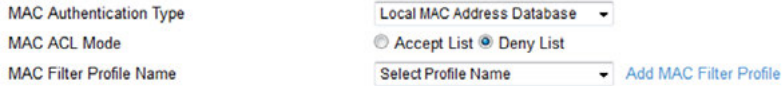
The screenshot shows the 'Edit Security Profile' configuration page for a NETGEAR WAC720 ProSAFE Dual Band Wireless AC Access Point. The page is divided into several sections:

- Profile Definition:** Includes fields for Profile Name (NETGEAR-1), Wireless Network Name (SSID) (NETGEAR_11ng-1), Broadcast Wireless Network Name (SSID) (Yes), Band Steering to 5GHz (Disable), Rssi Threshold 5GHz(-100 to -10) (-70), MAC Authentication Type (Disable), 802.11K(RRM) (checkbox), and Wireless Client Security Separation (Disable).
- Wireless Scheduling:** Includes a radio button for Wireless Scheduling (Disable).
- Authentication Settings:** Includes Network Authentication (Open System), Data Encryption (None), and VLAN ID (1).
- QoS Policies:** Includes a checkbox for Mode, and Apply Policy (Incoming and Outgoing) with Policy Details (None) and Bandwidth Limit (bits per second) (0).
- Captive Portal:** Includes a dropdown for Profile Name (None).

7. Specify the settings of the Profile Definition section as described in the following table.

Setting	Description
Profile Name	Enter a unique name of the security profile that makes it easy to recognize the profile. The default names are NETGEAR, NETGEAR-1, NETGEAR-2, and so on, through NETGEAR-7. You can enter a value of up to 32 alphanumeric characters.
Wireless Network Name (SSID)	The WiFi network name (SSID) for the security profile. The default names depend on the selected radio band: <ul style="list-style-type: none"> • 802.11 bg/ng/bgn. The default names are NETGEAR_11ng, NETGEAR_11ng-1, NETGEAR_11ng-2, and so on, through NETGEAR_11ng-7 for the eighth profile. • 802.11 a/a-na-ac. The default names are NETGEAR_11ac, NETGEAR_11ac-1, NETGEAR_11ac-2, and so on, through NETGEAR_11ac-7 for the eighth profile.

(Continued)

Setting	Description
Broadcast Wireless Network Name (SSID)	Select the Yes radio button to enable the access point to broadcast its SSID, allowing WiFi stations with a null (blank) SSID to adopt the access point's SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button.
Band Steering to 5GHz This setting does not apply to 802.11a/a-na-ac profiles.	Select the Enable radio button to enable band steering from the 2.4 GHz band to the 5 GHz band. Band steering can reduce the client density in the 2.4 GHz band by steering dual-band-capable clients to the 5 GHz band, thereby increasing the WiFi network capacity. By default, the Disable button is selected and band steering is disabled. If you enable band steering, you can set the RSSI threshold.
Rssi Threshold 5GHz (-100 to -10) This setting does not apply to 802.11a/a-na-ac profiles.	The received signal strength indicator (RSSI) threshold applies only if you enable band steering. Enter the minimum RSSI value that a dual-band-capable client must be able to receive from a 5 GHz radio before the client is steered from a 2.4 GHz radio to the 5 GHz radio. You can enter a value from -100 to -10. The default value is -70.
MAC Authentication Type	<p>By default, the selection from the MAC Authentication Type menu is Disable, and MAC address authentication is disabled. For you to enable MAC address authentication, you must either add a MAC address filter profile for local authentication (see <i>Manage MAC Address Filter Profiles in the Local MAC Address Database</i> on page 50) or specify the settings for a RADIUS server for remote authentication (see <i>Configure RADIUS Server Settings</i> on page 48).</p> <p>From the MAC Authentication Type menu, select one of the following options:</p> <ul style="list-style-type: none"> Local MAC Address Database. <div style="margin-left: 20px;">  <p>MAC Authentication Type: Local MAC Address Database</p> <p>MAC ACL Mode: <input type="radio"/> Accept List <input checked="" type="radio"/> Deny List</p> <p>MAC Filter Profile Name: Select Profile Name Add MAC Filter Profile</p> </div> <p>From the MAC Filter Profile Name menu, select the profile that you want to use and select one of the following MAC ACL Mode radio buttons:</p> <ul style="list-style-type: none"> - Accept List. All MAC address that are in the selected profile are allowed WiFi access and all MAC addresses that are not in the profile are denied WiFi access. - Deny List. All MAC address that are in the selected profile are denied WiFi access and all MAC addresses that are not in the profile are allowed WiFi access. (This is the default selection.) Remote MAC Address Database. The RADIUS server that you configured is used for MAC address authentication. <p>When you are configuring the access point from a WiFi computer whose MAC address is not in the MAC filter profile that you want to activate, you lose your WiFi connection when you click the Apply button. You then must access the access point from a wired computer or from a WiFi computer that is on the access control list to make any further changes.</p>

(Continued)

Setting	Description
802.11K (RRM)	Select the 802.11K(RRM) check box to allow the access point to support 802.11K radio resource management (RRM). 802.11K RRM allows for a better utilization of access points in a network. If some access points are underutilized because their signal is not as strong as that of other access points in the network and those other access points are used to their maximum capacity, 802.11K RRM can steer clients to the underutilized access points. By default, the 802.11K(RRM) check box is cleared and 802.11K RRM is disabled.
Wireless Client Security Separation	WiFi client separation is intended for hotspots and other public access situations. Make one of the following selections from the menu: <ul style="list-style-type: none"> Select the Enable radio button to enable WiFi client security separation. Clients that are connected to the WiFi network are prevented from communicating with each other. By default, the Disable button is selected and WiFi client security separation is disabled. Clients that are connected to the WiFi network are allowed to communicate with each other. This is the default selection.

8. To specify a schedule that allows the access point to turn broadcast of the WiFi network on and off, do the following:

a. Select the **Wireless Scheduling Enable** radio button.

Wireless Scheduling

The screenshot shows the 'Wireless Scheduling' configuration page. At the top, there are two radio buttons: 'Enable' (which is selected) and 'Disable'. Below this is a dropdown menu for 'Wireless Scheduling Type' currently set to 'Everyday'. At the bottom, there is a horizontal slider labeled 'Security Profile On & Off Time' with two circular markers. The left marker is positioned at 07:00 and the right marker is at 18:30.

The page expands to display scheduling options. By default, the **Disable** radio button is selected and the scheduling options do not display.

Note The Wireless Scheduling radio buttons are not shown for the NETGEAR_11ng and NETGEAR_11ac SSIDs because you cannot specify a WiFi schedule for these default WiFi networks. However, you can specify a WiFi schedule for a radio (see [Schedule the WiFi Radios to Be Turned Off](#) on page 57), which affects all WiFi networks on the radio, including the default WiFi network.

b. From the **Wireless Scheduling Type** menu, select one of the following options:

- Everyday.** The schedule applies every day of the week (Monday through Sunday). Set the start and end time for the schedule by moving the circles on the **Security Profile On & Off Time** bar. By default, this schedule enables the radio to be active from 7:00 a.m. to 6:30 p.m. (18:30).
- Weekdays.** The schedule applies every weekday of the week (that is, Monday through Friday). Set the start and end time for the schedule by moving the circles on the **Security Profile On**

& Off Time bar. By default, this schedule enables the radio to be active from 7:00 a.m. to 6:30 p.m. (18:30).

- **Weekend.** The schedule applies on the weekend only (Saturday and Sunday). Set the start and end time for the schedule by moving the circles on the **Security Profile On & Off Time** bar. By default, this schedule enables the radio to be active from 7:00 a.m. to 6:30 p.m. (18:30).
- **Custom.** This selection lets you define a schedule for each day of the week or selected days of the week by doing the following:
 1. Select the check boxes for the days for which you want to set and activate a schedule and clear the check boxes for the days for which you do not want to set and activate a schedule.
 2. For each active day, set the start and end time for the schedule by moving the circles on the bar that is associated with the individual day. By default, the schedule enables the radio to be active from 7:00 a.m. to 6:30 p.m. (18:30) on the individual day.

9. Specify the settings of the Authentication Settings section as described in the following table.

Note The access point is set by default as an open system with no authentication. However, we recommend that you configure security.

Setting	Description	
Network Authentication and Data Encryption The data encryption fields that display on the page depend on your selection from the Network Authentication menu.	Open System	This is the default setting. An open system does not provide any security or encryption.
	WPA2 with RADIUS	Configure the RADIUS server settings and select AES or TKIP + AES encryption. For more information, see the following sections: <ul style="list-style-type: none"> • About WPA2 With RADIUS and WPA & WPA2 With RADIUS on page 47 • Configure RADIUS Server Settings on page 48 Select this setting only if all clients support WPA2.
	WPA & WPA2 with RADIUS	Configure the RADIUS server setting. TKIP + AES encryption is the default encryption. For more information, see the following sections: <ul style="list-style-type: none"> • About WPA2 With RADIUS and WPA & WPA2 With RADIUS on page 47 • Configure RADIUS Server Settings on page 48 This setting allows clients to connect through either WPA with TKIP or WPA2 with AES.

(Continued)

Setting	Description	
Network Authentication and Data Encryption (continued)	WPA2-PSK	Enter a WPA passphrase and select AES or TKIP + AES encryption. For more information, see About WPA2-PSK and WPA-PSK & WPA2-PSK on page 46. Select this setting only if all clients support WPA2.
	WPA-PSK & WPA2-PSK	Enter a WPA passphrase. TKIP + AES encryption is the default encryption. For more information, see About WPA2-PSK and WPA-PSK & WPA2-PSK on page 46. This setting allows clients to connect through either WPA with TKIP or WPA2 with AES.
VLAN ID	Enter the VLAN ID to be associated with this security profile. The range for the VLAN ID is 1–4094. The default VLAN ID is 1. The VLAN ID must match the VLAN ID that is used by the other devices in your network.	

10. Specify the settings of the QoS Policy section as described in the following table.

Note To be able to select a QoS policy, you must first configure one or more policies (see [Configure and Manage Quality of Service Policies](#) on page 112).

Setting	Description
Mode	Select the Mode check box to enable the selection of QoS policies and bandwidth limits.
Policy Details	Select a QoS policy from the Incoming menu, Outgoing menu, or both menus. Depending on your selection, the policy is applied to incoming packets, outgoing packets, or both incoming and outgoing packets, and is displayed in the Policy Details fields.
Bandwidth Limit (bits per second)	As an option, specify the bandwidth limits in bits per second (bps) for incoming traffic, outgoing traffic, or both traffic streams. For example, to set a limit of 1 Mbps, enter 1048576 (or round down to 1000000).

11. To assign a captive portal profile to the WiFi security profile, select a captive portal instance from the **Profile Name** menu (**NETGEAR** or **NETGEAR-1**).

Note To be able to select a captive portal instance, you must configure and enable at least one captive portal instance and globally enable captive portals (see [Manage Captive Portals](#) on page 120).

12. Click the **Apply** button.
Your settings are saved.

13. Click the **Back** button.
The Profile Settings page displays again.
14. To enable the security profile that you just configured, make sure that the **Enable** check box for the profile is selected.
15. To enable Wireless Multicast Forwarding (WMF) for the security profile that you just configured, make sure that the **WMF-Enable** check box is enabled.



WARNING:

If you use a WiFi computer to configure WiFi security settings, you are disconnected when you click the **Apply** button. Reconfigure your WiFi computer to match the new settings, or access the access point from a wired computer to make further changes.

16. If you made any changes, click the **Apply** button again.
Your settings are saved.

About WPA2-PSK and WPA-PSK & WPA2-PSK

WPA2-PSK and WPA-PSK & WPA2-PSK authentication use a pre-shared key (PSK, also called a passphrase or a network key) and do not require authentication from a RADIUS server.

The selections that are available from the **Data Encryption** menu depend on the type of WPA-PSK authentication that you select from the **Network Authentication** menu and are shown in the following table.

Table 2. Security and encryption options for WPA2-PSK and WPA-PSK & WPA2-PSK

Setting	Descriptions	
Data Encryption	AES	Advanced Encryption Standard (AES) is the standard encryption method used with WPA2. Although some WiFi clients might support AES with WPA, the WAC720 and WAC730 access points do not support WPA with AES.
	TKIP + AES	TKIP + AES supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. For the WPA & WPA2 mixed mode, TKIP + AES is the only supported data encryption method.

Table 2. Security and encryption options for WPA2-PSK and WPA-PSK & WPA2-PSK (Continued)

Setting	Descriptions
Passphrase	Enter a passphrase. The passphrase length must be between 8 and 63 characters (inclusive). The default passphrase is sharedsecret. You can display the actual passphrase by selecting the Show Passphrase in Clear Text Yes radio button.
Show Passphrase in Clear Text	Select the Yes radio button to display the actual passphrase in the Passphrase field. The default setting is No.

About WPA2 With RADIUS and WPA & WPA2 With RADIUS

WPA2 and WPA & WPA2 security require RADIUS-based 802.1x authentication, so you also must define RADIUS server settings. For information about RADIUS servers, see [Configure RADIUS Server Settings](#) on page 48.

The selections that are available from the **Data Encryption** menu depend on the type of WPA authentication that you select from the **Network Authentication** menu and are shown in the following table.

Table 3. Encryption options for WPA with RADIUS and WPA & WPA2 with RADIUS

Setting	Descriptions
AES	Advanced Encryption Standard (AES) is the standard encryption method used with WPA2. Although some WiFi clients might support AES with WPA, the WAC720 and WAC730 access points do not support WPA with AES.
TKIP + AES	The TKIP + AES encryption method is supported both for WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. For the WPA & WPA2 mixed mode, TKIP + AES is the only supported data encryption method.

Change the QoS Policy for a WiFi Security Profile

► To change the QoS policy for a WiFi security profile:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Security > Profile Settings**.

The Profile Settings page displays.

5. Select the radio button the left of the security profile.
6. Click the **Edit** button.
The Edit Security Profile page displays.
7. From the menu from which you can select another QoS policy, select **None**.
8. Click the **Apply** button.
The old policy is removed from the security profile.
9. Select the new QoS policy from the same menu.
10. Click the **Apply** button.
Your settings are saved.

Configure RADIUS Server Settings

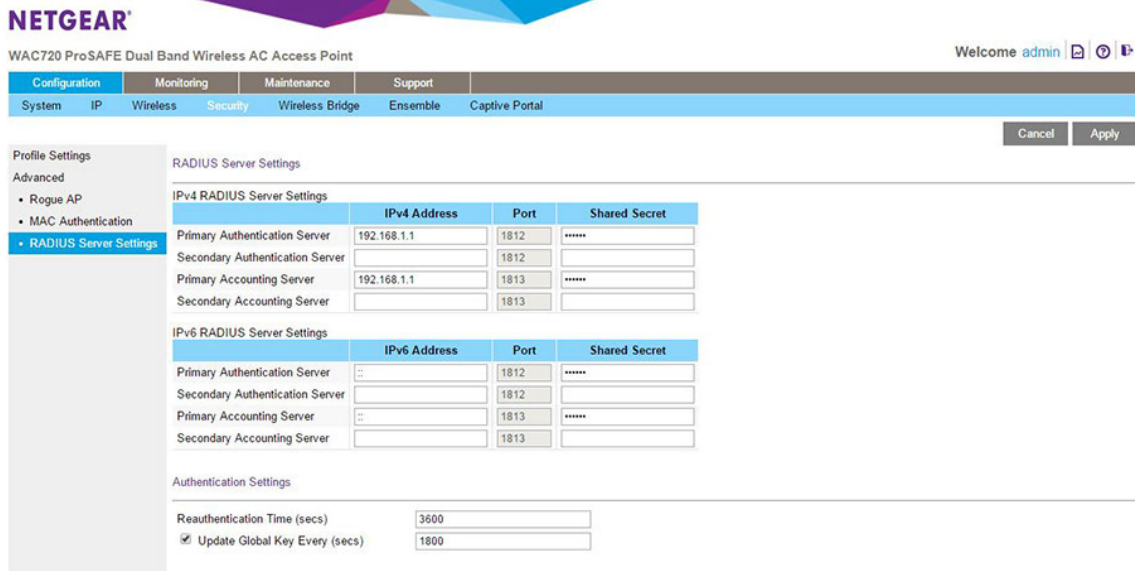
For authentication, accounting, or both authentication and accounting using RADIUS, you must configure primary servers and optional secondary servers. These RADIUS server settings can apply to all devices that are connected to the access point.

You can configure both IPv4 and IPv6 servers. In the IPv4 RADIUS Server Settings section, enter IPv4 addresses only. In the IPv6 RADIUS Server Settings section, enter IPv6 addresses only.

► To configure the RADIUS server settings:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Security > Advanced > RADIUS Server Settings**.

Dual-Band Wireless AC Access Point WAC720 and WAC730 User Manual



5. Specify the settings as described in the following table.

Setting	Descriptions	
RADIUS Server Settings		
Primary Authentication Server	IPv4 Address or IPv6 Address	Enter the IP address of the primary RADIUS server for authentication.
	Port	Enter the number of the UDP port on the access point that is used to access the primary RADIUS server for authentication. The default port number is 1812.
	Shared Secret	Enter the shared key that is used between the access point and the primary RADIUS server during authentication.
Secondary Authentication Server	IPv4 Address or IPv6 Address	Enter the IP address of the secondary RADIUS server for authentication. The secondary RADIUS server is used when the primary RADIUS server is not available.
	Port	Enter the number of the UDP port on the access point that is used to access the secondary RADIUS server for authentication. The default port number is 1812.
	Shared Secret	Enter the shared key that is used between the access point and the secondary RADIUS server during authentication.
Primary Accounting Server	IPv4 Address or IPv6 Address	Enter the IP address of the primary RADIUS server for accounting.
	Port	Enter the number of the UDP port on the access point that is used to access the primary RADIUS server for accounting. The default port number is 1813.
	Shared Secret	Enter the shared key that is used between the access point and the primary RADIUS server during the accounting process.

(Continued)

Setting	Descriptions	
Secondary Accounting Server	IPv4 Address or IPv6 Address	Enter the IP address of the secondary RADIUS server for accounting. The secondary RADIUS server is used when the primary RADIUS server is not available.
	Port	Enter the number of the UDP port on the access point that is used to access the secondary RADIUS server for accounting. The default port number is 1813.
	Shared Secret	Enter the shared key that is used between the access point and the secondary RADIUS server during the accounting process.
Authentication Settings		
Reauthentication Time (secs)	The interval in seconds after which the supplicant is reauthenticated with the RADIUS server. The default interval is 3600 seconds (1 hour). Enter 0 to disable reauthentication.	
Update Global Key Every (secs)	Select the check box to allow the global key update, and enter the interval in seconds. The check box is selected by default, and the default interval is 1800 seconds (30 minutes). Clear the check box to prevent the global key update.	

6. Click the **Apply** button.

Your settings are saved.

For information about assigning the configured RADIUS server to a WiFi security profile for MAC address authentication, see step 7 in *Configure and Enable WiFi Security Profiles* on page 39.

Manage MAC Address Filter Profiles in the Local MAC Address Database

For increased security, you can restrict access to an SSID by allowing access to only specific computers or WiFi stations based on their MAC addresses. You can restrict access to only trusted computers so that unknown computers cannot connect over WiFi to the access point. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the WiFi link is fully exposed if you do not also implement WiFi security.

Before you can implement MAC address filtering, you must add one or more MAC address filter profiles (which is described in this section) and then assign the profile to a WiFi security profile (see *Configure and Enable WiFi Security Profiles* on page 39). You can assign the same MAC address filter profile to multiple WiFi security profiles, or you can set up different MAC address filter profiles for different WiFi security profiles.

You can manually add MAC addresses to the MAC address filter profile and you can import a list of trusted MAC addresses. The file that you import must satisfy the following requirements:

- The file must be a plain-text file with a .txt or .cfg extension.
- Entries in the file must be MAC addresses in hexadecimal format with each octet separated by colons, for example 00:11:22:33:44:55.
- Entries must be separated with a single space.
- The file must contain only MAC addresses, no other information.

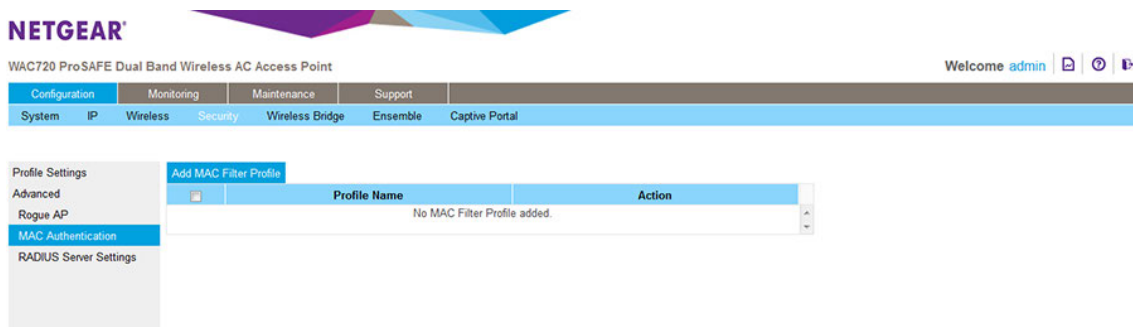
Note You cannot add multicast or broadcast MAC addresses to a MAC address filter profile.

For all MAC address filter profiles together, the access point can support a maximum number of 512 MAC addresses. For example, you can set up two MAC address filter profiles with 256 MAC addresses each, or you can set up 16 MAC address filter profiles with 32 MAC addresses each, provided that the total number of MAC addresses for all profiles together does not exceed 512.

Add a MAC Address Filter Profile

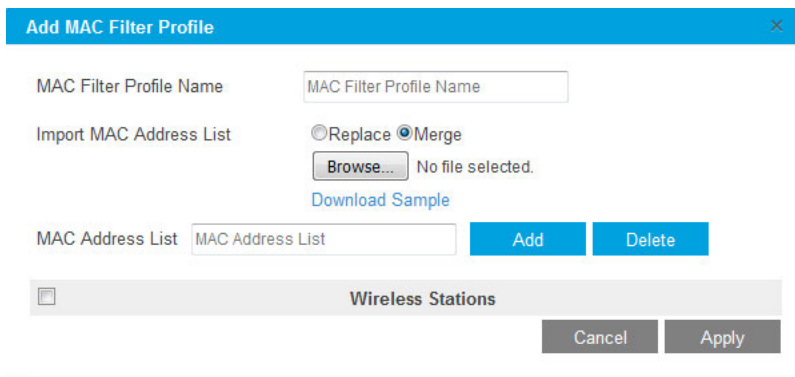
► To add a MAC address filter profile:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Security > Advanced > MAC Authentication**.



By default, no MAC filter profile exists.

5. Click the **Add MAC Filter Profile** button above the table.



6. In the **MAC Filter Profile Name** field, enter a name for the new profile.
This name identifies the profile and lets you assign it later to a WiFi security profile.
7. Populate the Wireless Stations table by one of the following methods or by a combination of the following methods:
 - Enter MAC addresses manually by doing the following:
 - a. Enter a MAC address in the **MAC Address List** field.
 - b. Click the **Add** button.
 - Import a list of trusted MAC addresses by doing the following:
 - a. Select the **Replace** radio button or **Merge** radio button.
The imported list either replaces the MAC addresses in the Wireless Stations table or merges with the MAC addresses in the Wireless Stations table.
 - b. Click the **Browse** button and navigate to and select the file with MAC addresses.

The file that you import must be a plain-text file with a .txt or .cfg extension. Entries in the file must be MAC addresses in hexadecimal format with each octet separated by colons, for example 00:11:22:33:44:55. Separate entries with a single space. For the file to be accepted, it must contain only MAC addresses.

Note To download a sample file, click the **Download Sample** link.

8. To fine-tune the Wireless Stations table and delete one or more MAC addresses from the Wireless Stations table, select individual check boxes for the MAC addresses and click the **Delete** button.
9. Click the **Apply** button.
Your settings are saved. The Add MAC Filter Profile pop-up window closes.

For information about assigning the MAC address filter profile to a WiFi security profile, see Step 7 in *Configure and Enable WiFi Security Profiles* on page 39.

Modify a MAC Address Filter Profile

► To modify an existing MAC address filter profile:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see *Log In to the Access Point* on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

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

The page that displays shows a table with MAC address filter profiles.

5. If more than one profile exists, select the check box for the profile that you want to modify.

6. Click the **Edit** button.

The Edit MAC Filter Profile pop-up window opens.

7. Modify the MAC address filter profile.

For more information, see [Add a MAC Address Filter Profile](#) on page 51.

8. Click the **Apply** button.

Your settings are saved. The Add MAC Filter Profile pop-up window closes.

Delete a MAC Address Filter Profile

► **To delete an existing MAC address filter profile:**

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.

For more information, see [Log In to the Access Point](#) on page 16.

2. In the address bar, enter the IP address of the access point.

A login window opens.

3. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

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

The MAC Authentication page displays and shows a table with MAC address filter profiles.

5. Select the check box for the profile that you want to delete.

You can select more than one check box and delete several profiles.

6. Click the **Delete Profile** button.

The profile or profiles are deleted.

Enable Rogue AP Detection and Monitor Rogue APs

Unidentified access points (APs) that use the SSID of a legitimate network can present a serious security threat. Detecting rogue access points involves scanning the WiFi environment on all available channels, looking for unidentified access points.

When rogue AP detection is enabled, the access point interacts only with devices in the Known AP list.

Enable Rogue AP Detection

When you enable rogue AP detection, the access point interacts only with devices in the Known AP list.

► To enable rogue AP detection:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Security > Advanced > Rogue AP**.

You can configure AP detection for 802.11 bg/ng/bgn devices, 802.11 a/a-na-ac devices, or both types of devices.

5. Select the **Turn Rogue AP Detection On** check box.
6. Select a detection policy from the **Rogue AP Detection Policy** menu:
 - **Mild**. The AP scans for unknown APs every 180 seconds.
 - **Moderate**. The AP scans for unknown APs every 60 seconds.
 - **Aggressive**. The AP scans for unknown APs every 10 seconds.

