NETGEAR®

User Manual

Insight Managed Smart Cloud Wireless Access Point

Model WAC510

February 2019
202-11840-05

NETGEAR, Inc.
350 E. Plumeria Drive
San Jose, CA 95134, USA

Support

Thank you for purchasing this NETGEAR product. You can visit https://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.

Compliance and Conformity

For regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.

See the regulatory compliance document before connecting the power supply.

Do not use this device outdoors. If you connect cables or devices that are outdoors to this device, see http://kb.netgear.com/000057103 for safety and warranty information.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-11840-05	February 2019	We published the manual in a new style and added About NETGEAR Insight on page 12. We made major changes to the following sections: Connect over WiFi using a WiFi-enabled computer or mobile device on page 27 Connect over Ethernet using a computer connected to the same network on page 31 Connect over Ethernet using a directly connected computer on page 34 Set up an open or secure WiFi network on page 41 Enable or disable band steering with 802.11k RRM and 802.11v WiFi network management on page 52 Change the channel width for a radio on page 70 Manage load balancing for the radios on page 82 Manage the maximum number of clients for a radio on page 80 Change the management mode to NETGEAR Insight or Web-browser on page 137 View the access point Internet, IP, and system settings on page 162 View the WiFi radio settings on page 165 Factory settings on page 197 We made other minor changes and corrections throughout the manual. We removed Set up a WiFi on/off schedule for the radios, which is replaced by Disable or enable a WiFi network or set up a WiFi activity schedule on page 48. We removed information about the Power LED alternating green and amber, which is not an option for the Power LED.
202-11840-04	July 2018	We added the following sections: Safety instructions and warnings on page 16 Enable or disable URL tracking for a WiFi network on page 55 Set a data volume limit for the access point on page 84 Router mode: Specify WAN Point-to-Point Protocol over Ethernet settings on page 115 Schedule the access point to reboot on page 154 View or download tracked URLs on page 175 View the data volume consumption on page 179 Check the Internet speed on page 186 We made major changes to the following sections: Set up an open or secure WiFi network on page 41 Disable or enable a WiFi network or set up a WiFi activity schedule on page 48 Register and configure Facebook Wi-Fi for the access point on page 58 Manage the advanced WiFi settings for the radios on page 77 Add a user account on page 101 Disable the DHCP client and configure a LAN or WAN IP address on page 112 Router mode: Disable the DHCP client and specify a fixed WAN IP address on page 113 Router mode: Enable the DHCP client and let the access point obtain a WAN IP address on page 118 Perform a ping test on page 185 We made other minor changes and corrections throughout the manual.

(Continued)

Publication Part Number	Publish Date	Comments
202-11840-03	February 2018	We added Connect over the Internet using the NETGEAR Insight Cloud Portal on page 26, and, throughout the manual, information about the NETGEAR Insight Cloud Portal. We made major changes to the following sections: Top panel with LEDs on page 13 Manage local MAC access control lists on page 94, including Manually set up a MAC access control List on page 95 and Import an existing MAC access control list on page 98 Enable or disable inter-VLAN routing on page 134 Insight LED is off on page 190 We made other minor changes and corrections throughout the manual. The client separation feature is now referred to as the client isolation feature (see Set up an open or secure WiFi network on page 41 and Enable or disable client isolation for a WiFi network on page 50)
202-11840-02	December 2017	We added or made major changes to the following sections: Set up an open or secure WiFi network on page 41 Enable or disable PMF for a WiFi network on page 54 Manage local MAC access control lists on page 94, including Manually set up a MAC access control List on page 95 and Import an existing MAC access control list on page 98 Change the management mode to NETGEAR Insight or Web-browser on page 137 Manually download firmware and upgrade the access point on page 147 Revert to the backup firmware on page 148 Perform a ping test on page 185 Technical specifications on page 200 For all sections to which it applies, we added a step that describes the action that is required in the pop-up warning window.
202-11840-01	September 2017	We added or made major changes to the following sections: Connect over WiFi using a WiFi-enabled computer or mobile device on page 27 Connect over Ethernet using a computer connected to the same network on page 31 Connect over Ethernet using a directly connected computer on page 34 Set up an open or secure WiFi network on page 41 Register and configure Facebook Wi-Fi for the access point on page 58 Set up a captive portal for a WiFi network on page 60 Unregister the access point from Facebook Wi-Fi on page 63 Manage the advanced WiFi settings for the radios on page 77 Manage neighbor AP detection on page 104 Set up RADIUS servers on page 109 Disable the DHCP client and configure a LAN or WAN IP address on page 112

