NETGEAR®

Insight Managed Smart Cloud Wireless Access Point

User Manual

Model WAC505

September 2017
202-11757-01

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

Contents

Hardware Overview of the Access Point 1

The NETGEAR Insight Managed Smart Cloud Wireless Access Point (WAC505) 802.11 Wave 2 AC1200, in this manual referred to as the access point, supports dual-band concurrent operation at 2.4 GHz and 5 GHz with combined throughput of 1.2 Gbps (300 Mbps at 2.4 GHz and 867 Mbps at 5 GHz). The access point supports Power over Ethernet (PoE) so that you can connected it to a PoE switch in an existing network. (An optional DC power adapter lets you connect the access point to a regular switch.)

The access point supports the NETGEAR Insight app, which lets you set up and manage the access point from your iOS or Android mobile device. However, this user manual describes local browser–based management interface, in this manual referred to as the local browser interface. For information about the NETGEAR Insight app, see the NETGEAR knowledge base articles at *netgear.com/support*.

This chapter contains the following sections:

Note For more information about the topics that are 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*. 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.

Related Documentation

The following related documentation is available at *downloadcenter.netgear.com*:

- Installation guide
- Ceiling and wall installation guide
- Data sheet

For information about the NETGEAR Insight app, see the NETGEAR knowledge base articles at *netgear.com/support*.

Unpack the Access Point

The package contains the access point, installation guide, ceiling and wall installation kit, and mounting installation guide. Because the access point supports Power over Ethernet (PoE), a power adapter is not included in the product package but is available as an option.

Top Panel With LEDs

The status LEDs are located on the top panel of the access point.

Figure 1. Status LEDs

Table 1. LED descriptions

LED	Description
Power LED 	**Off**. No power is supplied to the access point. **Solid green**. Power is supplied to the access point and the access point is ready. **Solid amber**. During startup, the Power LED lights solid amber. If after five minutes the amber light remains on, a boot error occurred. **Blinking amber temporarily**. The access point is upgrading firmware. **Blinking amber continuously**. The access point did not receive an IP address from a DHCP server. **Alternating green and amber**. The access point is receiving insufficient PoE power.
Activity LED 	**Off**. No link with the network is detected. **Solid green**. A link with the network is detected. **Blinking green**. Network traffic is detected. **Solid blue**. The management mode is Insight but the switch is not connected to the cloud server.
LAN LED 	**Off**. Either no powered-on Ethernet device is connected to the LAN port, or, if a powered-on Ethernet device is connected, no Ethernet link is detected. **Solid amber**. A 10 or 100 Mbps Ethernet link is detected on the LAN port. **Solid green**. A 1000 Mbps Ethernet link is detected on the LAN port.
2.4G WLAN LED 	**Off**. The 2.4 GHz WiFi radio is off. **Solid green**. The 2.4 GHz WiFi radio is on. **Solid blue**. One or more WLAN clients are connected to the 2.4 GHz WiFi radio. **Blinking blue**. Traffic is detected on the 2.4 GHz WiFi radio.
5G WLAN LED 	**Off**. The 5 GHz WiFi radio is off. **Solid green**. The 5 GHz WiFi radio is on. **Solid blue**. One or more WLAN clients are connected to the 5 GHz WiFi radio. **Blinking blue**. Traffic is detected on the 5 GHz WiFi radio.

Note For information about troubleshooting with the LEDs, see *Troubleshoot With the LEDs* on page 128.

Back Panel

The back panel of the access point provides the DC power connector, LAN port, and **Reset** button.

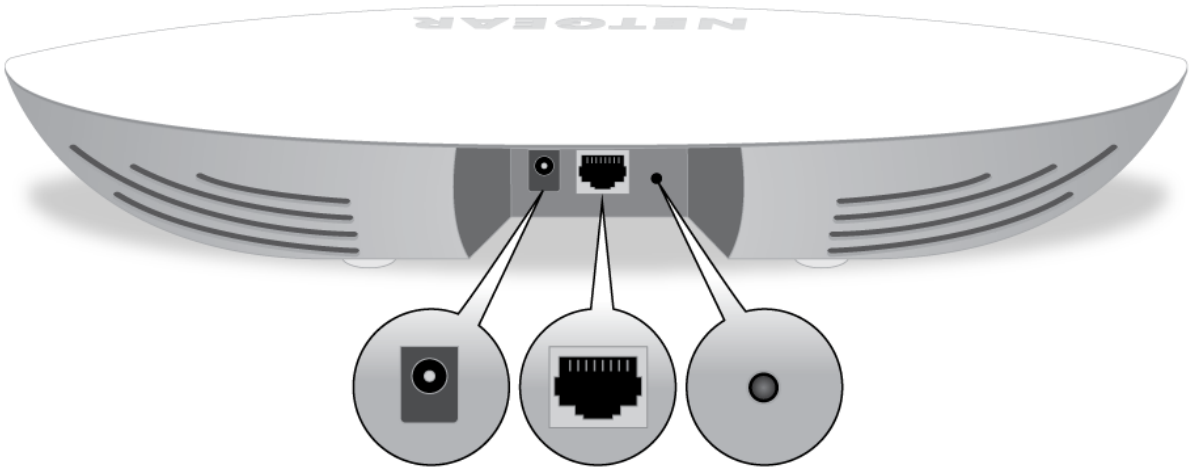


Figure 2. Access point back panel

Viewed from left to right, the back panel contains the following components:

- **DC power connector**. If you do not use a PoE connection, connect an optional power adapter to the DC power connector.
- **LAN port**. One Gigabit Ethernet RJ-45 LAN port that supports PoE. Use the LAN port to connect the access point to a switch or PoE switch that is connected to a network router, which, in turn, must be connected to the Internet, for example, through an Internet modem. You can also use the LAN port to connect the access point to a computer for initial configuration.
- **Reset button**. Press the **Reset** button for about 2 seconds to reboot the access point or for more than 10 seconds to reset the access point to factory default settings. If you added the access point to a network on the Insight app before, you must first use the NETGEAR Insight app to remove the access point from your network before the factory default settings function of the **Reset** button is available. For more information, see *Use the Reset Button* on page 104.

For more information about the LAN port connection, see *Set Up and Connect the Access Point to Your Network* on page 14.

Product Label

The product label on the bottom panel of the access point shows the serial number, MAC address, default WiFi network name (SSID), network key (password), and default login information of the access point.

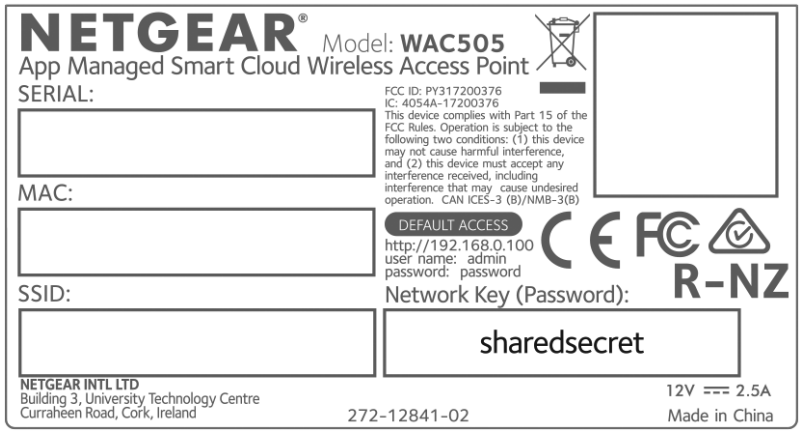


Figure 3. Access point label

Install the Access Point in Your Network and Access It for Initial Configuration

2

This chapter describes how you can install and access the access point in your network.

The chapter contains the following sections:

Position Your Access Point

Before you install your access point as described in the mounting installation guide, consider how you will position the access point.

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

Additionally, other WiFi access points in and around your home might affect your access point's signal. WiFi access points can be routers, repeaters, WiFi range extenders, and any other devices that emit WiFi signals for network access.

Position your access point according to the following guidelines:

- Place your access point near the center of the area where your computers and other devices operate and within line of sight to your WiFi devices.
- If you use a power adapter, make sure that the access point is within reach of an AC power outlet.
- Place the access point in an elevated location, minimizing the number walls and ceilings between the access point and your other devices.
- Place the access point away from electrical devices such as these:
  - Ceiling fans
  - Home security systems
  - Microwaves
  - Computers
  - Base of a cordless phone
  - 2.4 GHz cordless phone
  - 5.8 GHz cordless phone
- Place the access point away from large metal surfaces, large glass surfaces, insulated walls, and items such as these:
  - Solid metal door
  - Aluminum studs
  - Fish tanks
  - Mirrors
  - Brick
  - Concrete

If you are using adjacent access points, use different radio frequency channels to reduce interference.

Set Up and Connect the Access Point to Your Network

The access point is intended to function as a WiFi access point in your existing network.

The following sections describe how you can connect the access point to your network:

- *Set Up the Access Point With a PoE Network Connection* on page 14
- *Set Up the Access Point With a Non-PoE Network Connection* on page 15

To set up your access point, follow the procedure in *one* of these sections.

Set Up the Access Point With a PoE Network Connection

You can connect the access point to a Power over Ethernet (PoE) switch in your network and let WiFi clients connect to the access point and access your network and the Internet. The switch must be connected to a network router, which, in turn, must be connected to the Internet, for example, through an Internet modem. If you use a PoE connection, the access point does not require a power adapter.

Figure 4. Set up the access point with a PoE connection to your network

To set up the access point with a PoE connection to your network:

1. Connect an Ethernet cable to the LAN port on the access point.
2. Connect the other end of the Ethernet cable to a PoE port on a PoE switch that is connected to your network and to the Internet.

   The Power LED of the access point lights solid amber. After about one minute, if the access point is connected to a DHCP server, the Power LED turns solid green and the access point is ready for you to perform the initial configuration.

For information about accessing the access point for initial configuration, see *Connect to the Access Point for Initial Configuration* on page 15.

Set Up the Access Point With a Non-PoE Network Connection

You can connect the access point to a switch in your network and let WiFi clients connect to the access point and access your network and the Internet. The switch must be connected to a network router, which, in turn, must be connected to the Internet, for example, through an Internet modem. If you use a regular switch, that is, a non–Power over Ethernet (PoE) switch, the access point requires a power adapter, which is an option that you can purchase.

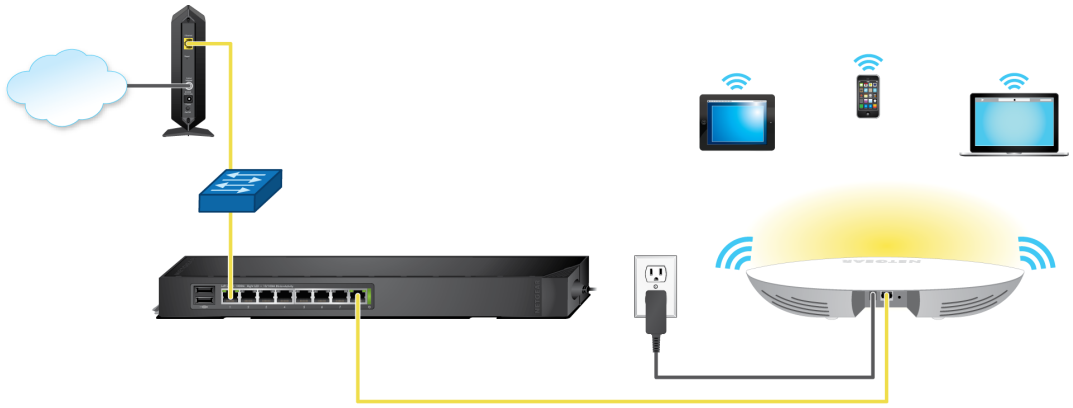


Figure 5. Set up the access point with a connection to your network

To set up the access point with a non-PoE connection to your network:

1. Connect an Ethernet cable to the LAN port on the access point.
2. Connect the other end of the Ethernet cable to a switch that is connected to your network and to the Internet.
3. Connect the power adapter to the access point and plug it into an electrical outlet.

   The Power LED of the access point lights solid amber. After about one minute, if the access point is connected to a DHCP server, the Power LED turns solid green and the access point is ready for you to perform the initial configuration.

For information about accessing the access point for initial configuration, see *Connect to the Access Point for Initial Configuration* on page 15.

Connect to the Access Point for Initial Configuration

After you set up the access point, you can use several methods to connect to it for initial configuration.

You can either connect to the access point by using the NETGEAR Insight app on an iOS or Android mobile device or by using the local browser interface. These two types of access are mutually exclusive.

The NETGEAR Insight app provides ease of access but lets you configure a limited number of features. The local browser interface lets you configure all features that are available on the access point.

For information about how you can connect to the access point by using the NETGEAR Insight app, see *Connect Over WiFi Using an iOS or Android Mobile Device* on page 16.

The following sections describe how you can connect to the access point by using the local browser interface (follow the procedure in *one* of these sections):

- *Connect Over WiFi Using a WiFi-Enabled Computer or Mobile Device* on page 17
- *Connect Over Ethernet Using a Computer Connected to the Same Network* on page 20
- *Connect Over Ethernet Using a Directly Connected Computer* on page 24

Note If your network does not include a DHCP server (or a router that functions as a DHCP server) and you do not perform the initial configuration of the access point as described in one of these sections, you can connect only two clients to the access point and the access point can provide an IP address to only two clients. To prevent this situation, make sure that you perform the initial configuration of the access point.

Connect Over WiFi Using an iOS or Android Mobile Device

You can install the NETGEAR Insight app on an iOS or Android mobile device and set up the access point (and perform many other tasks as well).

For information about the NETGEAR Insight app, see the NETGEAR knowledge base articles at *netgear.com/support*.

To connect to the access point over WiFi using an iOS or Android mobile device:

1. On your mobile device, go to the app store, search for NETGEAR Insight, and download the app.

2. Open the NETGEAR Insight app and log in to your existing NETGEAR account or create a new account to log in with.
3. Follow the prompts in the NETGEAR Insight app to discover and register the access point on the network so that you can configure and manage the access point.

Note If the access point is not connected to the Internet, you can still use the NETGEAR Insight app to configure the access point by connecting to the access point's default SSID. The default SSID is on the access point label on the bottom of the access point and is shown in the format NETGEARxxxxxx-SETUP, where xxxxxx is the last six hexadecimal digits of the access point's MAC address. The default password is **sharedsecret**.

Connect Over WiFi Using a WiFi-Enabled Computer or Mobile Device

This section describes how to connect to the access point for the first time over WiFi using a WiFi-enabled computer or mobile device (without using the NETGEAR Insight app).

To connect to the access point over WiFi using a WiFi-enabled computer or mobile device:

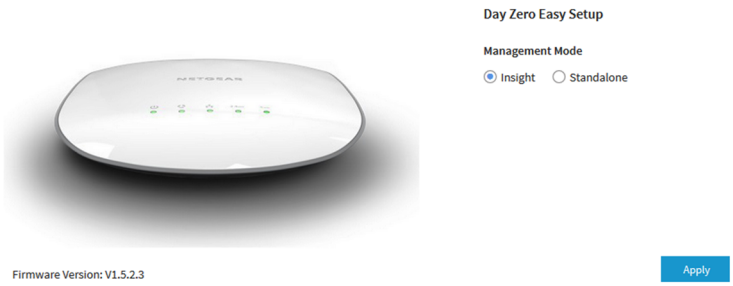
1. From your computer or mobile device, connect over WiFi to the access point's default WiFi network.

   The default SSID is on the access point label on the bottom of the access point and is shown in the format NETGEARxxxxxx-SETUP, where xxxxxx is the last six hexadecimal digits of the access point's MAC address. The default password is **sharedsecret**.

2. On the computer or mobile device, open a web browser and, in the address bar, enter **www.routerlogin.net** (or **www.aplogin.net**).

   Note You can use www.routerlogin.net (and www.aplogin.net) only during initial setup of the access point.

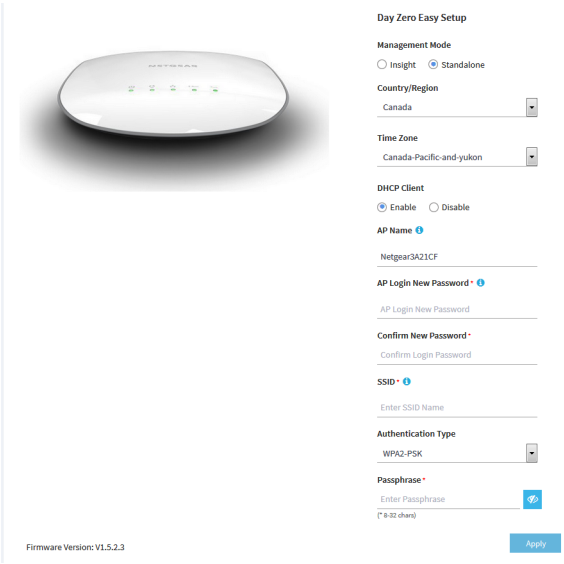
   The Day Zero Easy Setup page displays.



   In the address bar, www.routerlogin.net (or www.aplogin.net) is replaced by the IP address that is assigned to the access point by the DHCP server in your network.

3. Write down the IP address of the access point.
4. Select the **Standalone** radio button.

5. Click the **Apply** button.



Note After you save the basic settings that are shown on the page, the Day Zero Easy Setup page no longer displays when you log in. Instead, a login window opens. After you log in, the Dashboard page displays.

6. Enter the settings that are described in the following table.

Setting	Description
Country/Region	From the menu, select the country and region in which the access point is operating. **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. **Note** It might not be legal to operate the access point in a region other than the regions listed in the menu. If your country or region is not listed, check with your local government agency.
Time Zone	From the menu, select the time zone for the country and region in which the access point is operating.

(Continued)

Setting	Description
DHCP Client	By default, the DHCP client of the access point allows the access point to receive an IP address from a DHCP server (or router that functions as a DHCP server) in your network. To set up the access point with a static (fixed) IP address, do the following: a. Select the **Disable** radio button. Additional fields display. b. Specify the IP address, IP subnet mask, IP address of the default gateway, and IP address of the DNS server.
AP Name	As an option, enter a new system name for the access point. The name must contain alphanumeric characters, must contain at least one alphabetical character, cannot be longer than 15 characters, and can contain hyphens but cannot start or end with a hyphen. By default, the system name is Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address.
AP Login New Password	Enter a new admin password with a minimum of 6 characters and a maximum of 32 characters. The ideal password contains no English dictionary words and contains uppercase and lowercase letters, numbers, and symbols. However, do not include quotation marks (") in the password. Write down and save the password for future use. **Note** The admin password is the password that you use to log in to the access point's local browser interface. It is not the password that you use for WiFi access.
Confirm New Password	Enter exactly the same password that you entered in the **AP Login New Password** field.
SSID	You cannot use the default SSID for regular operation (the default SSID is for setup only). Enter a new name with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).

(Continued)

Setting	Description
Authentication Type	From the menu, select one of the following authentication types for the WiFi network: • **Open**. Authentication is not required and data encryption is not supported. This setting does not provide any security and is not appropriate for most situations. • **WPA2-PSK**. This option allows only WiFi clients that support WPA2 to connect to the SSID. Select this option if all WiFi clients are capable of supporting WPA2. This option uses AES encryption. • **WPA-PSK / WPA2-PSK**. This option allows both WPA and WPA2 WiFi clients to connect to the SSID. This option uses TKIP and AES encryption. Broadcast packets use TKIP. For unicast (that is, point-to-point) transmissions, WPA clients use TKIP and WPA2 clients use AES. **Note** For information about setting up WPA2 Enterprise security, see *Set Up an Open or Secure WiFi Network* on page 30.
Passphrase	Unless you select **Open** from the **Authentication Type** menu, enter a new passphrase (network key or WiFi password) for the WiFi network.

7. Click the **Apply** button.

   Your settings are saved and you are disconnected from the access point.

   If you changed the default country, the access point restarts.

8. Reconnect over WiFi to the access point's WiFi network using the new SSID and passphrase that you just defined on the Day Zero Easy Setup page.
9. In the web browser, enter the access point IP address that you wrote down in *Step 3*.

   If you assigned a static IP address to the access point, enter that IP address.

   A login window opens.

10. Enter the access point user name and password.

    The default user name is **admin**. The password is the one that you just defined on the Day Zero Easy Setup page. The user name and password are case-sensitive.

    The Dashboard page displays. You can now customize the access point settings for your network environment.

Connect Over Ethernet Using a Computer Connected to the Same Network

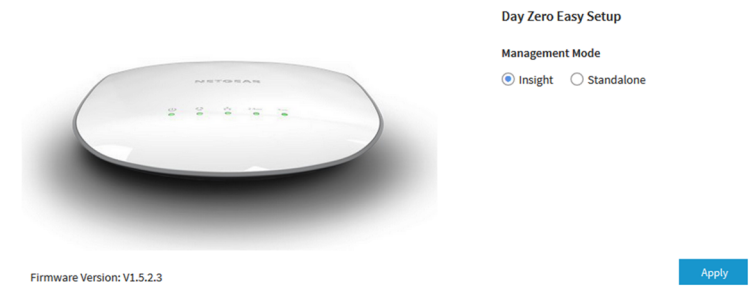
The following procedure assumes that your network includes a DHCP server (or router that functions as a DHCP server) and that the access point and the computer are on the same network. By default, the access

point functions as a DHCP client. If you want to set up the access point with a static (fixed) IP address, see *Connect Over Ethernet Using a Directly Connected Computer* on page 24.

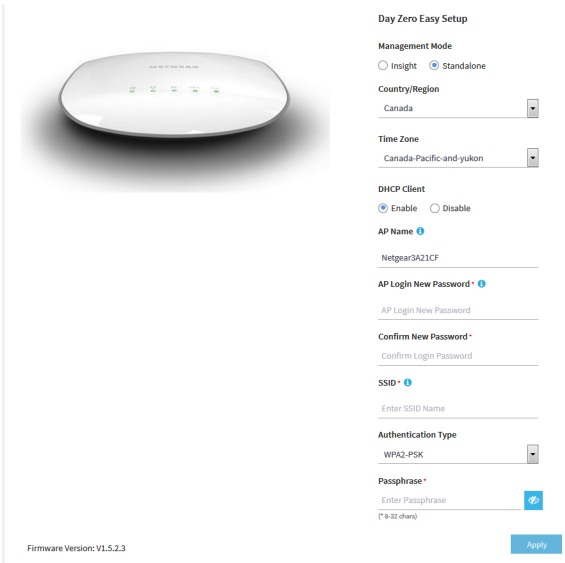
To connect to the access point using a computer that is connected to the same network as the access point:

1. To determine the IP address that the DHCP server assigned to the access point, access the DHCP server or use an IP network scanner.
2. On the computer, open a web browser and, in the address bar, enter the IP address that is assigned to the access point.

   The Day Zero Easy Setup page displays.



3. Select the **Standalone** radio button.
4. Click the **Apply** button.



Note After you save the basic settings that are shown on the page, the Day Zero Easy Setup page no longer displays when you log in. Instead, a login window opens. After you log in, the Dashboard page displays.

5. Enter the settings that are described in the following table.

Setting	Description
Country/Region	From the menu, select the country and region in which the access point is operating. **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. **Note** It might not be legal to operate the access point in a region other than the regions listed in the menu. If your country or region is not listed, check with your local government agency.
Time Zone	From the menu, select the time zone for the country and region in which the access point is operating.
DHCP Client	By default, the DHCP client of the access point allows the access point to receive an IP address from a DHCP server (or router that functions as a DHCP server) in your network. To set up the access point with a static (fixed) IP address, do the following: a. Select the **Disable** radio button. Additional fields display. b. Specify the IP address, IP subnet mask, IP address of the default gateway, and IP address of the DNS server.
AP Name	As an option, enter a new system name for the access point. The name must contain alphanumeric characters, must contain at least one alphabetical character, cannot be longer than 15 characters, and can contain hyphens but cannot start or end with a hyphen. By default, the system name is Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address.
AP Login New Password	Enter a new admin password with a minimum of 6 characters and a maximum of 32 characters. The ideal password contains no English dictionary words and contains uppercase and lowercase letters, numbers, and symbols. However, do not include quotation marks (") in the password. **Note** The admin password is the password that you use to log in to the access point's local browser interface. It is not the password that you use for WiFi access.
Confirm New Password	Enter exactly the same password that you entered in the **AP Login New Password** field.

(Continued)

Setting	Description
SSID	You cannot use the default SSID for regular operation (the default SSID is for setup only). Enter a new name with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).
Authentication Type	From the menu, select one of the following authentication types for the WiFi network: • **Open**. Authentication is not required and data encryption is not supported. This setting does not provide any security and is not appropriate for most situations. • **WPA2-PSK**. This option allows only WiFi clients that support WPA2 to connect to the SSID. Select this option if all WiFi clients are capable of supporting WPA2. This option uses AES encryption. • **WPA-PSK / WPA2-PSK**. This option allows both WPA and WPA2 WiFi clients to connect to the SSID. This option uses TKIP and AES encryption. Broadcast packets use TKIP. For unicast (that is, point-to-point) transmissions, WPA clients use TKIP and WPA2 clients use AES. **Note** For information about setting up WPA2 Enterprise security, see *Set Up an Open or Secure WiFi Network* on page 30.
Passphrase	Unless you select **Open** from the **Authentication Type** menu, enter a new passphrase (network key or WiFi password) for the WiFi network.