Detected rogue APs are placed in the Unknown AP List.

7. To move APs from the Unknown AP List to the Known AP List, do the following:
 - a. Select individual check boxes for MAC addresses, or select all MAC addresses by selecting the check box in the heading.
 - b. Click the **Move** button to transfer the MAC addresses from the Unknown AP List to the Known AP List.

8. To import a list of known APs, do the following:
 - a. Click the **Replace** or **Merge** button.
The imported list either replaces the Known AP List or merges with the Known AP List.
 - b. Click the **Choose File** button and navigate to and select the file with access points.

The file that you import must be a plain-text file with a .txt or .cfg extension. Entries in the file must be MAC addresses in hexadecimal format with each octet separated by colons, for example 00:11:22:33:44:55. Separate entries with a single space. For the file to be accepted, it must contain only MAC addresses.

9. To fine-tune the Known AP List and delete one or more MAC address from the Known AP List, select individual check boxes for the MAC addresses and click the **Delete** button.
10. Click the **Apply** button.
Your settings are saved.

Monitor Rogue APs

You can view a table with rogue access points that were detected. The table also provides detailed information about the rogue access points.

► To monitor rogue APs:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Monitoring > Rogue AP > Unknown AP List**.

The Unknown AP List shows information for each unknown device, including information about beacons.

5. To update the list, click the **Refresh** button.
6. To save the list as a text file, click the **Save** button and follow the instructions of your browser to save the file to your computer.

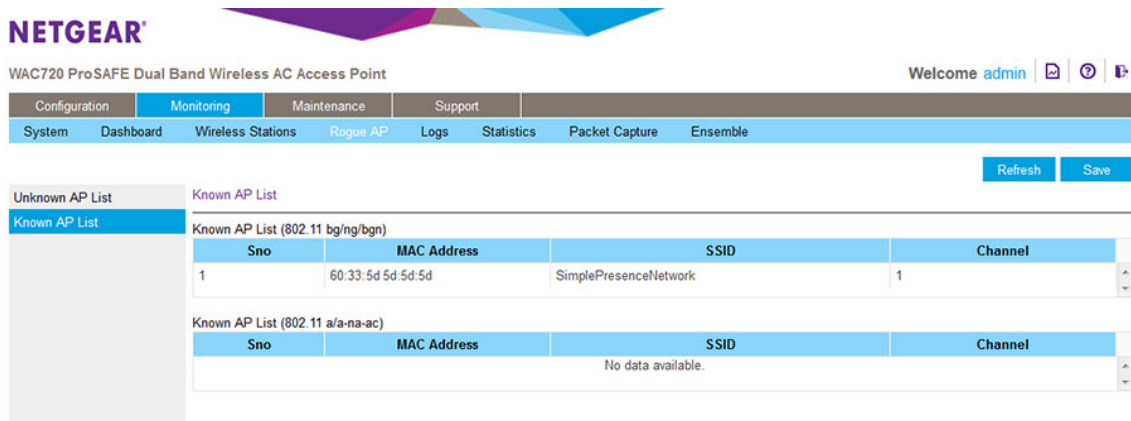
Monitor Known APs

You can view a table with known access points. The table also provides information about the known access points.

► To monitor known APs:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Monitoring > Rogue AP > Known AP List**.



The Known AP List shows information for each known device.

5. To update the list, click the **Refresh** button.
6. To save the list as a text file, click the **Save** button and follow the instructions of your browser to save the file to your computer.

Schedule the WiFi Radios to Be Turned Off

Scheduling the WiFi radios to be turned off is a green feature that allows you to turn off the WiFi radios during scheduled vacations, office shutdowns, on evenings, or on weekends.

The schedule applies to all WiFi networks that broadcast on a radio. For information about scheduling the broadcast of an individual WiFi network, see step 8 in *Configure and Enable WiFi Security Profiles* on page 39.

► To schedule the radios to be turned on and off:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see *Log In to the Access Point* on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Configuration > Wireless > Basic > Wireless Scheduling**.

The screenshot shows the NETGEAR configuration interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The user is logged in as 'admin'. The navigation menu includes Configuration, Monitoring, Maintenance, and Support. The 'Configuration' menu is expanded to show System, IP, Wireless, Security, Wireless Bridge, Ensemble, and Captive Portal. The 'Wireless' menu is selected, and the 'Basic' sub-menu is active. The 'Wireless Scheduling' page is displayed, showing the 'Wireless Scheduling - 802.11 bg/ng/bgn' section. The 'Wireless Scheduling' radio button is selected, and the 'Wireless Scheduling Type' is set to 'Custom'. The schedule is configured for every day of the week (Monday through Sunday) from 07:00 to 18:30. The 'Wireless Scheduling' radio button for 802.11 a/a-na-ac devices is currently disabled.

The previous show the page for a custom scheduling type. However, by default, the page for the Everyday scheduling type displays.

You can a schedule for 802.11 bg/ng/bgn devices, 802.11 a/a-na-ac devices, or both types of devices.

5. Select the **Wireless Scheduling Enable** radio button.

By default, the **Disable** radio button is selected.

6. From the Wireless Scheduling Type menu, select one of the following options:

- **Everyday.** The schedule applies every day of the week (Monday through Sunday). Set the start and end time for the schedule by moving the circles on the **Radio On & Off Time** bar. By default, this schedule enables the radio to be active from 7:00 a.m. to 6:30 p.m. (18:30).
- **Weekdays.** The schedule applies every weekday of the week (that is, Monday through Friday). Set the start and end time for the schedule by moving the circles on the **Radio On & Off Time** bar. By default, this schedule enables the radio to be active from 7:00 a.m. to 6:30 p.m. (18:30).
- **Weekend.** The schedule applies on the weekend only (Saturday and Sunday). Set the start and end time for the schedule by moving the circles on the **Radio On & Off Time** bar. By default, this schedule enables the radio to be active from 7:00 a.m. to 6:30 p.m. (18:30).
- **Custom.** This selection lets you define a schedule for each day of the week or selected days of the week by doing the following:

- a. Select the check boxes for the days for which you want to set and activate a schedule and clear the check boxes for the days for which you do not want to set and activate a schedule.
 - b. For each active day, set the start and end time for the schedule by moving the circles on the bar that is associated with the individual day. By default, the schedule enables the radio to be active from 7:00 a.m. to 6:30 p.m. (18:30) on the individual day.
7. Click the **Apply** button.
Your settings are saved.
The schedule is active and WiFi broadcast occurs according to the schedule that you defined.

Configure Basic WiFi Quality of Service

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

By enabling WMM, you allow Quality of Service (QoS) control for upstream traffic flowing from a WiFi station to the access point and for downstream traffic flowing from the access point to a WiFi station.

WMM defines the following four queues in decreasing order of priority:

- **Voice.** The highest priority queue with minimum delay, which makes it ideal for applications like VoIP and streaming media.
- **Video.** The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue.
- **Best Effort.** The medium priority queue with medium delay is given to this queue. Most standard IP applications use this queue.
- **Background.** Low priority queue with high throughput. Applications, such as FTP, that are not time-sensitive but require high throughput can use this queue.

The WMM Powersave feature saves power for battery-powered equipment by increasing the efficiency and flexibility of data transmission.

Note For information about how to configure advanced WiFi QoS, that is, to configure specific Enhanced Distributed Channel Access (EDCA) settings, see [Configure Advanced Quality of Service Settings](#) on page 109.

► To configure basic WiFi QoS:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.

3. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

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

The screenshot shows the NETGEAR configuration interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The user is logged in as 'admin'. The navigation menu includes Configuration, Monitoring, Maintenance, and Support. Under Configuration, there are sub-menus for System, IP, Wireless, Security, Wireless Bridge, Ensemble, and Captive Portal. The 'Basic' settings section is expanded, showing 'Wireless Settings', 'Wireless Scheduling', and 'QoS Settings'. The 'QoS Settings' page is displayed, showing options for 'Mode' (Enable/Disable), 'QoS Settings - 802.11 bg/ng/bgn', and 'QoS Settings - 802.11 a/a-na-ac'. Each of these sections has 'Enable Wi-Fi Multimedia (WMM)' and 'WMM Powersave' options, each with 'Enable' and 'Disable' radio buttons. The 'Apply' button is visible at the bottom right.

5. To turn on QoS globally, select the **Mode Enable** button.
6. Enable or disable individual WMM features for 802.11 bg/ng/bgn devices, 802.11 a/a-na-ac devices, or both types of devices:
 - **Enable Wi-Fi Multimedia (WMM)**. To enable this feature, select the Enable radio button, which is the default setting. Select the Disable radio button to disable the feature.
 - **WMM Powersave**. To enable this feature, select the Enable radio button, which is the default setting. Select the Disable radio button to disable the feature.
7. Click the **Apply** button.
Your settings are saved.

Manage and Monitor the Access Point

4

This chapter describes how to use the management and monitoring features of the access point.

The chapter includes the following sections:

- *Enable Remote Management*
- *Upgrade the Access Point Firmware*
- *Manage the Configuration File or Reset to Factory Defaults*
- *Change the Administrator Password*
- *Manage User Accounts*
- *Enable the Syslog Server*
- *Monitor the Access Point*
- *View the Activity Logs*
- *View the Traffic Statistics*
- *Set Up, Manage, and Monitor Ensembles*

Enable Remote Management

Both Simple Network Management Protocol (SNMP) and the remote console Secure Shell (SSH) are enabled by default, which allows for remote management of the access point from a client running SNMP management software, as well as from an SSH client. The Telnet console is disabled by default.

The following sections describe the remote management options:

- [SNMP Management](#) on page 62
- [Secure Shell and Telnet Management](#) on page 63

SNMP Management

► To set up an SNMP management interface:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Maintenance > Remote Management > SNMP**.

The screenshot shows the Netgear web interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The user is logged in as 'admin'. The navigation menu includes Configuration, Monitoring, Maintenance, and Support. Under Maintenance, there are sub-menus for Password, Reset, Remote Management, Upgrade, and Ensemble Upgrade. The 'Remote Management' sub-menu is selected, and the 'SNMP' configuration page is displayed. The 'SNMP' section has an 'Enable' radio button selected and a 'Disable' radio button. Below this are input fields for 'Read-Only Community Name' (public), 'Read-Write Community Name' (private), 'Trap Community Name' (NETGEAR), 'IP Address to Receive Traps' (empty), and 'Trap Port' (162). There are 'Cancel' and 'Apply' buttons at the bottom right of the form.

Specify the settings as described in the following table.

Setting	Description
SNMP	Select the Enable radio button to allow the SNMP network management software, such as HP OpenView, to manage the access point through SNMPv1/v2 protocol. By default, the Disable radio button is selected.
Read-Only Community Name	Enter the community string to allow the SNMP manager to read the access point's Management Information Base (MIB) objects. The default is public.
Read-Write Community Name	Enter the community string to allow the SNMP manager to read and write the access point's MIB objects. The default is private.

(Continued)

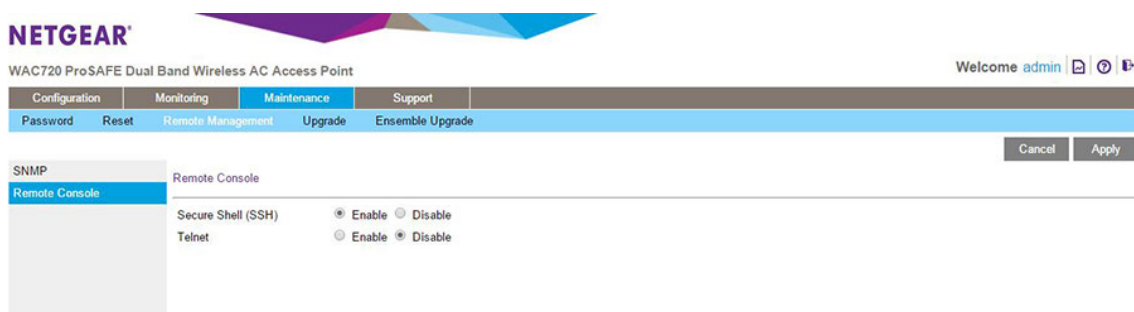
Setting	Description
Trap Community Name	Enter the community string to allow the SNMP manager to send traps. The default is trap.
IP Address to Receive Traps	Enter the IP address of the SNMP manager to receive traps sent from the access point.
Trap Port	Enter the number of the SNMP manager port to receive traps sent from the access point. The default is 162.

- Click the **Apply** button.
Your settings are saved.

Secure Shell and Telnet Management

► To configure remote console features:

- Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
- In the address bar, enter the IP address of the access point.
A login window opens.
- Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
- Select **Maintenance > Remote Management > Remote Console**.



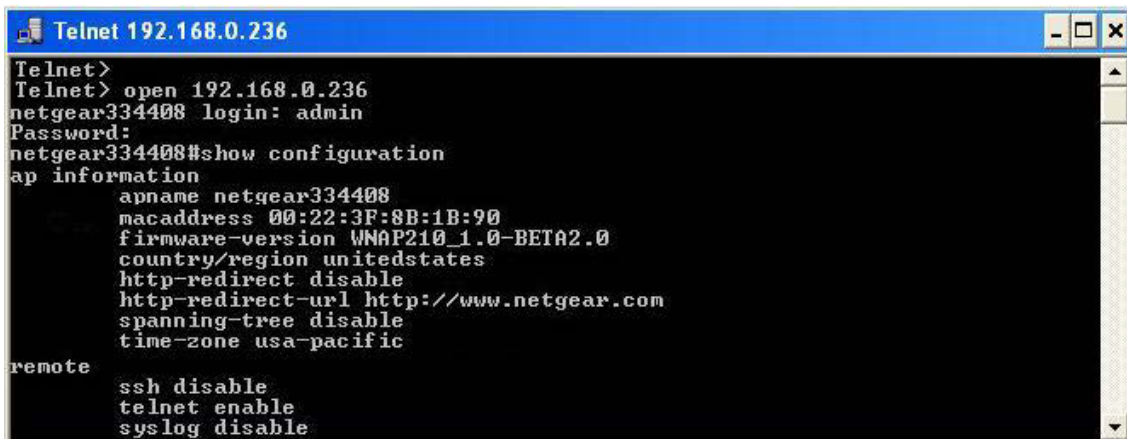
- Enable or disable the remote console features:

- **Secure Shell (SSH).** To enable this feature, select the Enable radio button, which is the default setting. Select the Disable button to disable the feature.
 - **Telnet.** To enable this feature, select the Enable radio button. Select the Disable button to disable the feature, which is the default setting.
6. Click the **Apply** button.
Your settings are saved.

Manage the Access Point over a Telnet Connection

► To manage the access point over a Telnet connection:

1. Connect an Ethernet cable to the console port of the access point.
2. Connect the other end of the cable to a VT100/ANSI terminal or a computer.
If you attach a computer that is running a Windows, Apple, or Linux operating system, start a secure terminal emulation program, and configure the terminal emulation program to use the following settings:
 - **Baud rate.** 9600 bps
 - **Data bits.** 8
 - **Parity.** None
 - **Stop bit.** 1
 - **Flow control.** None
3. Start a secure Telnet session from the terminal or workstation to the access point. A page similar to the following displays:



```
Telnet 192.168.0.236
Telnet>
Telnet> open 192.168.0.236
netgear334408 login: admin
Password:
netgear334408#show configuration
ap information
  apname netgear334408
  macaddress 00:22:3F:8B:1B:90
  firmware-version WNAP210_1.0-BETA2.0
  country/region unitedstates
  http-redirect disable
  http-redirect-url http://www.netgear.com
  spanning-tree disable
  time-zone usa-pacific
remote
  ssh disable
  telnet enable
  syslog disable
```

4. Enter the login name and password.
The default login name is **admin** and the default password is **password**.
After successful login, the > prompt appears, preceded by the name of the access point. In this example, the prompt is **netgear334408**.
5. Enter the CLI commands that you want to use.

You can enter show configuration to display the available CLI commands.

Note You can also access the access point remotely over a Telnet or SSH session using an application such as PuTTY, if such an encryption application is allowed by law in your country. After you connect to the access point, enter the login name and password to access the CLI.

Upgrade the Access Point Firmware

The firmware of the access point is stored in flash memory and can be upgraded as NETGEAR releases new firmware. You can download upgrade files from the NETGEAR website. You can send the upgrade file using your browser. Two methods are available to perform a firmware upgrade, which are described in the following sections:

- *Upgrade the Firmware Over a Web Browser* on page 65
- *Upgrade the Firmware Over a TFTP Server* on page 66

Note The web browser that you use to upload new firmware into the access point must support HTTP uploads. Use a browser such as Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome.



WARNING:

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

IMPORTANT:

In some cases, such as a major upgrade, you might need to erase the configuration and manually reconfigure your access point after upgrading it. See the release notes included with the firmware to find out if you must reconfigure the access point.

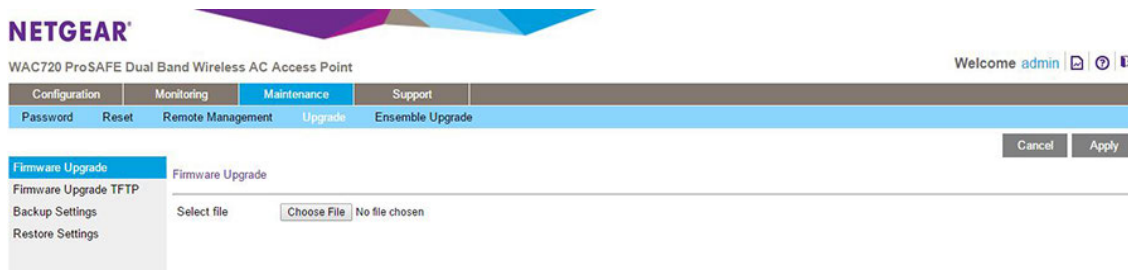
Upgrade the Firmware Over a Web Browser

► To use a web browser to upgrade the access point firmware:

1. Download the new firmware file from the NETGEAR website at downloadcenter.netgear.com and save it to your computer.
2. If available, read the release notes before upgrading the firmware.
3. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.

For more information, see [Log In to the Access Point](#) on page 16.

- In the address bar, enter the IP address of the access point.
A login window opens.
- Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
- Select **Maintenance > Upgrade > Firmware Upgrade**.



- Click the **Choose File** button and locate and select the firmware upgrade file.
The firmware upgrade file is a .tar file.
- Click the **Apply** button to initiate the upgrade process.
During the upgrade process, the access point automatically restarts. The upgrade process typically takes several minutes. When the Test LED turns off, wait a few more seconds before doing anything with the access point.
- Verify that the new firmware file was installed by selecting **Monitoring > System**.
The System page displays. The firmware version is shown in the Access Point Information section of the page.

Upgrade the Firmware Over a TFTP Server

To use this method, you need access to a TFTP server.

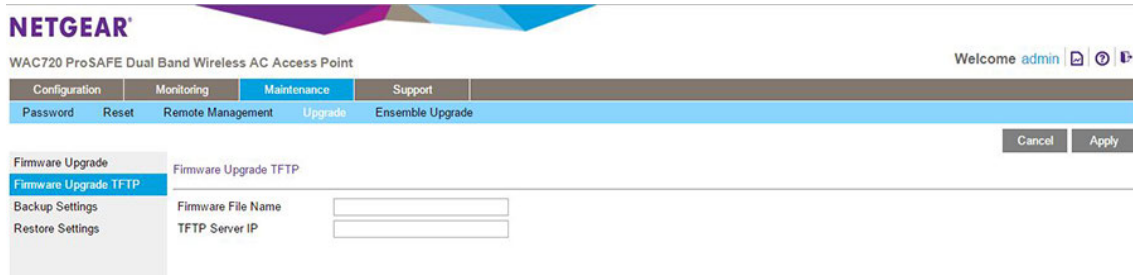
► To use a TFTP server to upgrade the access point firmware:

- Download the new firmware file from the NETGEAR website at downloadcenter.netgear.com and save it to your computer.
- Transfer the firmware file to your TFTP server.
- If available, read the release notes before upgrading the firmware.
- Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
- In the address bar, enter the IP address of the access point.
A login window opens.

6. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

7. Select **Maintenance > Upgrade > Firmware Upgrade TFTP**.



8. Specify the following information:

- **Firmware File Name.** The name of the firmware file.
- **TFTP Server IP.** The IP address of your TFTP server.

9. Click the **Apply** button to initiate the upgrade process.

During the upgrade process, the access point automatically restarts. The upgrade process typically takes several minutes. When the Test LED turns off, wait a few more seconds before doing anything with the access point.

10. Verify that the new firmware file was installed by selecting **Monitoring > System**.

The System page displays. The firmware version is shown in the Access Point Information section of the page.

Manage the Configuration File or Reset to Factory Defaults

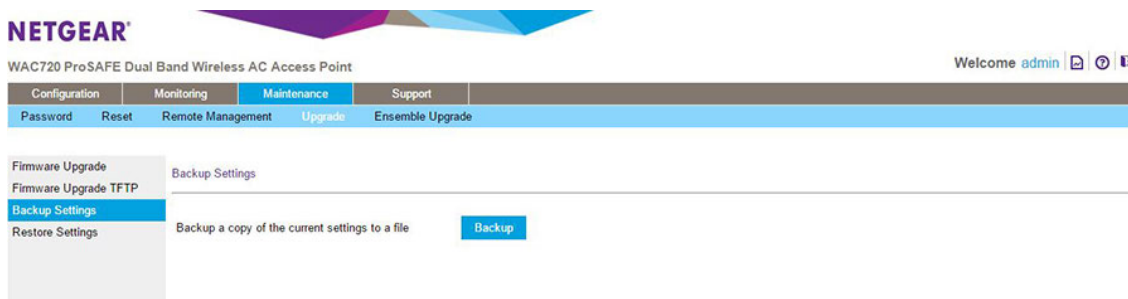
The access point settings are stored in the configuration file. You can save this file (back it up) to a computer, restore it from a computer, or reset it to factory default settings, as described in the following sections:

- *Save the Configuration* on page 68
- *Restore the Configuration* on page 68
- *Restore the Access Point to the Factory Default Settings* on page 69
- *Reboot the Access Point Without Restoring the Default Configuration* on page 71

Save the Configuration

► To save your settings:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Maintenance > Upgrade > Backup Settings**.

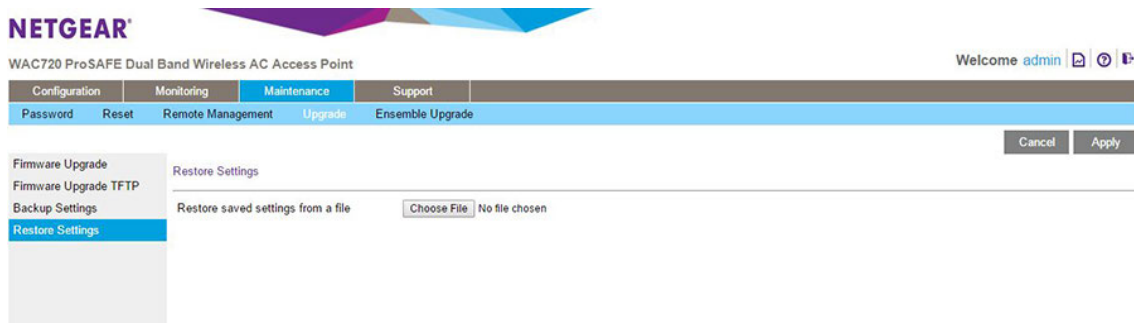


5. Click the **Backup** button.
Your browser extracts the configuration file (the file name is config) from the access point and prompts you for a location on your computer to store the file.
6. Follow the instructions of your browser to save the file.

Restore the Configuration

► To restore your settings from a saved configuration file:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Maintenance > Upgrade > Restore Settings**.



5. Click the **Choose File** button and locate and select the backup configuration file (the file name is config).

IMPORTANT:

During the restoration process, do not try to go online, turn off the access point, shut down the computer, or do anything else to the access point until it finishes restarting!

6. Click the **Apply** button to initiate the restoration process.
During the restoration process, the access point automatically restarts. The restoration process typically takes about one minute. When the Test LED turns off, wait a few more seconds before doing anything with the access point.

Restore the Access Point to the Factory Default Settings

You can restore the access point to the factory default settings by two methods that are described in the following sections:

- *Use the Local Browser Interface to Restore Factory Default Settings* on page 70
- *Use the Reset Button to Restore Factory Default Settings* on page 70

Note After you restore the factory default settings on the access point, the following occurs:

- All custom configurations are lost.
 - The login password is **password**.
 - The default LAN IP address is 192.168.0.100.
 - The DHCP client is enabled.
 - Business Central mode is enabled.
 - The name in the **Access Point Name** field is reset to the name that is printed on the access point label.
-

Use the Local Browser Interface to Restore Factory Default Settings

► To restore the factory default settings using the local browser interface:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Maintenance > Reset > Restore Defaults**.



5. Select the **Yes** radio button.
By default, the **No** radio button is selected.

IMPORTANT:

During the restoration process, do not try to go online, turn off the access point, shut down the computer, or do anything else to the access point until it finishes restarting!

6. Click the **Apply** button.
The access point is reset to the factory default settings.

During the restoration process, the access point automatically restarts. The restoration process typically takes about one minute. When the Test LED turns off, wait a few more seconds before doing anything with the access point.

After the restoration process is complete, Business Central mode is enabled on the access point. For information about disabling Business Central mode so that the access point can function in standalone mode, see [Disable Business Central Mode for a Standalone Access Point](#) on page 19.

Use the Reset Button to Restore Factory Default Settings

To restore the factory default settings when you do not know the login user name, login password, or IP address, you must use the **Reset** button on the rear panel of the access point (see [Rear Panel](#) on page 10).

► To restore the factory default settings using the Reset button:

1. Using a sharp object, press and hold the Reset button for about five seconds (until the Test LED blinks rapidly) to reset the access point to factory defaults settings.