(Continued)

Publication Part Number	Publish Date	Comments
202-11840-01	September 2017	(202-11840-01, September 2017, Continued) Enable the DHCP client on page 117 Set the 802.1Q VLAN and management VLAN on page 120 Enable or disable IGMP snooping on page 125 Router mode only: Manage DHCP servers on page 127, including Manage the default DHCP server on page 127 and Enable or disable inter-VLAN routing on page 134 Change the management mode to NETGEAR Insight or Web-browser on page 137 Manage the LEDs on page 160 View unknown and known neighbor access points on page 168 View client distribution, connected clients, and client trends on page 169 View WiFi and WAN traffic, traffic statistics, and channel utilization on page 173 View a WiFi bridge connection on page 178 Capture WiFi and Ethernet packets on page 183 In addition, we made minor changes to other sections and updated some figures.
202-11686-02	April 2017	We made major changes to the following sections: Connect over WiFi using the NETGEAR Insight Mobile App on an iOS or Android mobile device on page 25 Connect over WiFi using a WiFi-enabled computer or mobile device on page 27 Connect over Ethernet using a computer connected to the same network on page 31 Connect over Ethernet using a directly connected computer on page 34 Set up an open or secure WiFi network on page 41 Block specific URLs and keywords for Internet access on page 93 Change the system mode to Router mode or AP mode on page 138 In addition, we made minor changes to other sections and updated some figures.
202-11686-01	December 2016	First publication.

Contents

Chapter 6 Manage the Local Area Network and IP Settings

Chapter 7 Manage and Maintain the Access Point

1

Hardware Overview of the Access Point

The NETGEAR Insight Managed Smart Cloud Wireless Access Point (WAC510) 802.11 Wave 2 AC1300, in this manual referred to as the access point, supports dual-band concurrent operation at 2.4 GHz and 5 GHz with a combined throughput of 1300 Mbps (400 Mbps at 2.4 GHz and 867 Mbps at 5 GHz).

The access point can function as a Power over Ethernet (PoE) powered device (PD) in an existing network connected to a PoE switch, with a power adapter connected to a regular switch, or in standalone mode as both an access point and router connected to an Internet modem.

The 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 netgear.com/support/download/. 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 manual, you might need to update the firmware.

Note: In this user manual, *WiFi network* means the same as SSID (service set identifier or WiFi network name) or VAP (virtual access point). That is, in this user manual, when we refer to a WiFi network we mean an individual SSID or VAP.

About NETGEAR Insight

The access point supports the NETGEAR Insight mobile app, which lets you set up and manage the access point from your iOS or Android mobile device and connects to the Insight cloud-based management platform. For Insight Premium or Insight Pro subscribers, the access point also supports the Insight Cloud Portal, which is the website that provides access to the Insight cloud-based management platform. However, this user manual describes the local browser–based management interface, in this manual referred to as the local browser interface. For more information about NETGEAR Insight, visit insight.netgear.com and see the NETGEAR knowledge base at netgear.com/support/product/insight.aspx.

If you install the access point as a NETGEAR Insight managed device, the settings for features that you can manage through the Insight mobile app and Insight Cloud Portal are masked out in the local browser interface. However, using the local browser interface, you can still manage the settings for certain features that are not yet supported in Insight. For more information, visit the NETGEAR knowledge base at netgear.com/support/product/insight.aspx and search for *What is Hybrid Management Mode*.

Related documentation

The following related documentation is available at netgear.com/support/download/:

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

For information about the NETGEAR Insight mobile app and the Insight Cloud Portal, visit insight.netgear.com and see the NETGEAR knowledge base at netgear.com/support/product/insight.aspx.

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

Figure 1. Top panel with 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 fast, temporarily**. The access point is upgrading firmware. **Blinking amber slowly, continuously**. The access point did not receive an IP address from a DHCP server.	
Insight LED	**If the serial number begins with 5B4 or 5B5:**	**If the serial number begins with 4W8 or 4W9:**
	Off. The access point functions either in standalone mode or in Insight mode but is not connected to the Insight cloud-based management platform. **Solid blue**. The access point functions in Insight mode and is connected to the Insight cloud-based management platform.	**Off**. The access point functions either in standalone mode or in Insight mode but is not connected to the Insight cloud-based management platform. **Solid green**. The access point functions in Insight mode and is connected to the Insight cloud-based management platform.