6. Click the **Apply** button.

   Your settings are saved.

   If you changed the default country, the access point restarts.

   Note Do not close the page!

   After a short period, the Dashboard page displays automatically. If the Dashboard page does not display, for example, because you assigned a static IP address, see the next step.

   You can now customize the access point settings for your network environment.

7. If the Dashboard does not display automatically, do the following:

a. Take one of the following actions:

- If you assigned a static IP address to the access point, enter that IP address in the address bar of the web browser.
- If you did not assign a static IP address, reenter the IP address that is displayed in the address bar of the web browser. If that does not work, write down the IP address, close the web browser, reopen the web browser, and then reenter the IP address in the address bar of the web browser.
- If you did not assign a static IP address and you closed the page so that you cannot see the IP address of the access point, use an IP scanner tool, use a network discovery tool, or access the DHCP server to discover the IP address of the access point in your network. Then, open a browser and enter the IP address in the address bar of the web browser.

A login window opens.

b. Enter the access point user name and password.
The default user name is **admin**. The password is the one that you just defined on the Day Zero Easy Setup page. The user name and password are case-sensitive.
The Dashboard page displays. You can now customize the access point settings for your network environment.

Connect Over Ethernet Using a Directly Connected Computer

If your network does not include a DHCP server (or router that functions as a DHCP server), you can use a computer that is connected through an Ethernet cable to the LAN port of the access point.

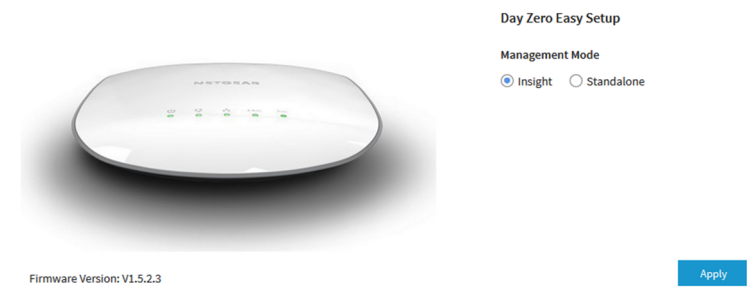
To connect to the access point using a computer that is connected to the LAN port of the access point:

1. Record the IP address and subnet mask of your computer so that you can reinstate these IP address settings later.
2. Temporarily change the IP address on your computer to 192.168.0.210 with 255.255.255.0 as the subnet mask.

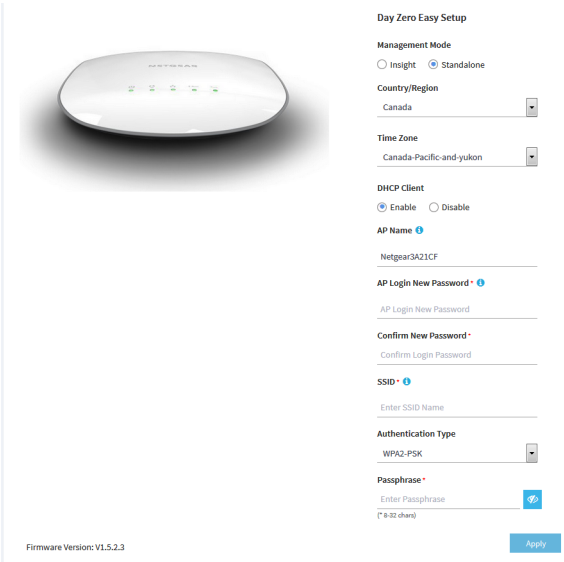
   (You can actually use any IP address in the 192.168.0.2–192.168.0.254 range, with the exception of IP address 192.168.0.100, which is the default IP address of the access point.)

   For more information about changing the IP address on your computer, see the help or documentation for your computer.
3. Use an Ethernet cable to connect your computer to the LAN port on the access point.
4. On the computer, open a web browser and enter **192.168.0.100** in the address bar.

The Day Zero Easy Setup page displays.



5. Select the **Standalone** radio button.
6. Click the **Apply** button.



Note After you save the basic settings that are shown on the page, the Day Zero Easy Setup page no longer displays when you log in. Instead, a login window opens. After you log in, the Dashboard page displays.

7. Enter the settings that are described in the following table.

Setting	Description
Country/Region	From the menu, select the country and region in which the access point is operating. **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. **Note** It might not be legal to operate the access point in a region other than the regions listed in the menu. If your country or region is not listed, check with your local government agency.
Time Zone	From the menu, select the time zone for the country and region in which the access point is operating.
DHCP Client	By default, the DHCP client of the access point allows the access point to receive an IP address from a DHCP server (or router that functions as a DHCP server) in your network. To set up the access point with a static (fixed) IP address, do the following: **a.** Select the **Disable** radio button. Additional fields display. **b.** Specify the IP address, IP subnet mask, IP address of the default gateway, and IP address of the DNS server.
AP Name	As an option, enter a new system name for the access point. The name must contain alphanumeric characters, must contain at least one alphabetical character, cannot be longer than 15 characters, and can contain hyphens but cannot start or end with a hyphen. By default, the system name is Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address.
AP Login New Password	Enter a new admin password with a minimum of 6 characters and a maximum of 32 characters. The ideal password contains no English dictionary words and contains uppercase and lowercase letters, numbers, and symbols. However, do not include quotation marks (") in the password. Write down and save the password for future use. **Note** The admin password is the password that you use to log in to the access point's local browser interface. It is not the password that you use for WiFi access.
Confirm New Password	Enter exactly the same password that you entered in the **AP Login New Password** field.

(Continued)

Setting	Description
SSID	You cannot use the default SSID for regular operation (the default SSID is for setup only). Enter a new name with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).
Authentication Type	From the menu, select one of the following authentication types for the WiFi network: • **Open**. Authentication is not required and data encryption is not supported. This setting does not provide any security and is not appropriate for most situations. • **WPA2-PSK**. This option allows only WiFi clients that support WPA2 to connect to the SSID. Select this option if all WiFi clients are capable of supporting WPA2. This option uses AES encryption. • **WPA-PSK / WPA2-PSK**. This option allows both WPA and WPA2 WiFi clients to connect to the SSID. This option uses TKIP and AES encryption. Broadcast packets use TKIP. For unicast (that is, point-to-point) transmissions, WPA clients use TKIP and WPA2 clients use AES. **Note** For information about setting up WPA2 Enterprise security, see *Set Up an Open or Secure WiFi Network* on page 30.
Passphrase	Unless you select **Open** from the **Authentication Type** menu, enter a new passphrase (network key or WiFi password) for the WiFi network.

8. Click the **Apply** button.

   Your settings are saved and you are disconnected from the access point.

   If you changed the default country, the access point restarts.

9. After a few minutes, if the login window does not open automatically, enter **192.168.0.100** in the address bar of your browser.

   If you changed the IP address (that is, you specified a static IP address), enter the new IP address.

   A login window opens.

10. Enter the access point user name and password.

    The default user name is **admin**. The password is the one that you just defined on the Day Zero Easy Setup page. The user name and password are case-sensitive.

    The Dashboard page displays. You can now customize the access point settings for your network environment.

11. After you complete the setup process, or both the setup and customization process, you can change the computer back to its original IP address settings.

Log In to the Access Point After Initial Setup to View or Change Settings

After you set up the access point, you can view or change the settings for the access point.

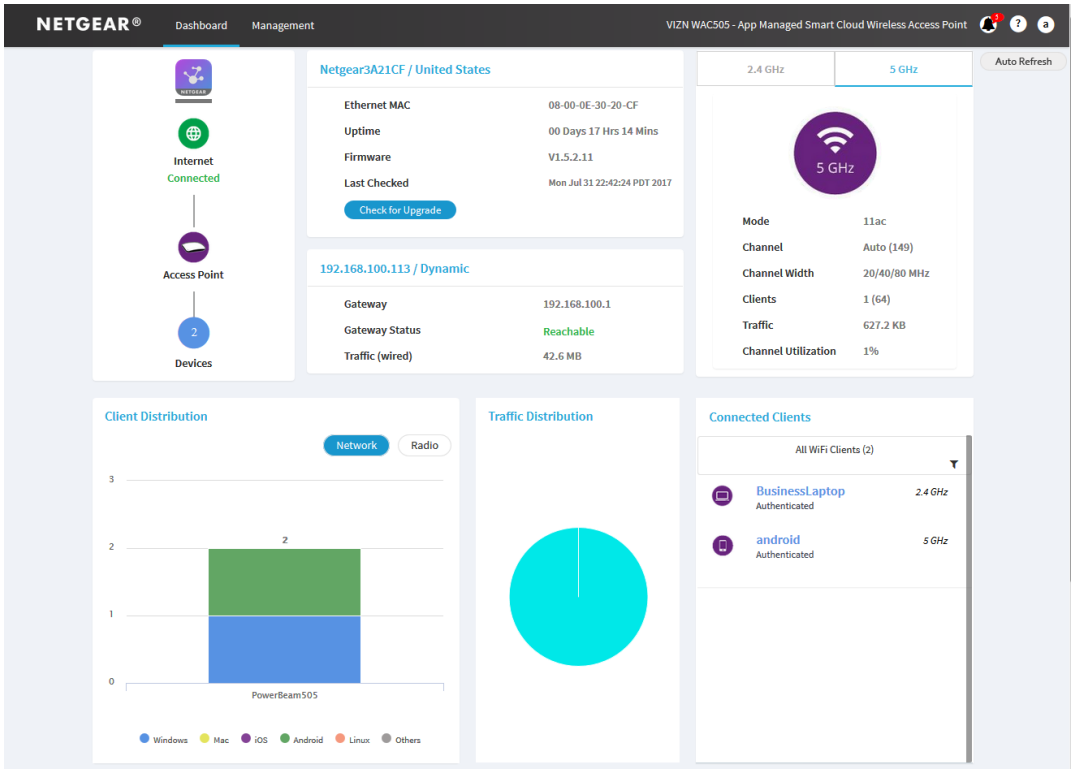
To log in to the access point's local browser interface:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays. The following figure shows part of the Dashboard page.



The Dashboard page displays various panes that let you see the status of your access point at a glance. For more information about the Dashboard page and its various panes, see *Monitor the Access Point and the Network* on page 110.

Manage the Basic WiFi and Radio Features

3

This chapter describes how you can manage the basic WiFi and radio settings of the access point. For information about the advanced WiFi and radio settings, see *Manage the Advanced WiFi and Radio Features* on page 58.

Tip If you want to change the settings of the access point's WiFi network, use a wired connection to avoid being disconnected when the new WiFi settings take effect.

The chapter includes the following sections:

Set Up and Manage WiFi Networks

The access point supports eight WiFi networks (four for each radio), each with its own unique WiFi settings. The following sections describe how you can set up and manage WiFi networks on the access point:

Set Up an Open or Secure WiFi Network

The access point provides one default SSID that is enabled by default and that broadcasts on the 2.4 GHz band and the 5 GHz band. This is the SSID that you were required to rename when you logged in to the access point for the first time. You can add more SSIDs: The access point supports four SSIDs for each radio for a total of eight SSIDs. (If you enable four SSIDs on both radios, the maximum number of SSIDs is reached.)

SSID stand for service set identifier, which is the WiFi network name. When you create a new SSID, you are actually defining the settings for a new virtual access point (VAP). That means that the access point supports up to eight VAPs.

The access point can simultaneously support the 2.4 GHz band for 802.11b/g/n WiFi devices and the 5 GHz band for 802.11a/n/ac WiFi devices.

If you plan to use WPA2 Enterprise security for your WiFi network, first set up RADIUS servers (see *Set Up RADIUS Servers* on page 80).

To set up a WiFi network:

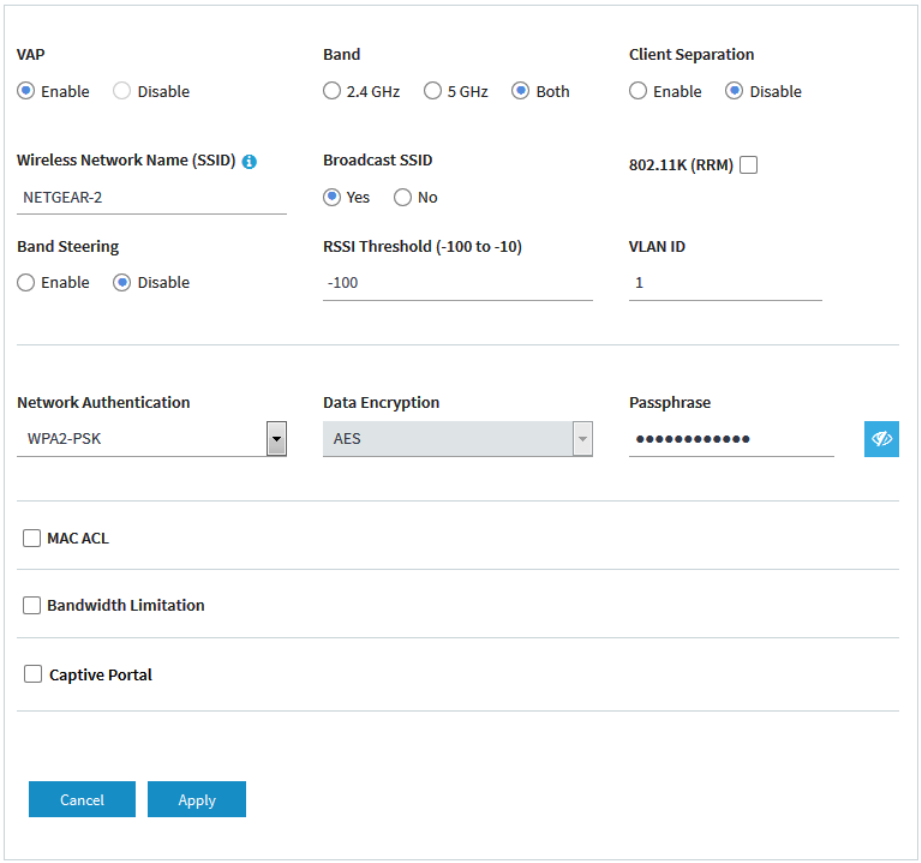
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard page displays.

4. Select **Management > Configuration > Wireless > Basic**.
   The page that displays lets you select and add an SSID.
5. Click the **+** button to the left of Add SSID.



6. Configure the WiFi, security, and radio settings as described in the following table.

Setting	Description
VAP	When you set up an SSID, you are creating a new virtual access point (VAP). By default, the new VAP is enabled. If you want to set up the SSID but temporarily disable the VAP, select the **No** radio button.
Band	Select a radio button for a single band (**2.4 GHz** or **5 GHz**) or keep the default selection, which is the **Both** radio button, to enable the VAP to broadcast on both bands.
Client Separation	By default, client separation is disabled for the VAP. To block communication between WiFi clients that are associated with different SSIDs on the access point, select the **Enable** radio button.

(Continued)

Setting	Description
Wireless Network Name (SSID)	The SSID is the WiFi network name of the VAP. Enter a name for the SSID with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\). For a WiFi device to be able to connect to the VAP, the SSID on the WiFi device must match the SSID of the VAP.
Broadcast SSID	By default, the VAP broadcasts its SSID so that WiFi clients can detect the SSID in their scanned network lists. To turn off the SSID broadcast, select the **No** radio button. Turning off the SSID broadcast provides additional WiFi security, but users must know the SSID to be able to join the VAP. If you set up a wireless distribution system (WDS; see *Set Up a WiFi Bridge Between Access Points* on page 63), you must keep the SSID broadcast enabled.
802.11K (RRM)	Select the **802.11K (RRM)** check box to enable 802.11k Radio Resource Management (RRM) so that the access point and 802.11k-aware clients can dynamically measure the available radio resources. By default, RRM is disabled. In an 802.11k-enabled network, access points and clients can send neighbor reports, beacon reports, and link measurement reports to each other, allowing 802.11k-aware clients to automatically select the best access point for initial connection or for roaming.
Band Steering	Select the **Enable** radio button to enable the access point to identify the WiFi devices that are dual-band capable and steer those devices to the 5 GHz band rather than the 2.4 GHz band of the VAP. Generally, more channels and bandwidth are available in the 5 GHz band, causing less interference and allowing for a better user experience. By default, band steering is disabled.
RSSI Threshold (-100 to -10)	You can enter the minimum received signal strength indicator (RSSI) value in decibel milliwatts (dBm) for a WiFi device to connect to the 2.4 GHz or 5 GHz radio on the access point. If the RSSI value on the WiFi device is less than the configured RSSI value on the access point, the WiFi device cannot connect to the access point. Enter a value in the range of –100 to –10 dBm. The default is –100 dBm. A higher value (for example, –10 dBm) indicates that the signal strength must be strong for a WiFi device to be able to connect to the radio. A lower value (for example, –100 dBm) indicates that the signal strength can be weak for a WiFi device to be able to connect to the radio. However, a connection that is based on a weak signal can be unreliable. For example, if the configured RSSI value on the access point is –70 dBm but the RSSI value on the WiFi device is –75 dBm, the WiFi device cannot connect to the access point. If the WiFi device is connected to the access point and then moves away from the access point, causing its RSSI value to become too low, the WiFi device is disconnected from the access point and an alarm is raised on the access point.

(Continued)

Setting	Description
VLAN ID	You can enter the VLAN ID that must be associated with the VAP. By default, the VLAN ID is 1. This VLAN ID is not the same as the 802.1Q VLAN ID that is used for the wired network (see *Set the 802.1Q VLAN and Management VLAN* on page 85).
Network Authentication, Data Encryption, and Passphrase	Select one of the following WiFi security options for the VAP: • **Open**. An open WiFi network does not provide any security. Any WiFi device can join the network. We recommend that you do *not* use an open WiFi network but configure WiFi security. However, an open network might be appropriate for a WiFi hotspot. • **WPA2-PSK**. This option is the default setting and uses AES encryption. This type of security enables only WiFi devices that support WPA2 to join the VAP. If you did not change the passphrase, the default passphrase displays. The default passphrase is sharedseceret. WPA2 provides a secure connection but some legacy WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select the mixed mode security, **WPA-PSK / WPA2-PSK**. In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To view the passphrase in clear text, click the eye icon. • **WPA-PSK / WPA2-PSK**. This mixed mode security enables WiFi devices that support either WPA or WPA2 to join the VAP. This option uses TKIP and AES encryption. WPA-PSK (which uses TKIP) is less secure than WPA2-PSK (which uses AES) and limits the speed of WiFi devices to 54 Mbps. In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To view the passphrase in clear text, click the eye icon. • **WPA2-enterprise**. This enterprise-level security uses RADIUS for centralized Authentication, Authorization, and Accounting (AAA) management. For WPA2 Enterprise security to function, you must set up RADIUS servers (see *Set Up RADIUS Servers* on page 80). From the **Data Encryption** menu, select the data encryption mode mode: - **TKIP + AES**. This type of data encryption enables WiFi devices that support either WPA or WPA2 to join the access point's WiFi network. This is the default mode. - **AES**. This type of data encryption provides a secure connection but some older WiFi devices do not detect WPA2 and support only WPA. Therefore, if your network includes such older devices, select **TKIP + AES** security.

7. Click the **Apply** button.
   Your settings are saved.
8. Make sure that you can connect to the new WiFi network.
   If you cannot connect to the new WiFi network, check the following:

- If your WiFi-enabled computer or mobile device is already connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the WiFi network that the access point provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
- If your WiFi-enabled computer or mobile device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your WiFi-enabled computer or mobile device to match the current settings for your network.
- Does your WiFi device display as a connected client? (See *View Client Distribution, Connected Clients, and Client Trends* on page 116.) If it does, it is connected to the network.
- Are you using the correct WiFi network name (SSID) and password?

View or Change the Settings of a WiFi Network

You can view or change the settings of the default WiFi network (SSID or VAP) or any custom WiFi network.

To view or change the settings of WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic**.

   The page that displays lets you select an SSID.
5. Click the **>** button to the left the SSID.

   The settings for the selected SSID display.
6. Change the settings of the WiFi network as needed.

   For detailed descriptions of the settings, see *Set Up an Open or Secure WiFi Network* on page 30.
7. If you made changes, click the **Apply** button.

   Your settings are saved.
8. If you made changes, make sure that you can reconnect over WiFi to the network with its new settings.

   If you cannot connect over WiFi, check the following:

   - If your WiFi-enabled computer or mobile device is already connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the WiFi network that the access point provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
   - If your WiFi-enabled computer or mobile device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your WiFi-enabled computer or mobile device to match the current settings for your network.

- Does your WiFi device display as a connected client? (See *View Client Distribution, Connected Clients, and Client Trends* on page 116.) If it does, it is connected to the network.
- Are you using the correct WiFi network name (SSID) and password?

Disable or Enable a WiFi Network

You can temporarily disable a WiFi network (SSID or VAP) and you can reenable the WiFi network.

To disable or enable a WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic**.
   The page that displays lets you select an SSID.
5. Click the **>** button to the left the SSID.
   The settings for the selected SSID display.
6. Under VAP, select one of the following radio buttons:
   - **Disable**. The WiFi network is disabled.
   - **Enable**. The WiFi network is enabled.
7. Click the **Apply** button.
   Your settings are saved.

Remove a WiFi Network

You can remove a custom WiFi network (SSID or VAP) that you no longer need. You cannot remove the default WiFi network.

To remove a WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.

The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard page displays.

4. Select **Management > Configuration > Wireless > Basic**.
   The page that displays lets you select an SSID.
5. Click the trash can icon to the right of the SSID.
   The WiFi network is removed.

Enable or Disable Client Separation for a WiFi Network

By default, client separation is disabled for a WiFi network (SSID or VAP), allowing communication between WiFi clients that are associated with different WiFi networks on the access point. For additional security, you can enable client separation.

To enable or disable client separation for a WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic**.
   The page that displays lets you select an SSID.
5. Click the **>** button to the left the SSID.
   The settings for the selected SSID display.
6. Under Client Separation, select one of the following radio buttons:

   - **Enable**. Client separation is enabled for the WiFi network.
   - **Disable**. Client separation is disabled for the WiFi network.

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

Hide or Broadcast the SSID for a WiFi Network

By default, a WiFi network (SSID or VAP) broadcasts its network name (also referred to as the SSID) so that WiFi clients can detect the SSID in their scanned network lists. For additional security, you can turn off the SSID broadcast and hide the SSID so that users must know the SSID to be able to join the WiFi network.

Note If you set up a wireless distribution system (WDS; see *Set Up a WiFi Bridge Between Access Points* on page 63), you must keep the SSID broadcast enabled.

To hide or broadcast the network name for a WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic**.
   The page that displays lets you select an SSID.
5. Click the **>** button to the left the SSID.
   The settings for the selected SSID display.
6. Under Broadcast SSID, select one of the following radio buttons:
   - **No**. The SSID is hidden for the WiFi network.
   - **Yes**. The SSID is broadcast for the WiFi network.
7. Click the **Apply** button.
   Your settings are saved.

Enable or Disable Radio Resource Management for a WiFi Network

Radio Resource Management (RRM), which is based on IEEE 802.11k, lets the access point and its clients dynamically measure the available radio resources. By default, RRM is disabled.

In an 802.11k-enabled network, access points and clients can send neighbor reports, beacon reports, and link measurement reports to each other, allowing 802.11k-aware clients to automatically select the best access point for initial connection or for roaming.

To enable or disable RRM:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.

The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard page displays.

4. Select **Management > Configuration > Wireless > Basic**.
   The page that displays lets you select an SSID.
5. Click the **>** button to the left the SSID.
   The settings for the selected SSID display.
6. Under 802.11K (RRM), select or clear the **802.11K (RRM)** check box:
   - Selecting the check box enables RRM.
   - Clearing the check box disables RRM.
7. Click the **Apply** button.
   Your settings are saved.

Enable or Disable Band Steering for a WiFi Network

Band steering enables the access point to identify the WiFi devices that are dual-band capable and steer those devices to the 5 GHz band rather than the 2.4 GHz band of a WiFi network (SSID or VAP). Generally, more channels and bandwidth are available in the 5 GHz band, causing less interference and allowing for a better user experience. By default, band steering is disabled.

To enable or disable band steering for a WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic**.
   The page that displays lets you select an SSID.
5. Click the **>** button to the left the SSID.
   The settings for the selected SSID display.
6. Under Band Steering, select one of the following radio buttons:

- **Enable**. Band steering is enabled for the WiFi network.
- **Disable**. Band steering is disabled for the WiFi network.

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

Change the RSSI Threshold for a WiFi Network

You can enter the minimum received signal strength indicator (RSSI) value in decibel milliwatts (dBm) for a WiFi device to connect to the 2.4 GHz or 5 GHz radio on the access point. If the RSSI value on the WiFi device is less than the configured RSSI value on the access point, the WiFi device cannot connect to the access point. For example, if the configured RSSI value on the access point is –70 dBm but the RSSI value on the WiFi device is –75 dBm, the WiFi device cannot connect to the access point. If the WiFi device is connected to the access point and then moves away from the access point, causing its RSSI value to become too low, the WiFi device is disconnected from the access point and an alarm is raised on the access point.

The value must be in the range of –100 to –10 dBm. The default is –100 dBm.