Pressing the **Reset** button for a shorter time simply causes the access point to reboot.

2. Release the **Reset** button.

During the restoration process, the access point automatically restarts. The restoration process typically takes about one minute. When the Test LED turns off, wait a few more seconds before doing anything with the access point.

After the restoration process is complete, Business Central mode is enabled on the access point. For information about disabling Business Central mode so that the access point can function in standalone mode, see [Disable Business Central Mode for a Standalone Access Point](#) on page 19.

Reboot the Access Point Without Restoring the Default Configuration

If you cannot physically access the access point to turn it off and on again, you can use the local browser interface to reboot the access point.

► To reboot the access point:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.

For more information, see [Log In to the Access Point](#) on page 16.

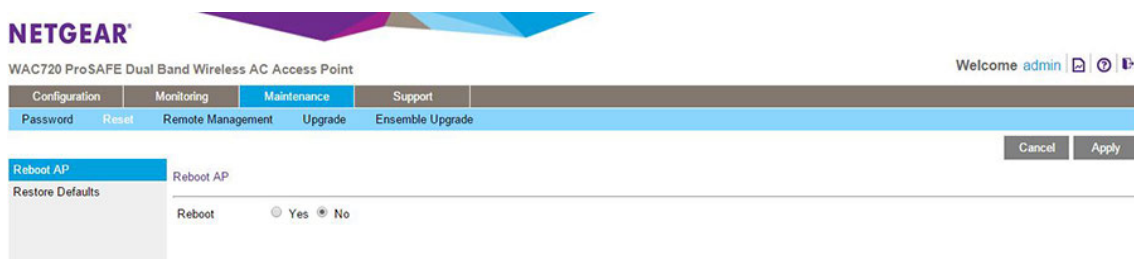
2. In the address bar, enter the IP address of the access point.

A login window opens.

3. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Maintenance > Reset > Reboot AP**.



5. Select the **Yes** radio button.

By default, the **No** radio button is selected.

6. Click the **Apply** button to reboot the access point.

The reboot process typically takes about one minute. When the Test LED turns off, wait a few more seconds before doing anything with the access point.

Change the Administrator Password

The default password is **password**. We recommend that you change this password to a more secure password. You cannot change the administrator login name (admin).

The ideal password contains no dictionary words from any language and is a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

► To change the administrator password:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Maintenance > Password > Change Password**.

The screenshot shows the Netgear web interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The user is logged in as 'admin'. The navigation menu includes Configuration, Monitoring, Maintenance (selected), and Support. Under Maintenance, there are links for Password, Reset, Remote Management, Upgrade, and Ensemble Upgrade. The 'Change Password' page is active, featuring a sidebar with 'Change Password' selected. The main content area contains the following fields and options:

- Current Password: [Text Input Field]
- New Password: [Text Input Field]
- Repeat New Password: [Text Input Field]
- Restore Default Password: Yes No

Buttons for 'Cancel' and 'Apply' are located at the top right of the form area.

5. Take one of the following actions:
 - Enter a new password twice, once in the **New Password** field and again in the **Repeat New Password** field.
 - To restore the default password, select the Restore Default Password **Yes** radio button.

By default, the **No** radio button is selected.

6. Click the **Apply** button.
Your settings are saved.

If you restored the default password, the login password is **password**. If you configured a new password, write it down in a secure place.

Manage User Accounts

The admin user account is the default user account, which you cannot delete. However, you can add other user accounts, modify them, and delete them. Users for whom you set up an account can access the local browser interface with read-only or read/write privileges.

Note Only the administrator can create, change, and delete user accounts.

Add a New User Account

► To add a new user account:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > Advanced > User Accounts**.

The screenshot shows the Netgear web interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The page title is "NETGEAR WAC720 ProSAFE Dual Band Wireless AC Access Point" and the user is logged in as "admin". The navigation menu includes Configuration, Monitoring, Maintenance, and Support. The Configuration menu is expanded to show System, IP, Wireless, Security, Wireless Bridge, Ensemble, and Captive Portal. The "User Accounts" page is displayed, featuring a sidebar with "Basic" and "Advanced" sections. Under "Advanced", "User Accounts" is selected. The main content area is divided into "Add User Accounts" and "Update User Accounts".

Add User Accounts

User Name:

Password:

Privilege:

Update User Accounts

Existing Users:

User Name:

Password:

Privilege:

5. Configure the settings in the upper part of the page as described in the following table.

Setting	Description
User Name	Enter a new user name.
Password	Enter a password between 4 and 12 characters in length.
Privilege	From the Privilege menu, select Read Write or Read Only .

6. Click the **Add** button.
The user account is added.
7. Click the **Apply** button.
Your settings are saved.

Change the Name for a User Account

► To change the name for a user account:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > Advanced > User Accounts**.
The User Accounts page displays.
5. In the Update User Accounts section, select a user from the **Existing Users** menu.
6. In the **User Name** field, modify the name.
7. Click the **Modify** button.
The user name is changed.
8. Click the **Apply** button.
Your settings are saved.

Change the Privilege for a User Account

► To change the privilege for a user account:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > Advanced > User Accounts**.
The User Accounts page displays.
5. In the Update User Accounts section, select a user from the **Existing Users** menu.
6. From the **Privilege** menu, select another privilege.
7. Click the **Reset Password** button.
The password is reset to the default password, which is **password**.
8. Click the **Apply** button.
Your settings are saved.

Reset the Password for a User Account

► To reset the password for a user account:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > Advanced > User Accounts**.
The User Accounts page displays.
5. In the Update User Accounts section, select a user from the **Existing Users** menu.
6. Click the **Reset Password** button.

The password is reset to the default password, which is password.

7. Click the **Apply** button.
Your settings are saved.

Note If you want to modify a password, delete the user account, and then recreate the user account with the password of your choice.

Delete a User Account

► To delete a user account:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > Advanced > User Accounts**.
The User Accounts page displays.
5. In the Update User Accounts section, select a user from the **Existing Users** menu.
6. Click the **Delete** button.
7. Click the **Apply** button.
Your settings are saved.

Enable the Syslog Server

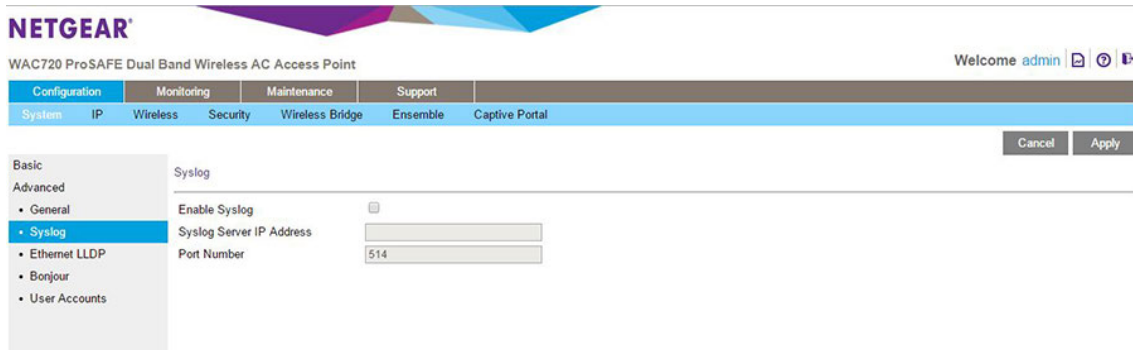
You can enable the syslog option if your LAN includes a syslog server. If syslog is enabled, the access point sends its syslog files to the syslog server.

► To enable a syslog server:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Configuration > System > Advanced > Syslog**.



Specify the settings as described in the following table.

Setting	Description
Enable Syslog	Select the check box to enable the syslog option. By default, the syslog option is disabled.
Syslog Server IP Address	Enter the IP address of the syslog server to which the access point sends the syslog files.
Port Number	Enter the port number that is configured on the syslog server. The default port number is 514.

5. Click the **Apply** button.
Your settings are saved.

Monitor the Access Point

The following sections describe how you can monitor the access point:

- [View System Information](#) on page 78
- [View Dashboard Information](#) on page 80
- [Monitor WiFi Clients](#) on page 83
- [View the Activity Logs](#) on page 85
- [View the Traffic Statistics](#) on page 86

For information about monitoring rogue access points, see [Enable Rogue AP Detection and Monitor Rogue APs](#) on page 53.

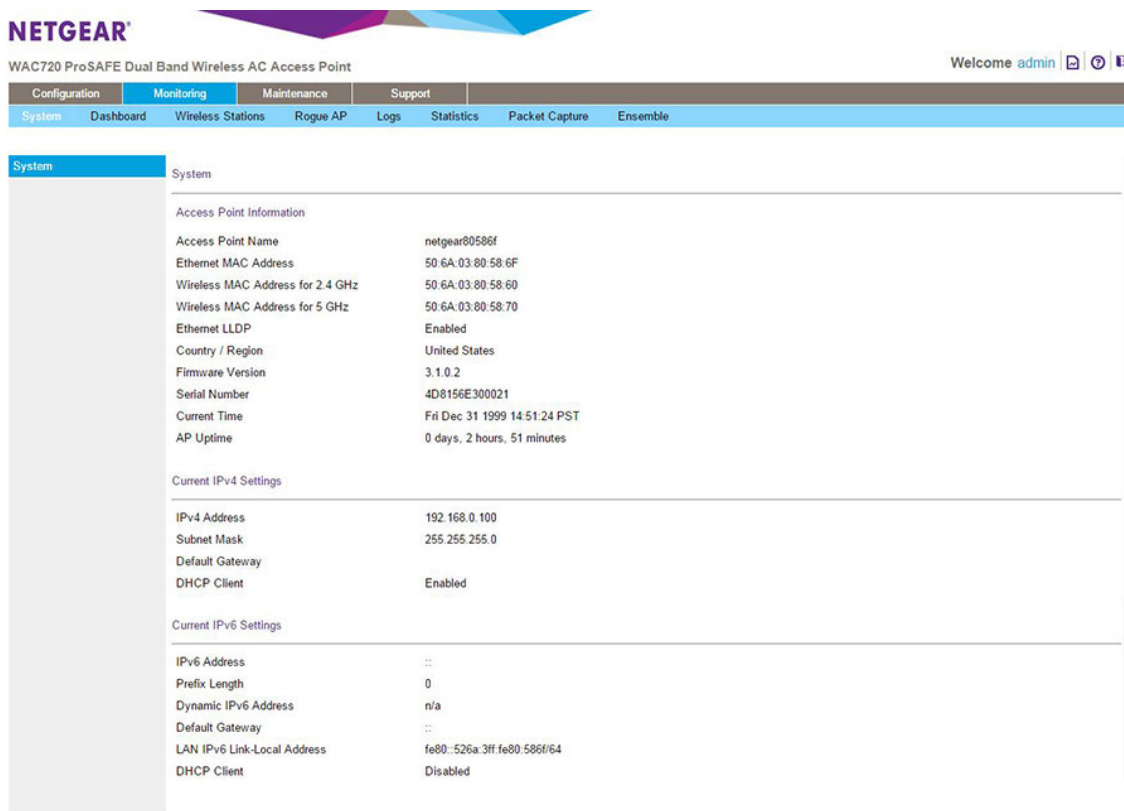
For information about monitoring ensembles, see [Set Up, Manage, and Monitor Ensembles](#) on page 87.

View System Information

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

► **To view the System page:**

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Monitoring > System**.



The following table explains the fields of the System page:

Setting	Description
Access Point Information	
Access Point Name	The NetBIOS name. For information about how to change the default name, see Configure Basic General System Settings on page 20.

(Continued)

Setting	Description
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 WiFi radio.
Wireless MAC Address for 5 GHz	The MAC address of the access point's 5 GHz WiFi radio.
Ethernet LLDP	Enabled indicates that LLDP is enabled. Disabled indicates that it is not.
Country/Region	<p>The country or region for which the access point is licensed for use. For information about how to change the country or region, see Configure Basic General System Settings on page 20.</p> <hr/> <p>Note Make sure that the country is set to the location where the device is operating. You are responsible for complying with the local, regional, and national regulations that are set for channels, power levels, and frequency ranges.</p> <hr/> <p>Note It might not be legal to operate this access point in a country or region other than one of those identified in this field.</p> <hr/>
Firmware Version	The version of the firmware that is currently installed.
Serial Number	The serial number of the access point.
Current Time	The current time. For information about how to change the time settings, see Configure Basic General System Settings on page 20.
AP Uptime	The length of time since the access point became active.
Current IPv4 Settings For information about how to change any of these IP settings, see Configure the IPv4 Settings on page 23.	
IP Address	The IPv4 address of the access point.
Subnet Mask	The subnet mask for the address of the access point.
Default Gateway	The default IPv4 gateway for the access point communication.
DHCP Client	Enabled indicates that the current IP address was obtained from a DHCPv4 server on your LAN network. Disabled indicates a static IP configuration.
Current IPv6 Settings For information about how to change any of these IP settings, see Configure IPv6 Settings on page 101.	
IPv6 Address	The default IPv6 address of the access point.
Prefix Length	The prefix length for the address of the access point.
Dynamic IPv6 Address	The dynamically assigned IPv6 address if the DHCPv6 server has the stateful option enabled.
Default Gateway	The default IPv6 gateway for the access point communication.
LAN IPv6 Link-Local Address	This is an automatically generated IPv6 address that uses the IPv4 address in the interface portion of its address.
DHCP Client	Enabled indicates that the current IP address was obtained from a DHCPv6 server on your LAN network. Disabled indicates a static IP configuration.

(Continued)

Setting	Description
Current Wireless Settings for 802.11 bg/ng/bgn and Current Wireless Settings for 802.11 a/a-na-ac	
Access Point Mode	The WiFi operation mode of the access point for the radio band. By default, the mode is 11bgn for the 2.4 GHz radio band and 11a-na-ac for the 5 GHz radio band.
Channel / Frequency	The channel that the WiFi port is using. For information about how to change the channel and frequency, see <i>Configure 802.11bg/ng/bgn WiFi Settings</i> on page 24 and <i>Configure 802.11a/a-na-ac WiFi Settings</i> on page 27.
Rogue AP Detection	Enabled indicates that rogue AP detection is enabled. Disabled indicates that it is not.

View Dashboard Information

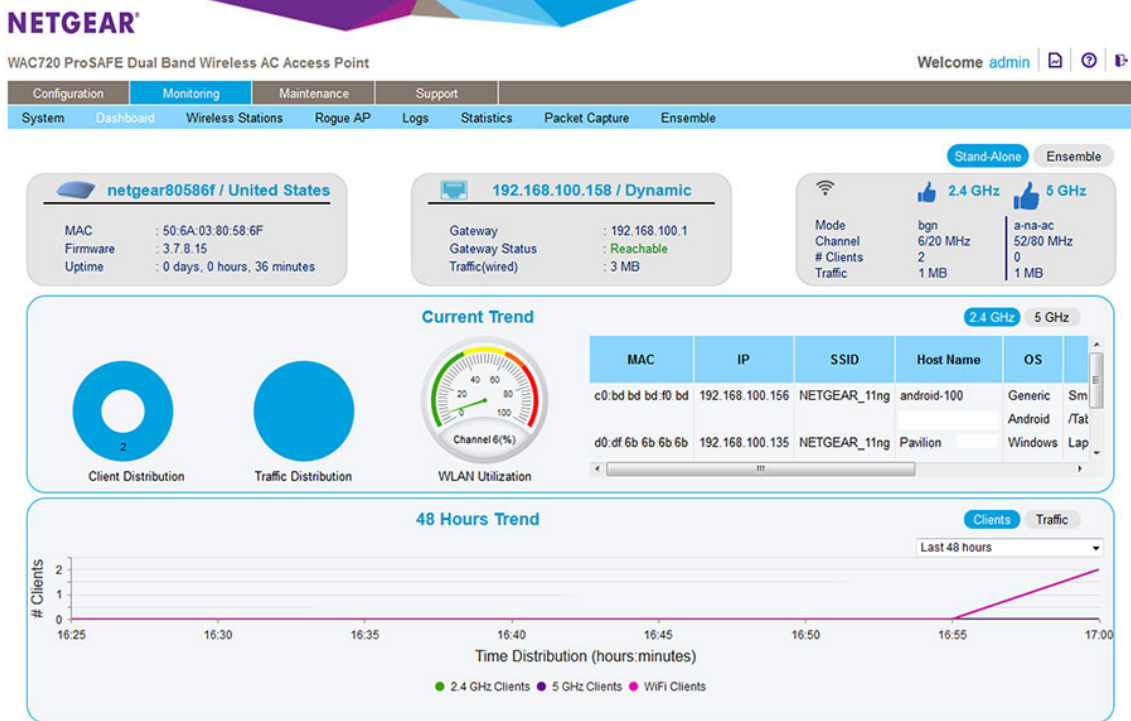
The Dashboard pages provide general information about the access point in standalone mode or ensemble mode. In addition, the pages provide real-time and historical information about client distribution, traffic distribution and WLAN utilization.

View the Standalone Dashboard

The Dashboard page for a standalone access point provides read-only information, so any changes must be made on other pages.

► To view the standalone Dashboard:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see *Log In to the Access Point* on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Monitoring > Dashboard**.
The Dashboard page displays.
5. Click the **Stand-Alone** button.
The Dashboard page displays information for the standalone access point.



6. To view more information, point to a graph.
7. To view real-time information for 5 GHz clients and traffic, click the **5 GHz** button. By default, the **2.4 GHz** button is selected.
8. To view historical traffic information, click the **Traffic** button. By default, the **Clients** button is selected.
9. To view historical information for another period, select the period from the menu below the **Clients** and **Traffic** buttons.

View the Ensemble Dashboard

The Dashboard page for an access point in ensemble mode provides read-only information, so any changes must be made on other pages.

► To view the ensemble Dashboard:

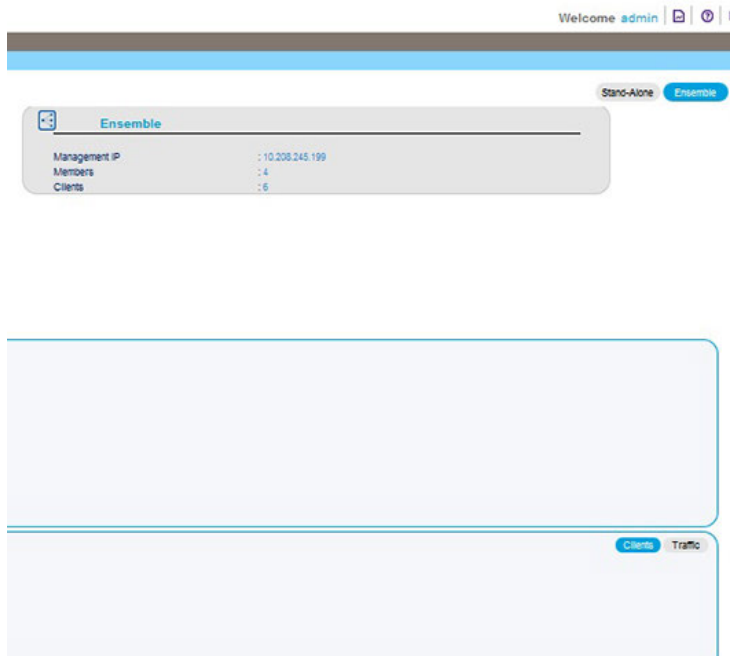
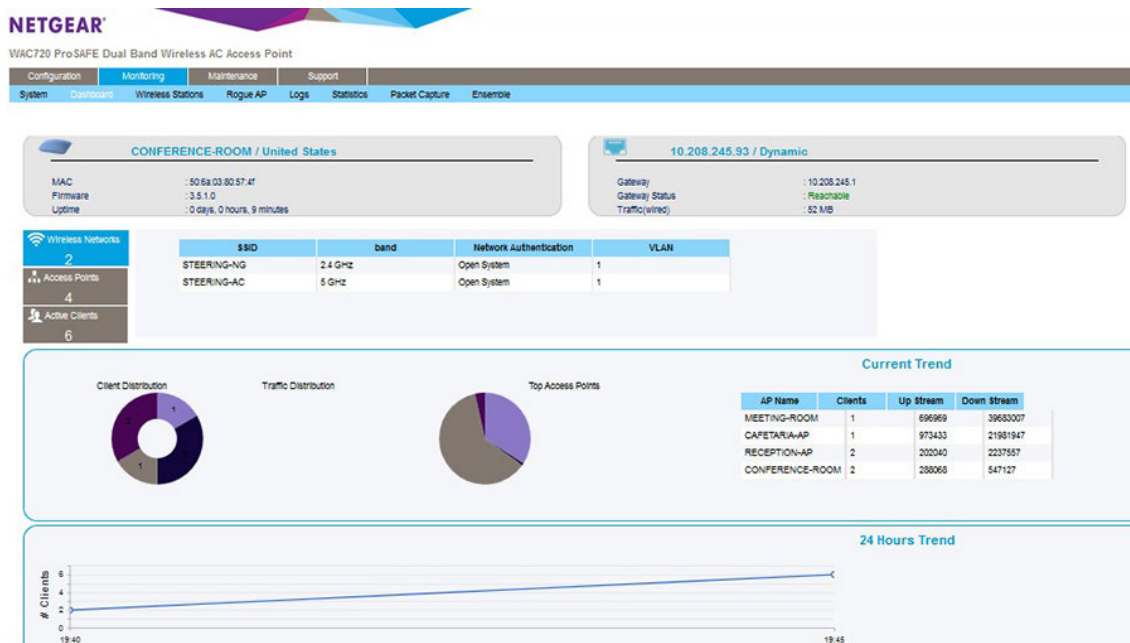
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Monitoring > Dashboard**.

The Dashboard page displays.

5. Click the **Ensemble** button.

The Dashboard page displays information for the access point in ensemble mode. The upper figure shows the left and middle of the page. The lower figure shows the right of the page.



6. To view more information, point to a graph.

7. To view historical traffic information for the past 24 hours, click the **Traffic** button in the lower right of the page.
By default, the **Clients** button is selected and the page shows historical client information.
8. To view details about access point in the ensemble, click the **Access Points** box on the left.
By default, the **Wireless Networks** box is selected.
9. To view details about active clients in the ensemble, click the **Active Clients** box on the left.

Monitor WiFi Clients

You can view all WiFi devices that are associated with a WiFi network name (SSID) on the access point.

Note A WiFi network can include multiple access points, all using the same SSID. This uniformity extends the reach of the WiFi network and allows users to roam from one access point to another, providing seamless network connectivity. Under these circumstances, be aware that the WiFi clients that you can monitor as described in the following procedure are the clients that are associated with this access point.

► To view the attached WiFi clients and details for an individual WiFi client:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Monitoring > Wireless Stations**.

The screenshot shows the NETGEAR web interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The 'Monitoring' tab is selected, and the 'Wireless Stations' sub-tab is active. The page displays a table of available wireless stations for two SSIDs: 'NETGEAR_11ng' and 'NETGEAR_11n'. The table columns include MAC Address, BSSID, SSID, Host Name, OS, Type, CP Authentication Type, CP Session Timeout (Sec), Channel, Rate, State, Type, Tx Bytes, Rx Bytes, Mode, and Status. Two devices are listed: a Windows Laptop/PC and a Generic Android Smartphone/PDA.

The Wireless Stations table shows the information for each device. For information about these and more fields, see the following table. Captive portal (CP) information is displayed only if you cond a captive portal. Otherwise, the CP fields show NA.

- To update the list, click the **Refresh** button.
- To view details of a WiFi station, select the corresponding radio button, and then click the **Details** button. The Wireless Stations Details pop-up window opens.

The following table explains the fields of the Wireless Stations Details pop-up window.

Setting	Description
MAC Address	The MAC address of the WiFi station.
BSSID	The BSSID that the WiFi station is using.
SSID	The SSID that the WiFi station is using.
Channel	The channel that the WiFi station is using.
Rate	The transmit data rate in Mbps of the WiFi station.
Type	The authentication and encryption type that the WiFi station is using.
Mode	The WiFi mode in which the WiFi station is operating.
Status	The WiFi status of the WiFi station (Associated).
RSSI	The received signal strength indicator (RSSI) of the WiFi station.
Idle Time	The time since the last frame was received from the WiFi station.
Recv. Bytes	The number of bytes received on the WiFi station since it last started.
Trans. bytes	The number of bytes transmitted by the WiFi station since it last started.
Assoc. Time Stamp	The time when these details of the WiFi station were retrieved.

(Continued)

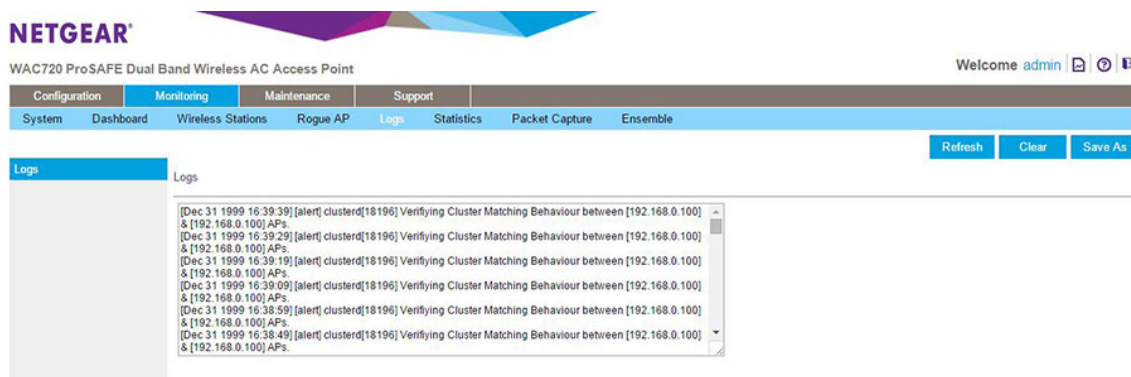
Setting	Description
IP Address	The IP address of the WiFi station.
Channel Width	The channel width at which the WiFi station operates.