To change the RSSI threshold for a WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic**.
   The page that displays lets you select an SSID.
5. Click the **>** button to the left the SSID.
   The settings for the selected SSID display.
6. In the **RSSI Threshold (-100 to -10)** field, enter a value from –100 to –10 dBm.
   A higher value (for example, –10 dBm) indicates that the signal strength must be strong for a WiFi device to be able to connect to the radio. A lower value (for example, –100 dBm) indicates that the signal strength can be weak for a WiFi device to be able to connect to the radio. However, a connection that is based on a weak signal can be unreliable.
7. Click the **Apply** button.
   Your settings are saved.

Change the VLAN ID for a WiFi Network

This VLAN ID is not the same as the 802.1Q VLAN ID that is used for the wired network (see *Set the 802.1Q VLAN and Management VLAN* on page 85).

To change the VLAN ID for a WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic**.

   The page that displays lets you select an SSID.
5. Click the **>** button to the left the SSID.

   The settings for the selected SSID display.
6. In the **VLAN ID** field, enter a value.

   By default, the VLAN ID for a WiFi network is 1.
7. Click the **Apply** button.

   Your settings are saved.

Select a MAC ACL for a WiFi Network

After you set up one or more local MAC access control lists (ACLs, also referred to as access lists; see *Manage Local MAC Access Control Lists* on page 69), you can select an ACL for use with an SSID.

You can also set up a RADIUS server (see *Set Up RADIUS Servers* on page 80) and select the RADIUS MAC ACL. You must define the ACL on the RADIUS server, using the following format for client MAC addresses in the RADIUS server: If the client MAC address is 00:0a:95:9d:68:16, specify it as 000a959d6816 in the RADIUS server.

Note A RADIUS MAC ACL cannot function if the WiFi security is WPA2 Enterprise. If you want to use a RADIUS MAC ACL, select a different type of WiFi security for the WiFi network (see *Set Up an Open or Secure WiFi Network* on page 30).

When selected, the MAC ACL blocks WiFi access to the SSID for WiFi devices that are not in the selected access list. The blockage applies only to the SSID for which you enable the MAC ACL. Only WiFi devices that are in the selected access list can connect to the SSID.

To select a MAC ACL for a WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic**.
   The page that lets you select an SSID displays.
5. Select the SSID.
   The WLAN settings for the SSID display.
6. Select the **MAC ACL** check box.
7. Do one of the following:
   - Select the **Local MAC ACL** radio button, and from the **Select Group** menu, select the MAC ACL that you defined earlier (see *Manage Local MAC Access Control Lists* on page 69).
   - Select the **Radius MAC ACL** radio button.
     This option functions only if you set up a RADIUS server (see *Set Up RADIUS Servers* on page 80).
8. Click the **Apply** button.
   Your settings are saved. Only WiFi devices for which the MAC address is on the MAC ACL can connect to the access point through this SSID. (These devices might be able to connect to the access point through another SSID if you did not set up MAC ACL security for that SSID.)

Set Bandwidth Rate Limits for a WiFi Network

You can set rate limits for the upload and download bandwidths for devices that are connected to a WiFi network. The minimum bandwidth rate is 64 Kbps, the maximum bandwidth rate is 1024 Mbps. You can set one rate for the upload bandwidth and another rate for the download bandwidth.

To set bandwidth rate limits for devices that are connected to a WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard page displays.

4. Select **Management > Configuration > Wireless > Basic**.
   The page that lets you select an SSID displays.
5. Select the SSID.
   The WLAN settings for the SSID display.
6. Select the **Rate Limit** check box.
7. Specify the values:
   - **Upload**. For the upload bandwidth limitation, enter a value from 64 to 1024 and select **Kbps** or **Mbps** from the menu.
   - **Download**. For the download bandwidth limitation, enter a value from 64 to 1024 and select **Kbps** or **Mbps** from the menu.
8. Click the **Apply** button.
   Your settings are saved.

Register the Access Point With Facebook Wi-Fi

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 an existing Facebook business page (see *Set Up a Captive Portal for a WiFi Network* on page 43), you must register the access point with Facebook. By default, the capability to register is disabled.

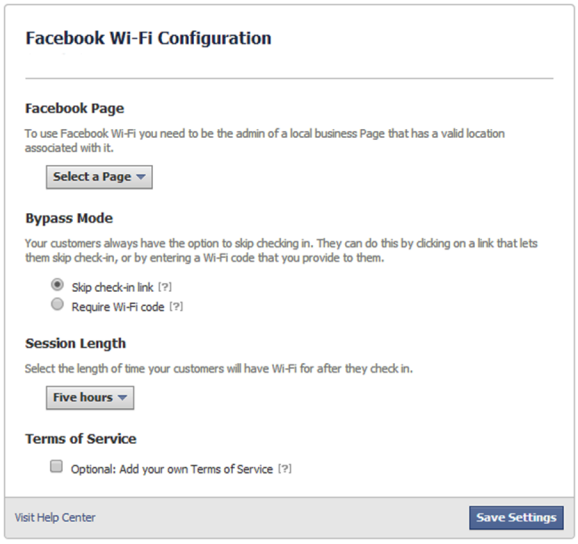
To register the access point with Facebook Wi-Fi:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic > Facebook Wi-Fi**.
   The Facebook Wi-Fi page displays.
5. Select the **Yes** radio button.
   The capability to register is enabled. By default, this capability is disabled.
6. Click the **Apply** button.
   Your settings are saved and the **Add Page** button displays.
7. Click the **Add Page** button.

A new browser page opens and displays the Facebook Login page.

8. Log in to the Facebook account with which the Facebook business page is associated.



9. From the **Select a Page** menu, select the Facebook business page.
10. Select one of the following bypass mode options:

    - 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.

11. From the **Session Length** menu, select the period after which users are automatically logged out.
12. 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.
13. 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.

Set Up a Captive Portal for a WiFi Network

Use a captive portal to welcome or instruct WiFi users and limit their sessions. You can require users to agree to an end user license agreement (EULA) and redirect them a specific website. A captive portal is specific to an SSID.

If you want to provide customers WiFi access by letting them check in to a Facebook business page, first register the access point with Facebook Wi-Fi (see *Register the Access Point With Facebook Wi-Fi* on page 42).

To set up a captive portal for a WiFi network:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

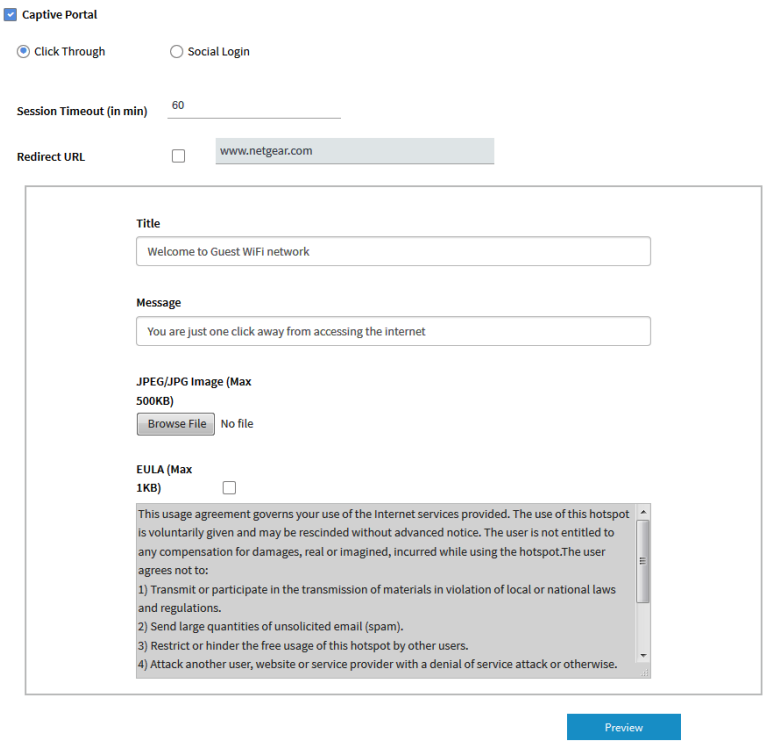
   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic**.

   The page that lets you select an SSID displays.
5. Select the SSID.

   The WLAN settings for the SSID display.
6. Select the **Captive Portal** check box.



7. Specify the type of captive portal by selecting one of the following radio buttons:

- **Click Through**. You must specify the captive portal settings as described in *Step 8*.
- **Social Login**. Customers receive WiFi access by checking in to a Facebook business page. To use this option, first register the access point with Facebook Wi-Fi (see *Register the Access Point With Facebook Wi-Fi* on page 42).
  If you select his option, you can skip *Step 8*.

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

Setting	Description
Session Timeout (in min)	Enter the time after which a WiFi session is terminated and a user must log in again. The period is in the range from 1 to 1440 minutes. The default is 60 minutes.
Redirect URL	To redirect a user to a specific website after login, select the **Redirect URL** check box and enter the URL to which the user must be directed. If the **Redirect URL** check box is cleared, a user is directed to a default web page.
Title	Enter the title that is displayed on the captive portal login page. If you do not customize the title, the default title displays on the captive portal login page.
Message	Enter a message to the user. This message is displayed on the captive portal login page. If you do not customize the message, the default message displays on the captive portal login page.
JPEG/JPG Image (Max 500KB)	To customize the image that is displayed on the captive portal login page, click the **Browse** button and navigate to and select an image. If you do not customize the image, the default image displays on the captive portal login page.
EULA (Max 1KB)	The field includes a default end user license agreement (EULA). You can enter or copy custom text into the field. To show the EULA on the captive portal login page, select the **EULA** check box.

9. To preview the captive portal login page, click the **Preview** button.

The following figure shows an example (that is, the figure does not show the default captive portal but a customized one).

10. Click the **Apply** button.

    Your settings are saved. WiFi clients attempting to connect to the SSID are presented with the captive portal login page.

Unregister the Access Point From Facebook Wi-Fi

If the access point is registered with Facebook Wi-Fi but you no longer want to use that option for a captive portal or you want to use another Facebook account, you can unregister the access point from Facebook Wi-Fi and remove the access point s entry.

To unregister the access point from Facebook Wi-Fi and remove the access point s entry:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic > Facebook Wi-Fi**.

   The Facebook Wi-Fi page displays.
5. Select the **No** radio button.

   The capability to register is disabled. However, the access point s entry on the Facebook business page is not yet removed.
6. Click the **Apply** button.

Your settings are saved.

7. Go to the Facebook business page and log in to your account.
8. Select the check box for the access point s entry.
9. Click the **Delete** button.
   The access point s entry is removed.

Manage the Basic Radio Features

You can manage the basic radio features that are described in the following sections:

For information about the advanced radio features, see *Manage the Advanced Radio Features* on page 59.

Manage the Basic Settings for the Radios

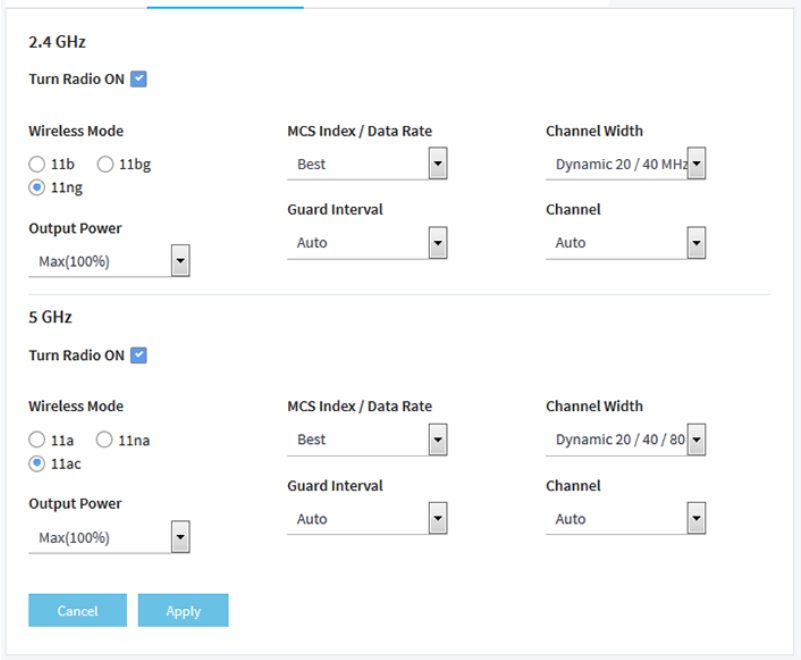
The basic WiFi settings for the radios apply to all WiFi networks (VAPs or SSIDs). You can specify the radio settings for the 2.4 GHz and 5 GHz radios individually. For information about the advanced radio settings, see *Manage the Advanced WiFi Settings for the Radios* on page 59.

To manage the basic WiFi settings for the radios:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

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



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

   The descriptions in the table apply to both radios, but you can specify the radio settings for the 2.4 GHz and 5 GHz radios individually.

Setting	Description
Turn Radio On	By default, the **Turn Radio On** check box is selected and the radio broadcasts. Turning off a radio disables WiFi access for the band, which can be helpful during configuration, network tuning, or troubleshooting.
Wireless Mode	Select one of the following WiFi modes for the 2.4 GHz radio: • **11b**. 802.11n, 802.11g, and 802.11b WiFi clients can connect to the access point. However, the speed of 802.11n and 802.11g clients is limited. • **11bg**. 802.11n, 802.11g, and 802.11b WiFi clients can connect to the access point. However, the speed of 802.11n clients is limited. • **11ng**. 802.11n, 802.11g, and 802.11b WiFi clients can connect to the access point. This is the default setting. Select one of the following WiFi modes for the 5 GHz radio: • **11a**. 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. However, the speed of 802.11ac and 802.11na clients is limited. • **11na**. 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. However, the speed of 802.11ac clients is limited. • **11ac**. 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. This is the default setting.

(Continued)

Setting	Description
MCS Index / Data Rate	From the menu, select the modulation and coding scheme (MCS) index and data transmit rate for the radio. The default is Best. For most networks, the default settings work fine. The available settings also depend on the selection from the **Channel Width** menu and the selection from the **Guard Interval** menu.
Channel Width	From the menu, select the channel width for the radio. Use the following guidelines: • A wider channel improves the performance. • The 802.11n specification allows a 40 MHz–wide channel in addition to the legacy 20 MHz channel that is available with other modes. • The 40 MHz channel enables higher data rates but leaves fewer channels available for use. • The 802.11ac specification allows an 80 MHz–wide channel in addition to the dynamic 20/40 MHz channel that is available with other modes. The channel width and guard interval determine the available MCS index and data transmit rates.
Output Power	From the menu, select the transmission power of the radio. You can select **Max(100%)**, **50%**, **25%**, **12.5%**, or **Min(4%)**. The default is Max(100%). **Note** If two or more access points are operating in the same area and on the same channel, interference can occur. In such a situation, you might want to decrease the output power for an access point. Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.

(Continued)

Setting	Description
Guard Interval	From the menu, select the value that protects radio transmissions from interference. An Auto guard interval (which is the default) improves performance, but some legacy devices can operate only with a long –800ns guard interval. The guard interval and channel width determine the available MCS index and data transmit rates.
Channel	From the menu, select the WiFi channel for the radio. The available WiFi channels and frequencies depend on the country and the radio. The default is Auto, which enables the radio to automatically select the most suitable channel. **Note** You do not need to change the WiFi channel unless you experience interference (which is indicated by lost connections). **Note** If you use multiple WiFi access points (APs), reduce interference by selecting different channels for adjacent APs. We recommend a channel spacing of four channels between adjacent APs (for example, use Channels 1 and 5, or 6 and 10).

6. Click the **Apply** button.
   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Turn a Radio On or Off

By default, both the 2.4 GHz and 5 GHz radios broadcast. Turning off a radio disables WiFi access for the associated band, which affects all VAPs (or SSIDs) in that band. Turning off a radio can be helpful during configuration, network tuning, or troubleshooting.

To turn a radio on or 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic > Wireless Settings**.
   The Wireless Settings page displays.
5. Take one of the following actions:

- **Turn a radio on**. Select the **Turn Radio ON** check box for the radio.
- **Turn a radio off**. Clear the **Turn Radio ON** check box for the radio.

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

Change the WiFi Mode for a Radio

By default, all types of WiFi clients can access a WiFi network on the access point, that is, the WiFi modes on the access point support 802.11n, 802.11g, 802.11b, 802.11ac, 802.11na, and 802.11a clients. You can change the modes to limit access to certain types of clients.

To change the WiFi mode for a radio:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic > Wireless Settings**.
   The Wireless Settings page displays.
5. Select the WiFi mode for the radio:

   - **2.4 GHz radio**. Select one of the following WiFi modes for the 2.4 GHz radio:
     - **11b**. 802.11n, 802.11g, and 802.11b WiFi clients can connect to the access point. However, the speed of 802.11n and 802.11g clients is limited.
     - **11bg**. 802.11n, 802.11g, and 802.11b WiFi clients can connect to the access point. However, the speed of 802.11n clients is limited.
     - **11ng**. 802.11n, 802.11g, and 802.11b WiFi clients can connect to the access point. This is the default setting.
   - **5 GHz radio**. Select one of the following WiFi modes for the 5 GHz radio:

- **11a**. 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. However, the speed of 802.11ac and 802.11na clients is limited.
- **11na**. 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. However, the speed of 802.11ac clients is limited.
- **11ac**. 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. This is the default setting.

6. Click the **Apply** button.

   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Change the MCS Index and Data Rate for a Radio

You can change the modulation and coding scheme (MCS) index and data transmit rate for a radio. By default, the setting is Best. The settings that are available also depend on the selected channel width (see *Change the Channel Width for a Radio* on page 52) and selected guard interval (see *Change the Guard Interval for a Radio* on page 54).

To change the MCS index and data rate for a radio:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic > Wireless Settings**.

   The Wireless Settings page displays.
5. From the **MCS Index / Data Rate** menu, select a setting.

   By default, the setting is Best.
6. Click the **Apply** button.

   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Change the Channel Width for a Radio

Use the following guidelines when you determine the channel width for a radio:

- A wider channel improves the performance.
- The 802.11n specification allows a 40 MHz–wide channel in addition to the legacy 20 MHz channel that is available with other modes.

- The 40 MHz channel enables higher data rates but leaves fewer channels available for use.
- The 802.11ac specification allows an 80 MHz–wide channel in addition to the dynamic 20/40 MHz channel that is available with other modes.

The channel width and guard interval determine the available MCS index and data transmit rates.

To change the channel width for a radio:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic > Wireless Settings**.
   The Wireless Settings page displays.
5. From the **Channel Width** menu, select one of the following settings.
   - **20 MHz**.
   - **40 MHz**.
   - **Dynamic 20 / 40 MHz**. This is the default setting for the 2.4 GHz radio.
   - **Dynamic 20 / 40 / 80 MHz**. This selection is available only for the 5 GHz radio and is the default setting for that radio.
6. Click the **Apply** button.
   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Change the Output Power for a Radio

By default, the output power of the access point is set at the maximum. If two or more access points are operating in the same area and on the same channel, interference can occur. In such a situation, you might want to decrease the output power for an access point. Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.

To change the output power for a radio:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.

The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard page displays.

4. Select **Management > Configuration > Wireless > Basic > Wireless Settings**.
   The Wireless Settings page displays.
5. From the **Output Power** menu, select **Max(100%)**, **50%**, **25%**, **12.5%**, or **Min(4%)**.
   The default is Max(100%).
6. Click the **Apply** button.
   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Change the Guard Interval for a Radio

The guard interval protects radio transmissions from interference. An automatic guard interval (which is the default) improves performance, but some legacy devices can operate only with a long –800ns guard interval.

The guard interval and channel width determine the available MCS index and data transmit rates.

To change the guard interval for a radio:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic > Wireless Settings**.
   The Wireless Settings page displays.
5. From the **Guard Interval** menu, select one of the following settings:

   - **Auto**. This is the default setting.
   - **Long-800 ns**.

6. Click the **Apply** button.
   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Change the Channel for a Radio

The available WiFi channels and frequencies depend on the country and the radio. The default is Auto, which enables the radio to automatically select the most suitable channel.

Note You do not need to change the WiFi channel unless you experience interference (which is indicated by lost connections).

Note If you use multiple WiFi access points (APs), reduce interference by selecting different channels for adjacent APs. We recommend a channel spacing of four channels between adjacent APs (for example, use Channels 1 and 5, or 6 and 10).

To change the channel for a radio:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Basic > Wireless Settings**.

   The Wireless Settings page displays.
5. From the **Channel** menu, select a channel.

   The default is Auto. When you select a particular channel, the channel selection becomes static.
6. Click the **Apply** button.

   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Set Up a WiFi On/Off Schedule for the Radios

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. You can set up one WiFi schedule that applies to both radios.

To set up and enable a WiFi on/off schedule:

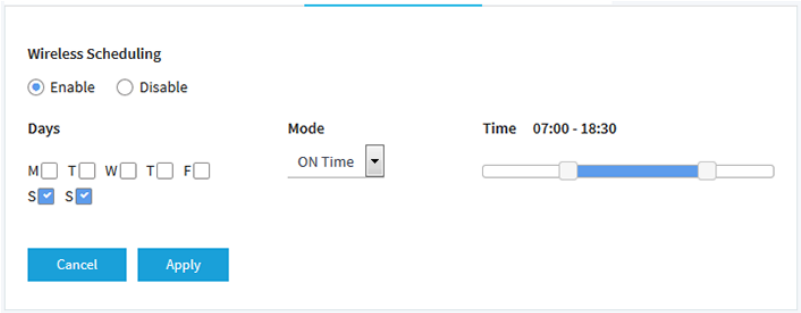
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard page displays.

4. Select **Management > Configuration > Wireless > Basic > Wireless Scheduling**.
   The Wireless Scheduling page displays.
5. Select the **Enable** radio button.



6. Specify the following settings:

   - **Days**. Select the check boxes for the days that you want the radios to be turned on or turned off. By default, Saturday and Sunday are selected.
   - **Mode**. From the menu, select whether the schedule turns on the radios (**ON Time**) or turns off the radios (**OFF Time**).
   - **Time**. Move the buttons on the slider to specify the time that you want the radios to be either turned on or turned off.

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

Manage Quality of Service for a WiFi Radio

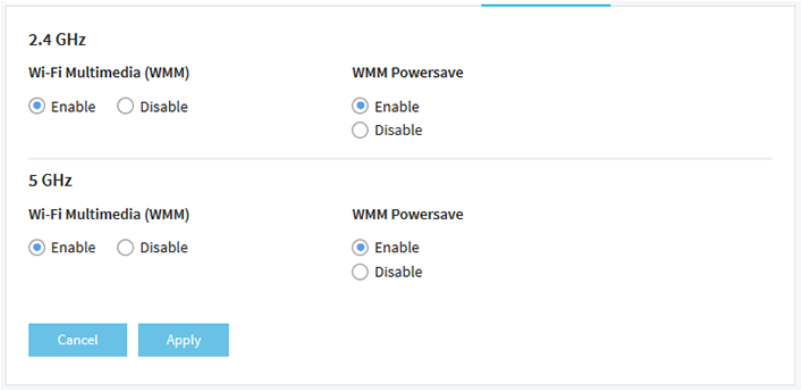
You can specify the Quality of Service (QoS) setting for the 2.4 GHz and 5 GHz radios separately. These settings are enabled by default for both radios.

To manage the QoS settings for WiFi:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

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



5. Enable or disable the following features for a radio by selecting the applicable **Enable** or **Disable** radio buttons:

   - **Wi-Fi Multimedia (WMM)**. WiFi Multimedia (WMM) is a subset of the 802.11e standard. Time-dependent information such as video or audio is given higher priority than normal traffic. For WMM to function correctly, WiFi clients must also support WMM. By enabling WMM, you allow WMM to control upstream traffic flowing from WiFi devices to the access point and downstream traffic flowing from the access point to WiFi devices. WMM defines the following four queues in decreasing order of priority:

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

   - **WMM Powersave**. Enabling the WMM Powersave feature saves power for battery-powered devices and fine-tunes power consumption.

6. Click the **Apply** button.

   Your settings are saved.

Manage the Advanced WiFi and Radio Features

4

This chapter describes how you can manage the advanced WiFi and radio features of the access point. For information about the basic WiFi and radio settings, see *Manage the Basic WiFi and Radio Features* on page 29.

Tip If you want to change the settings of the access point's WiFi network, use a wired connection to avoid being disconnected when the new WiFi settings take effect.

The chapter includes the following sections:

Manage the Advanced Radio Features

You can manage the advanced radio features that are described in the following sections:

For information about the basic radio features, see *Manage the Basic Radio Features* on page 47.

Manage the Advanced WiFi Settings for the Radios

The advanced WiFi settings for the radios apply to all WiFi networks (VAPs or SSIDs). You can specify the radio settings for the 2.4 GHz and 5 GHz radios individually. For information about the basic radio settings, see *Manage the Basic Settings for the Radios* on page 47.

A radio must be turned on for you to specify the settings. For more information about turning a radio on, see *Turn a Radio On or Off* on page 50.