View the Activity Logs

You can view the access point's activity logs and save the log entries.

► To display the activity logs and save the log entries:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Monitoring > Logs**.



5. Click the **Save As** button to save the log entries to a file on your computer or to a disk drive.
6. To update the information on the page, click the **Refresh** button.
7. To clear the log entries, click the **Clear** button.

View the Traffic Statistics

The Statistics page displays information for both wired (LAN) and WiFi (WLAN) network traffic.

► **To display the Statistics page:**

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Monitoring > Statistics**.

Wired Ethernet		
	Received	Transmitted
Packets	49083	43518
Bytes	20137972	20203394

Wireless 802.11 bg/ng/bgn		
	Received	Transmitted
Unicast Packets	14750	17570
Broadcast Packets	605	11163
Multicast Packets	1799	26575
Total Packets	17154	55308
Total Bytes	1958643	24519370

Wireless 802.11 a/a-na-ac		
	Received	Transmitted
Unicast Packets	0	0
Broadcast Packets	0	8540
Multicast Packets	0	20162
Total Packets	0	28702
Total Bytes	0	4552051

Client Association	
	Number of Associated Clients
802.11 bg/ng/bgn Radio	2

5. To update the statistics information, click the **Refresh** button.
The following table explains the fields of the Statistics page:

Setting	Description
Wired Ethernet	
Packets	The number of packets received and transmitted over the Ethernet connection since the access point was restarted.

(Continued)

Setting	Description
Bytes	The number of bytes received and transmitted over the Ethernet connection since the access point was restarted.
Wireless 802.11bgn and Wireless 802.11a-na-ac (The section heading depends on the configured WiFi mode.)	
Unicast Packets	The number of unicast packets received and transmitted over the WiFi connection since the access point was restarted.
Broadcast Packets	The number of broadcast packets received and transmitted over the WiFi connection since the access point was restarted.
Multicast Packets	The number of multicast packets received and transmitted over the WiFi connection since the access point was restarted.
Total Packets	The total number of packets received and transmitted over the WiFi connection since the access point was restarted.
Total Bytes	The total number of bytes received and transmitted over the WiFi connection since the access point was restarted.
Client Association	
802.11bgn Radio, 802.11a-na-ac Radio	The number of associated clients connected to the radio in the configured WiFi modes.

Set Up, Manage, and Monitor Ensembles

An access point (AP) ensemble is a dynamic, configuration-aware group of APs in the same subnet of a network. Each ensemble can include up to 10 members, which must be of the same model. Only one ensemble per WiFi network is supported. However, a network subnet can include multiple ensembles. Ensembles allow APs to share various configuration information, such as virtual AP (VAP) settings and QoS queue parameters. Ensemble members share the configuration of the master AP (also referred to as the dominant AP).

With ensemble mode enabled, you can initiate common firmware updates and use a centralized ensemble dashboard to monitor client connectivity and share of traffic across the ensemble members. If an ensemble member fails, the ensemble automatically makes adjustments to ensure that the remaining members work cooperatively.

An ensemble can be formed between two more APs if the following conditions are met:

- The APs are of the same model, with the exception of model WAC720 and model WAC730, which you can combine in an ensemble.
- The APs use the same country or region settings and the same radio mode.
- The APs are connected on the same bridged segment.

- The ensemble names of the APs that are joining are the same.
- Ensemble mode is enabled on all APs.

Configure Enable Ensemble Mode

► To configure enable ensemble mode on the access point:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Ensemble > Basic > General**.

NETGEAR

WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration Monitoring Maintenance Support

System IP Wireless Security Wireless Bridge Ensemble Captive Portal

Cancel Apply

Basic

General

Ensemble Mode Start Stop

Ensemble Name

AP Name

Priority (0 - 255)

5. In the **Ensemble Name** field, enter the ensemble name.
6. In the **AP Name** field, enter a custom name for the access point or use the default name.
7. In the **Priority (0 - 255)** field, enter the access point's priority in the ensemble.
The lowest-numbered AP becomes the master AP.
8. To enable ensemble mode, select the **Start** radio button.
9. Click the **Apply** button.
Your settings are saved.

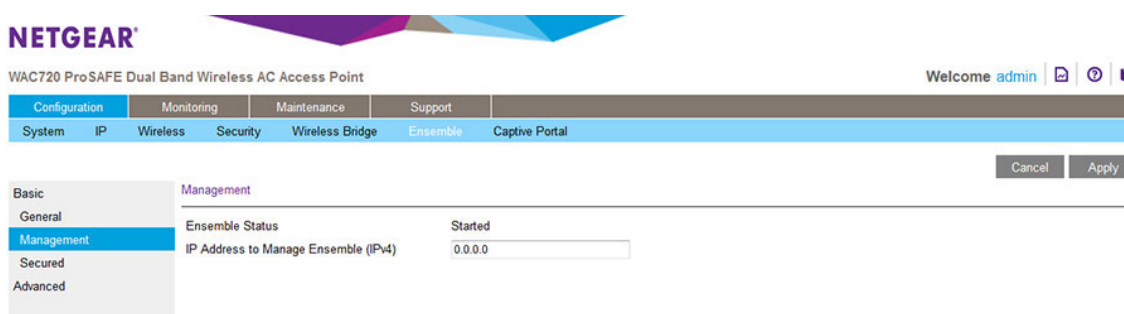
Manage an Ensemble

You can manage an ensemble through the master access point's local browser interface or you can specify a computer with an IP address in the same subnet as the management IP address. Through the master access point or management IP address you can run an ensemble's channel assignment, manage an ensemble's channel assignment settings, manage the firmware upgrade settings, and manage security settings.

Specify an Ensemble Management IP Address

► To specify an ensemble management IP address:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Ensemble > Basic > Management**.



The **Ensemble Status** field displays the status of the ensemble (Started or Stopped).

5. In the **IP Address to Manage Ensemble (IPv4)** field, enter the IP address of the computer that must function as the management IP address for the ensemble.
The management IP address and members of the ensemble must be on the same subnet.
6. Click the **Apply** button.
Your settings are saved.

Configure Ensemble Security With a Passphrase

By default, access points can become members of an ensemble without using authentication. That is, when access points form an ensemble, they do not authenticate each other. However, you can enable security for an ensemble by configuring the same passphrase on each access point that must become a member of the ensemble. When access points form an ensemble, they use the passphrase to authenticate each other. An access point for which you do not configure the ensemble passphrase cannot join the ensemble.

Using ensemble security allows you to set up more than one ensemble in the same subnet by specifying a different passphrase for each ensemble. Implementing ensemble security also prevents an access point from accidentally joining an ensemble if the ensemble mode is enabled on the access point.

In addition to the ensemble passphrase, you can specify the reauthentication time-out period, which is the time after which members of an ensemble must reauthenticate each other.

► To configure security settings with a passphrase for an ensemble:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Ensemble > Basic > Secured Ensemble**.

NETGEAR

WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration Monitoring Maintenance Support

System IP Wireless Security Wireless Bridge Ensemble Captive Portal

Cancel Apply

Basic

- General
- Management
- **Secured**

Advanced

Secured

Ensemble Status Stopped

Secure Mode Enabled Disabled

Passphrase (8 - 63 characters)

Re-authentication Timeout (300 - 86400 secs)

5. Select the **Enabled** radio button.
6. Enter a passphrase between 8 and 63 characters in the **passphrase** field.
7. Enter a time-out period between 300 and 86400 seconds.
The default is 300 seconds.
8. Click the **Apply** button.
Your settings are saved.

Specify an Ensemble's Channel Assignment Settings

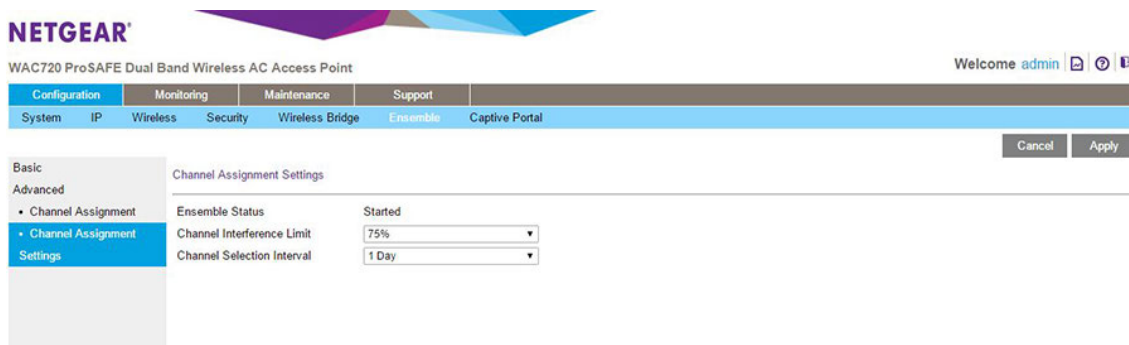
Before you enable automatic channel assignment for an ensemble (see [Manage Automatic Channel Assignment for an Ensemble](#) on page 91), you might want to specify a custom channel interference limit, which triggers channel reassignment. You can also specify the channel selection interval, which determines the schedule at which automatic channel assignment occurs.

The defaults are as follows:

- Channel interference limit. 75 percent (the range is from 5 percent to 75 percent).
- Channel selection interval. 1 day (the range is from 30 minutes to 6 months).

► To manage an ensemble's channel assignment settings:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Ensemble > Advanced > Channel Assignment Settings**.



5. From the **Channel Interference Limit** menu, select an interference limit percentage.
6. From the **Channel Selection Interval** menu, select a channel selection interval.
7. Click the **Apply** button.
Your settings are saved.

Manage Automatic Channel Assignment for an Ensemble

You can enable automatic channel assignment for an ensemble. The assignment is based on the channel assignment settings (see [Specify an Ensemble's Channel Assignment Settings](#) on page 90).

Automatic channel assignment reduces both mutual interference between the access points in an ensemble and interference with other access points outside the ensemble. It also maximizes WiFi bandwidth to help maintain efficient communication over the WiFi network.

Note When automatic channel assignment is enabled, the channel policy for the radios is automatically set to the static mode. That is, Auto is not available as a selection from the Channel / Frequency menu on the Wireless Settings page. For more information, see [Configure the Basic WiFi Settings](#) on page 24.

► To manage automatic channel assignment for an ensemble:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.

For more information, see [Log In to the Access Point](#) on page 16.

2. In the address bar, enter the IP address of the access point.

A login window opens.

3. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Configuration > Ensemble > Advanced > Channel Assignment**.

The Channel Assignment page displays. By default, automatic channel assignment is disabled.

5. Click the **Start** button.

Automatic channel assignment is enabled. The access point detects the channels that the access points in the ensemble are using.

NETGEAR
WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration | Monitoring | Maintenance | Support
System | IP | Wireless | Security | Wireless Bridge | Ensemble | Captive Portal

Channel Assignment

Ensemble Status: Started

Auto Assign Channels: [Start] [Stop] [Refresh]

IP Address	Radio	Band	Channel	Status	Assign to Static
10.208.245.55	DC:EF:09:90:B5:F0	11a-na-ac	36	up	<input type="checkbox"/>
10.208.245.55	DC:EF:09:90:B5:E0	11bgn	1	up	<input type="checkbox"/>
10.208.245.80	DC:EF:09:90:AF:10	11a-na-ac	36	up	<input type="checkbox"/>
10.208.245.80	DC:EF:09:90:AF:00	11bgn	11	up	<input type="checkbox"/>
10.208.245.88	50:6A:03:80:59:50	11a-na-ac	36	up	<input type="checkbox"/>
10.208.245.88	50:6A:03:80:59:40	11bgn	11	up	<input type="checkbox"/>
10.208.245.93	50:6A:03:80:57:50	11a-na-ac	36	up	<input type="checkbox"/>
10.208.245.93	50:6A:03:80:57:40	11bgn	1	up	<input type="checkbox"/>

Proposed Channel Assignments

IP Address	Radio	Proposed Channel
------------	-------	------------------

6. To select channels that must remain static, do the following:

- a. For each channel that must remain static, select the check box in the Assign to Static column.
- b. Click the **Apply** button.

The selected channels are not changed during the automatic channel assignment process.

When automatic channel assignment is running, the Channel Assignment page shows the proposed channels at the bottom. The following figure shows only part of the table with proposed channels.

The screenshot shows the NETGEAR web interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The user is logged in as 'admin'. The 'Channel Assignment' page is active, showing the Ensemble Status as 'Started'. There are buttons for 'Start', 'Stop', and 'Refresh' under 'Auto Assign Channels'. A table lists current channel assignments for various IP addresses and radio MAC addresses. Below this, a section titled 'Proposed Channel Assignments (3 minutes and 49 seconds ago)' shows a table with columns for IP Address, Radio, and Proposed Channel.

IP Address	Radio	Band	Channel	Status	Assign to Static
10.208.245.55	DC:EF:09:90:B5:F0	11a-na-ac	36	up	<input type="checkbox"/>
10.208.245.55	DC:EF:09:90:B5:E0	11bgn	1	up	<input type="checkbox"/>
10.208.245.80	DC:EF:09:90:AF:10	11a-na-ac	36	up	<input type="checkbox"/>
10.208.245.80	DC:EF:09:90:AF:00	11bgn	11	up	<input type="checkbox"/>
10.208.245.88	50:6A:03:80:59:50	11a-na-ac	36	up	<input type="checkbox"/>
10.208.245.88	50:6A:03:80:59:40	11bgn	11	up	<input type="checkbox"/>
10.208.245.93	50:6A:03:80:57:50	11a-na-ac	36	up	<input type="checkbox"/>
10.208.245.93	50:6A:03:80:57:40	11bgn	1	up	<input type="checkbox"/>

IP Address	Radio	Proposed Channel
10.208.245.55	DC:EF:09:90:B5:F0	48
10.208.245.55	DC:EF:09:90:B5:E0	6
10.208.245.80	DC:EF:09:90:AF:10	165

At any time, you can disable automatic channel assignment by clicking the Stop button.

Upgrade the Firmware of Ensemble Members From a Downloaded Firmware File

You can upgrade the firmware on all access points in an ensemble from the master access point. If you do not use a TFTP server, download the firmware to a computer and upload it to the master access point. Then, from the master access point, initiate the firmware for all or selected access points in the ensemble, including, if you want, the master access point.

► To upgrade the firmware of ensemble members from a downloaded firmware file:

1. Download the new firmware file from the NETGEAR website at downloadcenter.netgear.com and save it to your computer.
2. If available, read the release notes before upgrading the firmware.
3. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.

4. In the address bar, enter the IP address of the access point.
A login window opens.

5. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

6. Select **Maintenance > Ensemble Upgrade > Firmware Upgrade**.

NETGEAR

WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration Monitoring Maintenance Support

Password Reset Remote Management Upgrade Ensemble Upgrade

Firmware Upgrade

Member Selection

Members	IP Address	MAC Address	Master AP	Firmware Version	Firmware-transfer-status	
<input checked="" type="checkbox"/>	1	10.208.245.80	DC:EF:09:90:AF:0F	no	3.5.2.2	None
<input type="checkbox"/>	2	10.208.245.88	50:6A:03:80:59:4F	yes	3.5.2.2	None

Refresh Apply

Upload Firmware

New Firmware Image: No file selected.

Upgrade

Caution: Uploading the new firmware may take several minutes. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the process is complete the access point will restart and resume normal operation.

The Member Selection table shows the members of the ensemble, including the firmware versions of the members.

7. Click the **Browse** button.

A pop-up window opens.

8. Navigate to and select a firmware file to upload.

9. Click the **Upgrade** button.

An Alert pop-up window opens.

The firmware is uploaded to the master access point's memory.

Note The firmware is uploaded to but *not upgraded* on the master access point. However, in Step 13 you can select the firmware to be upgraded on the master access point.

10. In the Alert pop-up window, click the **OK** button.

The pop-up window closes. In the Upload Firmware section, a status bar shows the progress of the upload process. After the upload process is complete, the master access point restarts.

11. Log back in to the access point.

12. Select **Maintenance > Ensemble Upgrade > Firmware Upgrade**.

13. In the Member Selection table, select the check boxes for the members of the ensemble that you want to upgrade, including, if you want, the master access point.

If you want to upgrade firmware on all members of the ensemble, select the check box in the table heading.

14. Click the **Apply** button.

The firmware upgrade process starts.

The Firmware-transfer-status field in the table shows whether the firmware download to and validation in the member is successful.

Upgrade the Firmware of Ensemble Members Over a TFTP Server

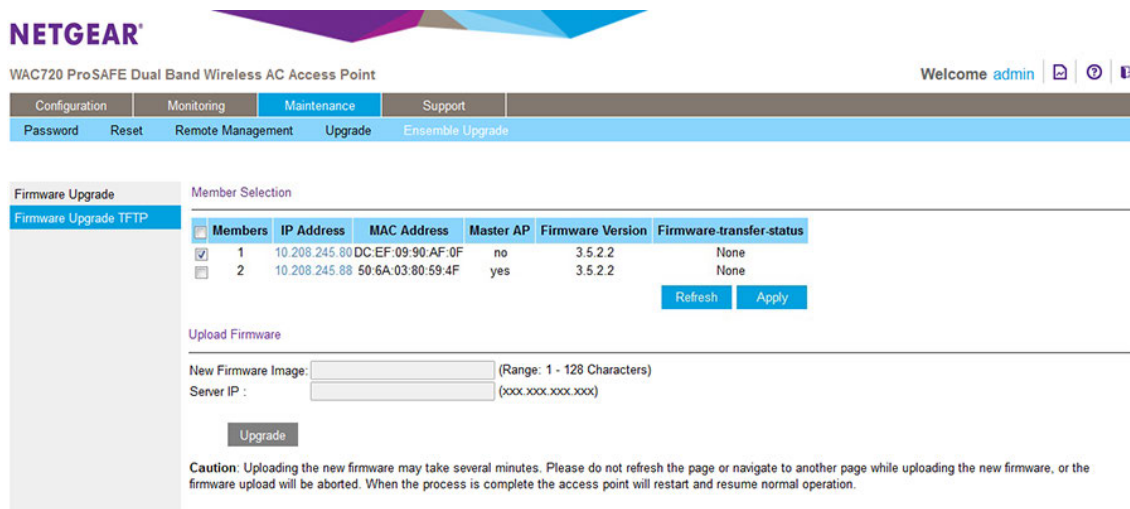
You can upgrade the firmware on all access points in an ensemble from the master access point. If you use a TFTP server, download the firmware from the TFTP server directly to the master access point. Then, from the master access point, initiate the firmware for all or selected access points in the ensemble, including, if you want, the master access point.

► **To upgrade the firmware of ensemble members using a TFTP server:**

1. Download the new firmware file from the NETGEAR website at downloadcenter.netgear.com and save it to your computer.
2. Transfer the firmware file to your TFTP server.
3. If available, read the release notes before upgrading the firmware.
4. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.

For more information, see [Log In to the Access Point](#) on page 16.

5. In the address bar, enter the IP address of the access point.
A login window opens.
6. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
7. Select **Maintenance > Ensemble Upgrade > Firmware Upgrade TFTP**.



The Member Selection section shows the members of the ensemble, including the firmware versions of the members.

8. Specify the following information:
 - **New Firmware Image.** The name of the firmware file.
 - **Server IP.** The IP address of your TFTP server.
9. Click the **Upgrade** button.

An Alert pop-up window opens.

The firmware is uploaded to the master access point's memory.

Note The firmware is uploaded to but *not upgraded* on the master access point. However, in step 13 you can select the firmware to be upgraded on the master access point.

10. In the Alert pop-up window, click the **OK** button.

The pop-up window closes. In the Upload Firmware section, a status bar shows the progress of the upload process. After the upload process is complete, the master access point restarts.

11. Log back in to the access point.

12. Select **Maintenance > Ensemble Upgrade > Firmware Upgrade**.

13. In the Member Selection table, select the check boxes for the members of the ensemble that you want to upgrade, including, if you want, the master access point.

If you want to upgrade firmware on all members of the ensemble, select the check box in the table heading.

14. Click the **Apply** button.

The firmware upgrade process starts.

The Firmware-transfer-status field in the table shows whether the firmware download to and validation in the member is successful.

Monitor an Ensemble

You can monitor the status of an ensemble from the ensemble dashboard. You can also monitor the devices connected to members of the ensemble as well as monitor networks neighboring the ensemble.

Monitor the Status of the Ensemble

You can monitor the status of the access point as member of the ensemble, including the access point's priority in the ensemble and whether the access point is the master AP in the ensemble.

► To monitor the status of the ensemble:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.

For more information, see [Log In to the Access Point](#) on page 16.

2. In the address bar, enter the IP address of the access point.

A login window opens.

3. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Monitor > Ensemble > Access Point**.

NETGEAR

WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration Monitoring Maintenance Support

System Dashboard Wireless Stations Rogue AP Logs Statistics Packet Capture Ensemble

Refresh

Access Point

Wireless Stations

Wireless Neighborhood

AP Name	MAC Address	IP Address	Ensemble Priority	Master AP	Firmware version	2.4GHz Channel	5GHz Channel	Uptime in Ensemble	Status
netgear90af0f	DC:EF:09:90:AF:0F	10.208.245.80	0	no	3.5.2.2	-	-	0 days 15 hours 10 minutes	Connected
netgear80594f	E0:6A:03:80:59:4F	10.208.245.88	0	yes	3.5.2.2	-	-	2 days 13 hours 37 minutes	Connected

**NOTE: This table takes few minutes to get updated.

- Click the **Refresh** button.
The information on the page refreshes.

Monitor the Devices Connected to the Ensemble

You can monitor the WiFi clients that are connected to all members of the ensemble. For each access point that is a member of the ensemble, up to 20 WiFi clients per radio can be displayed (although a radio can support more than 20 clients).

► To monitor the devices connected to the ensemble:

- Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
- In the address bar, enter the IP address of the access point.
A login window opens.
- Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Monitor > Ensemble > Wireless Stations**.

NETGEAR

WAC720 ProSAFE Dual Band Wireless AC Access Point Welcome admin

Configuration Monitoring Maintenance Support

System Dashboard Wireless Stations Rogue AP Logs Statistics Packet Capture Ensemble

Access Point Wireless Stations

Wireless Stations	AP Name	Station MAC	Station Idle Time	Rate	RSSI	Tx Bytes	Rx Bytes	Error Rate
Wireless Neighborhood	CONFERENCE-ROOM	4C:8D:79:E3:8F:62	0	0 Bytes	0	71144	43705	0
	CONFERENCE-ROOM	88:32:9B:26:7A:8D	1	0 Bytes	50	3614	4277	0
	RECEPTION-AP	08:11:96:DD:FC:C4	2	0 Bytes	50	526	1284	0
	CAFETARIA-AP	08:11:96:7D:EB:E0	0	0 Bytes	56	30124	19052	0
	CAFETARIA-AP	B8:76:3F:1A:83:EC	60	0 Bytes	63	4	55	0
	MEETING-ROOM	D0:7E:35:09:0F:56	0	0 Bytes	0	70328	23422	0

****NOTE: Maximum of 20 clients per radio of each AP will be displayed. To view all clients, please access individual AP.**

5. Click the **Refresh** button.
The devices connected to the ensemble display, listed by MAC address.

Monitor the Access Points and Networks Neighboring the Ensemble

You can display the access points (and their associated WiFi networks) that are the neighbors of the ensemble.

► To monitor the networks neighboring the ensemble:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Monitor > Ensemble > Wireless Neighborhood**.
The Wireless Neighborhood page displays.
5. From the **Neighbor APs** menu, select one of the following options:

Dual-Band Wireless AC Access Point WAC720 and WAC730 User Manual

- **Not in Ensemble.** The access points that are not in the ensemble are displayed.
- **In Ensemble.** The access points that are in the ensemble are displayed.
- **Both.** Both the access points that are in the ensemble and that are not in the ensemble are displayed. (The following figure shows this option.)

The screenshot shows the Netgear WAC720 ProSAFE Dual Band Wireless AC Access Point web interface. The 'Ensemble' tab is active, and the 'Both' option is selected in the 'Neighbor APs (In Ensemble/Not in Ensemble/Both)' dropdown. The table below shows the neighbor APs and steering actions.

Neighbor AP (B2)	10.208.245.93 50:6A:03:80:57:40 (CONFERENCE-ROOM)	10.208.245.93 50:6A:03:80:57:50 (CONFERENCE-ROOM)	10.208.245.88 50:6A:03:80:59:40 (RECEPTION-AP)	10.208.245.88 50:6A:03:80:59:50 (RECEPTION-AP)	10.208.245.80 DC:EF:09:90:AF:00 (CAFETARIA-AP)	10.208.245.80 DC:EF:09:90:AF:10 (CAFETARIA-AP)	10.208.245.80 DC:EF:09:90:AF:10 (CAFETARIA-AP)
STEERING-NG							
STEERING-AC							
STEERING-NG							
STEERING-AC							
STEERING-NG							
STEERING-AC							
STEERING-NG							
STEERING-AC							
NETGEAR 11ac							

Configure Advanced Network and WiFi Features

5

This chapter describes how to configure the advanced features of the access point.

The chapter includes the following sections:

- *Configure IPv6 Settings*
- *Configure Spanning Tree Protocol, 802.1Q VLAN, and Link Layer Discovery Protocol*
- *Configure Bonjour*
- *Configure Advanced WiFi Settings*
- *Configure Advanced Quality of Service Settings*
- *Configure and Manage Quality of Service Policies*
- *Configure Load Balancing*
- *Manage Captive Portals*
- *Configure WiFi Bridging*

Configure IPv6 Settings

The access point supports IPv6. You can manage the access point from an IPv6 address. The access point can also function as an IPv6 DHCP client.

Note For information about how to configure the IPv4 settings, see [Configure the IPv4 Settings](#) on page 23.



WARNING:

If you enable the DHCP client, the IP address of the access point changes when you click the Apply button, causing you to lose your connection to the access point. You then must use the new IP address to reconnect to the access point.