To manage the advanced WiFi settings for the radios:

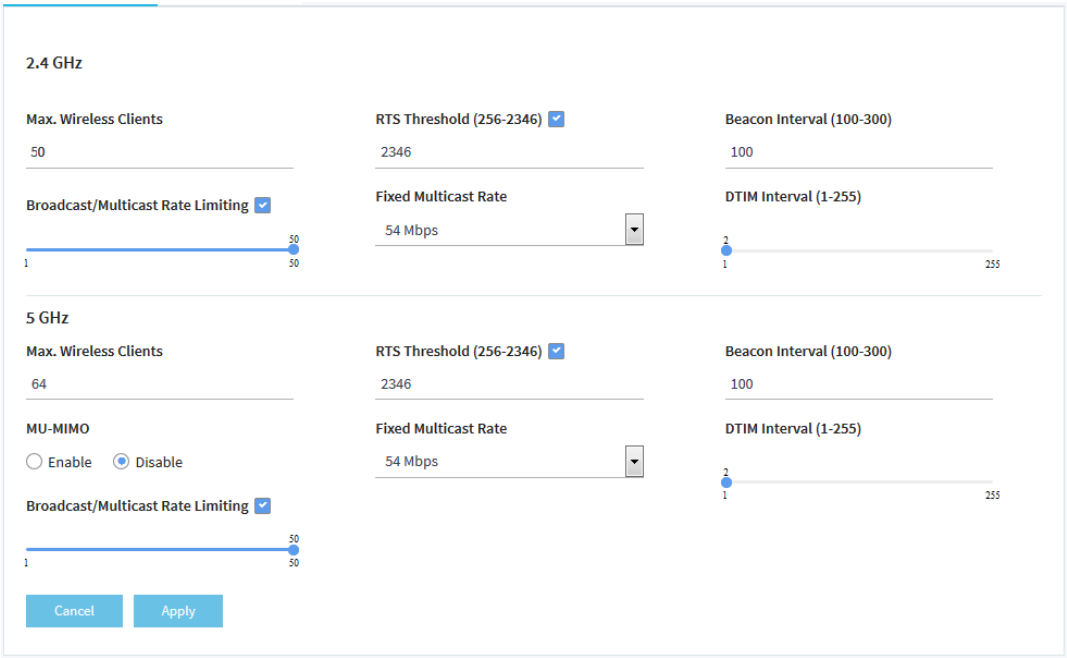
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Select **Management > Configuration > Wireless > Advanced**.



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

   The descriptions in the table apply to both radios. Except for the MU-MIMO feature, you can specify the radio settings for the 2.4 GHz and 5 GHz radios individually.

Setting	Description
Max. Wireless Clients	Enter the maximum number of WiFi clients that can simultaneously associate with the radio. The range is from 1 to 50. The default is 50 WiFi clients.
RTS Threshold (256-2346)	Enter the Request to Send (RTS) threshold. The range is from 256 to 2346. The default is 2346. If the packet size is equal to or less than the RTS threshold, the radio uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism and the data frame is transmitted immediately after the silence period. If the packet size is larger than the RTS threshold, the system uses the CSMA with Collision Avoidance (CSMA/CA) mechanism. In this situation, the transmitting device sends the RTS packet to the receiving device and waits for the receiving device to return a Clear to Send (CTS) packet before sending the actual packet data.
Beacon Interval (100-300)	Enter an interval between 100 ms and 300 ms for each beacon transmission, which allows the radio to synchronize the WiFi network. The default is 100 ms.
Broadcast/Multicast Rate Limiting	Multicast and broadcast rate limiting is enabled by default to improve the overall network performance by limiting the number of packets that are transmitted across the network. By default, the setting is 50 (the maximum possible value), which specifies a maximum rate limit of 50 packets per second. To change the setting, move the slider. To disable multicast and broadcast rate limiting, clear the small check box.
Fixed Multicast Rate	From the menu, select the multicast traffic transmission rate for the radio. The default is 54 Mbps (the maximum possible value). You can also select **Auto** and let the access point automatically adjust the multicast traffic transmission rate.

(Continued)

Setting	Description
DTIM Interval (1-255)	Move the slider to specify the delivery traffic indication message (DTIM) interval or 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 is 1.
MU-MIMO	Select the MU-MIMO **Enable** radio button to enable multiuser MIMO (MU-MIMO). By default, the MU-MIMO **Disable** radio button is selected and MU-MIMO is disabled. 802.11ac Wave 2 supports MU-MIMO, which enables multiple users to receive data from the access point simultaneously using the same channel. With MU-MIMO, the access point can transmit to multiple clients simultaneously using the same channel. MU-MIMO is used in the downstream direction and requires both the access point and the WiFi clients to be capable of 802.11ac Wave 2. You can enable or disable MU-MIMO for the 5 GHz radio but not for the 2.4 GHz radio.

6. Click the **Apply** button.
   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Manage the Maximum Number of Clients for a Radio

The number of clients that are allowed to associate with a radio affects the reliability and throughput of the WiFi connection. A smaller number can increase the reliability and throughput and a large number can decrease the reliability and throughput.

By default, a radio allows up to 50 client associations. You can specify a higher or lower number of clients. If the number of associated clients exceeds the specified number, the radio rejects new client associations until the number drops below the specified number.

To manage the maximum number of clients for a radio:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Advanced**.
   The Wireless Settings page displays.
5. In the **Max.Wireless Clients** field, enter the maximum number of WiFi clients that can simultaneously associate with the radio.

The range is from 1 to 50. The default is 50 WiFi clients.

6. Click the **Apply** button.

   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Manage the Broadcast and Multicast Settings for a Radio

Because multicast and broadcast traffic can adversely affect the throughput and latency of a WiFi network, you can change the multicast and broadcast rate limiting settings and the fixed multicast traffic transmission rate for a radio.

By default, multicast and broadcast rate limiting is enabled to improve the overall network performance by limiting the number of packets that are transmitted across the network. By default, the setting is 50 (the maximum possible value), which specifies a maximum rate limit of 50 packets per second. You can lower this number.

The multicast traffic transmission rate for the radio is 54 Mbps (the maximum possible value). You can specify a lower transmission rate.

To manage the broadcast and multicast settings for a radio:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.

3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Select **Management > Configuration > Wireless > Advanced**.

   The Wireless Settings page displays.

5. To change the multicast and broadcast rate limiting settings for a radio, under Broadcast/Multicast Rate Limiting, take one of the following actions in:

   - To change the rate limiting setting, move the slider. By default, the setting is 50 (the maximum possible value), which specifies a maximum rate limit of 50 packets per second.
   - To disable or enable multicast and broadcast rate limiting, clear or select the small check box.

6. To change the multicast traffic transmission rate for a radio, from the **Fixed Multicast Rate** menu, select a transmission rate.

   The default is 54 Mbps (the maximum possible value). You can also select **Auto** and let the access point automatically adjust the multicast traffic transmission rate.

7. Click the **Apply** button.

   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Manage Load Balancing for the Radios

You can configure the radio utilization thresholds to enable both radios to maintain the speed and performance of the WiFi network as clients associate with and disassociate from the WiFi network.

Client associations depend on the percentage of network bandwidth utilization that you specify and the WLAN utilization for each radio, which you can view in the Current Trend pane on the Dashboard page. New client associations are allowed if a radio's WLAN utilization is less than the percentage of network bandwidth utilization for the radio. New client associations are not allowed if a radio's WLAN utilization exceeds the percentage of network bandwidth utilization for the radio.

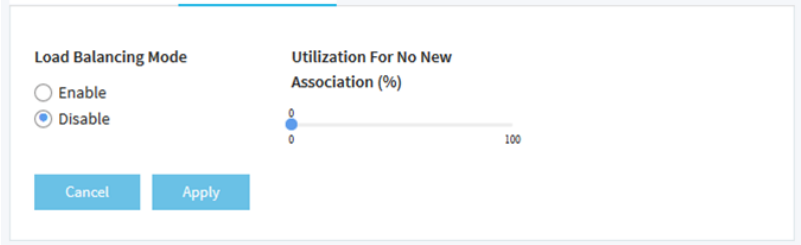
To manage load balancing for the radios:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Advanced > Load Balancing**.



5. To enable load balancing for both radios, select the Load Balancing Mode **Enable** radio button.

   By default, load balancing is disabled.
6. Move the slider to specify the percentage of network bandwidth utilization that is allowed on each radio before a radio stops accepting new client associations.

   The default is 0, which specifies that all new associations are allowed, regardless of the utilization rate. (In effect, a setting of 0 disables load balancing.) The configured settings applies to both radios.
7. Click the **Apply** button.

   Your settings are saved.

Set Up a WiFi Bridge Between Access Points

You can configure a wireless distribution system (WDS) that consists of point-to-point WiFi bridge connections between two access points. Each WiFi bridge connection requires a WDS profile for which the settings must match on the access points that make up the bridge.

If the access point is connected to the Internet over a wired connection, the access point can function as the WiFi base station for up to four other access points that function as WiFi repeaters. The access point itself can also function as a WiFi repeater if it is connected to another access point that functions as a WiFi base station.

A WiFi base station connects to the Internet, wired and WiFi clients can connect to the base station, and the base station sends its WiFi signal to one or more access points that function as WiFi repeaters. Wired and WiFi clients can also connect to a WiFi repeater, but the repeater connects to the Internet through the WiFi base station.

The following figure shows a WiFi repeating scenario with a WiFi base station on the left side and a single WiFi repeater on the right side.

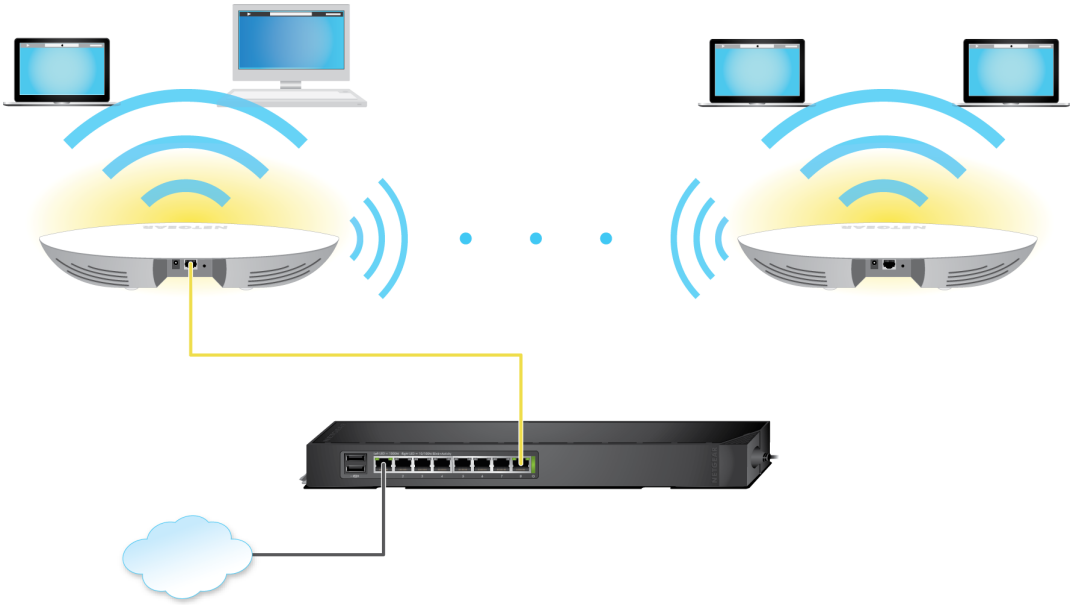


Figure 6. WiFi bridge configuration between two access points

To use a WiFi bridge, you cannot use the auto channel feature for the access point and the SSID broadcast must be enabled.

For a WiFi bridge, you must set up a WiFi base station (the master) and a WiFi repeater (the slave):

- **WiFi base station**. The access point functions as the master that bridges traffic to and from the repeater access point (the slave). The base station also handles local WiFi and wired traffic. To configure this mode, you must know the MAC address of the repeater access point. The MAC address is listed on on the product label or on the WiFi bridge configuration page of the local browser interface.
- **WiFi repeater**. The access point functions as the slave and sends all traffic from its local WiFi or wired computers to the WiFi base station (the master). To configure this mode, you must know the MAC address of the base station.

By default, the access point functions in dual-band concurrent mode. If you enable the WiFi repeater in either radio band, the WiFi base station or WiFi repeater cannot be enabled in the other radio band. However, if you enable the WiFi base station in either radio band and use the other radio band for either client access or as a WiFi base station, dual-band concurrent mode is not affected.

Before you can set up a WiFi network with WDS, your configuration must meet the following conditions:

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

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

CAUTION:

If you set up a WiFi bridge between two PoE access points, each of which is connected to a PoE switch with a network connection, you might be creating a loop and connectivity problems might occur. In such a situation, use a power adapter for the WiFi repeater (slave) so that you do not need to connect it to a PoE switch.

To set up a WiFi bridge between two access points:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

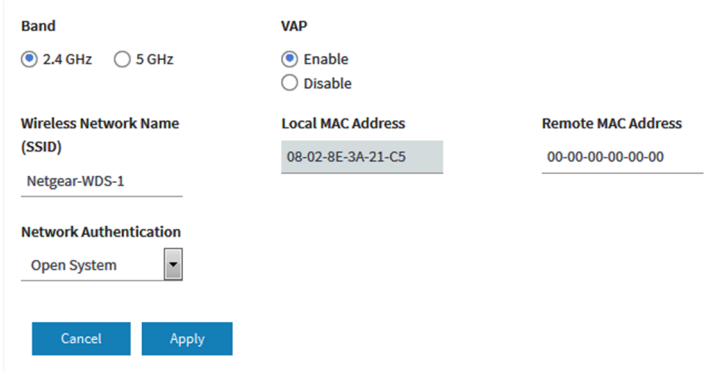
   The Dashboard page displays.
4. Select **Management > Configuration > Wireless > Wireless Bridge**.

   The page that displays lets you select a WDS profile (WDS 1, WDS 2, WDS 3, or WDS 4).
5. Click the **>** button to the left of a WDS profile.

   The WDS profile page displays.
6. Select the Band **2.4 GHz** or **5 GHz** radio button.

   Your selection determines the radio band on which the WDS is established. For countries that do not support dual-band operation, you cannot select the radio.
7. Select the VAP **Enable** radio button.

By default, a WDS profile is disabled.



8. Configure the WDS profile settings as described in the following table.

Setting	Description
Wireless Network Name (SSID)	The WiFi network name on which the WDS is established. The default name is Netgear-WDS-x, in which x is the number of the WDS (1, 2, 3, or 4).
Local MAC Address	The MAC address of the local WDS radio interface, that is, the MAC address of the local radio on which the WDS is established. You cannot change this MAC address on this page. The MAC address is displayed for your information. Enter this MAC address on the remote access point of the WDS connection.
Remote MAC Address	The MAC address of the remote WDS radio interface, that is, the MAC address of the remote radio on which the WDS is established.
Network Authentication, Data Encryption, and Passphrase	By default, the selection from the menu is Open System, in which case authentication and data encryption are not applicable. To secure the WDS connection, select **WPA2-PSK** and specify the following settings: • **Data Encryption**. The data encryption is AES and you cannot change this setting. • **Passphrase**. The passphrase for the WDS connection. For you to enable the WDS connection, the passphrase on the remote access point must match the passphrase that you define in this field.

9. Click the **Apply** button.
   Your settings are saved. The access point restarts with the new settings.

10. Configure the WiFi bridge settings on the access point at the other end of the WiFi bridge and restart that access point.
    The WiFi bridge is established.

11. Verify connectivity across the LANs of both access points.
    If the configuration is set up correctly, a computer on any WiFi or wired LAN segment of the access point that functions as the WiFi repeater can connect to the Internet or share files and printers with any other computer or server connected to the access point that functions as the WiFi base station.

Manage Access and Security

5

This chapter describes how you can manage access and security features and user accounts.

The chapter includes the following sections:

Note For information about essential WiFi security (network authentication and encryption), see *Set Up an Open or Secure WiFi Network* on page 30.

Block Specific URLs and Keywords for Internet Access

You can set up a blacklist by specifying URLs (web addresses) for which Internet access must be blocked. You can also specify keywords that cause the access point to reject URLs that contain those keywords.

To set up a blacklist with URLs and keywords for which Internet access must be blocked:

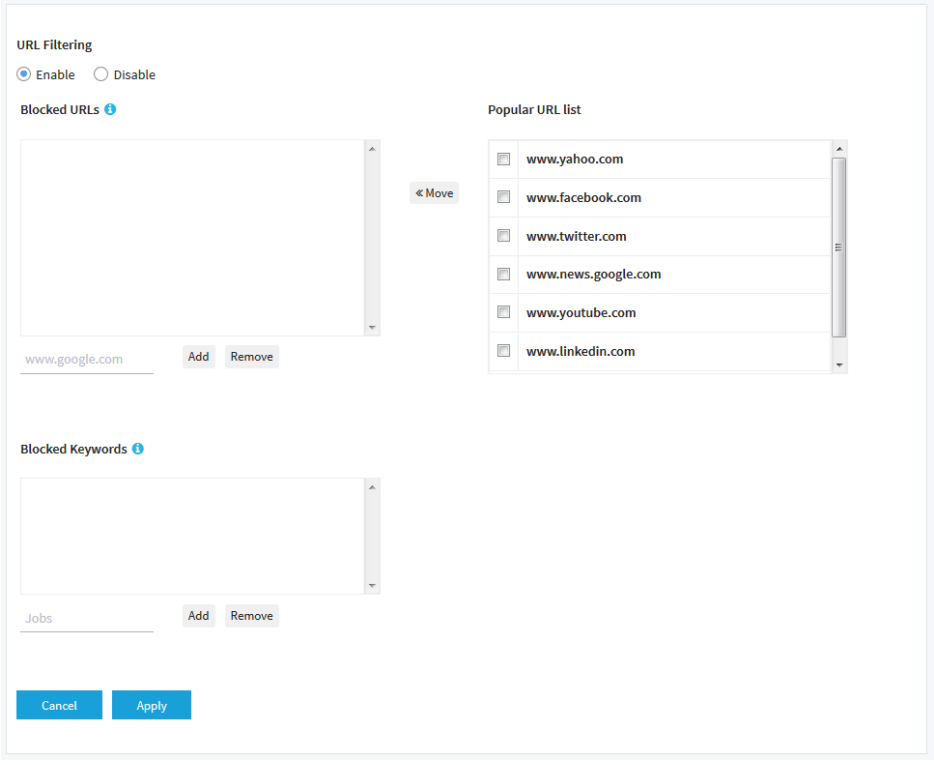
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Security > URL Filtering**.

   The URL Filtering page displays.
5. Select the **Enable** radio button.



6. Compose the blacklist in the following ways:

   - **Blocked URLs**. To add a URL to the blacklist, type or copy the URL in the upper field (to the left of the upper **Add** button) and click the upper **Add** button. You can also select one or more URLs

from the Popular URL list by selecting the check boxes for the URLS and clicking the **<< Move** button.
To remove a URL from the blacklist, select the check box for the URL and click the upper left **Remove** button.
When you block a URL, the domain and all URLs in the domain are blocked. For example, if you enter and add www.google.com, all web pages in the www.google.com domain are blocked, including, for example, www.google.com/finance.

- **Blocked Keywords**. To add a keyword entry to the blacklist, enter the keyword in the lower field (to the left of the lower **Add** button) and click the lower **Add** button.
  To remove a keyword entry from the blacklist, select the check box for the entry and click the lower **Remove** button.
  All URLs that contain the keyword are blocked. For example, if you enter and add Jobs, all URLs that contains Jobs (or jobs) are blocked.

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

Manage Local MAC Access Control Lists

The access point supports two local access control lists (ACLs) that are based on MAC addresses. Each local MAC ACL can contain a total number of 64 MAC addresses.

A WiFi device for which you place the MAC address on the ACL is allowed access to the WiFi network to which you apply the ACL. WiFi devices that are not on the ACL are not allowed access to the WiFi network to which you apply the ACL.

An ACL takes effect only after you apply it to a WiFi network. For information about applying an ACL to a WiFi network, see *Select a MAC ACL for a WiFi Network* on page 40. You can apply a MAC ACL to more than one WiFi network.

The following sections describe how you can manage MAC ACLs:

- *Manually Set Up a MAC Access Control List* on page 69
- *Import an Existing MAC Access Control List* on page 71

Manually Set Up a MAC Access Control List

You can compose up to two access control lists (ACLs) that are each based on up to 64 MAC addresses. The default name for the first MAC ACL (referred to as Group 1) is Corporate. The default name for the second MAC ACL (referred to as Group 2) is Guest.

You can use a MAC ACL to control which WiFi devices can access a WiFi network. You can apply a MAC ACL to more than one WiFi network.

To manually set up a MAC ACL:

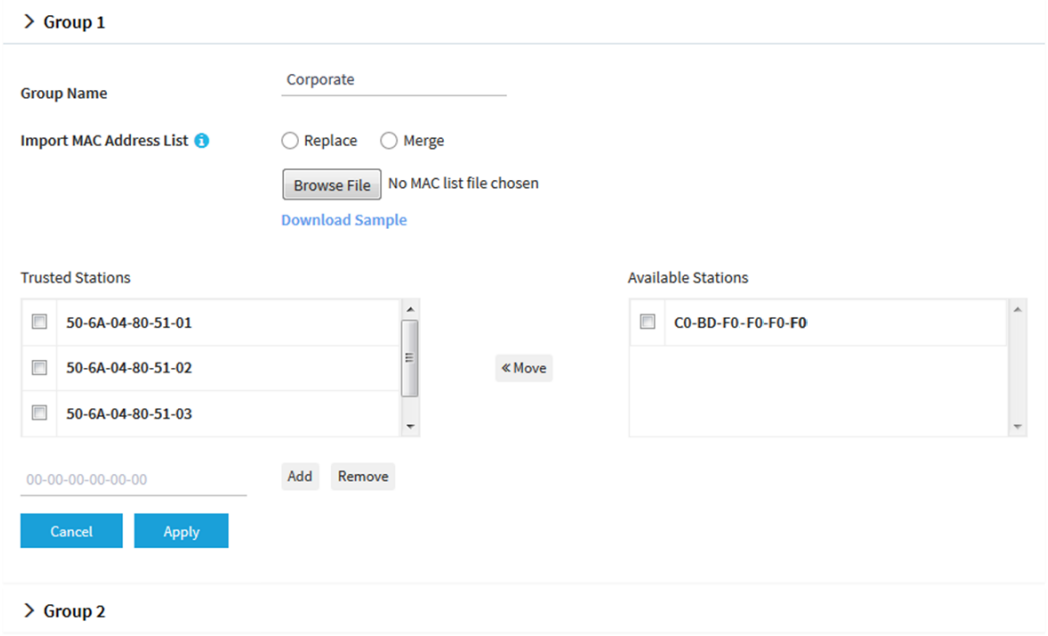
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.

3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Select **Management > Configuration > Security > MAC ACL**.



   The previous figure shows some examples. Devices in the Trusted Stations table are manually added, imported, or both added and imported. Devices in the Available Stations table are automatically detected by the access point, but you can also manually add devices to this table (see *Step 7*). All devices in the Available Stations table are common to Group 1 and Group 2, which allows you to add a device to both groups.

   By default, Group 1 is selected. Group 1 is the first MAC ACL.

5. To select Group 2 (which is the second MAC ACL), scroll down and click the **> Group 2** link.
6. To change the name for Group 1 or Group 2, enter a new name in the **Group Name** field.

   The default name for Group 1 is Corporate. The default name for Group 2 is Guest.

7. To manually add a device to the Available Stations table, do the following:

   a. Enter the MAC address in the format 00-00-00-00-00-00 in the field below the Available Stations table.

   b. Click the **Add** button.
      The device is added to the Available Stations table.

8. Compose the ACL in the following way:

- To move a device from the Available Stations table to the Trusted Stations table, select the check box for the device and click the **<< Move** button.
- To remove a device from the Trusted Stations table, select the check box for the device and click the **Remove** button.
  When you remove the device from the Trusted Stations table, the device is not moved to the Available Stations table.

9. Click the **Apply** button.

   Your settings are saved. WiFi devices in the Trusted Stations table can access the WiFi network to which you apply the ACL (see *Select a MAC ACL for a WiFi Network* on page 40).

Import an Existing MAC Access Control List

You can import an existing access control list (ACL) that is based on up to 64 MAC addresses. You can import the list into the first MAC ACL (referred to as Group 1 and named Corporate), into the second MAC ACL (referred to as Group 2 and named Guest), or into both.

The file with MAC addresses must be in the following format:

- Entries in the file must be MAC addresses only in hexadecimal format with each octet separated by a hyphen, for example 00-11-22-33-44-55.
- You must separate entries with a comma.
- The file must be in text format (that is, with a .txt or .cfg extension).

You can use a MAC ACL to control which WiFi devices can access a WiFi network. You can apply a MAC ACL to more than one WiFi network.