Tip If you enable the DHCP client on the access point, you can discover the new IP address of the access point by accessing the DHCP server on your LAN, or by using a network IP address scanner application.

► To configure the IPv6 settings:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > IP > IPv6 Settings**.

5. Configure the IPv6 settings as described in the following table.

Configure Advanced Network and WiFi Features

Setting	Description
DHCP Client	By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If your LAN includes a DHCPv6 server and you select the Enable radio button, the access point receives its dynamic IPv6 address, prefix length, and default gateway settings automatically from the DHCPv6 server on your network when you connect the access point to your LAN.
IPv6 Address	Enter the IP address of your access point. The default IPv6 address is 2001::21c:c0ff:fe69. To change the address, enter an unused IPv6 address from the address range used on your LAN.
Prefix Length	Enter the prefix length for the IPv6 address. The default prefix length is 64.
Default Gateway	Enter the IPv6 address of the ISP gateway to which the access point connects.
Dynamic IPv6 Address	The dynamic IPv6 address that is assigned by the DHCPv6 server on your network. This address does not overwrite the address in the IPv6 Address field.
Primary DNS Server	Enter the IP address of the primary and secondary DNS servers. A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your access point during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually in this field.
Secondary DNS Server	
Network Integrity Check	Select this check box to validate that the upstream link is active before allowing WiFi associations. Ensure that the default gateway is configured.

- Click the **Apply** button.
Your settings are saved.

Configure Spanning Tree Protocol, 802.1Q VLAN, and Link Layer Discovery Protocol

As part of the advanced system configuration, you can enable the Spanning Tree Protocol (STP), configure the VLANs, and enable Ethernet Link Layer Discovery Protocol (LLDP) as described in the following sections:

- [Configure STP and VLANs](#) on page 102
- [Configure Ethernet LLDP](#) on page 104

Configure STP and VLANs

STP provides network traffic optimization in locations where multiple access points are active by preventing path redundancy. If your location includes more than one active access point, we recommend that you enable STP.

The 802.1Q VLAN protocol on the access point logically separates traffic on the same physical network. The access point supports the following types of VLANs:

- **Untagged VLAN.** When the access point sends frames that are associated with the untagged VLAN from its Ethernet interface, those frames are untagged. When the access point receives untagged frames over its Ethernet interface, those frames are assigned to the untagged VLAN.

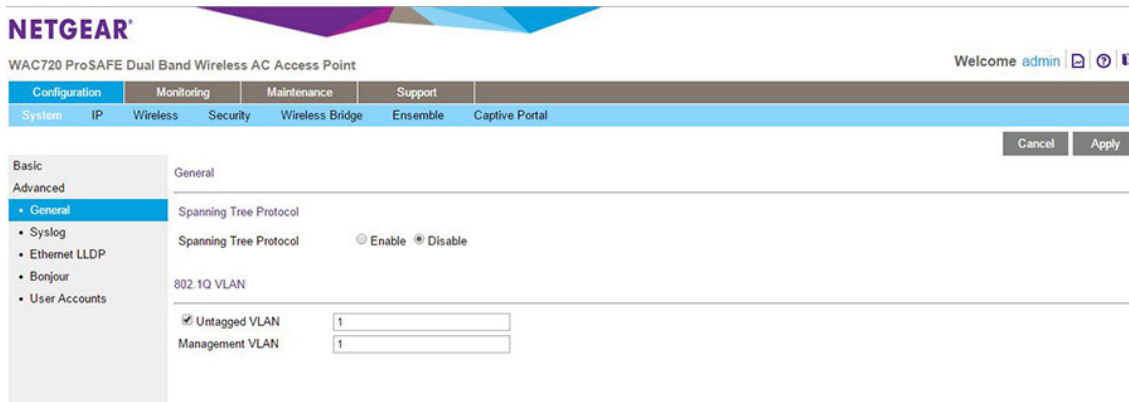
Note Select the **Untagged VLAN** check box only if the hubs and switches on your LAN support the 802.1Q VLAN protocol. Likewise, change the untagged VLAN value only if the hubs and switches on your LAN support the 802.1Q VLAN protocol.

- **Tagged VLAN.** When you clear the **Untagged VLAN** check box, the access point tags all frames that are sent from its Ethernet interface. Only incoming frames that are tagged with known VLAN IDs are accepted.
- **Management VLAN.** The management VLAN can be active only when the access point functions as a point-to-point or point-to-multipoint bridge (see [Configure WiFi Bridging](#) on page 132). The management VLAN is used for managing traffic (Telnet, SNMP, and HTTP) to and from the access point.

Frames belonging to the management VLAN are not given any 802.1Q header when they are sent over the trunk. If a port is in a single VLAN, it can be untagged. However, if the port is a member of multiple VLANs, it must be tagged.

► To configure STP and VLANs:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuring > System > Advanced > General**.



5. Specify the settings as described in the following table.

Setting	Description
Spanning Tree Protocol	
Spanning Tree Protocol	Select the Enable radio button to enable STP to prevent path redundancy. By default, the Disable radio button is selected.

Configure Advanced Network and WiFi Features

(Continued)

Setting	Description
802.1Q VLAN	
Untagged VLAN	Select the Untagged VLAN check box to configure one VLAN as an untagged VLAN. By default, the Untagged VLAN check box is selected. Specify a VLAN ID. The default VLAN ID is 1.
Management VLAN	Specify an ID for the VLAN from which the access point can be managed. The default VLAN ID is 1. If you configure the management VLAN ID as 0 (zero), the access point can be managed over any VLAN, and frames that belong to the management VLAN are not tagged with an 802.1Q header when sent over the trunk.



WARNING:

Selecting the Untagged VLAN check box or changing the untagged VLAN value causes loss of IP connectivity if the hubs and switches on your LAN are not yet configured with the corresponding VLAN.

- Click the **Apply** button.
Your settings are saved.

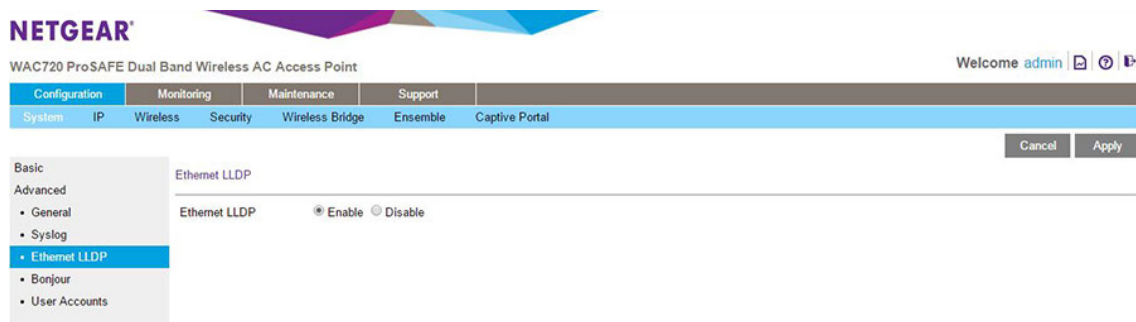
Configure Ethernet LLDP

Link Layer Discovery Protocol (LLDP), IEEE 802.1ab, is a management tool that delivers link-layer messages to adjacent network devices. For example, LLDP messages enable networking devices such as switches and management tools to discover the access point in the network, and might indicate whether the access point receives power through a PoE connection. LLDP is inter-vendor compatible. By default, LLDP is enabled on the access point.

► **To turn off LLDP:**

- Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
- In the address bar, enter the IP address of the access point.
A login window opens.
- Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Configuring > System > Advanced > Ethernet LLDP**.



5. Select the **Disable** radio button.
By default, the **Enable** radio button is selected.
6. Click the **Apply** button.
Your settings are saved.

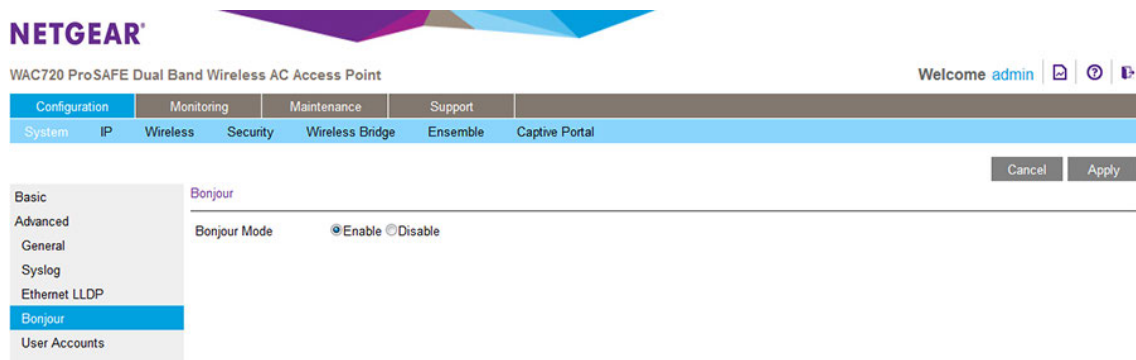
Configure Bonjour

Bonjour allows computers on the network to discover the access point more easily after it connects to a LAN that includes a DHCP server.

By default, Bonjour is enabled on the access point.

► To disable Bonjour:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > Advanced > Bonjour**.



5. Select the **Disable** radio button.
6. Click the **Apply** button.
Your settings are saved.

Configure Advanced WiFi Settings

You can enable various WLAN features and configure WLAN settings for the 802.11b/bg/ng and 802.11a/na modes.

The default WLAN settings normally work well. However, you can use the advanced settings to fine-tune the overall performance of the access point for your specific environment.

► To configure advanced WiFi settings:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Wireless > Advanced > Wireless Settings**.

Dual-Band Wireless AC Access Point WAC720 and WAC730 User Manual

The screenshot shows the Netgear configuration interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The 'Wireless Settings' section is active, showing configuration for two radio bands: 802.11 b/g/n and 802.11 a/a-na-ac. The 'Antenna' setting is set to 'Internal' (selected) and 'External'. The 'CTF' (Calibration Training Frame) setting is set to 'Enabled' (selected). Other settings include RTS Threshold (65535), Fragmentation Length (2346), Beacon Interval (100), AMPDU (Enable), RIFS Transmission (Disable), DTIM Interval (2), 802.11d (checked), Max. Wireless Clients (200), Frame Burst (Disable), Fixed Multicast Rate (Auto), Broadcast/Multicast Rate Limiting (checked), Rate Limit (50), Rate Limit Burst (75), and 802.11n 256 QAM (unchecked).

The previous figure shows part of the page.

5. Select an Antenna radio button to specify whether the settings apply to the default internal antenna or to one or more optional external antennas:
 - **Internal.** Enables the internal antenna. This is the default setting.
 - **External.** Enables an optional external antenna or antennas.
6. If you want to disable the calibration training frame (CTF) for the antenna, clear the **CTF** radio button. By default, the CTF radio button is selected and we recommend that you keep the CTF enabled. Disabling the CTF reduces the throughput and performance of the access point and causes connected users to experience slow Internet access.
7. Specify the settings as described in the following table.

Dual-Band Wireless AC Access Point WAC720 and WAC730 User Manual

Setting	Description
RTS Threshold (0–2347)	<p>Enter the Request to Send (RTS) threshold. The default setting is 2347.</p> <p>If the packet size is equal to or less than the RTS threshold, the access point uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism, and the data frame is transmitted immediately after the silence period.</p> <p>If the packet size is larger than the RTS threshold, the access point uses the CSMA with Collision Avoidance (CSMA/CA) mechanism. In this situation, the transmitting station sends an RTS packet to the receiving station and waits for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data.</p>
Fragmentation Length (256–2346)	<p>Enter the maximum packet size that is used for the fragmentation of data packets. Packets that are larger than the specified fragmentation length are broken up into smaller packets before being transmitted. The fragmentation length must be an even number. The default setting is 2346.</p>
Beacon Interval (100–1000)	<p>Enter the interval between 100 ms and 1000 ms for each beacon transmission, which allows the access point to synchronize the WiFi network. The default setting is 100.</p>
AMPDU	<p>Select the Enable radio button to allow the aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabling the aggregated MAC protocol data unit (A-MPDU) could lead to better network performance. By default, the Enable radio button is selected.</p>
RIFS Transmission	<p>Select the Enable radio button to allow transmission of successive frames at different transmit powers. Enabling reduced interframe space (RIFS) could lead to better network performance. By default, the Disable radio button is selected.</p>
DTIM Interval (1–255)	<p>Enter the delivery traffic indication message (DTIM) interval, also referred to as the data beacon rate, which indicates the beacon delivery traffic indication message period in multiples of beacon intervals. This value must be between 1 and 255. The default setting is 3.</p>
802.11d This setting does not apply to the 802.11a/a-na-ac modes.	<p>Select this check box to enable support for additional regulatory domains that are not in the current standard; support includes the addition of a country information element to beacons, probe requests, and probe responses. This check box is selected by default.</p>
Max. Wireless Clients	<p>Enter the maximum number of WiFi clients that can simultaneously connect to the access point at one time. The default setting is 200 clients.</p>
Frame Burst	<p>Select the Enable radio button to allow frame burst. Frame burst can boost the downstream throughput. By default, the Disable radio button is selected.</p>
Fixed Multicast Rate	<p>Select the multicast traffic transmission rate you want the AP to support. The default value is Auto. For the 2.4 GHz radio, the Auto value is 1 Mbps. For the 5 GHz radio, the Auto value is 6 Mbps.</p>
Broadcast/Multicast Rate	<p>Enabling multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network.</p> <p>By default the Multicast/Broadcast Rate Limiting check box is selected and you can configure the rate limit and rate limit burst.</p>
Rate Limit	<p>For multicast and broadcast rate limiting, the default and maximum rate limit setting is 50 packets per second. The supported range is from 1 to 50 pps.</p>

(Continued)

Setting	Description
Rate Limit Burst	For multicast and broadcast rate limiting, The default and maximum rate limit burst setting is 75 packets per second. The supported range is from 1 to 75 pps.
802.11n 256 QAM This setting does not apply to the 802.11a/a-na-ac modes.	Select the 802.11n 256 QAM check box to enable the 2.4 GHz radio to function over 256-quadrature amplitude modulation (QAM). By default, 256-QAM is enabled for the 5 GHz radio but the 2.4 GHz radio is not enabled to function over 256-QAM, that is, the check box is cleared.

- Click the **Apply** button.
Your settings are saved.

Configure Advanced Quality of Service Settings

For most networks, the default Quality of Service (QoS) queue settings work well. For information about how to configure basic QoS, see [Configure Basic WiFi Quality of Service](#) on page 59.

You can specify the settings on multiple queues for increased throughput and better performance of differentiated WiFi traffic such as Voice over IP (VoIP), other types of audio, video, and streaming media, as well as traditional IP data.

The advanced QoS options on the access point are as follows:

- AP EDCA parameters.** Specify the access point (AP) Enhanced Distributed Channel Access (EDCA) settings for different types of data transmitted from the access point to WiFi clients.
- Station EDCA parameters.** Specify the station EDCA parameters for different types of data transmitted from the WiFi clients to the access point. If WMM is disabled, you cannot configure the Station EDCA parameters. (For information about how to enable WMM, see [Configure Basic WiFi Quality of Service](#) on page 59.)

When you configure the EDCA settings, the access point can leverage existing information in the IP packet header that is related to the Type of Service (ToS). The access point examines the ToS field in the headers of all packets that it processes. Based on the value in a packet's ToS field, the access point prioritizes the packet for transmission by assigning it to one of the queues. A different type of data is associated with each queue. You can configure how the access point treats each queue.

The queues defined for different types of data transmitted from AP-to-station and station-to-AP are as follows:

- Data 0 (Best Effort).** Medium priority queue, medium throughput and delay. Most traditional IP data is 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 2 (Video).** Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
- Data 3 (Voice).** Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.

► To configure advanced QoS:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Wireless > Advanced > QoS Settings**.

NETGEAR
WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration | Monitoring | Maintenance | Support

System | IP | Wireless | Security | Wireless Bridge | Ensemble | Captive Portal

Cancel | Apply

Basic
Advanced

- Wireless Settings
- QoS Settings
- QoS Policies
- Load Balancing

QoS Settings - 802.11 b/g/n

AP EDCA parameters

Queue	AIFS	cwMin	cwMax	Max.Burst
Data 0 (Voice)	1	3	7	1.5
Data 1 (Video)	1	7	15	3.0
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Station EDCA parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 0 (Voice)	2	3	7	47
Data 1 (Video)	2	7	15	94
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

QoS Settings - 802.11 a/a-na-ac

AP EDCA parameters

Queue	AIFS	cwMin	cwMax	Max.Burst
Data 0 (Voice)	1	3	7	1.5
Data 1 (Video)	1	7	15	3.0
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Station EDCA parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 0 (Voice)	2	3	7	47
Data 1 (Video)	2	7	15	94
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

5. Specify the settings as described in the following table.

Setting	Description
AP EDCA parameters	
AIFS	Enter the Arbitration Inter-Frame Spacing (AIFS) interval that specifies the wait time (in milliseconds) between data frames. A higher AIFS value means a higher priority for a queue. Valid values for AIFS are 0 through 8. The default values are Data 0: 3; Data 1: 7; Data 2: 1; Data 3: 1.

(Continued)

Setting	Description
cwMin	<p>Enter the minimum contention window (cwMin) value that 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 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023.</p> <p>The default values are Data 0: 15; Data 1: 15; Data 2: 7; Data 3: 3.</p>
cwMax	<p>Enter the maximum contention window (cwMax) value that specifies the upper limit (in milliseconds) 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 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023.</p> <p>The default values are Data 0: 63; Data 1: 1023; Data 2: 15; Data 3: 7.</p>
Max. Burst	<p>Enter the maximum burst value that specifies the maximum burst length (in microseconds) allowed for packet bursts on the WiFi 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 all multiples of 32 between 0 and 8192, inclusive of 0 and 8192.</p> <p>The default values are Data 0: 0; Data 1: 0; Data 2: 3008; Data 3: 1504.</p>
Station EDCA parameters	
AIFS	<p>Enter the Arbitration Inter-Frame Spacing (AIFS) interval that specifies the wait time (in milliseconds) between data frames. A higher AIFS value means a higher priority for a queue. Valid values for AIFS are 0 through 8.</p> <p>The default values are Data 0: 3; Data 1: 7; Data 2: 2; Data 3: 2.</p>
cwMin	<p>Enter the minimum contention window (cwMin) value that 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 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023.</p> <p>The default values are Data 0: 15; Data 1: 15; Data 2: 7; Data 3: 3.</p>
cwMax	<p>Enter the maximum contention window (cwMax) value that specifies the upper limit (in milliseconds) 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 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023.</p> <p>The default values are Data 0: 1023; Data 1: 1023; Data 2: 15; Data 3: 7.</p>
TXOP Limit	<p>Enter the transmission opportunity (TXOP) value that specifies the time interval (in microseconds) in which a client station can initiate transmissions on the WiFi medium (WM). Decreasing this value increases the priority of the queue. Valid values for TXOP Limit are all multiples of 32 between 0 and 8192, inclusive of 0 and 8192.</p> <p>The default values are Data 0: 0; Data 1: 0; Data 2: 3008; Data 3: 1504.</p>

6. Click the **Apply** button.
Your settings are saved.

Configure and Manage Quality of Service Policies

The access point lets you configure and apply QoS policies to WiFi clients. In each QoS policy, you can specify multiple classifications (match clauses) and apply traffic to eight priority queues based on the following information in the Layer 2, Layer 3, Layer 3 IP headers, and Layer 4:

- **IP precedence.** Indicates the IP Type of Service (ToS) or precedence in the IP headers.
- **IP DSCP.** Indicates the Differentiated Services Code Point (DSCP) marking in the IP header.
- **IP protocol 119.** Indicates the IP protocol field in the IP header with value 119.
- **802.1P.** Indicates the 3-bit Class of Service (CoS) field in the class header.
- **IP protocol.** Indicates the protocol field in the IP header.
- **EtherType.** Indicates the EtherType field in Ethernet-II frame header.
- **Source MAC.** Indicates the source MAC address in Ethernet-II frame header.
- **Destination MAC.** Indicates the destination MAC address in Ethernet-II frame header.
- **Source IP.** Indicates the source IP address in the IP header.
- **Destination IP.** Indicates the destination IP address in the IP header.
- **Source port.** Indicates the source port number in the port header.
- **Destination port.** Indicates the destination port number in the port header.

For each classification in a QoS policy, you can configure rate limiting by specifying the maximum bit rate and maximum burst rate. Packets that exceed the maximum bit rate are retained in the traffic queue and are processed when transmission falls again below the maximum bit rate. You can also configure the overall maximum bit rate and maximum burst rate for the entire WiFi interface.

Configure a New QoS Policy

You can configure up to eight QoS policies.

► To configure a new QoS policy:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Configuration > Wireless > Advanced > QoS Policies**.

You can configure QoS policies for 802.11 bg/ng/bgn devices, 802.11 a/a-na-ac devices, or both types of devices.

5. From the Create Policy menu, select **NEW**.
If you did not yet set up any QoS policies, **NEW** is the only selection possible.
6. In the **Policy Name** field, enter a name for the new QoS policy.
7. Specify a classification for the QoS policy as described in the following table.

Note Depending on your selection from the **Match Frame Fields** menu, **Match Classifications** appears either as a menu from which you must make a selection or as a field in which you must enter information.

Setting	Description	
Match Frame Fields and Match Classifications	IP Precedence	<p>From the Match Classifications menu, select the DSCP traffic class against which the information in the IP header must be matched:</p> <ul style="list-style-type: none"> • Routine(0) • Priority(1) • Immediate(2) • Flash(3) • Flash Override(4) • Critic/CCP(5) • Inter Control(6) • Network Control(7)
Match Frame Fields and Match Classifications (continued)	IP DSCP	<p>From the Match Classifications menu, select the DSCP marking against which the information in the IP header must be matched:</p> <ul style="list-style-type: none"> • Best Effort • Assured Forwarding - Class 1 Low • Assured Forwarding - Class 1 Medium • Assured Forwarding - Class 1 High • Assured Forwarding - Class 2 Low • Assured Forwarding - Class 2 Medium • Assured Forwarding - Class 2 High • Assured Forwarding - Class 3 Low • Assured Forwarding - Class 3 Medium • Assured Forwarding - Class 3 High • Assured Forwarding - Class 4 Low • Assured Forwarding - Class 4 Medium • Assured Forwarding - Class 4 High • Class Selector 1 • Class Selector 2 • Class Selector 3 • Class Selector 4 • Class Selector 5 • Class Selector 6 • Class Selector 7 • Expedited Forwarding

(Continued)

Setting	Description	
Match Frame Fields and Match Classifications (continued)	IP Protocol 119	Traffic is matched against value 119 in the IP protocol field in the IP header.
Match Frame Fields and Match Classifications (continued)	802.1P	<p>From the Match Classifications menu, select the CoS priority value against which the information in the IP header must be matched:</p> <ul style="list-style-type: none"> • Routine(0) • Priority(1) • Immediate(2) • Flash(3) • Flash Override(4) • Critic/CCP(5) • Inter Control(6) • Network Control(7)
Match Frame Fields and Match Classifications (continued)	IP Protocol	<p>In the Match Classifications field, enter the IP protocol value against which the information in the IP header must be matched. A list of protocol values is available at http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml.</p>
Match Frame Fields and Match Classifications (continued)	Ether Type	<p>In the Match Classifications field, enter the Ether type value against which the information in the IP header must be matched. A list of Ether type values is available at http://standards.ieee.org/develop/regauth/ethertype/eth.txt.</p>
Match Frame Fields and Match Classifications (continued)	Source MAC	<p>In the Match Classifications field, select or enter the source MAC address against which the information in the IP header must be matched.</p> <p>To select the MAC address of a WiFi client that is connected to the access point:</p> <ol style="list-style-type: none"> a. Select the radio button to the left of the Match Classifications menu. b. From the menu, select a MAC address. <p>To enter a MAC address:</p> <ol style="list-style-type: none"> a. Select the radio button to the right of the Match Classifications menu. b. In the field to the right of the radio button, enter a MAC address.

(Continued)

Setting	Description	
Match Frame Fields and Match Classifications (continued)	Destination MAC	In the Match Classifications field, select or enter the destination MAC address against which the information in the IP header must be matched. To select the MAC address of a WiFi client that is connected to the access point: a. Select the radio button to the left of the Match Classifications menu. b. From the menu, select a MAC address. To enter a MAC address: a. Select the radio button to the right of the Match Classifications menu. b. In the field to the right of the radio button, enter a MAC address.
Match Frame Fields and Match Classifications (continued)	Source IP	In the Match Classifications field, enter the source IP address against which the information in the IP header must be matched.
Match Frame Fields and Match Classifications (continued)	Destination IP	In the Match Classifications field, enter the destination IP address against which the information in the IP header must be matched.
Match Frame Fields and Match Classifications (continued)	Source Port	The Match Classifications field is separated into two sections. In the left section, enter the source port number, and optionally, in the right section, enter the associated IP address against which the information in the IP header must be matched.
Match Frame Fields and Match Classifications (continued)	Destination Port	The Match Classifications field is separated into two sections. In the left section, enter the destination port number, and optionally, in the right section, enter the associated IP address against which the information in the IP header must be matched.
Apply Classification	From the Apply Classification menu, select the traffic class that must be applied to the packets that match the selection in the Match Classifications field: <ul style="list-style-type: none"> • Best Effort(0) • Background(1) • Spare(2) • Excellent(3) • Control Load(4) • Video < 100 ms Latency(5) • Voice < 10 ms Latency(6) • Network Control(7) 	

8. (Optional) Specify rate limiting for the classification as described in the following table.

Setting	Description	
Classification Rate Limiting	Basic Rate	<p>Enter a value between 1 and 1,000,000 Kbytes/sec to specify the maximum data rate up to which packets that match the classification are queued for transmission and sent immediately over the WiFi interface. This value applies only to traffic that matches the classification.</p> <hr/> <p>Note When the maximum rate is exceeded, packets are retained in the queue and sent when the transmission falls again below the maximum rate.</p> <hr/>
	Burst Rate	<p>Enter a value between 1 and 204,800,000 bytes to specify the maximum amount of data that can be transmitted in a burst for packets that match the classification. This value applies only to traffic that matches the classification.</p>

9. Click the **Add** button.
The classification is added to the Classifications field.
10. To add another classification to the QoS policy, repeat Step 7, Step 8, and Step 9.
11. Click the **Apply** button.
The QoS policy is saved.

Note Rate limiting for the WiFi interface is an optional setting that applies to all traffic on the WiFi interface. Unlike classification rate limiting, which you can specify for each classification, rate limiting for the WiFi interface you must specify only once.

Modify a QoS Policy

▶ To modify a QoS policy:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Wireless > Advanced > QoS Policies**.
The QoS Policies page displays.
5. From the **Create Policy** menu, select the policy that you want to modify.
6. To modify a classification, you must delete the classification and add a new classification:

- a. In the **Classification** field, select the old classification.
- b. Click the **Delete Classification** button.
- c. Add a new classification.

For information about how to add a classification, see Step 7 through Step 9 in the procedure to configure a new QoS policy.

7. To change the name of the policy, in the **Policy Name** field, enter a new name for the QoS policy.
8. Click the **Apply** button.
Your settings are saved.

Delete a QoS Policy

► To delete a QoS policy:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Wireless > Advanced > QoS Policies**.
The QoS Policies page displays.
5. From the **Create Policy** menu, select the policy that you want to delete.
6. Click the **Delete Policy** button.
7. Click the **Apply** button.
Your settings are saved.

Configure Load Balancing

You can set network utilization thresholds on the access point to maintain the speed and performance of the WiFi network as clients associate with and disassociate from the access point. The load balancing settings apply to both radios.

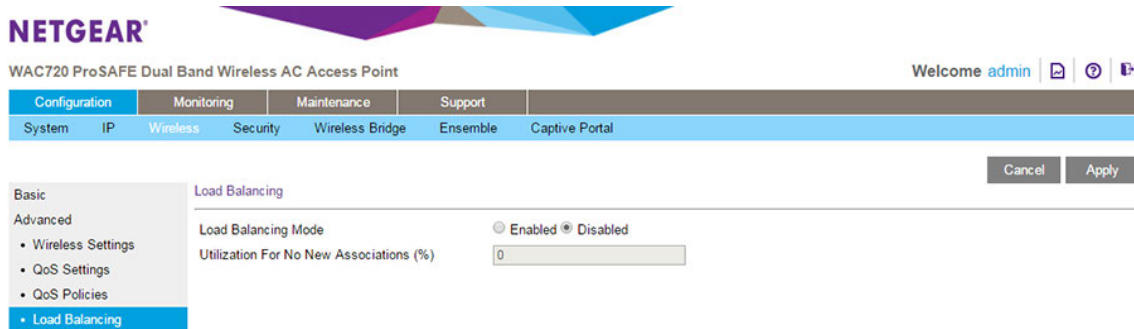
As an option, you can specify the percentage of network bandwidth utilization that is allowed on a radio before the access point stops accepting new client associations. Whether client associations are allowed depends on the specified percentage and the WLAN utilization of the radio:

- New client associations are allowed if the radio's WLAN utilization is lower than the specified percentage of network bandwidth utilization.
- New client associations are prevented if the radio's WLAN utilization is higher than the specified percentage of network bandwidth utilization.

For more information about the WLAN utilization, see [View the Standalone Dashboard](#) on page 80.

▶ To enable and configure load balancing:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Wireless > Advanced > Load Balancing**.



5. To enable load balancing, select the **Enabled** radio button.
By default, the **Disabled** radio button is selected and load balancing is disabled.
6. In the **Utilization For No New Associations (%)** field, enter the percentage of network bandwidth utilization that is allowed on the radios before the access point stops accepting new client associations.
The default is 0, which means that all new associations are allowed, regardless of the utilization rate.
7. Click the **Apply** button.
Your settings are saved.

Manage Captive Portals

A captive portal requires users to log in through a special login page (splash page, also referred to as web locale) so that guests or users with a valid user name and password can access the Internet through the access point.

The access point supports two captive portal instances (NETGEAR and NETGEAR-1). You can create up to six splash pages (three per captive portal profile). However, for each captive portal instance, only one splash page can be active at any time.

The following sections describe chronologically the procedures that are involved in setting up a captive portal:

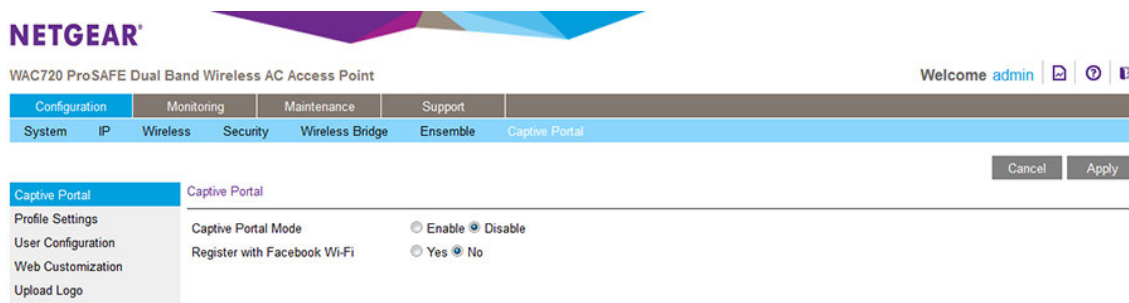
1. If you want to use the Facebook Wi-Fi capability as an authentication mode, do the following:
 - a. *Enable the Access Point to Register With Facebook* on page 121
 - b. *Set Up Facebook Wi-Fi for a Captive Portal Profile* on page 124
2. *Specify Captive Portal Profile Settings and Enable the Captive Portal Instance* on page 121
For each captive portal instance that you want to be available, you must specify the protocol, whether users are redirected to a specific website, the time-outs, and the authentication mode.
3. *Add User Accounts to the Local Database for Captive Portal Access* on page 126
If a captive portal instance uses the local database for user authentication, you must add a user account to the local database for each user that you want to grant access through the captive portal. You do not need to add users accounts to the local user database if the authentication for a captive portal instance is configured for guest access or uses a RADIUS server.
4. (Optional) *Upload a Custom Logo* on page 128
Follow this procedure only if you want to be able to select a custom logo when you configure a custom splash page.
5. *Configure a Default or Custom Captive Portal Splash Page* on page 129
You can use the default splash page that the access point provides or set up a custom splash page.
6. *Enable the Global Captive Portal Mode* on page 131
You only need to enable the captive portal mode once on the access point. After the mode is enabled, it applies to both captive portal instances.
7. Select one of the captive portal instances for a WiFi security profile (see *Configure and Enable WiFi Security Profiles* on page 39).
After you select the captive portal instance for a WiFi security profile, the WiFi network that is associated with the WiFi security profile becomes accessible only through the captive portal.

Enable the Access Point to Register With Facebook

Before you can set up Facebook Wi-Fi on the access point so that you can provide customers WiFi access by letting them check in to a Facebook business page (see *Specify Captive Portal Profile Settings and Enable the Captive Portal Instance* on page 121), you must enable the access point to register with Facebook. By default, the capability to register is disabled.

► To enable the capability to register with Facebook Wi-Fi:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see *Log In to the Access Point* on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Captive Portal > Captive Portal**.



5. Select the Register with Facebook Wi-Fi **Yes** radio button.
6. Click the **Apply** button.
Your settings are saved.

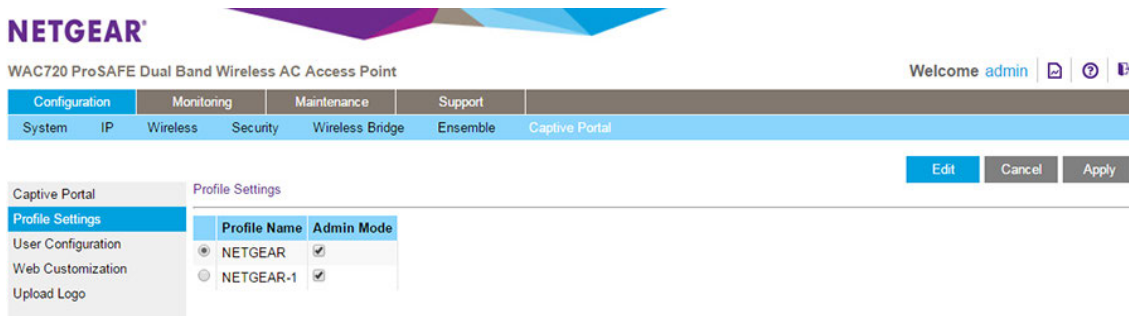
Specify Captive Portal Profile Settings and Enable the Captive Portal Instance

For each of the two captive portal instances (NETGEAR and NETGEAR-1), you can specify the type of captive portal (HTTP or HTTPS), whether users are redirected to a website, the idle time-out settings, and the user authentication mode.

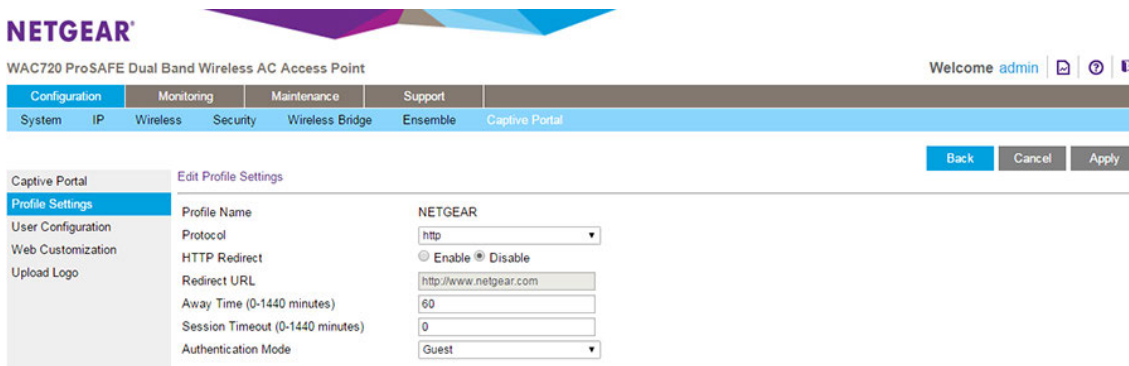
In addition, make sure that the captive portal instance is administratively enabled.

► **To specify captive profile settings and enable a captive portal instance:**

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Captive Portal > Profile Settings**.



5. Select the radio button to the left of the profile name for the captive portal.
6. Click the **Edit** button.



7. Specify the profile settings as described in the following table.

Field	Description
Profile Name	This is a nonconfigurable field that shows the profile name that is used for the captive portal.
Protocol	From the Protocol menu, specify the protocol that is used for the captive portal (http or https).
HTTP Redirect	To specify a website to which users are redirected, select the Enable radio button. By default, the Disable radio button is selected.

(Continued)

Field	Description
Redirect URL	<p>If the Enable radio button is selected, enter the website or enter the IP v4 or IPv6 address:</p> <ul style="list-style-type: none"> • IPv4 address. Must be in a format similar to <code>http://xxx.xxx.xxx.xxx</code>, for example, <code>http://192.0.2.10</code>. • IPv6 address. Must be in a format similar to <code>http://[xxxx:xxxx:xxxx:xxxx::xxxx:xxxx:xxxx:xxxx:xxxx]</code>, for example, <code>http://[2001:DB8::CAD5:7D91]</code>.
Away Time (0-1440 minutes)	<p>Enter the period during which a user remains in the authenticated client list after the user disassociates from the captive portal. If the period expires before the user attempts to reauthenticate, the entry is removed from the authenticated client list.</p> <p>The range is from 0 to 1440 minutes. The default period is 60 minutes.</p>
Session Timeout (0-1440 minutes)	<p>Enter the period after which a captive portal session is automatically terminated and a user is logged out.</p> <p>The range is from 0 to 1440 minutes. The default value is 0, which effectively disables the session time-out.</p> <hr/> <p>Note If you select Facebook Wi-Fi from the Authentication Mode menu (see Step 8), the session time-out overrides the session length value that you configure on the Facebook Wi-Fi Configuration page.</p> <hr/>

8. From the **Authentication Mode** menu, select the authentication database against which captive portal users are authenticated:

- **Guest.** Although guest users must enter a name, they are not authenticated for the captive portal. These users are not in the local database or the database on a RADIUS server. This mode is suitable for an open network, for example, a hotspot with free access. However, if the network is not open, users must enter the passphrase or password that is associated with the WiFi security profile (see *Configure and Enable WiFi Security Profiles* on page 39).
- **Local.** Users are authenticated against the local database. You must add each user to the local database (see *Add User Accounts to the Local Database for Captive Portal Access* on page 126). This mode is suitable for a secured WiFi network with returning users.
- **Radius.** Users are authenticated against the database on a RADIUS server. The user information must be in the database. This mode is suitable for a secured WiFi network with returning users. Specify the following settings so that the access point can reach the RADIUS server
 - **Radius IP Network.** From the menu, select **ipv4** or **ipv6**.
 - **Primary Authentication IP.** Enter the IPv4 or IPv6 address for the primary RADIUS server.
 - **Secondary Authentication IP.** Enter the IPv4 or IPv6 address for the secondary RADIUS server. This setting is optional.

- **Primary Authentication Key.** Enter the shared key that is used between the access point and the primary RADIUS server during authentication.
 - **Secondary Authentication Key.** Enter the shared key that is used between the access point and the secondary RADIUS server during authentication. This setting is required only if you specify a secondary RADIUS server.
- **Facebook Wi-Fi.** You can set up Facebook Wi-Fi on the access point so that you can provide customers WiFi access by letting them check in to a Facebook business page. For more information, see [Set Up Facebook Wi-Fi for a Captive Portal Profile](#) on page 124.
9. Click the **Apply** button.
Your settings are saved.
 10. Click the **Back** button.
The Profile Settings page displays again.
 11. Make sure that the **Admin Mode** check box is selected for the selected captive portal instance so that the instance is administratively enabled and becomes available after you select it for a WiFi profile (see [Configure and Enable WiFi Security Profiles](#) on page 39).
If the **Admin Mode** check box is cleared, the captive portal instance is administratively disabled and does not become available after you select the instance for a WiFi security profile.
 12. Click the **Apply** button.
The captive portal instance is administratively enabled.

Set Up Facebook Wi-Fi for a Captive Portal Profile

You can set up a captive portal on a WiFi network to offer free access through check-in to a Facebook business page. Make sure that the capability to register with Facebook is enabled (see [Enable the Access Point to Register With Facebook](#) on page 121).



ATTENTION:

After you add a captive portal for Facebook Wi-Fi, the associated portal splash page might not open under some circumstances, allowing users Internet access without logging in. This security limitation is implemented by Facebook Wi-Fi, not by NETGEAR. If a user opens a browser and attempts to access a website over HTTP (by default, over port 80), the user is directed to the splash page. However, if a user attempts to access a website that does not use HTTP, the splash page might not open and the user can access the website without logging in. For example, this situation occurs if a user opens a browser and accesses a secure website over HTTPS (by default, over port 443), or if an application uses HTTPS to send traffic to the Internet.

► To set up Facebook Wi-Fi:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Captive Portal > Profile Settings**.
The Profile Settings page displays.
5. Select the radio button to the left of the WiFi network name (SSID) with which you want to associate the captive portal.
6. Click the **Edit** button.
The Edit Profile Settings page displays.
7. From the **Authentication Mode** menu, select **Facebook Wi-Fi**.
The page adjust and displays the **Add Page** button.
8. Click the **Add Page** button.
The Facebook Login page displays.
9. Log in to a Facebook account.

Facebook Wi-Fi Configuration

Facebook Page
To use Facebook Wi-Fi you need to be the admin of a local business Page that has a valid location associated with it.
Select a Page ▾

Bypass Mode
Your customers always have the option to skip checking in. They can do this by clicking on a link that lets them skip check-in, or by entering a Wi-Fi code that you provide to them.
 Skip check-in link (?)
 Require Wi-Fi code (?)

Session Length
Select the length of time your customers will have Wi-Fi for after they check in.
Five hours ▾

Terms of Service
 Optional: Add your own Terms of Service (?)

[Visit Help Center](#) **Save Settings**

10. From the **Select a Page** menu, select a Facebook business page.
11. Select the bypass mode option:
 - To allow customers to skip check-in, select the **Skip check-in link** radio button.

If you enable this option, users can either check in to the selected Facebook business page or skip the check-in.

- To require users to enter a WiFi code before they can gain WiFi access, select the **Require Wi-Fi code** radio button and type a WiFi code in the field that displays.
If you enable this option, users can either check in to the selected Facebook business page or skip the check-in by using the WiFi code.

12. From the **Session Length** menu, select the period after which users are automatically logged out.

13. To add terms of service to the Facebook check-in page, select the **Terms of Service** check box and type or copy the terms of service.

14. Click the **Save Settings** button.

The Facebook Wi-Fi settings are saved.

The name of the selected Facebook business page displays on the Facebook Wi-Fi configuration page, along with the **Change Page** button, which lets you replace the selected Facebook business page with another one.

15. On the Edit Profile Settings page, click the **Apply** button.

Your settings are saved.

16. Click the **Back** button.

The Profile Settings page displays again.

17. Make sure that the **Admin Mode** check box is selected for the selected captive portal instance so that the instance is administratively enabled and becomes available after you select it for a WiFi profile (see *Configure and Enable WiFi Security Profiles* on page 39).

If the **Admin Mode** check box is cleared, the captive portal instance is administratively disabled and does not become available after you select the instance for a WiFi security profile.

18. Click the **Apply** button.

The captive portal instance is administratively enabled.

Add User Accounts to the Local Database for Captive Portal Access

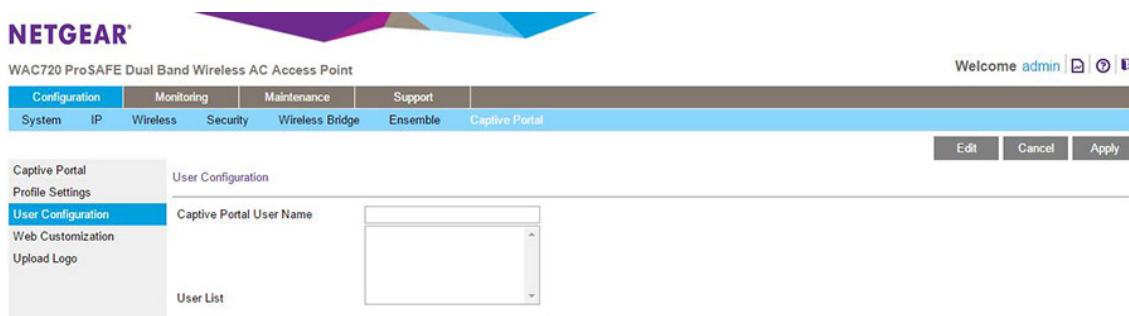
Note You do not need to add users accounts to the local user database if the authentication for a captive portal instance is configured for guest access or uses a RADIUS server.

If a captive portal instance uses the local database for authentication (see *Specify Captive Portal Profile Settings and Enable the Captive Portal Instance* on page 121), you must add a user account to the local database for each user that you want to grant access through the captive portal.

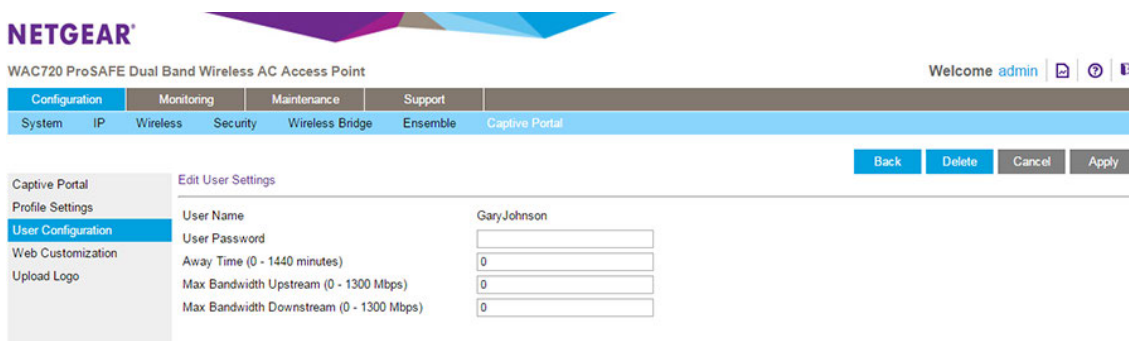
A user who wants to log in through the captive portal must use the user name and password that you assign to him or her.

► **To add a user account to the local database for a captive portal:**

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Captive Portal > User Configuration**.



5. Enter the name of the user in the **Captive Portal User Name** field.
6. Click the **Apply** button.
The user is added.
7. Select the user from the user list.
8. Click the **Edit** button.



9. In the **User Password** field, enter a password.
The user must use the assigned user name and password to gain access through the captive portal.
10. In the **Away Time** field, enter a time-out period between 0 and 1440 minutes.
The user is logged out if they are idle longer than the time that you enter.

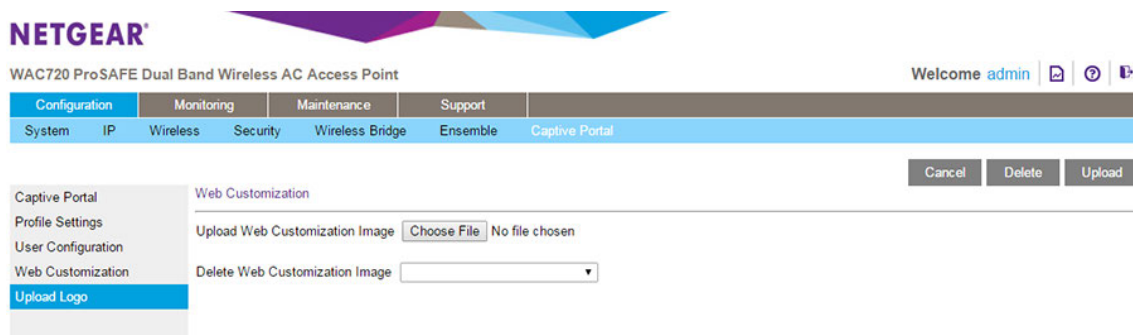
11. In the **Max Bandwidth Upstream** field, enter the maximum upstream bandwidth allowed to the user, in megabits per second.
This setting is optional.
12. In the **Max Bandwidth Downstream** field, enter the maximum downstream bandwidth allowed to the user, in megabits per second.
This setting is optional.
13. Click the **Apply** button.
Your settings are saved.

Upload a Custom Logo

If you want to use a custom logo on the splash page for captive portal, you must upload it before you can select it. If you do not need to use a custom logo, skip this procedure.

► To upload a custom logo:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Captive Portal > Upload Logo**.



5. Click the **Choose File** button.
6. Navigate to and select the logo file.
The file name including the file extension (.jpg or .gif) is limited to 32 characters and the file size cannot exceed 5 KB.
7. Click the **Upload** button.
The logo file is uploaded and is selectable when you configure the splash page for a captive portal.

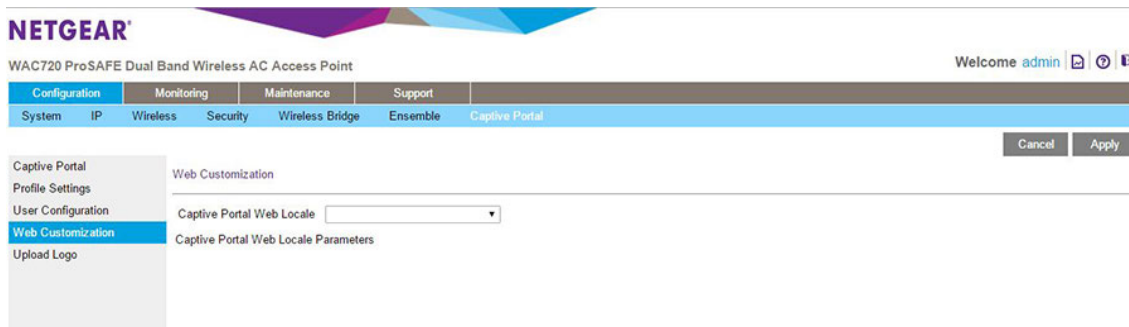
Configure a Default or Custom Captive Portal Splash Page

The splash page (also referred to as web locale) is the page that users see when they access the captive portal. You can use the default splash page that the access point provides or set up a custom splash page.

You can create up to six splash pages (three per captive portal instance). However, for each captive portal instance, only one splash page can be active at any time.

► To configure a captive portal splash page:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Captive Portal > Web Customization**.



5. From the **Captive Portal Web Locale** menu, select **Create**.
6. In the **Web Local Name** field, enter a name for the splash page.
A splash page is also referred to as web locale. This name that you specify is for internal management purposes only. A user does not see this name.
7. From the **Captive Portal Instances** menu, select the captive instance (NETGEAR or NETGEAR-1) with which the splash page must be associated.

Note You can configure up to three splash pages for the same captive portal instance but only one splash page can be the active page for a captive portal instance.

8. Click the **Apply** button.

Your settings are saved and the splash page fields display.

Captive Portal Web Locale

Captive Portal Web Locale Parameters

Instance Name	<input type="text" value="NETGEAR"/>
Logo Image Name	<input type="text" value="logo.jpg"/>
Browser Title	<input type="text" value="Captive Portal"/>
Browser Content	<input type="text" value="Welcome to the Wireless Network"/>
Content	<input type="text" value="To start using this service, enter your credentials and click the connect button."/>
Acceptance Use Policy	<input type="text" value="Acceptance Use Policy."/>
Welcome Title	<input type="text" value="Congratulations!"/>
Welcome Content	<input type="text" value="You are now authorized and connected to the network."/>
Delete Locale	<input type="checkbox"/>

- To set up a custom splash page, specify the settings as described in the following table.