To import an existing MAC ACL:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

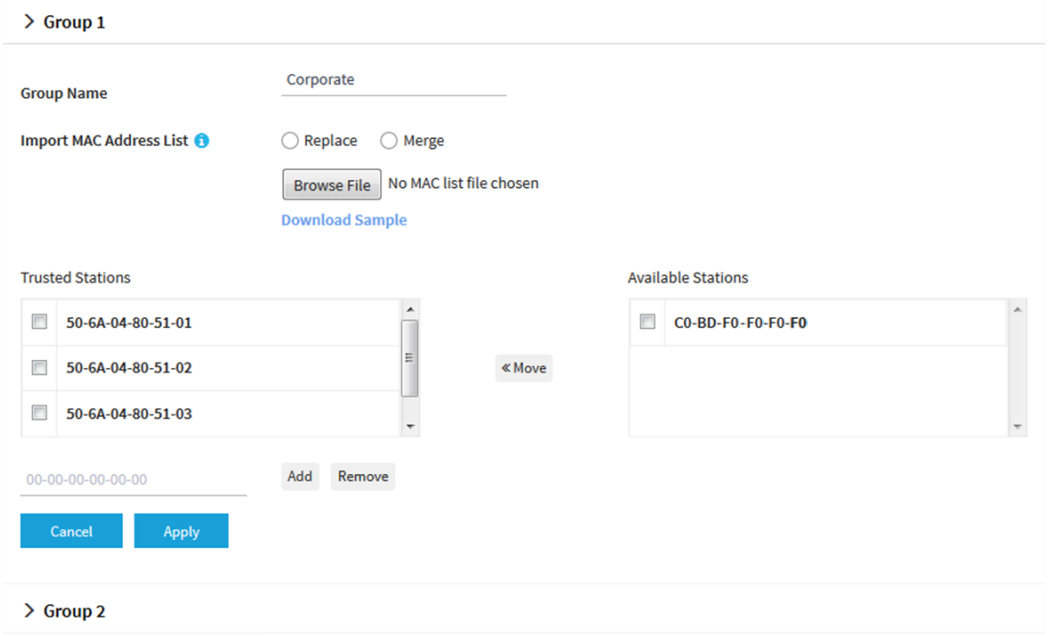
   A login window opens.

3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Select **Management > Configuration > Security > MAC ACL**.



The previous figure shows some examples. Devices in the Trusted Stations table are manually added, imported, or both added and imported. Devices in the Available Stations table are automatically detected by the access point, but you can also manually add devices to this table (see *Manually Set Up a MAC Access Control List* on page 69). All devices in the Available Stations table are common to Group 1 and Group 2, which allows you to add a device to both groups.

By default, Group 1 is selected. Group 1 is the first MAC ACL.

5. To select Group 2 (which is the second MAC ACL), scroll down and click the **> Group 2** link.
6. To change the name for Group 1 or Group 2, enter a new name in the **Group Name** field.
   The default name for Group 1 is Corporate. The default name for Group 2 is Guest.
7. To download a sample of a MAC ACL in the format that is required for importing, click the **Download Sample** link.
8. Import and compose the ACL in the following way:

   a. Replace or merge the MAC addresses in the import list with the MAC addresses in the Trusted Stations table by selecting one of the following radio buttons:

      - **Replace**. MAC addresses in the Trusted Stations table are replaced with the ones in the import list.
      - **Merge**. MAC addresses in the Trusted Stations table are merged with the ones in the import list.

   b. Click the **Browse** button and navigate to and select the import file.
      The MAC addresses on the import list are placed in the Trusted Stations table.
   c. To remove a MAC address from the Trusted Stations table, select the MAC address and click the **Remove** button.

When you remove the device from the Trusted Stations table, the device is not moved to the Available Stations table.

9. Click the **Apply** button.

   Your settings are saved. For information about manually adding MAC addresses to those in the Trusted Stations table, see *Manually Set Up a MAC Access Control List* on page 69.

   WiFi devices in the Trusted Stations table can access the WiFi network to which you apply the ACL (see *Select a MAC ACL for a WiFi Network* on page 40).

Manage User Accounts

User accounts provide either read/write or read-only access to the local browser interface of the access point. You can add, change, or delete user accounts. You cannot delete or change the default admin user account except for the password.

The following sections describe how you can manage user accounts:

For information about changing the password for the default admin user account, see *Change the Admin User Account Password* on page 94.

Add a User Account

To add 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

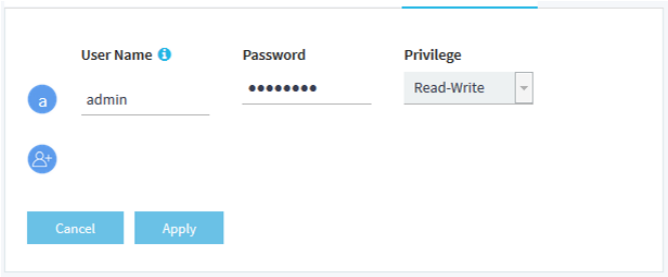
   A login window opens.

3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Select **Management > Configuration > System > Advanced > User Accounts**.



5. Click the add user account icon.
   Additional fields and a menu display.
6. Specify the settings for the new user account:
   - **User Name**. Enter a user name.
   - **Password**. Enter a password between 4 and 12 characters in length.
     The ideal password contains no English dictionary words and contains uppercase and lowercase letters, numbers, and symbols. However, do not include quotation marks (") in the password.
   - **Privilege**. From the menu, select **Read-Write** or **Read-Only**.
7. Click the **Apply** button.
   Your settings are saved.

Change the Settings for a User Account

You cannot change the access privilege for the default admin user account.

To change the user name, password, or access 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > System > Advanced > User Accounts**.
   The existing user accounts display.
5. To the right of the user account, change the existing settings as needed:
   - **User Name**. Enter another user name.
   - **Password**. Enter another password between 4 and 12 characters in length.

The ideal password contains no English dictionary words and contains uppercase and lowercase letters, numbers, and symbols. However, do not include quotation marks (") in the password.

- **Privilege**. From the menu, select **Read-Write** or **Read-Only**.

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

Remove a User Account

You can remove a user account that you no longer need. You cannot remove the default admin user account.

To remove 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > System > Advanced > User Accounts**.
   The existing user accounts display.
5. Click the **X** to the right of the user account.
   The user account is removed.

Manage Neighbor AP Detection

The access point can detect neighbor access points (APs) and you can classify them as known APs.

If you enable neighbor AP detection, the access point continuously scans the WiFi network, collects information about all access points on the channels, and maintains a list of access points it detects in the area. Initially all detected access points are displayed in the Unknown AP List. You can add access points that you are familiar with to the Known AP List. You can also import a list of known access points in the Known AP List.

CAUTION:

Access points in the Unknown AP List require further investigation. They could be rogue access points, which use the SSID of a legitimate network. These types of access points can present a serious security threat.

The following sections describe how you can manage neighbor AP detection and add neighbor access points to the Known AP List:

Enable Neighbor Access Points Detection and Move Access Points to the Known AP List

The access point can detect neighbor access points (APs) and lets you classify them as known APs. After you enable neighbor AP detection, the access point maintains a list of access points it detects in the area. Initially all detected access points are displayed in the Unknown AP List. You can manually move access points from the Unknown AP List to the Known AP List.

By default neighbor access point detection is disabled.

To enable neighbor access point detection and move detected access points to the Known AP List:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

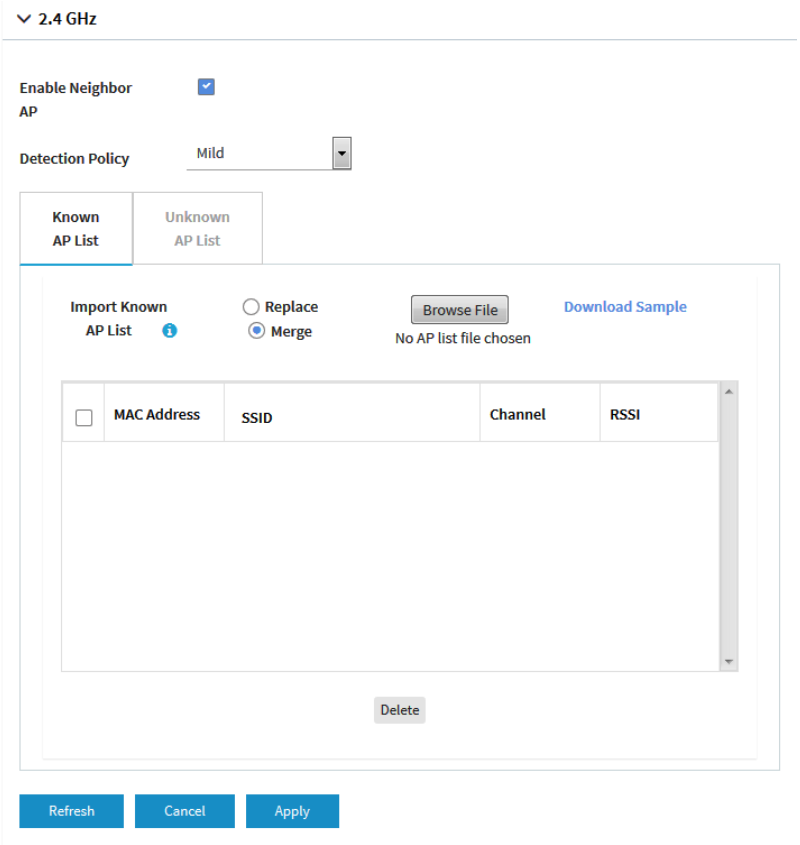
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Security > Neighbor AP**.

   The page that displays lets you select the radio band (2.4GHz or 5GHz).
5. Click the **>** button to the left of the radio band.

   The Neighbor AP page displays for the selected radio band.
6. Select the **Enable Neighbor AP** check box.
7. Click the **Apply** button.

Your settings are saved. Neighbor AP detection is now enabled.

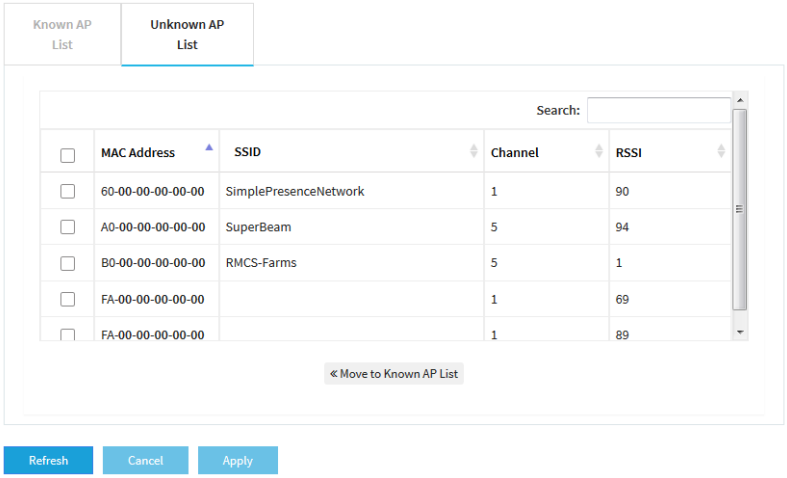


8. From the **Detection Policy** menu, select the scan method:

   - **Mild**. The access point scans for neighbor access points every 15 minutes. This is the default setting.
   - **Moderate**. The access point scans for neighbor access points every 5 minutes.
   - **Aggressive**. The access point scans for neighbor access points every 1 minute.

9. To move access points from the Unknown AP List to the Known AP List, do the following:

a. Click the **Unknown AP List** tab.



b. If no access points display, click the **Refresh** button.

c. Select the check boxes for the access points that you are familiar with.

d. Click the **<< Move to Known AP List** button.

e. Click the **Known AP List** tab.
The selected access points display in the Known AP List.

Note You can delete access points from the Known AP List. After being detected, these access points once more display in the Unknown AP List.

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

Import an Existing Neighbor Access Point List in the Known AP List

You can import a list with MAC addresses of known neighbor access points in the Known AP List.

The file with MAC addresses must be in the following format:

- Entries in the file must be MAC addresses only in hexadecimal format with each octet separated by a hyphen, for example 00-11-22-33-44-55.
- You must separate entries with a comma.
- The file must be in text format (that is, with a `.txt` or `.cfg` extension).

For information about enabling neighbor AP detection, see *Enable Neighbor Access Points Detection and Move Access Points to the Known AP List* on page 76.

To import a list with MAC addresses of known neighbor access points in the Known AP List:

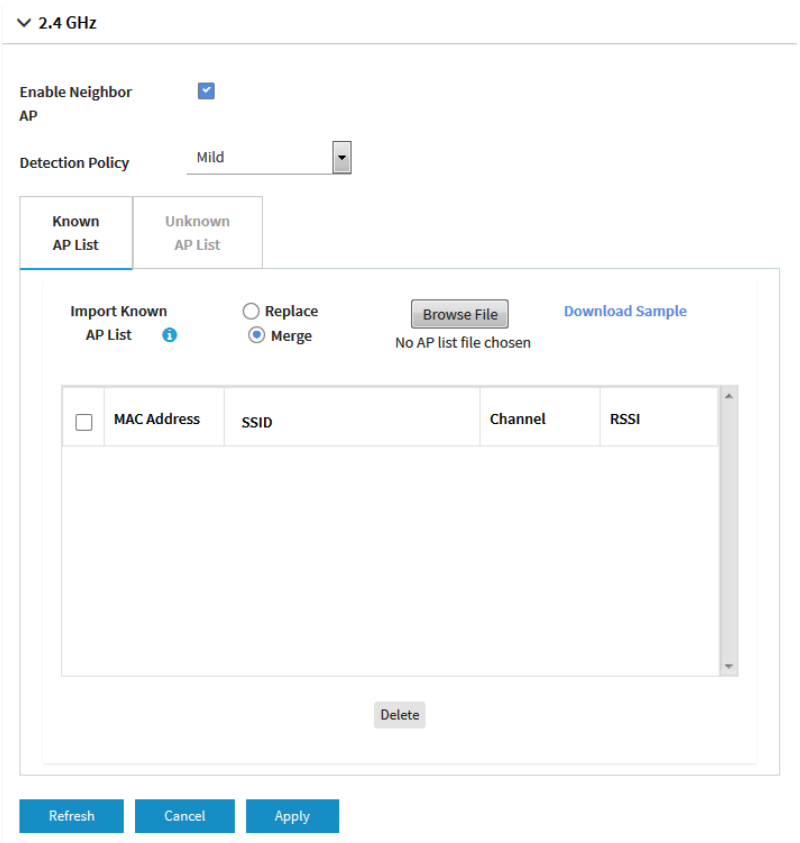
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > Security > Neighbor AP**.

   The page that displays lets you select the radio band (2.4GHz or 5GHz).
5. Click the **>** button to the left of the radio band.



6. To download a sample of a MAC ACL in the format that is required for importing, click the **Download Sample** link.
7. Import and compose the Known AP List in the following way:

a. Replace or merge the MAC addresses in the import list with the MAC addresses in the Known AP List by selecting one of the following radio buttons:

- **Replace**. MAC addresses in the Known AP List are replaced with the ones in the import list.
- **Merge**. MAC addresses in the Known AP List are merged with the ones in the import list.

b. Click the **Browse** button and navigate to and select the import file.
The MAC addresses on the import list are placed in the Known AP List.

c. To remove a MAC address from the Known AP List, select the MAC address and click the **Delete** button.
When you remove the device from the Known AP List, the device is not moved to the Unknown AP List.

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

Set Up RADIUS Servers

If you use WPA2 Enterprise security or a RADIUS MAC ACL, you must set up RADIUS servers for authentication, accounting, or both authentication and accounting using RADIUS. You must set up primary IPv4 servers and you can set up secondary IPv4 servers. These RADIUS server settings apply either to all WiFi networks that use WPA2 Enterprise security (see *Set Up an Open or Secure WiFi Network* on page 30) or to all WiFi networks that use a RADIUS MAC ACL.

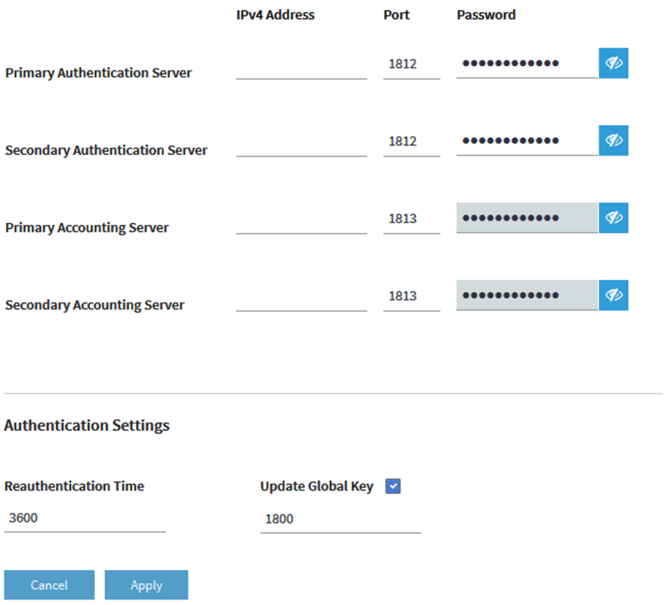
Note WPA2 Enterprise security and a RADIUS MAC ACL are mutually exclusive. If you want to use a RADIUS MAC ACL for a WiFi network, select a different type of WiFi security (see *Set Up an Open or Secure WiFi Network* on page 30). If you want to use WPA2 Enterprise security for a WiFi network, use a local MAC ACL (see *Manage Local MAC Access Control Lists* on page 69).

If you use a RADIUS MAC ACL, you must define the ACL on the RADIUS server, using the format in the following example for client MAC addresses in the RADIUS server: If the client MAC address is 00:0a:95:9d:68:16, specify it as 000a959d6816 in the RADIUS server.

To set up RADIUS servers:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
A login window opens.
3. Enter the access point user name and password.
The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The Dashboard page displays.

4. Select **Management > Configuration > Security > RADIUS Settings**.



5. For each RADIUS server that you want to set up, configure the following settings:

   - **IPv4 Address**. Enter the IPv4 address of the RADIUS server. The access point must be able to reach this IP address.
   - **Port**. Enter the number of the UDP port on the access point that is used to access the RADIUS server. For authentication servers, the default port number is 1812. For accounting servers, the default port number is 1813.
   - **Password**. Enter the password (shared key) that is used between the access point and the RADIUS server during the authentication or accounting process. By default, the password is sharedsecret.

6. Configure the following authentication settings, which apply to all RADIUS server that you set up:

   - **Reauthentication time**. Enter the interval in seconds after which the supplicant (the WiFi client) must be reauthenticated with the RADIUS server. The default interval is 3600 seconds (1 hour). Enter **0** to disable reauthentication.
   - **Update Global Key**. 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.

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

Manage the Local Area Network and IP Settings

6

This chapter describes how you can manage the local area network (LAN) and IP settings of the access point.

The chapter includes the following sections:

Disable the DHCP Client and Specify a Fixed IP Address

By default, the DHCP client of the access point is enabled and the access point receives an IP address from a DHCP server (or a router that functions as a DHCP server) in your network. If your network does not include a DHCP server or you prefer to specify a fixed (static) IP address, disable the DHCP client of the access point.

To disable the DHCP client and specify a fixed IP address:

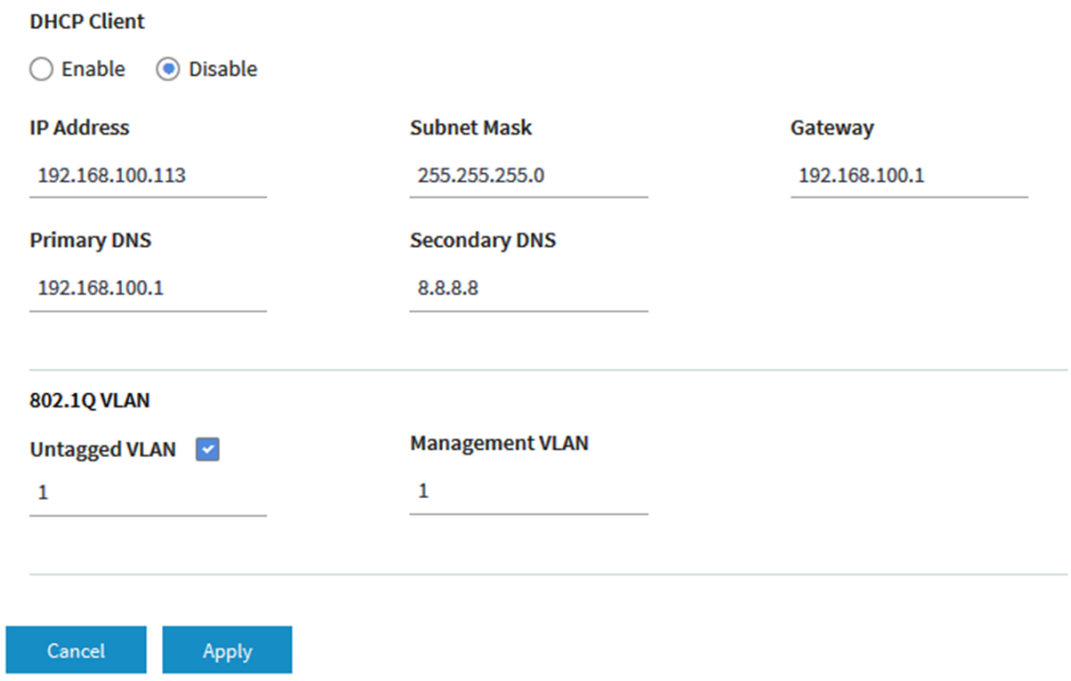
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > IP > LAN**.

   The page that displays lets you specify the LAN settings, but the fields are masked because the DHCP client is enabled.
5. Select the **Disable** radio button.



6. Specify the settings that are described in the following table.

Setting	Description
IP Address	IP address in the range that is used by your LAN (usually 255.255.255.0).
Subnet Mask	The subnet mask must be compatible with your LAN.
Gateway	IP address of the gateway on your LAN.
Primary DNS	IP address of the primary Domain Name System (DNS) server on your LAN.
Secondary DNS	IP address of the secondary DNS server on your LAN, or leave this field blank.

7. Click the **Apply** button.

   Your settings are saved. The access point restarts with the new IP settings.

Enable the DHCP Client

By default, the DHCP client of the access point is enabled and the access point receives an IP address from a DHCP server (or a router that functions as a DHCP server) in your network.

If you disabled the DHCP client, you can reenable it.

To enable the DHCP 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

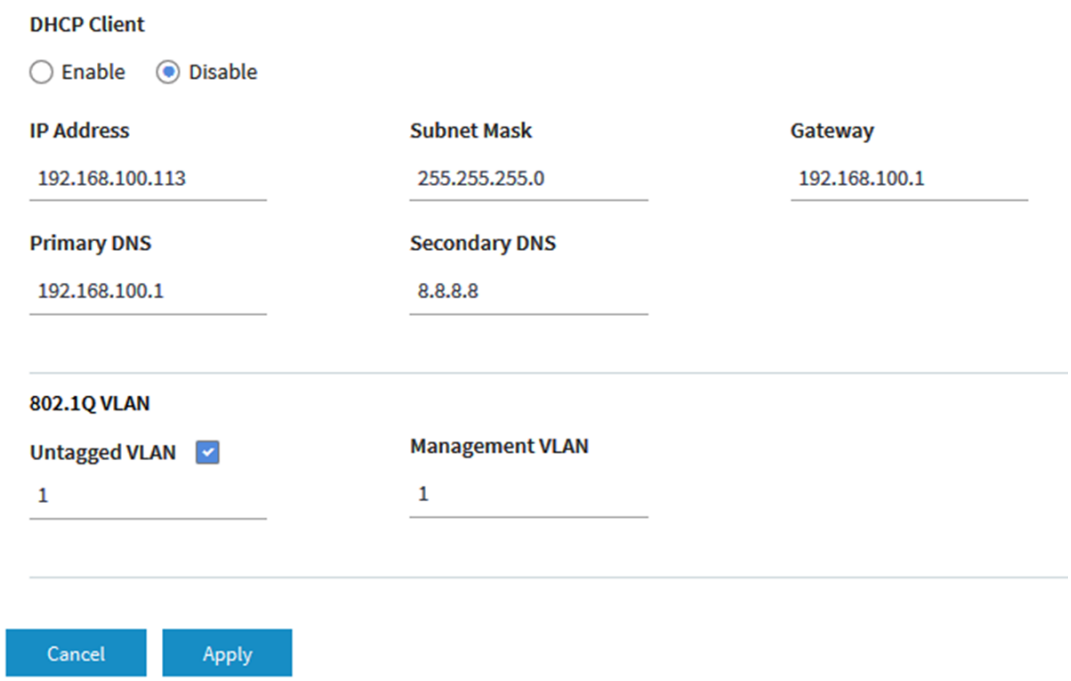
   A login window opens.

3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Select **Management > Configuration > IP > LAN**.



5. Select the **Enable** radio button.
   The fields are masked.
6. Click the **Apply** button.
   Your settings are saved. The access point restarts with the new IP settings. It might take a while before the access point receives its IP address setting from the DHCP server.

Set the 802.1Q VLAN and Management VLAN

The 802.1Q VLAN protocol on the access point logically separates traffic on the same physical (wired) network. This protocol can work with tagged and untagged VLANs, as follows:

- **Untagged VLAN**. The access point sends untagged frames from its Ethernet interface. Incoming untagged frames are assigned to the untagged VLAN. By default, the untagged VLAN is VLAN 1. By default, the access point functions with an untagged VLAN.
- **Tagged VLAN**. The access point tags all frames that it sends from its Ethernet interface. Only the incoming frames that are tagged with known VLAN IDs are accepted.

The management VLAN is used for managing traffic such as Telnet, SNMP, and HTTP traffic to and from the access point. Frames that belong to the management VLAN and that are sent over the trunk do not receive an 802.1Q header. If a port is a member of a single VLAN, its traffic can be untagged.

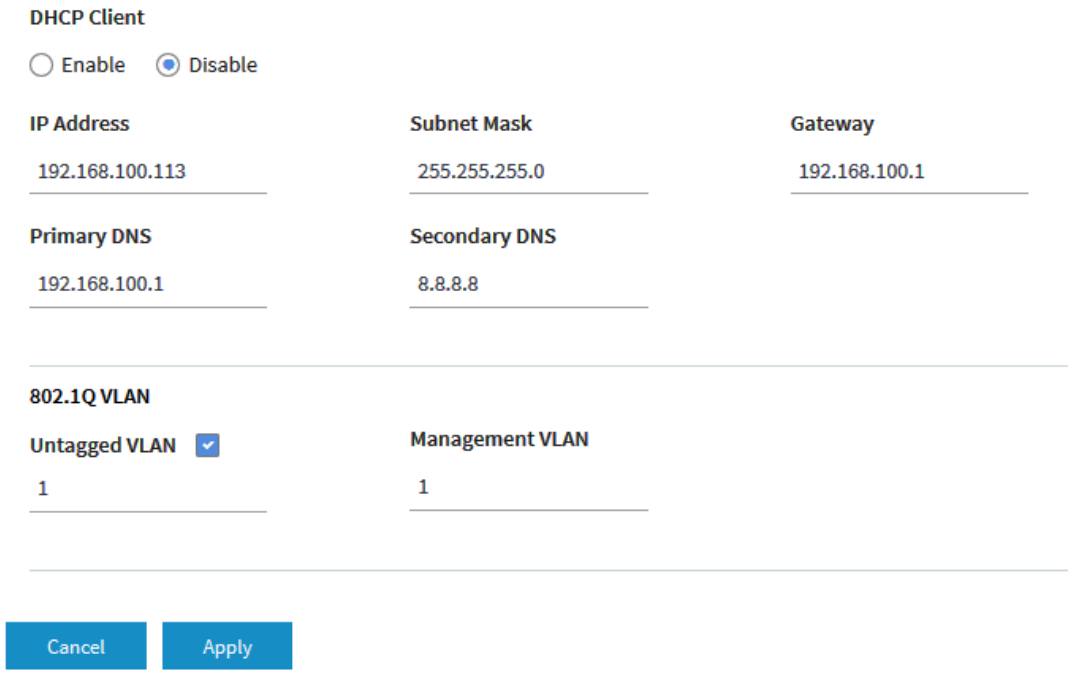
To set the 802.1Q VLAN and management VLAN:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > IP > LAN**.



5. To change the 802.1Q VLAN, either clear or select the **Untagged VLAN** check box:

   - **Untagged VLAN**. By default, the **Untagged VLAN** check box is selected. The access point sends untagged frames from its Ethernet interface. Incoming untagged frames are assigned to the untagged VLAN. By default, the untagged VLAN is VLAN 1 but you can enter another VLAN ID in the field if that VLAN ID is supported on your network.
   - **Tagged VLAN**. Clear the **Untagged VLAN** check box only if the hubs and switches on your LAN support the 802.1Q VLAN protocol. The access point tags all frames that it sends from its Ethernet interface. Only the incoming frames that are tagged with known VLAN IDs are accepted. Similarly, change the ID for the untagged VLAN only if the hubs and switches on your LAN support the 802.1Q VLAN protocol and the new VLAN ID is supported on your network.

6. To change the VLAN ID for the management VLAN, enter another VLAN ID in the **Management VLAN** field.

   By default, the management VLAN is VLAN 1. If you change the VLAN ID, be sure that the VLAN ID is supported on your network.

7. Click the **Apply** button.

   Your settings are saved. The access point restarts with the new VLAN settings.

Enable or Disable Spanning Tree Protocol

For locations where multiple access points are active, Spanning Tree Protocol (STP) can provide network traffic optimization by preventing path redundancy. If your location includes more than one access point, we recommend that you enable STP.

To enable or disable Spanning Tree Protocol:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.

3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Select **Management > Configuration > System > Advanced > General**.

   The General page displays.

5. Select one of the following radio buttons:

   - **Enable**. STP is enabled.
   - **Disable**. STP is disabled. This is the default setting.

6. Click the **Apply** button.

   Your settings are saved.

Enable or Disable Network Integrity Check

The network integrity check function enables the access point to validate whether the upstream link is active before the access point allows WiFi associations. Make sure that the default gateway is configured correctly. By default, the network integrity check function is disabled.

To enable or disable the network integrity check function:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > System > Advanced > General**.
   The General page displays.
5. Select one of the following radio buttons:
   - **Enable**. The network integrity check function is enabled.
   - **Disable**. The network integrity check function is disabled. This is the default setting.
6. Click the **Apply** button.
   Your settings are saved.

Enable or Disable IGMP Snooping

IGMP snooping allows IP multicast packets to be transmitted only to the members of a corresponding multicast group. Enabling IGMP snooping prevents flooding of multicast traffic to all the ports in a broadcast domain. By default IGMP snooping is disabled on the access point.

To enable or disable IGMP snooping:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > System > Advanced > General**.
   The General page displays.
5. Select one of the following radio buttons:

- **Enable**. IGMP snooping is enabled.
- **Disable**. IGMP snooping is disabled. This is the default setting.

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

Enable or Disable Ethernet LLDP

Link Layer Discovery Protocol (LLDP), as specified in IEEE 802.1AB, can provide link-layer messages to adjacent network devices. For example, LLDP lets network devices such as switches and management devices discover the access point in a network and detect if the access point receives power through PoE. By default, LLDP is enabled.

To enable or disable the LLDP:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > System > Advanced > Ethernet LLDP**.
   The Ethernet LLDP page displays.
5. Select one of the following radio buttons:

   - **Enable**. LLDP is enabled. This is the default setting.
   - **Disable**. LLDP is disabled.

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

Enable or Disable UPnP

Universal Plug and Play (UPnP) lets the access point be discovered by other devices in the network that support UPnP. UPnP is enabled by default.

To enable or disable UPnP:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

A login window opens.

3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Select **Management > Configuration > System > Advanced > UPnP**.
   The UPnP page displays.

5. Select one of the following radio buttons:

   - **Enable**. UPnP is enabled. This is the default setting.
   - **Disable**. UPnP is disabled.

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

Manage and Maintain the Access Point 7

This chapter describes how you can manage and maintain the access point.

The chapter includes the following sections:

Change the Management Mode to Insight or Standalone Mode

The access point can function in one of the following management modes:

- **Insight**. Select the **Insight** radio button to manage the access point from a mobile device on which the NETGEAR Insight app is installed. This is the default setting. Although you *can* connect to the access point over the local browser interface, only a basic and limited local browser interface is available. For information about the NETGEAR Insight app, see the NETGEAR knowledge base articles at *netgear.com/support*.
- **Standalone**. Select the **Standalone** radio button to manage the access point from a WiFi or wired device through the local browser interface.

IMPORTANT:
When you change the management mode, the configuration of the access point is reset (cleared) with the exception of the IP address, access point name, and password for the local browser interface. The access point restarts and broadcasts SSID Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address. The MAC address is listed on the product label. The default WiFi passphrase is sharedsecret.

To change the management mode to Insight mode or Standalone 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > System > Basic**.
   The General page displays the basic system settings.
5. Select one of the following radio buttons:
   - **Insight**. The access point functions in Insight management mode.
   - **Standalone**. The access point functions in Standalone management mode.

WARNING:
The configuration of the access point is reset (cleared) with the exception of the IP address, access point name, and password for the local browser interface. The access point restarts and broadcasts SSID Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address. The MAC address is listed on the product label. The default WiFi passphrase is sharedsecret.

6. Click the **Apply** button.
   Your settings are saved. The access point restarts in the new management mode.

Change the Country or Region of Operation

You can change the country or region in which the access point operates. Note the following:

- For products sold in the Unites States, the default country is preset and cannot be changed.
- For products sold outside the United States, you must select a country or region.
- 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.
- It might not be legal to operate the access point in a country or region other than those listed in the menu. If your country or region is not listed in the menu, you must check with your local government agency or check the NETGEAR website for information about which channels you can use.

To change the country or region of operation:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Configuration > System > Basic**.
   The General page displays the basic system settings.
5. Select a country or region from the **Country / Region** menu.
6. Click the **Apply** button.
   Your settings are saved. The access point restarts with the default WiFi settings that are specific to the selected country or region.

Change the Admin User Account Password

This admin user account password is the password that you use to log in to the local browser interface of the access point with the user name admin. It is not the passphrase that you use for WiFi access.

The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. However, do not include quotation marks in the password. The password must be between 6 and 32 characters in length.

To change the password for the user name admin:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in to the access point. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > System > Advanced > User Accounts**.

   The page that displays lets you change the user accounts.
5. Next to admin, in the **Password** field, enter the new password.
6. In the **Confirm Password** field, enter the same new password.

   Note You cannot change the user name. The name must remain admin.
7. Click the **Apply** button.

   Your settings are saved. The next time that you log in to the access point, you must use the new password. If you forget the new password, you must reset the access point to factory default settings. Doing so restores the password to the default password.

Change the System Name

The system name is a unique NetBIOS name for the access point. The default system name is located on the access point label. By default, the system name is Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address.

To change the system name:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.

3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Select **Management > Configuration > System > Basic**.
   The General page displays the basic system settings.

5. Enter a new name in the **System Name** field.
   Using the following guidelines:

   - The name must contain alphanumeric characters, can contain hyphens, and cannot be longer than 15 characters.
   - The name cannot start or end with a hyphen.
   - The name must contain at least one alphabetical character.

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

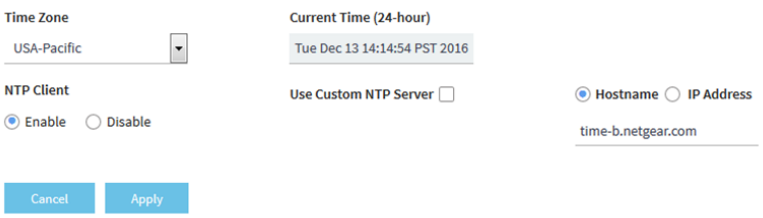
Specify a Custom NTP Server

By default, the access point receives its time from a default NETGEAR Network Time Protocol (NTP) server, but you can also specify a custom NTP server.

To specify a custom NTP 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > System > Basic > Time**.



By default, the **Enable** radio button is selected and the access point receives its time from a default NETGEAR NTP server.

5. Select the **Use Custom NTP Server** check box.
6. Take one of the following actions:

   - Enter the host name of the NTP server.
     By default, the **Hostname** radio button is selected.
   - Select the **IP address** radio button and enter the IP address of the NTP server.

7. Click the **Apply** button.

   Your settings are saved. When the access point connects over the Internet to the new NTP server, the date and time that display on the page are adjusted according to your settings.

   For information about setting the time zone, see *Set the Time Zone* on page 96.

Set the Time Zone

The access point might detect the time zone automatically or you might need to adjust the time zone and daylight saving time settings. When the access point synchronizes its clock with a Network Time Protocol (NTP) server, the page shows the date and time. If the page does not show the correct date and time, you might need to set the time zone and adjust the daylight saving time setting.

To set the time zone and adjust the daylight saving time setting:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.

3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Select **Management > Configuration > System > Basic > Time**.

   The page that displays lets you change the time settings.

5. From the **Time Zone** menu, select the time zone for the area in which the access point operates.
6. Click the **Apply** button.

   Your settings are saved. When the access point connects over the Internet to an NTP server, the date and time that display on the page are adjusted according to your settings.

   For information about other time settings, see *Specify a Custom NTP Server* on page 95.

Manage the Syslog Settings

If a syslog server is present on your network, you can configure the access point to send its system logs to the syslog server.

To manage the syslog settings and enable the syslog function:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Configuration > System > Advanced > Syslog**.

5. Specify the IP address and port number for the syslog server:

   - **Syslog Server IP Address**. Enter the IP address of the syslog server on your network.
   - **Port Number**. Enter the port number at which the syslog can be reached. By default, the port number is 514.
6. To enable the syslog server function, select the **Enable Syslog** check box.
7. Click the **Apply** button.

   Your settings are saved.

Upgrade the Firmware of the Access Point

The access point firmware is stored in flash memory.

You can check to see if new firmware is available and upgrade the access point to the new firmware. You can also visit the NETGEAR support website, download the firmware manually to a local computer, and update the access point to the new firmware. If someone (usually the network administrator) places new firmware on a TFTP or FTP server in the network, you can load the firmware from the server and upgrade the firmware of the access point.

The following sections describe the firmware upgrade methods:

Check for New Firmware and Upgrade the Access Point

For you to check for new firmware, the access point must be connected to the Internet.

To check for new firmware and upgrade your 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Click the **Check for Upgrade** button.

   The access point detects new firmware if any is available and displays a message asking if you want to download and install it.
5. To download and install the new firmware, follow the prompts and dialog boxes.

   The access point locates the firmware, downloads it, and begins the upgrade.

   WARNING:
   To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting and the Power LED turns solid green.

   The firmware upgrade process takes several minutes. When the upgrade is complete, your access point restarts.
6. Verify that the access point runs the new firmware version by logging back in to the access point.

   The firmware version is stated on the Dashboard page.
7. Read the new firmware release notes to determine whether you must reconfigure the access point after upgrading.

Manually Download Firmware and Upgrade the Access Point

Downloading firmware to a local computer and upgrading the access point are two separate tasks that are combined in the following procedure.

To download firmware manually and upgrade your access point:

1. Visit *downloadcenter.netgear.com*, locate the support page for your product, and download the new firmware.
2. Read the new firmware release notes to determine whether you must reconfigure the access point after upgrading.
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 or WiFi connection.
4. Enter the IP address that is assigned to the access point.

   A login window opens.
5. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
6. Select **Management > Maintenance > Upgrade > Firmware Upgrade**.

   The Firmware Upgrade page displays.
7. Make sure that **Local** is selected from the **Upgrade Options** menu.

   Local is the default selection.
8. Locate and select the firmware file on your computer by doing the following:

   a. Click the **Browse** button.

   b. Navigate to the firmware file.

      The file ends in `.tar`. An example of a firmware file name is `WAC510_V1.2.0.8_firmware.tar`.

   c. Select the firmware file.
9. Click the **Upgrade** button.

   WARNING:
   To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting and the Power LED remains solid green.

   The firmware upgrade process takes several minutes. When the upgrade is complete, the access point restarts.
10. Verify that the access point runs the new firmware version by logging back in to the access point.

    The firmware version is stated on the Dashboard page.

Use a TFTP Server to Upgrade the Access Point

If someone (usually the network administrator) places new firmware on a TFTP server in the network, you can load the firmware from the TFTP server and upgrade the firmware of the access point.

To upgrade the firmware of the access point from a TFTP 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Maintenance > Upgrade > Firmware Upgrade**.

   The Firmware Upgrade page displays.
5. From the **Upgrade Options** menu, select **TFTP**.
6. Specify the following server settings:

   - **Firmware File Name**. The name of the access point firmware file on the TFTP server.
   - **TFTP Server IP**. The IP address of the TFTP server on your network.
7. Click the **Upgrade** button.

   WARNING:
   To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting and the Power LED remains solid green.

   The firmware upgrade process takes several minutes. When the upgrade is complete, the access point restarts.
8. Verify that the access point runs the new firmware version by logging back in to the access point.

   The firmware version is stated on the Dashboard page.

Use an FTP Server to Upgrade the Access Point

If someone (usually the network administrator) places new firmware on an FTP server in the network, you can load the firmware from the FTP server and upgrade the firmware of the access point.

To upgrade the firmware of the access point from an FTP 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Maintenance > Upgrade > Firmware Upgrade**.

   The Firmware Upgrade page displays.
5. From the **Upgrade Options** menu, select **FTP**.
6. Specify the following server settings:

   - **Firmware File Name**. The name of the access point firmware file on the FTP server.
   - **FTP Server IP**. The IP address of the FTP server on your network.
   - **User Name**. The user name that is required to access the FTP server.
   - **Password**. The password that is required to access the FTP server.
7. Click the **Upgrade** button.

   WARNING:
   To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting and the Power LED remains solid green.

   The firmware upgrade process takes several minutes. When the upgrade is complete, the access point restarts.
8. Verify that the access point runs the new firmware version by logging back in to the access point.

   The firmware version is stated on the Dashboard page.

Manage the Configuration File of the Access Point

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

Back Up the Access Point Configuration

You can save a copy of the current configuration settings. If necessary, you can restore the configuration settings later.

To back up the access point's configuration 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Maintenance > Upgrade > Backup and Restore > Backup Settings**.

   The backup settings display.
5. Click the **Backup** button.
6. Choose a location to store the file on your computer.

   The name of the backup file is `wac505-Netgearxxxxxx-dd-mm-yy_hh-mm-ss-config.tar`, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address, dd is the date, mm is the month, yy is the year, hh is the hour (in 24-hour format), mm is the minutes, and ss is the seconds.

   An example of a name of a backup file is `wac505-Netgear01ABCD-02-08-17_19-57-54-config.tar`.
7. Follow the directions of your browser to save the file.

Restore the Access Point Configuration

If you backed up the configuration file, you can restore the configuration from this file.

To restore configuration settings that you backed up:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard page displays.

4. Select **Management > Maintenance > Upgrade > Backup and Restore > Restore Settings**.
   The restore settings display.
5. Click the **Browse** button and navigate to and select the saved configuration file.
   The name of the backup file from which you can restore the configuration is `wac505-Netgearxxxxxx-dd-mm-yy_hh-mm-ss-config.tar`, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address, dd is the date, mm is the month, yy is the year, hh is the hour (in 24-hour format), mm is the minutes, and ss is the seconds.
   An example of a name of a backup file is `wac505-Netgear01ABCD-02-08-17_19-57-54-config.tar`.
6. Choose a location to store the file on your computer.
   The configuration is uploaded to the access point. When the restoration is complete, the access point reboots. This process takes about two minutes.

WARNING:
To avoid the risk of corrupting the firmware, do not interrupt the restoration. For example, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting and the Power LED turns solid green.

Reboot the Access Point From the Local Browser Interface

If you cannot physically access the access point to reboot it (that is, disconnect the power and reconnect the power), 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Maintenance > Reset > Reboot AP**.
   The Reboot AP page displays.
5. Click the **Reboot AP** button.
   The reboot process typically takes about one minute.

Return the Access Point to Its Factory Default Settings

Under some circumstances (for example, if you lost track of the changes that you made to the access point settings or you move the access point to a different network), you might want to erase the configuration and reset the access point to factory default settings.

If you do not know the current IP address of the access point, first try to use an IP scanner application to detect the IP address before you reset the access point to factory default settings.

To reset the access point to factory default settings, you can use either the **Reset** button on the side of the access point or the use the erase function in the local browser interface. However, if you cannot find the IP address or lost the password to access the access point, you must use the **Reset** button.

After you reset the access point to factory default settings, the user name is admin, the password is password, the LAN IP address is 192.168.0.100, the access point's DHCP client is enabled, the default SSID is shown in the format NETGEARxxxxxx-SETUP, and the default password for WiFi access is sharedsecret.

For an extensive list of factory default settings, see *Factory Settings* on page 136.

Use the Reset Button

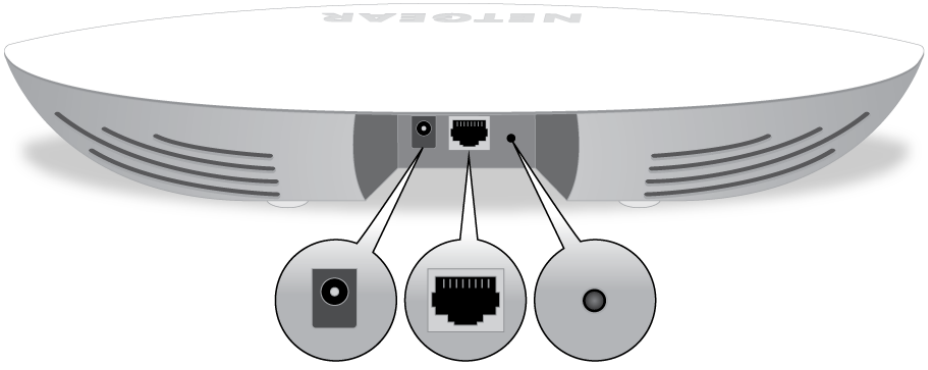
You can use the **Reset** button to return the access point to its factory default settings. However, if you added the access point to a network on the Insight app before, you must first use the NETGEAR Insight app to remove the access point from your network before the factory default settings function of the **Reset** button is available.

CAUTION:

This process erases all settings that you configured in the access point.

To reset the access point to factory default settings:

1. On the back panel of the access point, locate the recessed **Reset** button to the right of the LAN port.



2. Using a straightened paper clip, press and hold the **Reset** button for at least 10 seconds.

Note If you hold the **Reset** button for less than 10 seconds and then release it, the access point reboots rather than returning to its factory default settings.

3. Release the **Reset** button.

   The configuration is reset to factory default settings. When the reset is complete, the access point reboots. This process takes about two minutes.

WARNING:

To avoid the risk of corrupting the firmware, do not interrupt the reset. For example, if you are connected to the access point's local browser interface, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting and the Power LED turns solid green.

Use the Local Browser Interface

You can use the access point's local browser interface to return the access point to its factory default settings.

CAUTION:

This process erases all settings that you configured in the access point.

To erase the 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Maintenance > Reset > Restore Defaults**.

   The Restore Defaults page displays.
5. Click the **Restore Defaults** button.

   The configuration is reset to factory default settings. When the reset is complete, the access point reboots. This process takes about two minutes.

WARNING:
To avoid the risk of corrupting the firmware, do not interrupt the reset. For example, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting and the Power LED turns solid green.

Enable or Disable Telnet

By default, you cannot access the access point over a Telnet connection. You first must enable the access point for a Telnet connection.

To enable or disable Telnet:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Maintenance > Remote Management**.
   The Remote Management page displays.
5. Select one of the following Telnet radio buttons:
   - **Enable**. Telnet is enabled.
   - **Disable**. Telnet is disabled. This is the default setting.
6. Click the **Apply** button.
   Your settings are saved.

Enable or Disable Secure Shell

By default, you can access the access point over a Secure Shell (SSH) connection.

To enable or disable SSH:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.

3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Maintenance > Remote Management**.
   The Remote Management page displays.
5. Select one of the following Secure Shell (SSH) radio buttons:
   - **Enable**. SSH is enabled. This is the default setting.
   - **Disable**. SSH is disabled.
6. Click the **Apply** button.
   Your settings are saved.

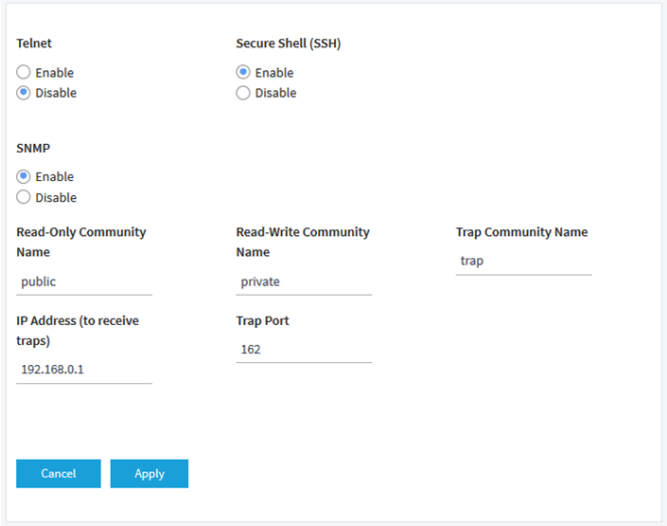
Enable SNMP and Manage the SNMP Settings

You can access the access point over a Simple Network Management Protocol (SNMP) connection, which allows SNMP network management software such as HP OpenView to manage the access point by using the SNMPv1 or v2 protocol. By default, SNMP is disabled.

To enable SNMP and manage the SNMP 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Select **Management > Maintenance > Remote Management**.
   The Remote Management page displays.
5. Select the SNMP **Enable** radio button.

By default, SNMP is disabled.



6. Specify the following settings:

   - **Read-Only Community Name**. The community string that allows the SNMP manager to read the access point's MIB objects. The default is public.
   - **Read-Write Community Name**. The community string that allows the SNMP manager to read and write the access point's MIB objects. The default is private.
   - **Trap Community Name**. The community name that is associated with the IP address at which traps must be received. The default is trap.
   - **IP address (to receive traps)**. The IP address of the SNMP manager that must receive the traps.
   - **Trap Port**. The port number at which the SNMP manager must receive traps. The default is 162.

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

Manage the LEDs

By default, all LEDs are enabled and function as described in *Top Panel With LEDs* on page 8. You can manage whether the LEDs light at all. This function is useful if the access point must function in a dark environment.

To enable or disable the LEDs:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.

The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard page displays.

4. Select **Management > Configuration > System > Advanced > LED Control**.
   The LED Control page displays.
5. Select one of the following radio buttons:

   - **Enable All LEDs**. All LEDs are enabled. This is the default setting.
   - **Disable All LEDs**. All LEDs are disabled.
   - **Enable Power LED**. All LEDs are disabled except for the Power LED.