Note If you want to use the default splash page settings, skip this step and go to the next step.

Field	Description
Logo Image Name	This menu displays the names of image files that you uploaded (see Upload a Custom Logo on page 128).
Browser Title	The browser title appears in the title bar of the browser.
Browser Content	This is the text that will appear on the body of the page.
Content	You can enter instructions for logging in to the portal here.
Acceptance Use Policy	Text entered here will display in a user agreement.
Welcome Title	This is the title of the welcome page that displays after the user successfully logs in.
Welcome Content	This is the content of the welcome page that displays after the user successfully logs in.

- Click the **Apply** button.
Your settings are saved.

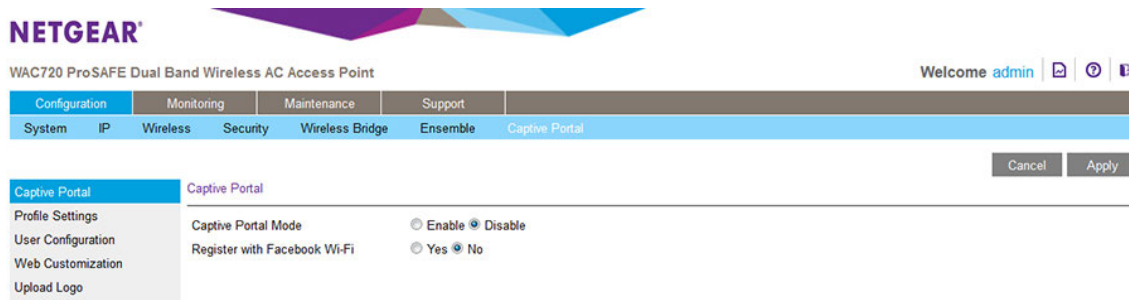
Enable the Global Captive Portal Mode

By default, the global captive portal mode is disabled on the access point. If you do not want to use a captive portal, leave the mode disabled because it globally disables captive portals on the access point.

If you do want to use a captive portal, enable the global captive portal mode. You must still enable each individual captive portal instance before it can become accessible.

► To enable the global captive portal mode:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Captive Portal > Captive Portal**.



5. Select the **Enable** radio button.
6. Click the **Apply** button.
Your settings are saved.

IMPORTANT:

Before you can use a captive portal that you configured, you must select the captive portal instance for a WiFi security profile (see [Configure and Enable WiFi Security Profiles](#) on page 39). After you do so, the WiFi network that is associated with the WiFi security profile becomes accessible only through the captive portal.

Configure WiFi Bridging

The access point supports a wireless distribution system (WDS) that lets you build large bridged WiFi networks.

Point-to-Point Bridge and Point-to-Multipoint Bridge

You can set up a single point-to-point bridge or create a point-to-multipoint bridge by setting up to four point-to-point bridges with your access point functioning as the master:

- **WiFi point-to-point bridge.** The access point communicates with another bridge-mode access point and with WiFi clients. You can use WPA2-PSK to secure the communication. The following figure shows an example in which two access points (APs) function in point-to-point bridge mode.



Figure 7. Point-to-point WiFi network

- **WiFi point-to-multipoint bridge.** The access point is the master for a group of bridge-mode access points. You can configure up to four WiFi bridges. The other bridge-mode WiFi access points must be set to point-to-point bridge mode, using the MAC address of your access point (that is, the master). Rather than communicating directly with each other, all other bridge-mode access points send their traffic to the master access point. You can use WPA2-PSK to secure the communication.



Figure 8. Point-to-multipoint WiFi network

Configure a WiFi Bridge

In bridge mode, the access point communicates with one or more other bridge-mode access points. By default, the connection is an open system but you can use WPA2-PSK security to protect this communication.

Note You cannot configure WiFi bridging when automatic channel selection is enabled. On the basic Wireless Settings page, make sure that Auto is not selected from the Channel / Frequency menu (see *Configure the Basic WiFi Settings* on page 24).

► To configure a WiFi bridge:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see *Log In to the Access Point* on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Configure the access point (AP1 on LAN Segment 1 in the previous figures) as a point-to-point bridge:
 - a. Select **Configuration > Wireless Bridge**.

NETGEAR
WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration Monitoring Maintenance Support
System IP Wireless Security Wireless Bridge Ensemble Captive Portal

Bridging

Enable Wireless Bridging

#	Profile Name	Radio	Local MAC Address	Security	Enable
1	NETGEAR-WDS-1	2.4 GHz	50:6A:03:80:58:60	Open System	<input checked="" type="checkbox"/>
2	NETGEAR-WDS-2	2.4 GHz	50:6A:03:80:58:60	Open System	<input checked="" type="checkbox"/>
3	NETGEAR-WDS-3	2.4 GHz	50:6A:03:80:58:60	Open System	<input checked="" type="checkbox"/>
4	NETGEAR-WDS-4	2.4 GHz	50:6A:03:80:58:60	Open System	<input checked="" type="checkbox"/>

- b. Select the **Enable Wireless Bridging** check box.
- c. Click the **Apply** button.
Your settings are saved and the WiFi bridging feature is enabled. However, you still must configure one or more WiFi bridges and enable them.
You can configure up to four profiles. By default, a profile does not provide security (it is an open system), but you can configure WPA2-PSK. The **Local MAC Address** field is a nonconfigurable field that shows the MAC address of the access point.
- d. Select the radio button for a profile.

- e. From the **Radio** menu, select the WiFi band (**2.4 GHz** or **5 GHz**) on which the bridge must be established.

Note Both sides of the bridge must use the same WiFi band and the same channel. If differences exist, the bridge cannot be established.

- f. Click **Edit** button.
The Edit Security Profile page displays.
- g. Specify the settings as described in the following table.

Setting	Description
Profile Definition	
Profile Name	As an option, enter a profile name that is easy to remember. The default name is NETGEAR-WDS-1.
Remote MAC Address	Enter the MAC address of the remote access point (in the previous figures, this can be the MAC address of AP2 or AP3). Without this MAC address, the WiFi bridge cannot function.
Authentication Settings	
Network Authentication and Data Encryption	If you want to secure the bridge (which is what we recommend), from the Network Authentication menu, select WPA2-PSK, This selection automatically sets the selection from the Data Encryption menu to AES (Advanced Encryption Standard). In the WPA Passphrase (Network Key) field, enter a passphrase. The passphrase length must be between 8 and 63 characters (inclusive).

- h. Click the **Apply** button.
Your settings are saved.
- i. Click the **Back** button.

The Bridging page displays again.

5. Configure another access point in point-to-point bridge mode.
Your access point must include the MAC address of the other access point in its **Remote MAC Address** field, and the other way around, the other access point must include the MAC address of your access point in its **Remote MAC Address** field.

Note Both sides of the bridge must use the same WiFi band and the same channel. If differences exist, the bridge cannot be established.

6. Verify the following settings for both access points:
- Both access points must operate in the same LAN network address range as the LAN devices.
 - Both access points must use the same channel, authentication mode, and security settings.

7. Go back to the Bridging page on your access point and select the **Enable** check box for the profile.

8. Click the **Apply** button.

Your settings are saved.

9. Enable bridging on the other access point.

10. Verify connectivity across the LAN segments.

A computer on either LAN segment must be able to connect to the Internet and share files and printers of any other computers or servers on the other LAN segment.

11. To set up a point-to-multipoint WiFi network, repeat Step 4 through Step 10 for another profile and another access point.

In point-to-multipoint WiFi network, your access point becomes the master for all WiFi bridges. For each access point that you want the master to be able to connect to, you must configure a security profile with a unique name and the MAC address of the access point. You can configure up to four such security profiles (NETGEAR-WDS-1, NETGEAR-WDS-2, and so on).

Note You can extend the range of a WiFi bridge with NETGEAR WiFi antenna accessories.

This chapter provides information about troubleshooting the access point. After each problem description, instructions are given to help you diagnose and solve the problem.

For the common problems listed, go to the section indicated.

- Is the access point on?
Go to *Troubleshoot the Basic Functions* on page 137.
- Did I connected the access point correctly?
Go to *Troubleshoot the Basic Functions* on page 137.
- I cannot access the Internet or the LAN.
Go to *You Cannot Access the Internet or the LAN From a WiFi Computer* on page 138.
- I cannot access the access point from a browser.
Go to *You Cannot Configure the Access Point From a Browser* on page 139.
- A time-out occurs.
Go to *When You Enter a URL or IP Address a Time-Out Error Occurs* on page 140.
- Problems with the LAN connection occur.
Go to *Troubleshoot a TCP/IP Network Using the Ping Utility* on page 140.
- I cannot remember the access point's configuration password.
Go to *Change the Administrator Password* on page 72.
- I want to clear the configuration and start over again.
Go to *Restore the Access Point to the Factory Default Settings* on page 69.
- The date or time is not correct.
Go to *Problems With Date and Time* on page 141.

The access point provides a packet capture tool that enables you to perform problem diagnoses. For information about how to use this tool, see *Use the Packet Capture Tool* on page 142.

Troubleshoot the Basic Functions

The following sections describe how you can troubleshoot the basic functions of the access point:

- [Verify the Correct Sequence of Events at Startup](#) on page 137
- [No LEDs Are Lit on the Access Point](#) on page 137
- [The Active LED or the LAN LED Is Not Lit](#) on page 138
- [The WLAN LED Does Not Light](#) on page 138

Note For descriptions of the LEDs, see [Top Panel](#) on page 9.

Verify the Correct Sequence of Events at Startup

- After you turn on power to the access point, check that the following sequence of events occurs:
- The Power/Test LED is first steady amber, then goes off, and then blinks green before turning steady green after about 45 seconds.
- The Active LED is lit or blinks green when Ethernet traffic is detected.
- The LAN LED indicates the LAN speed: green for 1000 Mbps, amber for 100 Mbps, and no light for 10 Mbps.
- The WLAN LED is lit or blinks green when the WiFi LAN (WLAN) is ready.

If any of these conditions does not occur, see the appropriate following section.

No LEDs Are Lit on the Access Point

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

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

- If you use one or more PoE switches to provide power to the access point, check these items:
 - Make sure that the Ethernet cables between the access point and the PoE switches are correctly connected at both ends.
 - Make sure that the power cords of the PoE switches are plugged into working power outlets or power strips.
 - Make sure that the PoE switches are functioning normally.
- If you use a power cord to provide power to the access point, check these items:

- 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 that is supplied with your access point.

The Active LED or the LAN LED Is Not Lit

A hardware connection problem occurs.

Check these items:

- Make sure that the cable connectors are securely plugged in at the access point and the network device—hub, (PoE) switches, or router.
- 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 has Auto Uplink (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

The WLAN LED Does Not Light

The access point's antenna is not working.

Check these items:

- If the WLAN LED remains off, either disconnect the cables to the PoE switches and then reconnect them again, or disconnect the adapter from its power source and then plug it in again.
- Make sure that optional external antennas are tightly connected to the access point.

Contact NETGEAR technical support if the WLAN LED remains off.

You Cannot Access the Internet or the LAN From a WiFi Computer

A configuration problem occurred.

Check these items:

- Maybe you did not restart the WiFi computer to allow TCP/IP changes to take effect. If so, restart the computer.
- The WiFi computer might not include 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.
- The access point's default values might not work with your network. Check the access point's default configuration against the configuration of other devices in your network.

- Make sure that the SSID, network authentication, and data encryption settings of the WiFi computer are the same as those of the access point.
- Ping the IP address of the access point to verify that a WiFi connection exists between the WiFi computer and the access point. If the ping fails, check the network configuration (for the access point, see [Configure the IPv4 Settings](#) on page 23).
- Ping the default gateway to verify that a path exists from the WiFi computer to the default gateway. If the ping fails, check the network configuration or call the Internet service provider (ISP).

You Cannot Configure the Access Point From a Browser

Check these items:

- The access point is correctly installed, it is powered on, and LAN connections are okay. Check to see that the Active LED and LAN LED are on to verify that the Ethernet connection is okay.
- 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 access point's default IP address is 192.168.0.100, and its subnet mask is 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 your network includes a WINS server.
- If your computer is set to obtain an IP address automatically (DHCP client), restart it.
- Make sure that Java, JavaScript, or ActiveX is enabled in your browser. If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.
- Try quitting the browser, clearing the cache, deleting the cookies, and launching the browser again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when entering this information.

If the access point does not save changes that you made in the local browser interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another page or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might occur, but the web browser might be caching the old configuration.

When You Enter a URL or IP Address a Time-Out Error Occurs

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

- Check to see whether other computers on the LAN work correctly. If they do, ensure that your computer's TCP/IP settings are correct. If you use a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP addresses of the access point (see *Configure the IPv4 Settings* on page 23).
- If the computer is configured correctly but still not working, ensure that the access point is connected and turned on. Access it and check its settings. If you cannot connect to the access point, check the LAN and power connections.
- If the access point is configured correctly, check your Internet connection (for example, your cable modem) to make sure that it is working correctly.

Troubleshoot a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your computer, as described in the following sections:

- *Test the LAN Path to Your Access Point* on page 140
- *Test the Path from Your Computer to a Remote Device* on page 141

Test the LAN Path to Your Access Point

You can ping the access point from your computer to verify that the LAN path to your access point is set up correctly.

► To ping the access point from a computer running Windows:

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the field provided, type ping followed by the IP address of the access point, as in this example:
ping 192.168.0.100

3. Click the **OK** button.

A message like the following one displays:

```
Pinging <IP address> with 32 bytes of data
```

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, one of the following problems could be occurring:

- Make sure that the Active LED and LAN LED are on. If one or both of these LEDs are off, follow the instructions in *The Active LED or the LAN LED Is Not Lit* on page 138.
- Check to see that the corresponding link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and access point.
- Wrong network configuration:
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
 - Verify that the IP address for your access point and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device.

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the field provided, enter **ping -n 10 IP address**.

where *IP address* is the IP address of a remote device such as the DNS server of your ISP.

If the path is functioning correctly, replies as in *Test the LAN Path to Your Access Point* on page 140 display. If you do not receive replies, do the following:

- Check to see that the IP address of your access point is listed as the IP address of the default router in your computer. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the access point is listed as the IP address of the default router.
- Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check to see that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name on the basis General system settings page (see *Configure Basic General System Settings* on page 20).

Problems With Date and Time

The Time Settings page that is accessible through the Configuration > System > Basic > Time menu choices displays the current date and time of day. The access point uses the Network Time Protocol (NTP) to obtain the current time from a network time server on the Internet that you specify in the Time Settings page (see *Configure Basic General System Settings* on page 20). Each entry on the Logs page is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date and time shown is Fri Dec 31 00:00:00 1999 or a similar incorrect date and time. Cause: The access point did not yet successfully reach the network time server. Check to see that your Internet

access settings are configured correctly. If you just completed configuring the access point, wait at least 5 minutes and check the date and time again.

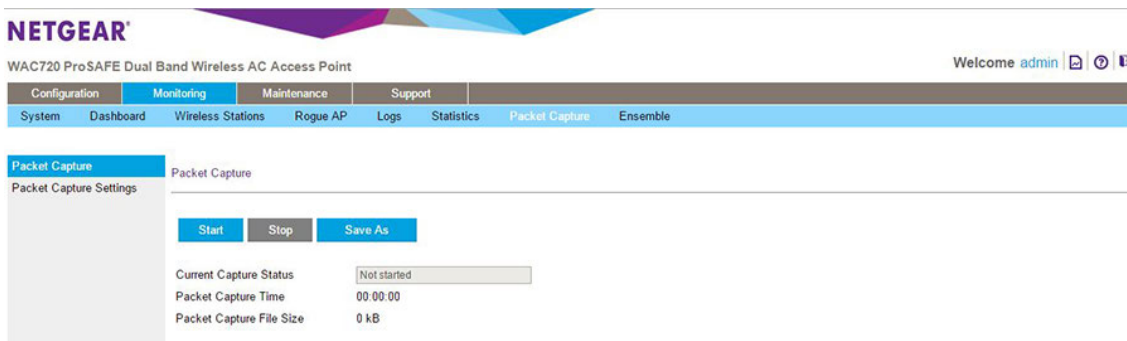
- The day is correct or one day ahead or behind, and the hours are ahead or behind. Cause: You selected an incorrect time zone for your area. Specify the correct time zone on the basic General system settings page (see [Configure Basic General System Settings](#) on page 20).

Use the Packet Capture Tool

You can capture WiFi packets to analyze traffic patterns with a network traffic analyzer tool. The captured packet flow can show if traffic is flowing correctly to its destinations or if packets are dropped. The size of the packet flow that you can capture in a file is limited.

► To capture packets:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Monitoring > Packet Capture**.



5. Click the **Start** button to start capturing WiFi packets leaving or entering the access point on the active operating channel.
Packets on the 2.4 GHz interface and 5 GHz interface are captured. Normal functioning of the access point is not affected during the packet capture process.
If any previously captured packets exist, you are prompted to delete them, and only then can you capture new packets.
6. Click the **Stop** button to stop capturing packets.
7. Click the **Save as** button to save the `capture.pcap` file on your computer or to a disk drive.

Configure the Access Point in Business Central Mode

A

This appendix provides information about the features that you can manually control while the access point functions in Business Central mode (also referred to as cloud mode), that is, when the access point is cloud managed by the NETGEAR Business Central Wireless Manager (BCWM) application.

For information about the BCWM application, see the *Business Central Wireless Manager Application Quick Start Guide* and the *Business Central Wireless Manager Application User Manual*, both of which you can download from downloadcenter.netgear.com.

The appendix includes the following sections:

- [Enable Business Central Mode](#)
- [Configure the IP and 802.1Q VLAN Settings in Business Central Mode](#)
- [Reboot the Access Point in Business Central Mode](#)
- [Reset the Access Point in Business Central Mode to Factory Default Settings](#)
- [Upgrade Access Point Firmware in Business Central Mode](#)
- [Configure MAC Authentication in Business Central Mode](#)
- [Monitor the Access Point in Business Central Mode](#)

Note For information about disabling Business Central mode, see [Disable Business Central Mode for a Standalone Access Point](#) on page 19.

Enable Business Central Mode

By enabling Business Central mode, you can convert the access point from a standalone access point to a state in which the access point can be cloud managed by the NETGEAR BCWM application.

When the access point functions in Business Central mode, the local browser interface is a restricted interface that shows only the Configuration and Monitoring menu tabs with limited configuration options.

► To enable Business Central mode:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > Basic > General**.

NETGEAR

WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration Monitoring Maintenance Support

System IP Wireless Security Wireless Bridge Ensemble Captive Portal

Cancel Apply

Basic

General

Access Point Name netgear0586f

Country / Region US - United States

Business Central Settings

Business Central Enabled Yes No

Business Central Activation Status Pending

Business Central Connectivity Status Disconnected

[Click here to open Business Central Management](#)

NOTE: If Business Central Enabled is set to Yes, this Access Point will periodically attempt to contact NETGEAR Business Central Wireless Server to check if this Access Point has been registered for business central management.

5. Select the Business Central Enabled **Yes** radio button.
6. Click the **Apply** button.
The access point restarts with factory default settings but retains its IP configuration and management VLAN.
The access point is now ready for cloud management with a restricted local browser interface.

Configure the IP and 802.1Q VLAN Settings in Business Central Mode

In most situations, the NETGEAR BCWM applications assign IP settings to an access point that functions in Business Central mode. However, you can manually configure the IP and 802.1Q VLAN settings in Business Central mode.

► To configure the IP and 802.1Q VLAN settings in Business Central mode:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > IP Settings**.

The screenshot shows the NETGEAR web interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The user is logged in as 'admin'. The navigation menu includes Configuration, Monitoring, System, and Security. The 'IP Settings' page is active, showing options for DHCP Client (Enable/Disable), IP Address, IP Subnet Mask, Default Gateway, Primary DNS Server, Secondary DNS Server, and Network Integrity Check. Below this, the '802.1Q VLAN' section is visible, with 'Untagged VLAN' and 'Management VLAN' both set to 1.

5. Configure the IPv4 settings as described in the following table.

Setting	Description
IP Settings	
DHCP Client	By default, the Dynamic Host Configuration Protocol (DHCP) client is enabled. The access point receives 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	Enter the IP address of your access point. The default IP address is 192.168.0.100. To change the address, enter an unused IP address from the address range used on your LAN, or enable DHCP the server.

(Continued)

Setting	Description
IP Subnet Mask	Enter the network number portion of an IP address. Unless you are implementing subnetting, enter 255.255.0.0 as the subnet mask.
Default Gateway	Enter the IP address of the ISP gateway to which the access point connects.
Primary DNS Server	Enter the IP address of the primary and secondary DNS servers. A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your access point during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually in this field.
Secondary DNS Server	
Network Integrity Check	Select this check box to validate that the upstream link is active before allowing WiFi associations. Ensure that the default gateway is configured.
802.1Q VLAN	
Untagged VLAN	Select the Untagged VLAN check box to configure one VLAN as an untagged VLAN. By default, the Untagged VLAN check box is selected. Specify a VLAN ID. The default VLAN ID is 1.
Management VLAN	Specify an ID for the VLAN from which the access point can be managed. The default VLAN ID is 1. If you configure the management VLAN ID as 0 (zero), the access point can be managed over any VLAN, and frames that belong to the management VLAN are not tagged with an 802.1Q header when sent over the trunk.

- Click the **Apply** button.

Your settings are saved.

If you changed the IP address settings and want to log in to the access point again, you must use the new IP address of the access point.

Reboot the Access Point in Business Central Mode

Situations might occur in which you must manually reboot the access point in Business Central mode.

► To reboot the access point in Business Central mode:

- Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
- In the address bar, enter the IP address of the access point.
A login window opens.
- Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
- Select **Configuration > System > Reset**.

The Reboot AP and Restore Defaults page displays.

5. Select the Reboot **Yes** radio button.

By default, the Reboot **No** radio button is selected.

6. Click the **Apply** button.

The access point reboots.

The reboot process typically takes about one minute. When the Test LED turns off, wait a few more seconds before doing anything with the access point.

Reset the Access Point in Business Central Mode to Factory Default Settings

Situations might occur in which you must manually reset the access point in Business Central mode to factory default settings.

► To reset the access point in Business Central mode to factory default settings:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.

For more information, see [Log In to the Access Point](#) on page 16.

2. In the address bar, enter the IP address of the access point.

A login window opens.

3. Enter the user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Configuration > System > Reset**.

The Reboot AP and Restore Defaults page displays.

5. Select the Restore to Factory Default Settings **Yes** radio button.

By default, the Restore to Factory Default Settings **No** radio button is selected.

6. Click the **Apply** button.

IMPORTANT:

During the restoration process, do not try to go online, turn off the access point, shut down the computer, or do anything else to the access point until it finishes restarting!

7. Click the **Apply** button.

The access point is reset to the factory default settings.

During the restoration process, the access point automatically restarts. The restoration process typically takes about one minute. When the Test LED turns off, wait a few more seconds before doing anything with the access point.

Upgrade Access Point Firmware in Business Central Mode

In most situations, the NETGEAR BCWM application upgrades firmware to an access point that functions in Business Central mode. However, situations might occur in which you must manually upgrade the firmware on the access point in Business Central mode.

► **To upgrade the access point firmware in Business Central mode if you already downloaded the firmware file:**

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > Reset**.
The Firmware Upgrade page displays.
5. Click the **Browse** button and locate and select the firmware upgrade file.
The firmware upgrade file is a .tar file.
6. Click the **Apply** button.



WARNING:

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

During the upgrade process, the access point automatically restarts. The upgrade process typically takes several minutes. When the Test LED turns off, wait a few more seconds before doing anything with the access point.

7. Verify that the new firmware file was installed by selecting **Configuration > General**.
The Business Central Settings and Access Point Information page displays. The firmware version is shown in the Access Point Information section of the page.

Configure MAC Authentication in Business Central Mode

All WiFi networks for an access point that functions in Business Central mode are managed by the BCWM application. Any changes that you make to a WiFi security profile must be made through the BCWM application, with one exception: On the access point in Business Central mode, you can set up a MAC address filter profile using the local MAC address database and assign that profile to a cloud-managed WiFi

network. You perform those actions on the access point in Business Central mode itself rather than through the BCWM application.

For increased security, you can restrict access to an SSID by allowing access to only specific computers or WiFi stations based on their MAC addresses. You can restrict access to only trusted computers so that unknown computers cannot connect over WiFi to the access point. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the WiFi link is fully exposed if you do not also implement WiFi security.

Before you can implement MAC address filtering, you must set up one or more MAC address filter profiles (which is described in this section) and then assign the profile to a WiFi security profile (see [Assign a MAC Address Filter Profile on an Access Point in Business Central Mode](#) on page 151). You can assign the same MAC address filter profile to multiple WiFi security profiles, or you can set up different MAC address filter profiles for different WiFi security profiles.

You can manually add MAC addresses to the MAC address filter profile and you can import a list of trusted MAC addresses.

The file that you import must satisfy the following requirements:

- The file must be a plain-text file with a `.txt` or `.cfg` extension.
- Entries in the file must be MAC addresses in hexadecimal format with each octet separated by colons, for example `00:11:22:33:44:55`.
- Entries must be separated with a single space.
- The file must contain only MAC addresses, no other information.

Note You cannot add multicast or broadcast MAC addresses to a MAC address filter profile.