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

Monitor the Access Point and the Network

8

This chapter describes how you can monitor the access point and the network.

The chapter includes the following sections:

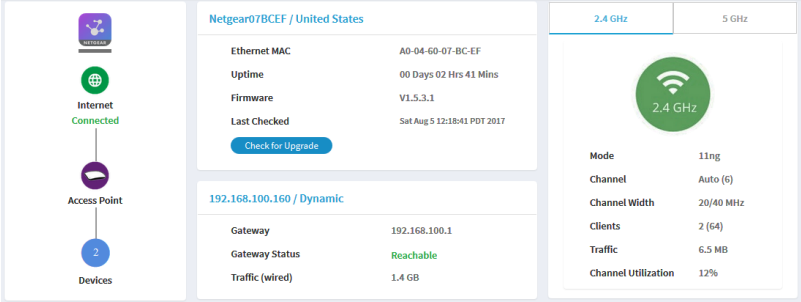
View the Access Point Internet, IP, and System Settings

To view the access point, Internet, IP, and 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.



4. Look at the following panes:

   - **Connection Status Information pane**. The Connection Status Information pane is in the top, left corner of the Dashboard (if the page width on your device is sufficient; otherwise, it might be elsewhere) and displays the following:

     - Status of the Insight app connection
     - Status of the Internet connection
     - Functioning mode of the access point, which is always Access Point
     - Number of clients connected to the access point

   - **System Information pane**. The System Information pane is in the center at the top of the Dashboard (if the page width on your device is sufficient; otherwise, it might be elsewhere) and displays the following:

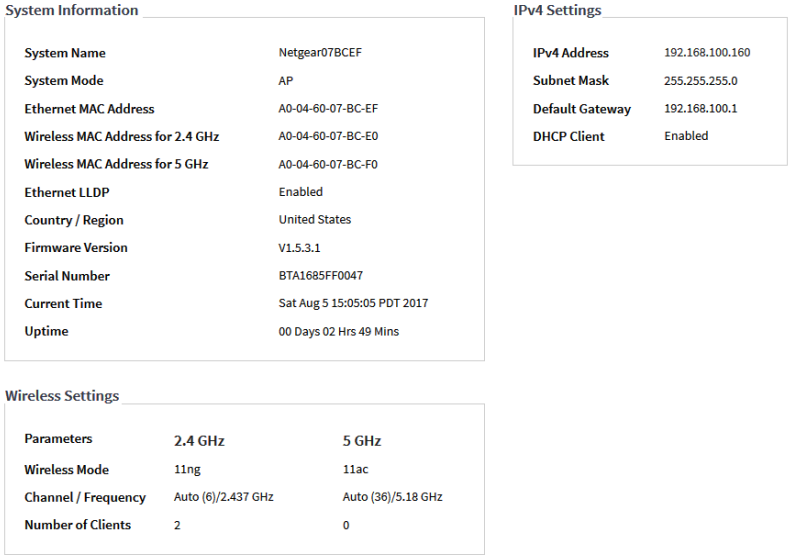
     - System name of the access point and country or region of operation
     - Ethernet MAC address
     - Device uptime
     - Firmware version
     - The date and time that someone last checked if new firmware was available for the access point

This pane also contains a button that you can click to check for firmware updates for the access point (see *Check for New Firmware and Upgrade the Access Point* on page 98).

- **IP Settings Information pane**. The IP Settings Information pane is in the center of the Dashboard page (if the page width on your device is sufficient; otherwise, it might be elsewhere) and displays the following:

  - IP address of the access point and its DHCP status
  - Gateway IP address
  - Gateway status
  - Wired traffic volume

5. To view more detailed information, select **Management > Monitoring > System**.



The page shows three sections:

- **System Information section**. The following settings are displayed:

  - **System Name**. The access point NetBIOS name.
  - **System Mode**. The access point system mode (AP).
  - **Ethernet MAC Address**. The MAC address of the Ethernet port of the access point.
  - **Wireless MAC Address for 2.4 GHz**. The MAC address of 2.4 GHz WiFi interface (radio) of the access point.
  - **Wireless MAC Address for 5 GHz**. The MAC address of 5 GHz WiFi interface (radio) of the access point.
  - **Ethernet LLDP**. The status of Ethernet LLDP feature (Enabled or Disabled).
  - **Country / Region**. The country or region in which the access point operates or for which the access point is licensed.
  - **Firmware Version**. The version of the firmware that is installed on the access point.

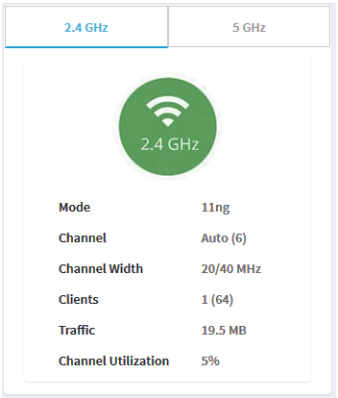
- **Serial Number**. The serial number of the access point.
- **Current Time**. The current system time of the access point.
- **Uptime**. The time since the access point was last restarted.

- **Wireless Settings section**. The following settings are displayed, with separate columns for the 2.4 GHz and 5 GHz radios:
  - **Wireless Mode**. The operating WiFi mode of the radio.
  - **Channel / Frequency**. The channel and frequency that are used by the radio.
  - **Number of Clients**. The number of clients that are connected to the radio.
- **IPv4 Settings section**. The following settings are displayed:
  - **IPv4 Address**. The IPv4 address of the access point.
  - **Subnet Mask**. The subnet mask of the access point.
  - **Default Gateway**. The default gateway for the access point.
  - **DHCP Client**. The status of DHCP client (Enabled or Disabled).

View the WiFi Radio Settings

To view the WiFi radio settings of 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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

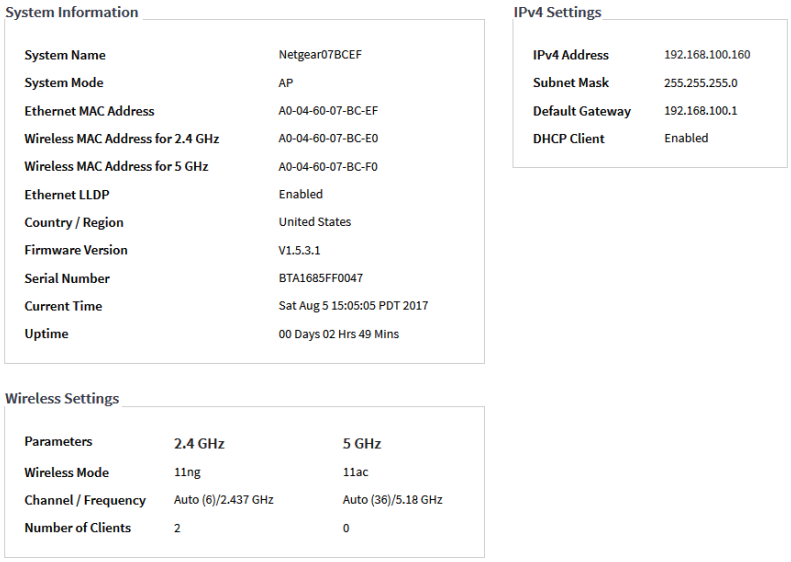


4. Look at the Radio Information pane at the top, right corner of the Dashboard page (if the page width on your device is sufficient; otherwise, it might be elsewhere). The following settings are displayed:

   - Radio status (If the 2.4 GHz or 5 GHz icon is displayed as gray, the radio is turned off.)
   - Mode
   - Channel width
   - Number of connected clients and maximum number of supported clients
   - WiFi traffic volume
   - Channel utilization

5. To view information for the 5 GHz radio, click the **5 GHz** tab.
   By default, information for the 2.4 GHz tab is shown.

6. To view more detailed information, including the MAC addresses of the WiFi radios, select **Management > Monitoring > System**.



The page shows three sections:

- **System Information section**. The following settings are displayed:
  - **System Name**. The access point NetBIOS name.
  - **System Mode**. The access point system mode (AP).
  - **Ethernet MAC Address**. The MAC address of the Ethernet port of the access point.
  - **Wireless MAC Address for 2.4 GHz**. The MAC address of 2.4 GHz WiFi interface (radio) of the access point.
  - **Wireless MAC Address for 5 GHz**. The MAC address of 5 GHz WiFi interface (radio) of the access point.
  - **Ethernet LLDP**. The status of Ethernet LLDP feature (Enabled or Disabled).

- **Country / Region**. The country or region in which the access point operates or for which the access point is licensed.
- **Firmware Version**. The version of the firmware that is installed on the access point.
- **Serial Number**. The serial number of the access point.
- **Current Time**. The current system time of the access point.
- **Uptime**. The time since the access point was last restarted.

- **Wireless Settings section**. The following settings are displayed, with separate columns for the 2.4 GHz and 5 GHz radios:
  - **Wireless Mode**. The operating WiFi mode of the radio.
  - **Channel / Frequency**. The channel and frequency that are used by the radio.
  - **Number of Clients**. The number of clients that are connected to the radio.
- **IPv4 Settings section**. The following settings are displayed:
  - **IPv4 Address**. The IPv4 address of the access point.
  - **Subnet Mask**. The subnet mask of the access point.
  - **Default Gateway**. The default gateway for the access point.
  - **DHCP Client**. The status of DHCP client (Enabled or Disabled).

View Unknown and Known Neighbor Access Points

If you enabled neighbor access point (AP) detection (see *Manage Neighbor AP Detection* on page 75), you can view the unknown access points in the Unknown AP list and the known access points in the Known AP list.

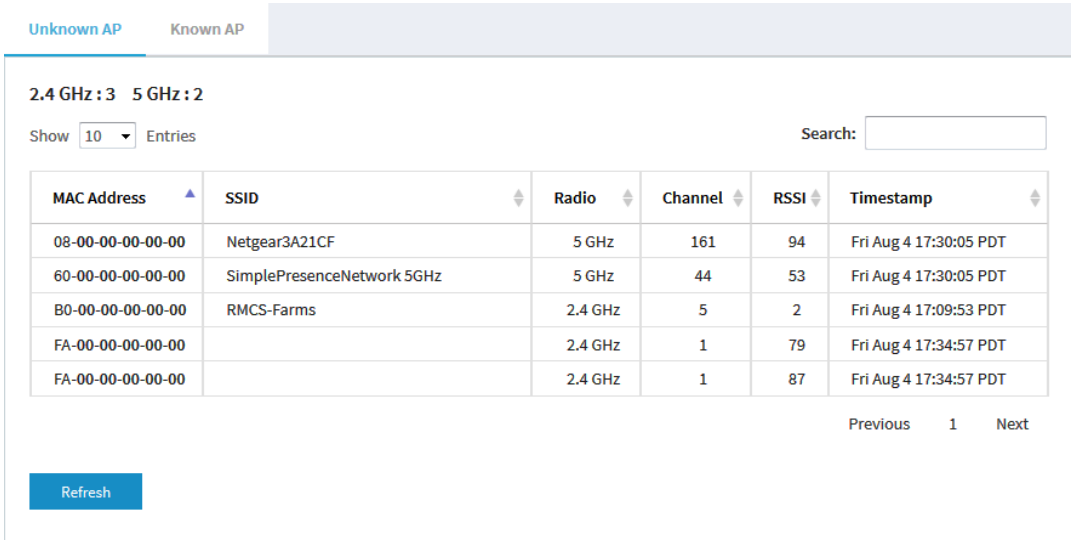
To view the detected neighbor access points:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

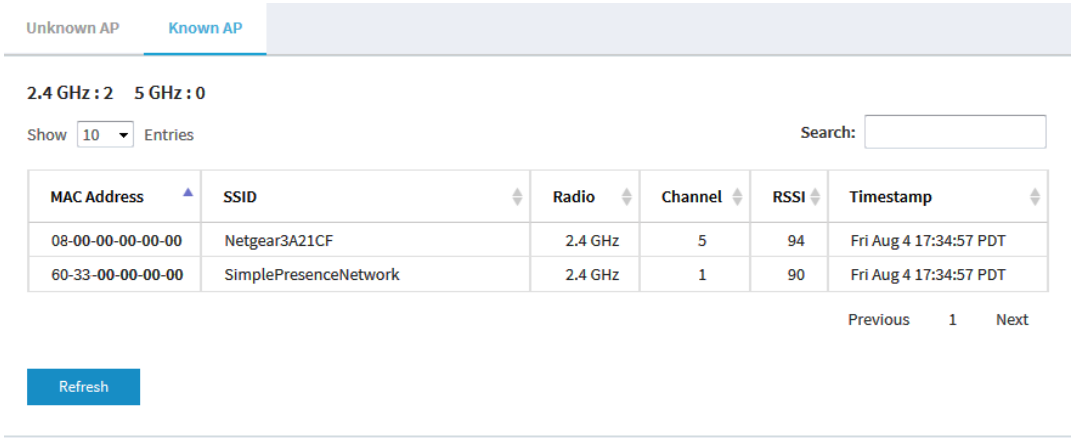
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

4. Select **Management > Monitoring > Neighbor AP**.



At the top of the page, for each radio band, the page states the total number of unknown access points.

5. To display the most recent unknown access points, click the **Refresh** button.
6. To view the Known AP list, click the **Known AP** tab.



At the top of the page, for each radio band, the page states the total number of known access points.

7. To display the most recent known access points, click the **Refresh** button.

View Client Distribution, Connected Clients, and Client Trends

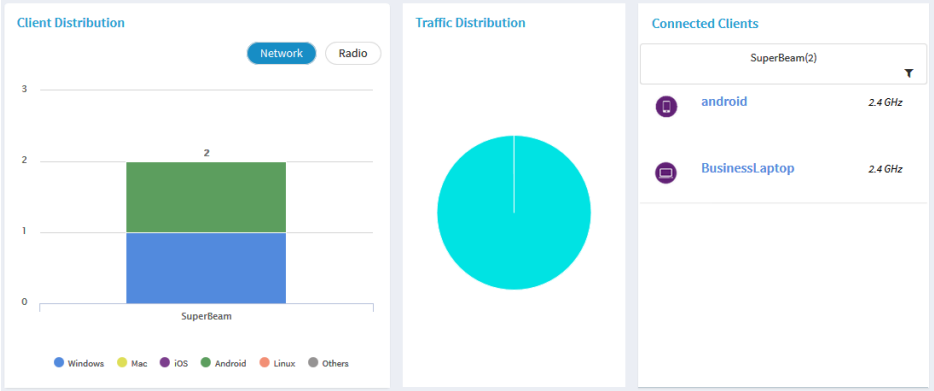
To view the clients that are connected to the access point over WiFi:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

A login window opens.

3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.



   The Client Distribution pane (shown on the left side in the previous figure) shows the types of clients (Windows, Mac, iOS, Android, Linux, and other operating systems) and how these clients are distributed over the networks. (By default, the **Network** button is selected.)

   The Connected Clients pane (shown on the right side in the previous figure) shows the top clients list (clients with the highest level of traffic).

4. To see how the clients are distributed over the radios, click the **Radio** button in the Client Distribution pane.

   The page adjusts and shows the types of clients for each radio.

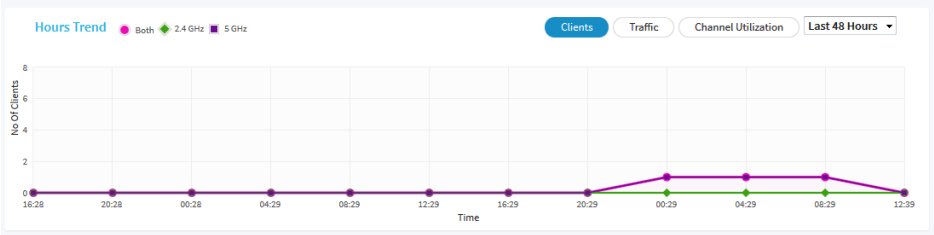
5. To see connected clients for all networks or a single network, in the Connected Clients pane, click the icon in the menu under Connected Clients, and select **All WiFi Clients** or the clients for a specific WiFi network (SSID).

   For your selection, the pane displays the total number of connected clients and the device names of the connected clients.

6. To view information about a connected client, click its device name.

   The page displays the MAC address, device name, IP address, and SSID for the client. You can also view more information, including very detailed information (see *Step 10*).

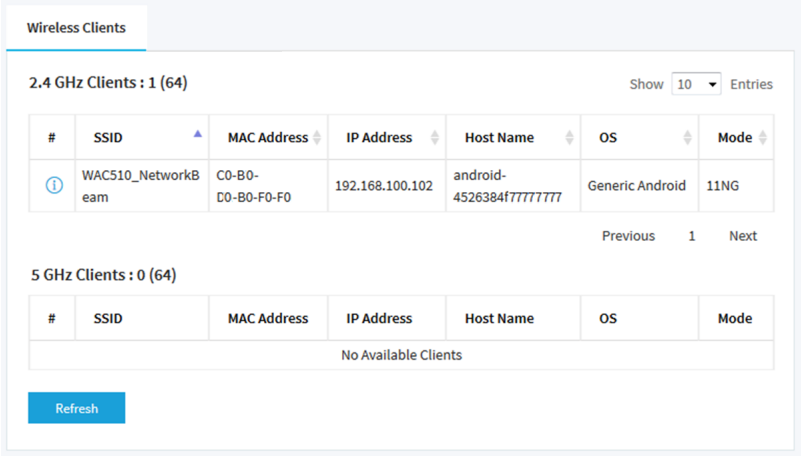
7. To view trends about clients, scroll down to the Hours Trend pane.



   The Hours Trend pane shows a graph with either the number of clients or the traffic in MB over a period that you can select. By default, the client information is selected (that is, the **Client** button is selected)

and the graph shows the total number of clients for both radios and the number of clients for each radio (2.4 GHz and 5 GHz).

8. To view more information, point to a node on one of the lines on the graph.
9. To change the period over which information is filtered and displayed, select the number of recent hours from the menu to the right of the buttons.
10. To view more information about currently connected WiFi, select **Management > Monitoring > Connected Clients**.



For each radio, the page displays the number of connected clients and the maximum number of supported clients.

For each radio and each WiFi client, the page displays the SSID, MAC address, IP address, host name, operating system (OS), and WiFi mode.

11. To view very detailed information about a WiFi client, click the information icon to the left of the client.

    The Detailed Client Information page displays and shows the following information:

- **MAC Address**. The MAC address of the client.
- **IP Address**. The IP address associated with the client.
- **Host Name**. The host name of the client.
- **OS**. The operating system that runs on the client.
- **BSSID**. The BSSID that the client connects to.
- **SSID**. The SSID of the radio that the client connects to.
- **Channel**. The channel that the client connects to.
- **Channel Width**. The width of the channel that the client connects to.
- **Tx Rate**. The rate of traffic transmission of the client.
- **Rx Rate**. The rate of traffic reception of the client.
- **RSSI**. The RSSI threshold value of the client.
- **Tx Bytes**. The number of bytes that the client transmitted.
- **Rx Bytes**. The number of bytes that the client received.

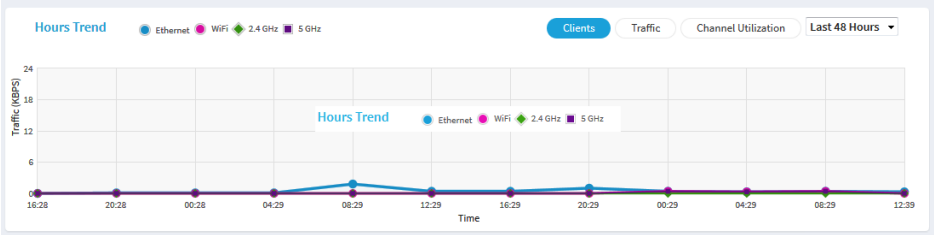
- **State**. The QoS state of the connection.
- **Type**. The type of WiFi security that is used for the connection.
- **Device Type**. The type of device that the client is.
- **Mode**. The WiFi mode of the connection.
- **Status**. The security status of the connection.
- **Idle Time**. The time that the client remained idle.
- **Assoc Time Stamp**. The time that is associated with the information on the Detailed Client Information page.

12. To display the most recent information, click the **Refresh** button.

View WiFi and Ethernet Traffic, Traffic Statistics, and Channel Utilization

To view WiFi and Ethernet traffic, traffic statistics, and channel utilization:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.
4. Scroll down to the Hours Trend pane at the bottom of the Dashboard page.
   By default, the **Clients** button is selected.



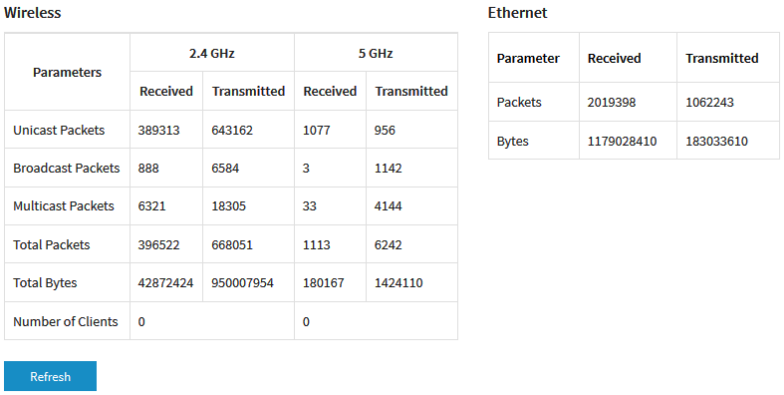
5. To view traffic information, do the following:
   a. Click the **Traffic** button.
      The graph shows the information for Ethernet traffic, total WiFi traffic, WiFi traffic for the 2.4 GHz radio, and WiFi traffic for the 5 GHz radio.
   b. To view more information, point to a node on one of the lines on the graph.
6. To view channel utilization, do the following:

a. Click the **Channel Utilization** button.
The graph shows the channel utilization for the 2.4 GHz radio.

b. To view the channel utilization for the 5 GHz radio, click the **5 GHz** button.

c. To view more information, point to a bar.

7. To change the period over which information is filtered and displayed, select the number of recent hours from the menu to the right of the buttons.
8. To view traffic statistics, select **Management > Monitoring > Statistics**.



Wireless

Parameters	2.4 GHz		5 GHz	
	Received	Transmitted	Received	Transmitted
Unicast Packets	389313	643162	1077	956
Broadcast Packets	888	6584	3	1142
Multicast Packets	6321	18305	33	4144
Total Packets	396522	668051	1113	6242
Total Bytes	42872424	950007954	180167	1424110
Number of Clients	0		0	

Refresh

Ethernet

Parameter	Received	Transmitted
Packets	2019398	1062243
Bytes	1179028410	183033610

The page displays the network traffic statistics for both the WiFi and wired (Ethernet) interfaces of the access point since the access point started or rebooted. The page also displays the number of clients that are associated with each radio.

9. To display the most recent information, click the **Refresh** button.

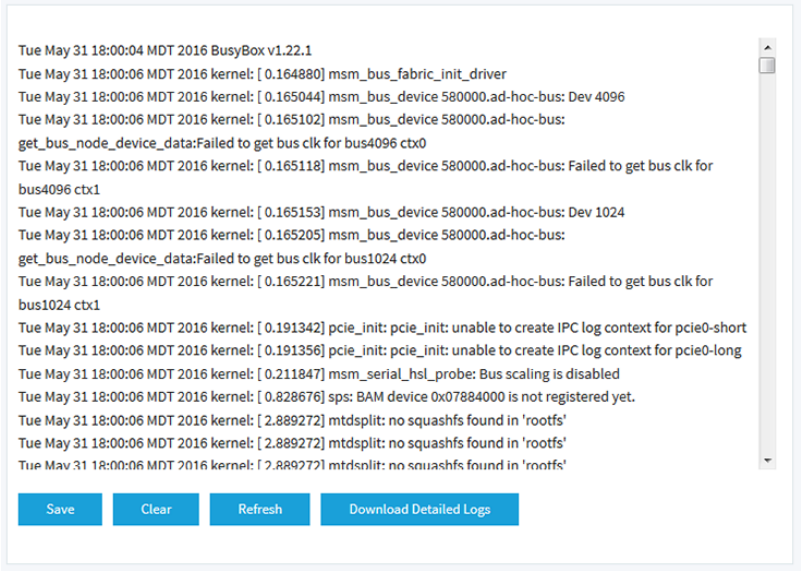
View, Save, Download, or Clear the Logs

You can view and manage the activity logs of the access point. You can also download a detailed log file.

To view, save, download, or clear the logs:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and password.
   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard page displays.

4. Select **Management > Monitoring > Logs**.



The page shows the following information for each log entry:

- **Date and time**. The date and time that the entry was logged.
- **Action**. The action that occurred, such as whether a WLAN connection was made.
- **Source**. The name, IP address, or MAC address of a source device, application, or website, if applicable.
- **Target**. The name, IP address, or MAC address of a target device, application, or website, if applicable.

5. To save the logs, do the following:

   a. Click the **Save** button.

   b. Follow the directions of your browser to save the file to your computer.

6. To download the detailed log entries, do the following:

   a. Click the **Download Detailed Logs** button.
   Depending on the size of the file, downloading the detailed log entries might take several minutes.

   b. Follow the directions of your browser to save the file to your computer.

7. To refresh the log entries onscreen, click the **Refresh** button.

WARNING:
After you clear the log entries, you can no longer save or download them.