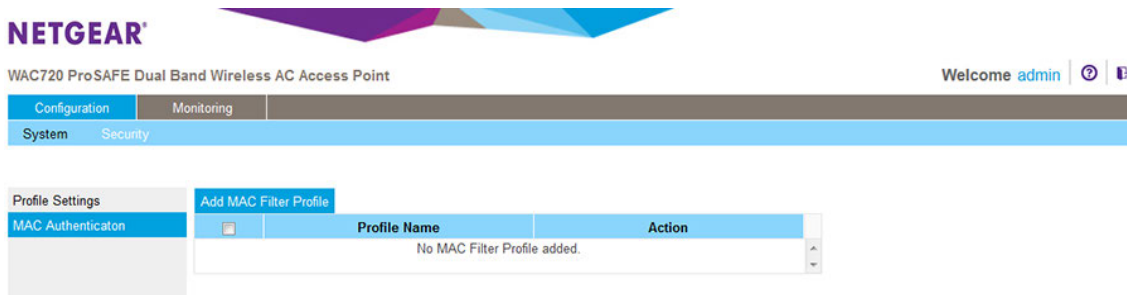
For all MAC address filter profiles together, the access point can support a maximum number of 512 MAC addresses. For example, you can set up two MAC address filter profiles with 256 MAC addresses each, or you can set up 16 MAC address filter profiles with 32 MAC addresses each, provided that the total number of MAC addresses for all profiles together does not exceed 512.

Add a MAC Address Filter Profile on an Access Point in Business Central Mode

► To add a MAC address filter profile on an access point in Business Central mode:

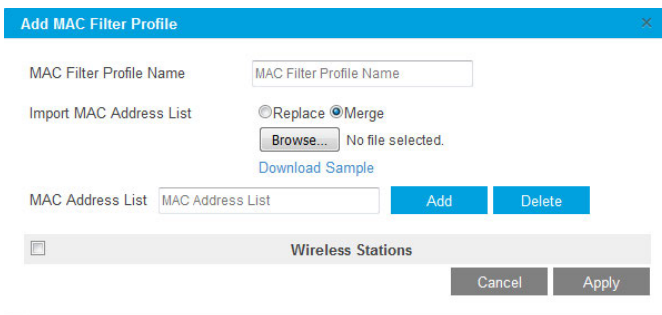
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

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



By default, no MAC filter profile exists.

5. Click the **Add MAC Filter Profile** button above the table.



6. In the **MAC Filter Profile Name** field, enter a name for the new profile.
This name identifies the profile and lets you assign it later to a WiFi security profile.
7. Populate the Wireless Stations table by one of the following methods or by a combination of the following methods:
 - Enter MAC addresses manually by doing the following:
 - a. Enter a MAC address in the **MAC Address List** field.
 - b. Click the **Add** button.
 - Import a list of trusted MAC addresses by doing the following:
 - a. Select the **Replace** radio button or **Merge** radio button.
The imported list either replaces the MAC addresses in the Wireless Stations table or merges with the MAC addresses in the Wireless Stations table.
 - b. Click the **Browse** button and navigate to and select the file with MAC addresses.

The file that you import must be a plain-text file with a .txt or .cfg extension. Entries in the file must be MAC addresses in hexadecimal format with each octet separated by colons, for example 00:11:22:33:44:55. Separate entries with a single space. For the file to be accepted, it must contain only MAC addresses.

Note To download a sample file, click the **Download Sample** link.

8. To fine-tune the Wireless Stations table and delete one or more MAC addresses from the Wireless Stations table, select individual check boxes for the MAC addresses and click the **Delete** button.
9. Click the **Apply** button.

Your settings are saved. The Add MAC Filter Profile pop-up window closes.

For information about assigning the MAC address filter profile to a WiFi security profile, see *Assign a MAC Address Filter Profile on an Access Point in Business Central Mode* on page 151.

Assign a MAC Address Filter Profile on an Access Point in Business Central Mode

For you to enable MAC address authentication on a cloud-managed WiFi network, you must first set up a MAC address filter profile for local authentication (see *Add a MAC Address Filter Profile on an Access Point in Business Central Mode* on page 149).

You enable MAC address authentication on a cloud-managed WiFi network by assigning a MAC address filter profile to the WiFi security profile for the WiFi network.

► To assign a MAC address filter profile to a cloud-managed WiFi network on an access point in Business Central mode:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see *Log In to the Access Point* on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

4. Select **Configuration > Security > Profile Settings**.

The screenshot shows the NETGEAR configuration interface for a WAC720 ProSAFE Dual Band Wireless AC Access Point. The user is logged in as 'admin'. The navigation menu includes Configuration, Monitoring, System, and Security. The 'Profile Settings' page is displayed, showing two sections: 'Profile Settings - 802.11 bg/ng/bgn' and 'Profile Settings - 802.11 a/a-na-ac'. Each section contains a table of eight WiFi security profiles. The 'Enable' checkbox for profile 0 is checked in both tables.

#	Profile Name	SSID	Security	VLAN	Enable	WMF-Enable
0	NETGEAR	NETGEAR_11ng	Open System	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1	NETGEAR-1	NETGEAR_11ng-1	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
2	NETGEAR-2	NETGEAR_11ng-2	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
3	NETGEAR-3	NETGEAR_11ng-3	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
4	NETGEAR-4	NETGEAR_11ng-4	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
5	NETGEAR-5	NETGEAR_11ng-5	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
6	NETGEAR-6	NETGEAR_11ng-6	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
7	NETGEAR-7	NETGEAR_11ng-7	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>

#	Profile Name	SSID	Security	VLAN	Enable	WMF-Enable
0	NETGEAR	NETGEAR_11ac	Open System	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1	NETGEAR-1	NETGEAR_11ac-1	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
2	NETGEAR-2	NETGEAR_11ac-2	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
3	NETGEAR-3	NETGEAR_11ac-3	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
4	NETGEAR-4	NETGEAR_11ac-4	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
5	NETGEAR-5	NETGEAR_11ac-5	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
6	NETGEAR-6	NETGEAR_11ac-6	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>
7	NETGEAR-7	NETGEAR_11ac-7	Open System	1	<input type="checkbox"/>	<input type="checkbox"/>

The Profile Settings page for the 802.11bg/ng/bgn and 802.11a/a-na-ac modes shows eight WiFi security profiles for each mode.

Note You cannot enable or disable a WiFi security profile, nor can you enable or disable Wireless Multicast Forwarding (WMF). These actions must be performed through the BCWM application that manages the access point.

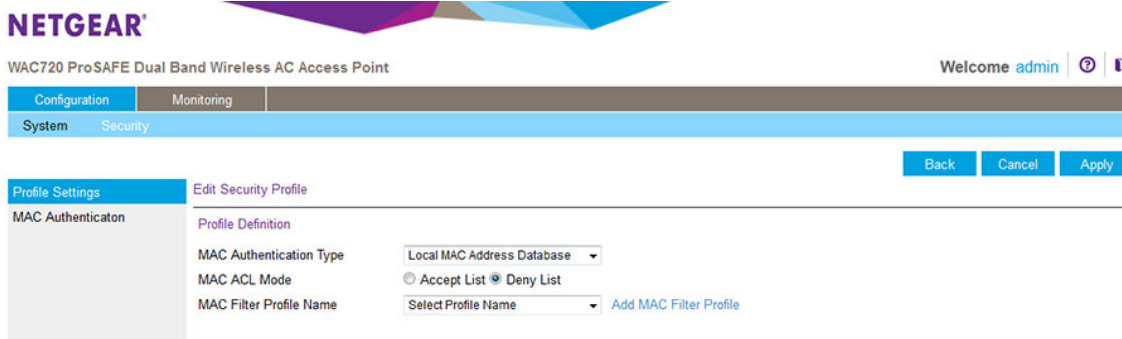
5. To assign a MAC address filter profile to a WiFi security profile, select the corresponding radio button to the left of the WiFi security profile.

6. Click the **Edit** button.

The Edit Security Profile page displays.

By default, the selection from the **MAC Authentication Type** menu is Disable, and MAC address authentication is disabled.

7. From the **MAC Authentication Type** menu, select **Local MAC Address Database**.



8. From the **MAC Filter Profile Name** menu, select the profile that you want to use.
9. Select one of the following MAC ACL Mode radio buttons:
 - **Accept List.** All MAC address that are in the selected profile are allowed WiFi access and all MAC addresses that are not in the profile are denied WiFi access.
 - **Deny List.** All MAC address that are in the selected profile are denied WiFi access and all MAC addresses that are not in the profile are allowed WiFi access. (This is the default selection.)
10. Click the **Apply** button.
Your settings are saved.
11. Click the **Back** button.
The Profile Settings page displays again.

Modify a MAC Address Filter Profile on an Access Point in Business Central Mode

► To modify an existing MAC address filter profile:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Security > MAC Authentication**.
The MAC Authentication page displays and shows a table with MAC address filter profiles.
5. If more than one profile exists, select the check box for the profile that you want to modify.
6. Click the **Edit** button.
The Edit MAC Filter Profile pop-up window opens.

7. Modify the MAC address filter profile.

For more information, see [Add a MAC Address Filter Profile on an Access Point in Business Central Mode](#) on page 149.

8. Click the **Apply** button.

Your settings are saved. The Add MAC Filter Profile pop-up window closes.

Delete a MAC Address Filter Profile on an Access Point in Business Central Mode

► To delete an existing MAC address filter profile:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > Security > MAC Authentication**.
The MAC Authentication page displays and shows a table with MAC address filter profiles.
5. Select the check box for the profile that you want to delete.
You can select more than one check box and delete several profiles.
6. Click the **Delete Profile** button.
The profile or profiles are deleted.

Monitor the Access Point in Business Central Mode

You can view the activity logs of an access point in Business Central mode, which can be useful if you are troubleshooting a problem.

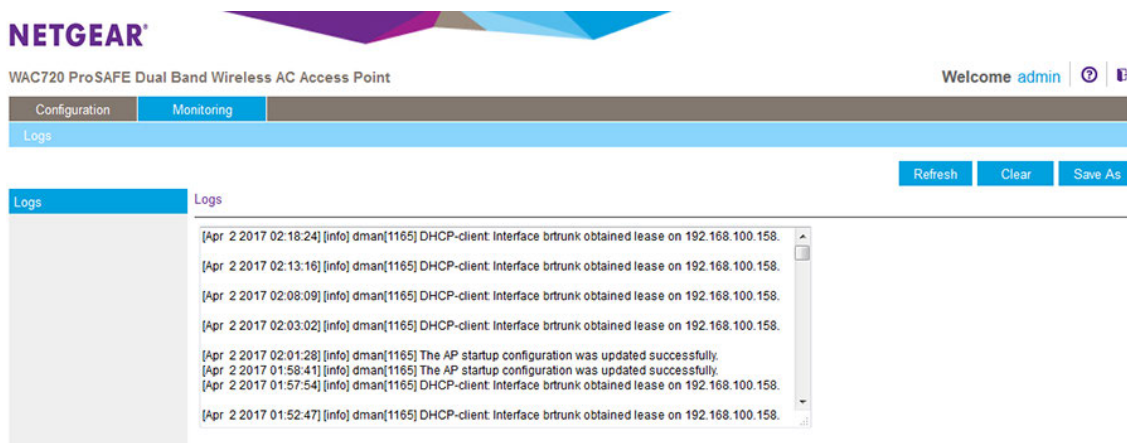
You can also view basic information about the access point.

View the Activity Logs of an Access Point in Business Central Mode

You can view the access point's activity logs and save the log entries.

► To display the activity logs and save the log entries:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Monitoring > Logs**.



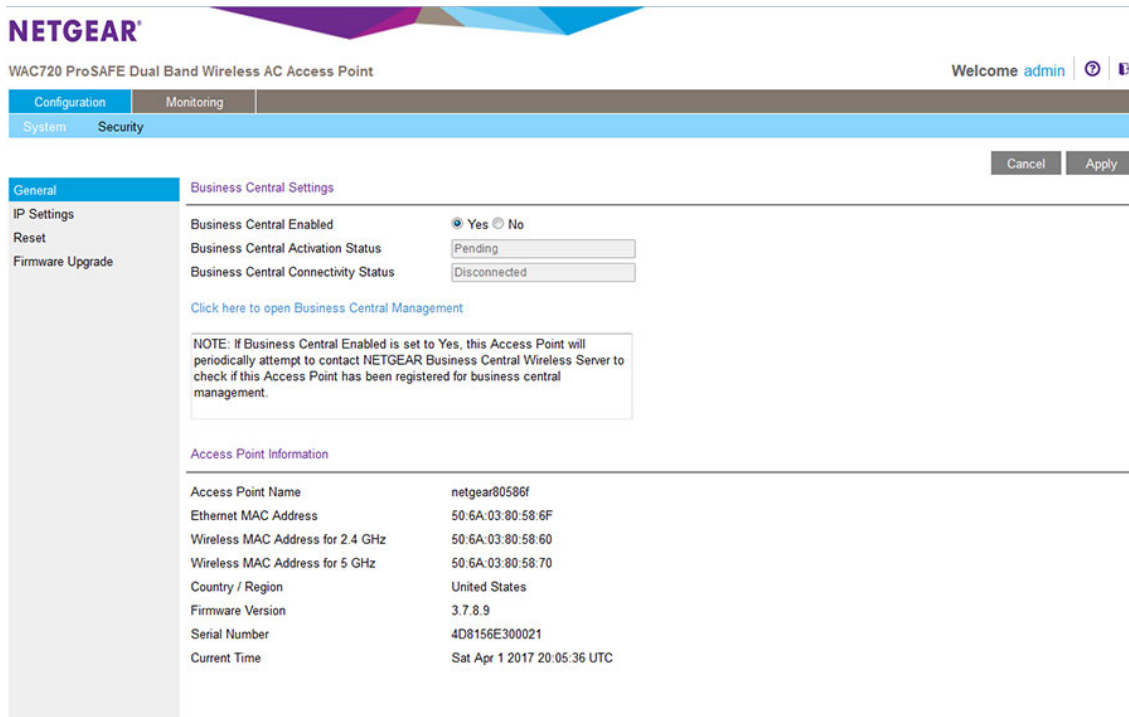
5. Click the **Save As** button to save the log entries to a file on your computer or to a disk drive.
6. To update the information on the page, click the **Refresh** button.
7. To clear the log entries, click the **Clear** button.

View Basic Information About the Access Point In Business Central Mode

You can view basic information about the access point in Business Central mode, such as the MAC addresses of the access point and some of its components, firmware version, and serial number.

► To view basic information about the access point:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable.
For more information, see [Log In to the Access Point](#) on page 16.
2. In the address bar, enter the IP address of the access point.
A login window opens.
3. Enter the user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. Select **Configuration > System > General**.



NETGEAR

WAC720 ProSAFE Dual Band Wireless AC Access Point

Welcome admin

Configuration Monitoring

System Security

Cancel Apply

General Business Central Settings

IP Settings
Reset
Firmware Upgrade

Business Central Enabled Yes No

Business Central Activation Status

Business Central Connectivity Status

[Click here to open Business Central Management](#)

NOTE: If Business Central Enabled is set to Yes, this Access Point will periodically attempt to contact NETGEAR Business Central Wireless Server to check if this Access Point has been registered for business central management.

Access Point Information

Access Point Name	netgear80586f
Ethernet MAC Address	50:6A:03:80:58:6F
Wireless MAC Address for 2.4 GHz	50:6A:03:80:58:60
Wireless MAC Address for 5 GHz	50:6A:03:80:58:70
Country / Region	United States
Firmware Version	3.7.8.9
Serial Number	4D8156E300021
Current Time	Sat Apr 1 2017 20:05:36 UTC

The Access Point Information section shows information about the access point in Business Central mode.

Note For information about the Business Central activation status and connectivity states, see the *Business Central Wireless Manager Application User Manual*, which you can download from downloadcenter.netgear.com.

This appendix provides factory default settings and technical specifications for the access point. The appendix includes the following sections:

- *Technical Specifications*
- *Factory Default Settings*

Technical Specifications

Table 4. Technical specifications

Feature	Description
802.11bg/ng/bgn WiFi 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
802.11bgn 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 / 86.6 Mbps, 9 / 101.1 Mbps, 10 / 115.5 Mbps, 11 / 130 Mbps, 12 / 144.4 Mbps, 13 / 158.8 Mbps, 14 / 173.3 Mbps, 15 / 187.7 Mbps, 16 / 216.7 Mbps, 17 / 231.6 Mbps, 18 / 246.5 Mbps, 19 / 261.4 Mbps, 20 / 276.3 Mbps, 21 / 291.2 Mbps, 22 / 306.1 Mbps, 23 / 321.0 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 / 65 Mbps, 7 / 78 Mbps, 8 / 91 Mbps, 9 / 104 Mbps, 10 / 117 Mbps, 11 / 130 Mbps, 12 / 143 Mbps, 13 / 156 Mbps, 14 / 169 Mbps, 15 / 182 Mbps, 16 / 195 Mbps, 17 / 208 Mbps, 18 / 221 Mbps, 19 / 234 Mbps, 20 / 247 Mbps, 21 / 260 Mbps, 22 / 273 Mbps, 23 / 286 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 / 75 Mbps, 5 / 90 Mbps, 6 / 105 Mbps, 7 / 120 Mbps, 8 / 135 Mbps, 9 / 150 Mbps, 10 / 165 Mbps, 11 / 180 Mbps, 12 / 210 Mbps, 13 / 240 Mbps, 14 / 270 Mbps, 15 / 300 Mbps, 16 / 330 Mbps, 17 / 360 Mbps, 18 / 390 Mbps, 19 / 420 Mbps, 20 / 450 Mbps, 21 / 480 Mbps, 22 / 510 Mbps, 23 / 540 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 / 67.5 Mbps, 5 / 81 Mbps, 6 / 94.5 Mbps, 7 / 108 Mbps, 8 / 121.5 Mbps, 9 / 135 Mbps, 10 / 157.5 Mbps, 11 / 171 Mbps, 12 / 184.5 Mbps, 13 / 216 Mbps, 14 / 243 Mbps, 15 / 270 Mbps, 16 / 301.5 Mbps, 17 / 324 Mbps, 18 / 351 Mbps, 19 / 378 Mbps, 20 / 405 Mbps, 21 / 436.5 Mbps, 22 / 463.5 Mbps, 23 / 490.5 Mbps, and auto-rate capable
802.11bg/ng/bgn operating frequencies	<ul style="list-style-type: none"> • 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)

Table 4. Technical specifications (Continued)

Feature	Description
802.11 bg/ng/bgn encryption	<ul style="list-style-type: none"> • WPA-PSK & WPA2-PSK • AES • TKIP
802.11a/a-na-ac WiFi specifications	
802.11a data rates	6, 9, 12, 18, 24, 36, 48, 54 Mbps, and auto-rate capable
802.11a/a-na-ac data rates	<p>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 / 84.4 Mbps, 9 / 98.8 Mbps, 10 / 113.3 Mbps, 11 / 128.7 Mbps, 12 / 144.6 Mbps, 13 / 161.5 Mbps, 14 / 180 Mbps, 15 / 198.4 Mbps, 16 / 217 Mbps, 17 / 236 Mbps, 18 / 256 Mbps, 19 / 276 Mbps, 20 / 297 Mbps, 21 / 318 Mbps, 22 / 340 Mbps, 23 / 363 Mbps, and auto-rate capable</p> <p>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 / 65 Mbps, 7 / 78 Mbps, 8 / 91 Mbps, 9 / 104 Mbps, 10 / 117 Mbps, 11 / 130 Mbps, 12 / 143 Mbps, 13 / 156 Mbps, 14 / 169 Mbps, 15 / 182 Mbps, 16 / 195 Mbps, 17 / 208 Mbps, 18 / 221 Mbps, 19 / 234 Mbps, 20 / 247 Mbps, 21 / 260 Mbps, 22 / 273 Mbps, 23 / 286 Mbps, and auto-rate capable</p> <p>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 / 180 Mbps, 9 / 240 Mbps, 10 / 300 Mbps, 11 / 360 Mbps, 12 / 420 Mbps, 13 / 480 Mbps, 14 / 540 Mbps, 15 / 600 Mbps, 16 / 660 Mbps, 17 / 720 Mbps, 18 / 780 Mbps, 19 / 840 Mbps, 20 / 900 Mbps, 21 / 960 Mbps, 22 / 1020 Mbps, 23 / 1080 Mbps, and auto-rate capable</p> <p>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 / 135 Mbps, 7 / 162 Mbps, 8 / 189 Mbps, 9 / 243 Mbps, 10 / 306 Mbps, 11 / 369 Mbps, 12 / 432 Mbps, 13 / 495 Mbps, 14 / 558 Mbps, 15 / 621 Mbps, 16 / 684 Mbps, 17 / 747 Mbps, 18 / 810 Mbps, 19 / 873 Mbps, 20 / 936 Mbps, 21 / 1000 Mbps, 22 / 1063 Mbps, 23 / 1126 Mbps, and auto-rate capable</p> <p>Data rates for an 80 MHz channel width and an automatic guard interval: 0 / 97.5 Mbps, 1 / 195 Mbps, 2 / 292.5 Mbps, 3 / 390 Mbps, 4 / 585 Mbps, 5 / 780 Mbps, 6 / 975 Mbps, 7 / 1170 Mbps, 8 / 1365 Mbps, 9 / 1560 Mbps, and auto-rate capable</p> <p>Data rates for an 80 MHz channel width and a long guard interval (800 ms): 0 / 87.9 Mbps, 1 / 175.5 Mbps, 2 / 263.4 Mbps, 3 / 351 Mbps, 4 / 526.5 Mbps, 5 / 702 Mbps, 6 / 879 Mbps, 7 / 1053 Mbps, 8 / 1227 Mbps, 9 / 1401 Mbps, and auto-rate capable</p>

Table 4. Technical specifications (Continued)

Feature	Description
802.11a-na-ac operating frequencies	<ul style="list-style-type: none"> • 5.180–5.240 GHz (US, lower frequencies) • 5.260–5.320 GHz (US, middle frequencies) • 5.720–5.825 GHz (US, upper frequencies) • 5.180–5.240 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-ac encryption	<ul style="list-style-type: none"> • WPA-PSK & WPA2-PSK • AES • TKIP
Management and Other Specifications	
Network management	<ul style="list-style-type: none"> • Remote configuration and management through the local browser interface, through SNMP, or through Telnet or SSH with the command-line interface (CLI). • SNMP management supports SNMP MIB II, 802.11 MIB and proprietary configuration MIB.
Maximum clients	Limited by the amount of WiFi network traffic generated by each node; a maximum of 400 clients is supported.
Status LEDs	<ul style="list-style-type: none"> • Power/Test LED • Activity LED • Ethernet LAN • WiFi LAN (2.4 GHz and 5 GHz)
Electrical and Physical Specifications	
Power adapter	12 VDC, 2.5A; plug is localized to country of sale
Physical specifications	<ul style="list-style-type: none"> • Dimensions (h x w x d): 197.3 x 197.3 x 40 mm (7.76 x 7.76 x 1.57 in.) • Weight: 762 g (1.6 lb)

Table 4. Technical specifications (Continued)

Feature	Description
Environmental specifications	Operating temperature: 0 to 40°C (32 to 104°F) Operating humidity: 10–90%, noncondensing
Electromagnetic compliance	<ul style="list-style-type: none"> • FCC Part 15 SubPart B • FCC Part 15 SubPart C • FCC Part 15 SubPart E • CE • C-TICK

Factory Default Settings

You can use the **Reset** button located on the rear of the access point to reset all settings to their factory defaults. This is called a hard reset.

To perform a hard reset, use a sharp object to press and hold the **Reset** button for approximately five seconds (until the Test LED blinks rapidly). This returns the access point to the factory configuration settings that are shown in the following table.

Pressing the **Reset** button for a shorter period of time simply causes the access point to reboot.

Table 5. Default configuration 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
LAN IPv6 management address	2001::21c:c0ff:fe69
User name (case-sensitive) for login	admin
Login password (case-sensitive) for login	password
LAN and management features	
DHCPv4 client	Enabled
DHCPv6 client	Disabled
Untagged VLAN	Enabled, VLAN ID 1
Management VLAN	VLAN ID 1
SNMP	Enabled
Syslog	Disabled
Spanning Tree Protocol (STP)	Disabled
Link Layer Discovery Protocol (LLDP)	Enabled
Secure Shell (SSH)	Enabled

Table 5. Default configuration settings (Continued)

Feature	Description
Telnet	Disabled
Time zone	USA-Pacific
NTP client	Enabled
Custom NTP server	Disabled
Port speed	10/100/1000
Ethernet MAC address	See bottom label
Radio and WiFi settings	
Operating mode	Access point, infrastructure mode
WiFi access point name	netgearxxxxxx, where xxxxxx are the last 6 digits of the WiFi access point MAC address
Country and region	Varies by region
WiFi communication	2.4 GHz radio enabled 5 GHz radio enabled
WiFi modes	11bg/ng/bgn 11a/a-na-ac
WiFi 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 <hr/> Note Maximum WiFi 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. <hr/>
Channel width	11ng: 20 MHz 11ac: Dynamic 20/40 MHz
Guard interval	Auto
Output power	Full
WiFi on/off (radio scheduling)	Disabled
RTS threshold	2347
Fragmentation length	2346
Beacon interval	100

Table 5. Default configuration settings (Continued)

Feature	Description
Aggregation length	65535
A-MPDU	Enabled
RIFS transmission	Disabled
DTIM interval	3
Preamble type	Auto
Antenna	Internal
802.11d	Enabled
Maximum WiFi clients	400
Wi-Fi Multimedia (WMM)	Enabled
WMM powersave	Enabled
AP EDCA parameters (QoS settings)	See <i>Configure and Manage Quality of Service Policies</i> on page 112.
Station EDCA parameters (QoS settings)	
QoS policies	None
WiFi bridging	Disabled
Default WiFi profile and profile security	
Profile name	NETGEAR
Profile state	Enabled
WiFi network names (SSIDs)	NETGEAR_11ng NETGEAR_11ac
Broadcast WiFi network names (SSIDs)	Enabled
Network authentication	Open system (no authentication)
Data encryption	None
WiFi client security separation	Disabled
VLAN ID	1
WiFi security features	
Rogue AP detection	Disabled
Rogue AP detection policy	Moderate
MAC authentication	Disabled
RADIUS servers	None
RADIUS authentication port number	1812
RADIUS shared secret	sharedsecret
RADIUS accounting port number	1813
RADIUS reauthentication time	3600 seconds
RADIUS update of the global key	1800 seconds