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

View a WiFi Bridge Connection

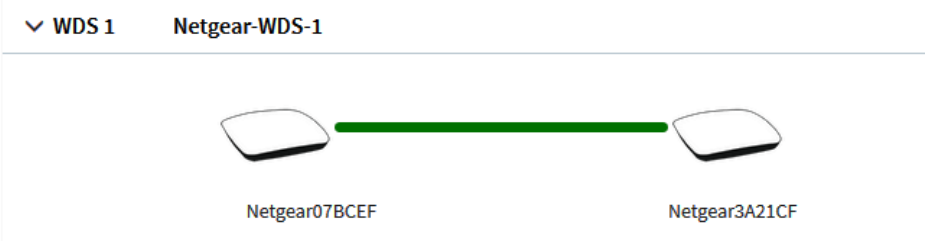
You can view whether a WiFi bridge is established and view the function (master or slave), MAC addresses, and IP addresses of the access points that form the WiFi bridge.

To view a WiFi bridge connection:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
4. Select **Management > Monitoring > Wireless Bridge**.



5. To view the function, MAC address, and IP address of an access point, point to the access point.

View Alarms and Notifications

You can view the alarms and notifications from any access point page. The following procedure describes how you can view them from the Dashboard page.

To view the alarms and notifications:

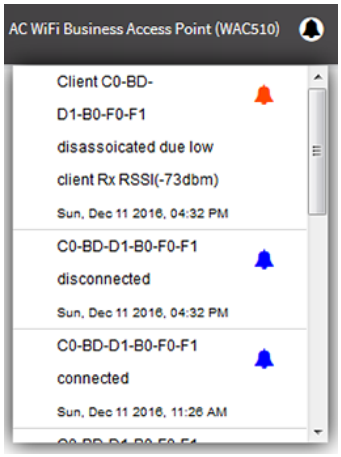
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.

4. Click the alarm bell icon on the top right of the page.



The pop-up window shows the alarms (indicated by a red bell) and notifications (indicated by a blue bell) with a description and time.

5. To view more alarms and notification, scroll down in the pop-up window.

Diagnostics and Troubleshooting

9

This chapter describes how you can capture WiFi packets and troubleshoot the access point and network.

The chapter includes the following sections:

Capture WiFi Packets

You can capture WiFi and Ethernet packets that are received and transmitted by the access point and save the file with captured packets to your computer. During the packet capture process, normal functioning of the access point is not affected.

The packet capture capability can be useful for analyzing a WiFi deployment, monitoring a WiFi network, debugging protocols, determining WiFi network bottlenecks, and, in general, troubleshooting any irregularities in a WiFi network.

You can select to capture all packets or only the Ethernet interface, 2.4 GHz radio, or 5 GHz radio packets.

Note To view the captured packets, you need an application that can open `.pcap` files.

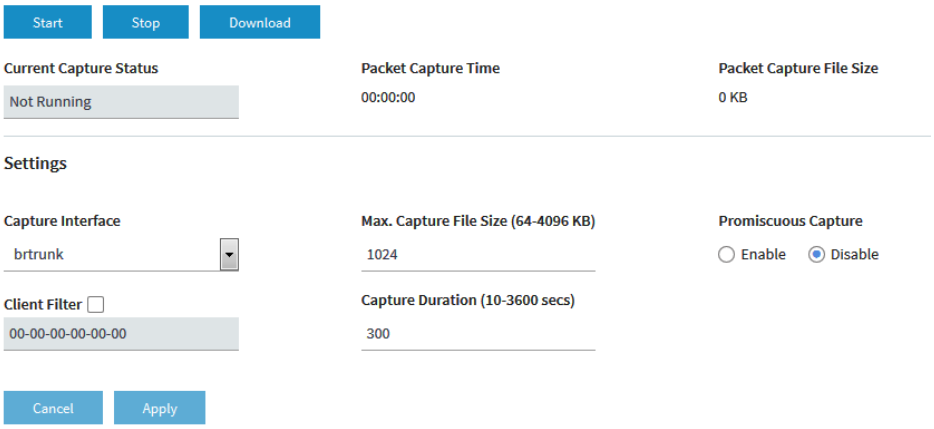
To capture packets:

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 or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window opens.
3. Enter the access point user name and password.

   The default user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard page displays.
4. Select **Management > Monitoring > Packet Capture**.



5. Specify the settings that are described in the following table.

Setting	Description
Capture Interface	From the **Capture Interface** menu, select one of the following interfaces on which packets must be captured: • **brtunk**. All packets are captured, that is, packets on the Ethernet interface, 2.4 GHz radio, and 5 GHz radio. This is the default setting. • **Eth0**. Only packets on the Ethernet interface are captured. • **radio1**. Only packets on the 2.4 GHz radio are captured. • **radio2**. Only packets on the 5 GHz radio are captured.
Max. Capture File Size (64-4096 KB)	Enter the maximum size that the file with captured packets is limited to. The range is from 64 to 4096 KB. The default is 64 KB.
Promiscuous Capture	To enable the access point to capture packets in promiscuous mode, select the **Enable** check box. By default, promiscuous mode is disabled. In promiscuous mode the radio or radios receive all traffic on the channel, including traffic that is not destined for the access point. While the radio or radios are operating in promiscuous mode, they continue to serve associated clients. Packets that are not destined for the access point are not forwarded. When the capture process stops, the radio or radios revert to nonpromiscuous mode.
Client Filter	To capture packets for a specific client only, select the **Client Filter** check box and enter the client's MAC address in the **Client Filter MAC Address** field.
Client Filter MAC Address	If you select the **Client Filter** check box, enter the client's MAC address to capture the packets only for the specific client on the selected interface. You must enter the MAC address in hexadecimal format with each octet separated by a hyphen, for example 00-11-22-33-44-55.
Capture Duration (10-3600 secs)	Enter the maximum duration of the capture process (that is, if you do not click the **Stop** button). The range is from 10 to 3600 seconds. By default, the maximum duration is 60 seconds.

6. To start the packet capture process, click the **Start** button.

   If any captured packets are already stored on the access point, you are prompted to allow the packet capture process to overwrite the old information.

7. To stop the packet capture process, click the **Stop** button.
8. To download the file with captured packets, do the following:

   a. Click the **Download** button.

   b. Follow the directions of your browser to save the file to your computer.

9. To display the latest information on the page, click the **Refresh** button.

Quick Tips for Troubleshooting

If your network is unresponsive or does not function normally, restart your network:

1. Unplug the Ethernet cable from the access point to your network switch or Internet modem.
2. If you use a power adapter, disconnect it from the access point.
3. Plug in the Ethernet cable from the access point to your network switch or Internet modem. Wait two minutes.
4. If you use a power adapter, connect it to the access point and wait two minutes.

If you cannot connect over WiFi to the access point, try the following:

- Make sure that the WiFi LED on the access point is not off.
  If the WiFi LED is off, one or both WiFi radios are probably off too. For more information about the WiFi radios, see *Turn a Radio On or Off* on page 50.
- Make sure that the WiFi settings in your WiFi device and access point match exactly.
  For a device that is connected over WiFi, the WiFi network name (SSID) and WiFi security settings of the access point and WiFi device must match exactly.
  For information about accessing the access point for initial configuration over a WiFi connection, see *Connect to the Access Point for Initial Configuration* on page 15.
- Make sure that your WiFi device supports the security that you are using for your WiFi network (WPA2-PSK or WPA-PSK and WPA2-PSK). For more information, see *Set Up and Manage WiFi Networks* on page 30.
- Make sure that your WiFi device is not too far from the access point or too close. To see if the signal strength improves, move your WiFi device near the access point but at least 6 feet (1.8 meters) away.
- Make sure that the WiFi signal is not blocked by objects between the access point and your WiFi device.
- Make sure that the access point's SSID broadcast is not disabled.
  If the access point's SSID broadcast is disabled, the WiFi network name is hidden and does not display in your WiFi device's scanning list. To connect to a hidden network, you must enter the network name and the WiFi password. For more information about the SSID broadcast, see *Set Up and Manage WiFi Networks* on page 30.
- Make sure that your WiFi device does not use a static IP address but is configured to receive an IP address automatically with DHCP. (For most devices, DHCP is the default setting.)

If you cannot connect over an Ethernet cable to the access point, try the following:

- Make sure that the Ethernet cables are securely plugged in.
- Make sure that your network includes a DHCP server that can issue an IP address to the access point or, if your access point requires a fixed (static) IP address, that the IP address and subnet are correct.

Troubleshoot With the LEDs

When you turn on the power, the LEDs light as described here:

1. The Power LED lights solid amber. After about one minute, the Power LED turns solid green, indicating that the startup procedure is complete and the access point is ready.
2. When the startup procedure is complete, verify the following:

   - The Activity LED lights solid green or blinks green.
   - The 2.4G WLAN LED, 5G WLAN LED, or both LEDs light solid green or solid blue or blink blue (unless one or both WiFi radios are turned off).
   - If a LAN device is connected to the LAN port, the LAN LED lights solid amber or solid green.

You can use the LEDs for troubleshooting. For more information, see the following sections:

- *Power LED Is Off* on page 128
- *Power LED Remains Solid Amber* on page 129
- *Power LED Is Blinking Amber Continuously* on page 129
- *Power LED Is Alternating Green and Amber* on page 129
- *Activity LED Is Off* on page 129
- *2.4G or 5G WLAN LED Is Off* on page 130
- *LAN LED Is Off While a Switch Is Connected* on page 130

Power LED Is Off

If you use a Power over Ethernet (PoE) connection and the Power LED and other LEDs are off when the Ethernet cables are connected, do the following:

- Make sure that the Ethernet cable between the access point and the PoE switch is correctly connected at both ends.
- Make sure that the other end of the Ethernet cable is plugged into a PoE port (not a non-PoE port) on a PoE switch (not a non-PoE switch) that is receiving power.
- Make sure that the PoE power budget of the PoE switch is not oversubscribed and that the PoE switch is capable of delivering PoE power to the access point. Also see *Power LED Is Alternating Green and Amber* on page 129.

If you use a power adapter and the Power LED and other LEDs are off when the access point is turned on, do the following:

- Make sure that the power adapter is correctly connected to the access point and that the power adapter is correctly 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 the outlet is not switched off.
- Make sure that you are using the NETGEAR 12V, 2.5A power adapter for this product.

If the error persists, a hardware problem might exist. For recovery instructions or help with a hardware problem, contact technical support at *netgear.com/support*.

Power LED Remains Solid Amber

When you turn on the power to the access point, the Power LED lights solid amber temporarily and then turns solid green, indicating that the startup procedure is complete and the access point is ready.

If the Power LED remains solid amber and does not turn solid green, a failure occurred or the access point is malfunctioning.

If the Power LED does not turn solid green, do the following:

1. Turn the power off and back on and wait several minutes to see if the access point recovers.
2. If the access point does not recover, you can use the **Reset** button to return the access point to its factory default settings. For more information, see *Use the Reset Button* on page 104.

If the error persists, a hardware problem might exist. For recovery instructions or help with a hardware problem, contact technical support at *netgear.com/support*.

Power LED Is Blinking Amber Continuously

When you turn on the power to the access point, the Power LED lights solid amber temporarily and then turns solid green, indicating that the startup procedure is complete and the access point is ready. During regular operation, the only time that the Power LED blinks amber temporarily is when firmware is being upgraded.

If the Power LED blinks amber continuously and does not turn solid green, the access point did not receive an IP address from a DHCP server.

Check to make sure that the DHCP client of the access point is enabled (see *Enable the DHCP Client* on page 84), that your network includes a DHCP server (or a router that functions as a DHCP server), and that the DHCP server can reach the access point (both must be on the same network).

If you network does not include a DHCP server, you might need to configure a fixed (static) IP address on the access point (see *Disable the DHCP Client and Specify a Fixed IP Address* on page 83).

Power LED Is Alternating Green and Amber

If the Power LED is alternating green and amber, the access point is receiving insufficient Power over Ethernet (PoE).

Check to see why the PoE switch cannot provide sufficient PoE power to the access point. Most likely, the PoE power budget of the PoE switch is oversubscribed and you might need to disconnect another PoE device from the PoE switch to make sufficient PoE power available for the access point.

Activity LED Is Off

If the LAN port of the access point is connected to a PoE switch or non-PoE switch and the LAN LED lights amber or green but the Activity LED is off, the access point cannot detect a link with the network and the Internet.

If the LAN LED lights amber or green but the Activity LED is off, do the following:

1. Disconnect and reconnect the Ethernet cable and wait several minutes to see if the Activity LED lights solid green or blinks green.
2. If you use a power adapter with the access point, disconnect and reconnect the power adapter and wait several minutes to see if the Activity LED lights solid green or blinks green.
3. If the LAN LED lights amber or green but the Activity LED is still off, you can use the **Reset** button to return the access point to its factory default settings. For more information, see *Use the Reset Button* on page 104.

If the error persists, a hardware problem might exist. For recovery instructions or help with a hardware problem, contact technical support at *netgear.com/support*.

2.4G or 5G WLAN LED Is Off

If the 2.4G WLAN LED or 5G WLAN LED is off, do the following:

- Check to see if a radio is disabled (see *Turn a Radio On or Off* on page 50). By default, both radios are enabled and the WLAN LEDs light solid green or solid blue or blink blue.
- If you are using a Power over Ethernet (PoE) connection, make sure that the PoE switch is providing sufficient power to the access point. Insufficient PoE power can affect the radios. Also see *Power LED Is Alternating Green and Amber* on page 129.

If the error persists, a hardware problem might exist. For recovery instructions or help with a hardware problem, contact technical support at *netgear.com/support*.

LAN LED Is Off While a Switch Is Connected

When a PoE switch or non-PoE switch is connected to the LAN port of the access point, the LAN LED lights amber or green, depending on the speed of the connection.

If the LAN LED remains off, a hardware connection problem might be occurring. Check these items:

- Make sure that the Ethernet cable connectors are securely plugged in at the access point and the network device.
- Make sure that the connected network device is actually turned on.
- Make sure that you are using the correct Ethernet cable. Use a standard Category 5 Ethernet patch cable. If the network device incorporates Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

Troubleshoot the WiFi Connectivity

If you are experiencing trouble connecting over WiFi to the access point, try to isolate the problem:

- Make sure that the WiFi settings in your WiFi device and access point match exactly.
  For a device that is connected over WiFi, the WiFi network name (SSID) and WiFi security settings of the access point and WiFi device must match exactly.
  For information about accessing the access point for initial configuration over a WiFi connection, see *Connect to the Access Point for Initial Configuration* on page 15.
- Does the WiFi device that you are using find your WiFi network?
  If not, check the WLAN LEDs. If a WLAN LED is off, the associated WiFi radio is probably off too. For more information about the WiFi radios, see *Turn a Radio On or Off* on page 50.
- If you disabled the access point's SSID broadcast, your WiFi network is hidden and does not display in your WiFi client's scanning list. (By default, SSID broadcast is enabled.) For more information about the SSID broadcast, see *Set Up and Manage WiFi Networks* on page 30.
- Does your WiFi device support the security that you are using for your WiFi network (WPA2-PSK or WPA-PSK and WPA2-PSK). For more information, see *Set Up and Manage WiFi Networks* on page 30.

Tip If you want to change the WiFi settings of the access point's network, use a wired connection to avoid being disconnected when the new WiFi settings take effect.

If your WiFi device finds your network but the signal strength is weak, check these conditions:

- Is your access point too far from your WiFi device or too close? Place your WiFi device near the access point but at least 6 feet (1.8 meters) away and see whether the signal strength improves.
- Are objects between the access point and your WiFi device blocking the WiFi signal?

Troubleshoot Internet Browsing

If your computer or WiFi device is connected to the access point but unable to load any web pages from the Internet, it might be for one of the following reasons:

- Your computer might not recognize any DNS server addresses.
  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. If you manually entered a DNS address when you set up the access point (that is, the access point uses static IP address settings), reboot your computer and verify the DNS address. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.
- Your computer might not use the correct TCP/IP settings.
  If your computer obtains its information by DHCP, reboot the computer and verify the address of the switch or Internet modem to which the access point is connected.
  For information about TCP/IP problems, see *Troubleshoot Your Network Using the Ping Utility* on page 132.

You Cannot Log In to the Access Point Over a LAN Connection

If you are unable to log in to the access point from a computer on your local network and use the access point's local browser interface, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet cable between the computer and the access point.
- Make sure that the IP address of your computer is in the same subnet as the access point.
  If you disabled the access point's DHCP client and configured a fixed (static) IP address when you connected the access point to network or Internet modem (see *Disable the DHCP Client and Specify a Fixed IP Address* on page 83), change the IP address and subnet mask on your computer to so that the IP addresses of your computer and the access point are in the same IP subnet.
- If your access point's IP address was changed (for example, the DHCP server in your network issued an IP address to the access point) and you do not know the current IP address, use an IP scanner application to detect the IP address. If you still cannot find the IP address, reset the access point's configuration to factory defaults. This sets the access point's IP address to 192.168.0.100. For more information, see *Use the Reset Button* on page 104.
- 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 and launching it again.
- Make sure that you are using the correct login information. The user name is **admin** and the password is the one that you specified the first time that you logged in. Make sure that Caps Lock is off when you enter this information.

Changes Are Not Saved

If you are logged in to the access point's local browser interface and the access point does not save the changes that you make on a page, do the following:

- When entering configuration settings, always 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. It is possible that the changes occurred but that the old settings remain in the web browser's cache.

Troubleshoot Your Network Using the Ping Utility

Most network 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 network using the ping utility in your computer or workstation.

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 Windows computer:

1. From the Windows taskbar, click the **Start** button and select **Run**.
2. In the field provided, enter **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 such as 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 might be occurring:

- Wrong physical connections
  For a wired connection, make sure that the numbered LAN LED is lit for the port to which you are connected.
  Check that the appropriate LEDs are on for your network devices. If your access point and computer are connected to a separate Ethernet switch, make sure that the link LEDs are lit for the switch ports that are connected to your computer 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 computer are correct and that the addresses are in the same subnet.

Test the Path From Your Computer to a Remote Device

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

To 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*.
   IP address is the IP address of a remote device such as a remote DNS server.

If the path is functioning correctly, replies as described in *Test the LAN Path to Your Access Point* on page 133 display. If you do not receive replies, do the following:

- Check to see that your computer lists the IP address of the router to which the access point is connected as the default router. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel.
- 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.

Factory Default Settings and Technical Specifications

A

This appendix includes the following sections:

Factory Settings

You can reset the access point to the factory default settings, which are shown in the following table.

For more information about resetting the access point to its factory settings, see *Return the Access Point to Its Factory Default Settings* on page 104.

Table 2. Access point factory default settings

Feature	Default Setting
Access point login	
Management mode	Insight mode for the NETGEAR Insight app
User login URL	192.168.0.100
User name (case-sensitive)	admin, nonconfigurable
Login password (case-sensitive)	password, configurable
General system settings	
Operating mode	AP mode
DHCP client	Enabled so that the access point receives an IP address from a DHCP server in the network.
Country/region	For products purchased in North America: Canada For products purchased outside of North America: Germany
NTP client	Enabled
Spanning Tree Protocol	Disabled
Network integrity check	Disabled
802.1Q VLAN	Untagged VLAN with VLAN ID 1
Management VLAN	VLAN ID 1
Syslog	Disabled
Ethernet LLDP	Enabled
UPnP	Enabled
LEDs	Enabled
WiFi network for initial setup	
SSID name	SSID for initial setup is NETGEARxxxxxx-SETUP, where xxxxxx is the last six hexadecimal digits of the access point's MAC address.
Security	WPA2-PSK WiFi password (network key): sharedsecret

Table 2. Access point factory default settings (Continued)

Feature	Default Setting
RF channel	Auto. The available channels depend on the region.
WLAN settings for an individual WiFi network (SSID or VAP)	
WiFi communication	Both the 2.4 GHz radio and the 5 GHz radio are enabled.
Client separation	Disabled
Broadcast SSID	Enabled
802.11K (RRM)	Disabled
Band steering	Disabled
RSSI threshold	–100 dBm
VLAN ID (for WiFi clients)	1
Network authentication	WPA2-PSK
Data encryption	AES
Passphrase	sharedsecret
MAC ACL	None assigned
Rate limit	None
Captive portal	None
Basic WiFi settings for all WiFi networks (SSIDs or VAPs)	
Radios	Both the 2.4 GHz radio and the 5 GHz radio are enabled.
WiFi mode	2.4 GHz radio: 11ng mode, which also supports 11b and 11bg 5 GHz radio: 11ac mode, which also support 11a and 11na
MCS index / data rate	Best
Channel width	Dynamic 20/40 MHz for the 2.4 GHz radio Dynamic 20/40/80 MHz for the 5 GHz radio
Output power	Maximum (100%)
Guard interval	Auto
Channel	Auto
WiFi schedule	None
Wi-Fi Multimedia (WMM)	Enabled

Table 2. Access point factory default settings (Continued)

Feature	Default Setting
WMM powersave	Enabled
Advanced WiFi settings for all WiFi networks (SSIDs or VAPs)	
Maximum number of WiFi clients	50 per radio
Beacon interval	100 millisec.
RTS threshold	2346
DTIM interval	1 sec.
Broadcast/multicast rate limiting	Enabled with a limit of 50 packets per second
Fixed multicast rate	54 Mbps
Load balancing between radios	Disabled
Wireless bridge	None configured
General security	
URL filtering	None
MAC ACLs	None

Technical Specifications

The following table shows the technical specifications of the access point.

Table 3. Access point specifications

Feature	Description
Supported WiFi radio frequencies and WiFi modes	2.4 GHz band: 802.11ng, 801.11bg, and 802.11b 5 GHz band: 802.11ac, 802.11na, and 802.11a Supports 2.4 GHz and 5 GHz concurrent operation
Maximum theoretical throughput	About 1.2 Mbps simultaneous throughput (300 Mbps on the 2.4 GHz band and 867 Mbps on the 5 GHz band) **Note**: Throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, affect the data throughput rate.
Maximum number of supported clients	Maximum number of 2.4 GHz WiFi clients: 50 Maximum number of 5 GHz WiFi clients: 50
WiFi standards	IEEE 802.11ac Wave 2 standard WiFi Multimedia Prioritization (WMM) Wireless distribution system (WDS)
802.11 security	WPA2-PSK, WPA and WPA2 (mixed mode), and WPA2 Enterprise
Operating frequency range	2.4 GHz band: • US and Canada: 2.412–2.462 GHz • Europe: 2.412–2.472 GHz • Australia: 2.412–2.472 GHz • Japan: 2.412–2.472 GHz 5 GHz band: • US and Canada: 5.18–5.24 + 5.745–5.825 GHz • Europe: 5.18–5.24 GHz • Australia: 5.18–5.24 + 5.745–5.825 GHz • Japan: 5.18–5.24 GHz
Power over Ethernet	IEEE 802.3af and IEEE 802.3at **Note** PoE might be considered a network environment 0 per IEC TR 62101, and thus the interconnected ITE circuits might be considered safety extra low voltage (SELV).

Table 3. Access point specifications (Continued)

Feature	Description
PoE consumption	8.53W
Power adapter (not included but can be ordered as an option)	12 VDC, 2.5A The plug is localized to the country of sale.
Hardware interfaces	One LAN 10/100/1000BASE-T Gigabit Ethernet (RJ-45) port with Auto Uplink (Auto MDI-X) that supports IEEE 802.3af or 802.3at Power over Ethernet (PoE).
Dimensions (W x D x H)	175 x 165 x 35 mm (6.89 x 6.49 x 1.38 in.)
Weight	256 g (0.56 lb)
Operating temperature	0° to 40°C (32º to 104ºF)
Operating humidity	10 to 90% maximum relative humidity, noncondensing
Storage temperature	–20º to 70ºC (–4° to 158°F)
Storage humidity	5 to 95% maximum relative humidity, noncondensing
Regulatory compliance US	47 CFR FCC Part 15, Subpart B, Class B ICES-003:2016 Issue 6, Class B 47 CFR FCC Part 15, Subpart C (Section 15.247) 47 CFR FCC Part 15, Subpart E (Section 15.407) FCC Part 2 (Section 2.1091) KDB 447498 D01 General RF Exposure Guidance v06
Regulatory compliance Canada	47 CFR FCC Part 15, Subpart B, Class B ICES-003:2016 Issue 6, Class B Canada RSS-247 Issue 1 (2015-05) Canada RSS-Gen Issue 4 (2014-11)

Table 3. Access point specifications (Continued)

Feature	Description
Regulatory compliance Europe	EN 55032:2015 + AC: 2016, Class B CISPR 32:2015 + AC:2016, Class B EN 61000-3-2:2014, Class A EN 61000-3-3:2013 EN 55024:2010 + A1:2015 EN 301 489-1 V2.1.1 (2017-02) EN 301 489-17 V3.1.1 (2017-02) EN 505032:2015 + AC:2016, Class B CISPR 32:2015 + COR1:2016, Class B EN 300 328 V2.1.1 (2016-11) EN 301 893 V2.1.1 (2017-05) EN 50385:2002 IEC 60950-1:2005 + A1:2009 + A2:2013 EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
Regulatory compliance Australia	AS/NZS CISPR 32:2015, Class B AS/NZS 4268:2017 AS/NZS 2772.2:2011 AS/NZS 60950.1:2015