Table 1. LED descriptions (Continued)

LED	Description
WAN PoE LED 	**Off**. Either no powered-on Ethernet device is connected to the WAN PoE 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 WAN PoE port. **Blinking amber**. 10 or 100 Mbps traffic activity is detected on the WAN PoE port. **Solid green**. A 1000 Mbps Ethernet link is detected on the WAN PoE port. **Blinking green**. 1000 Mbps traffic activity is detected on the WAN PoE port.
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. **Blinking amber**. 10 or 100 Mbps traffic activity is detected on the LAN port. **Solid green**. A 1000 Mbps Ethernet link is detected on the LAN port. **Blinking green**. 1000 Mbps traffic activity 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 188.

Back panel

The back panel of the access point provides two ports and a DC power connector.

Figure 2. Access point back panel

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

- **LAN port**. One black Gigabit Ethernet RJ-45 LAN port to connect the access point to Ethernet devices. You can use the LAN port to connect the access point to a switch, computer, or other Ethernet device.
- **WAN PoE port**. One yellow Gigabit Ethernet RJ-45 WAN PoE port that provides a connection to a PoE switch or regular switch that is connected to your network and the Internet, for example, through an Internet modem. If the access point functions in Router mode (see Change the system mode to Router mode or AP mode on page 138), you can connect the WAN PoE port directly to the LAN port of an Internet modem.
- **DC power connector**. If you do not use a PoE connection, connect an optional power adapter to the DC power connector.

For more information about WAN PoE and LAN port connections, see Set up and connect the access point to your network or Internet modem on page 21.

Note: The **Reset** button is located on the left side panel of the access point. 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 NETGEAR Insight network location, you must first use the Insight mobile app or Insight Cloud Portal to remove the access point from your Insight network location before the factory default settings function of the **Reset** button is available. For more information, see Use the Reset button on page 155.

Product label

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

Figure 3. Product label, part 1

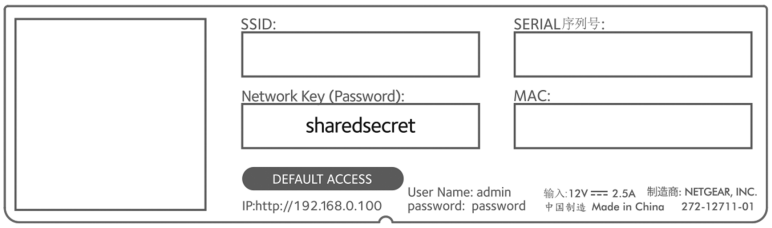


Figure 4. Product label, part 2

Safety instructions and warnings

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage.

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions:

- This product is designed for indoor use only in a temperature-controlled and humidity-controlled environment. For more information, see the environmental specifications in the appendix or the data sheet.
  Any device that is located outdoors and connected to this product must be properly grounded and surge protected.
  Failure to follow these guidelines can result in damage to your NETGEAR product, which might not be covered by NETGEAR's warranty, to the extent permissible by applicable law.
- Observe and follow service markings:
  - Do not service any product except as explained in your system documentation. Some devices should never be opened.
  - If applicable to your device, opening or removing covers that are marked with the triangular symbol with a lightning bolt can expose you to electrical shock. We recommend that only a trained technician services components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
  - Depending on your device, the power adapter, power adapter cable, power cable, extension cable, or plug is damaged.
  - An object fell into the product.
  - The product was exposed to water.

  - The product was dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.

- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide, or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- If applicable to your device, allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To avoid damaging your system, if your device uses a power supply with a voltage selector, be sure that the selector is set to match the power at your location:
  - 115V, 60 Hz in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
  - 100V, 50 Hz in eastern Japan and 100V, 60 Hz in western Japan
  - 230V, 50 Hz in most of Europe, the Middle East, and the Far East
- Be sure that attached devices are electrically rated to operate with the power available in your location.
- Depending on your device, use only a supplied power adapter or approved power cable:
  If your device uses a power adapter:
  - If you were not provided with a power adapter, contact your local NETGEAR reseller.
  - The power adapter must be rated for the product and for the voltage and current marked on the product electrical ratings label.

  If your device uses a power cable:
  - If you were not provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable approved for your country.

  - The power cable must be rated for the product and for the voltage and current marked on the product electrical ratings label. The voltage and current rating of the cable must be greater than the ratings marked on the product.

- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets.
- If applicable to your device, the peripheral power cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a three-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables, power adapter cables, or power cables carefully. Route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power adapters, power adapter cables, power cables or plugs. Consult a licensed electrician or your power company for site modifications.
- Always follow your local and national wiring rules.

2

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

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 and 5.8 GHz cordless phones
- 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 or Internet modem

The access point can function in AP system mode as a WiFi access point in your existing network or in Router system mode as both a WiFi access point and router connected to your DSL or cable Internet modem.

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

- Set up the access point with a PoE network connection
- Set up the access point with a non-PoE network connection
- Set up the access point with a connection to your Internet modem

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. The switch must be connected to a network router that is connected to the Internet. If you use a PoE connection, the access point does not require a power adapter.

In the access point default AP mode, WiFi clients can connect to the access point and access your network and the Internet.

Figure 5. 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 WAN PoE port on the access point.

   Note: Do not use the LAN port for a connection to the PoE switch.

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 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 24.

Set up the access point with a non-PoE network connection

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

In the access point default AP mode, WiFi clients can connect to the access point and access your network and the Internet.

Figure 6. 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 WAN PoE 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 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 24.

Set up the access point with a connection to your Internet modem

You can connect the access point directly to a LAN port on your DSL or cable Internet modem and let the access point function as both a WiFi access point and a router. In this configuration, WiFi clients can connect to the access point and access your network and the Internet and you also can attach a switch to the access point to enhance your network. Because you cannot use Power over Ethernet (PoE) in this setup, the access point requires a power adapter, which is an option that you can purchase.

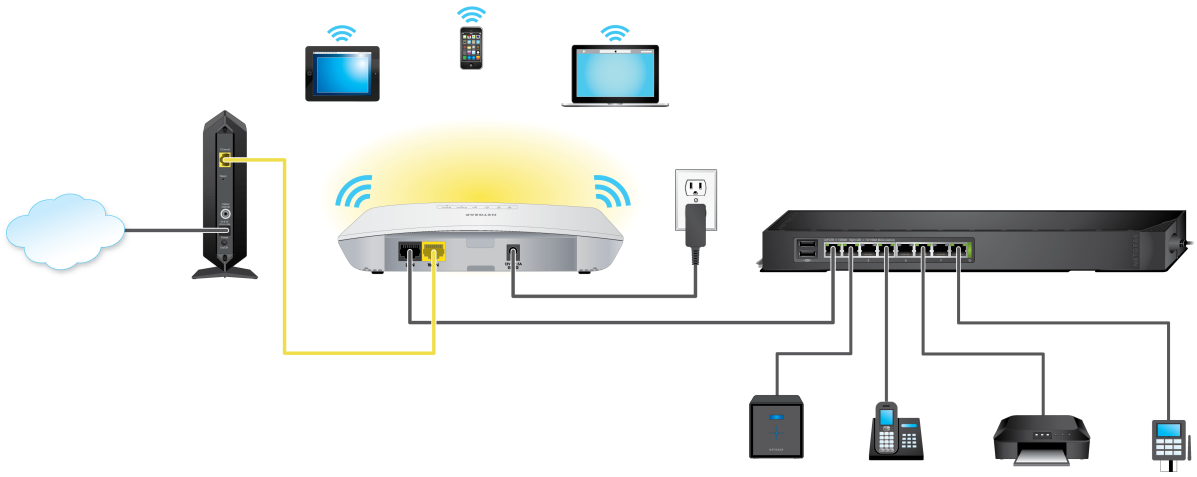


Figure 7. Set up the access point with a connection to a LAN port on your Internet modem

To connect the access point to your Internet modem:

1. Unplug your Internet modem's power, leaving the modem connected to the wall jack for your Internet service.
2. If your Internet modem includes a battery backup, remove the battery.
3. Use an Ethernet cable to connect the yellow WAN PoE port on the access point to a LAN port on the Internet modem.

   Note: Do not use the LAN port on the access point for a connection to the Internet modem.

4. If your Internet modem includes a battery backup, reinsert the battery.
5. Plug in your Internet modem's power and turn on your Internet modem.
6. To attach a switch to the access point, use an Ethernet cable to connect the switch to the black LAN port on the access point.
7. Connect the power adapter to the access point and plug it into an electrical outlet.

   The Power LED lights solid amber. After about one minute, if the access point is connected to a DHCP server (an Internet modem usually also functions as a DHCP server), the Power LED turns solid green and the access point is ready for you to perform the initial configuration.

   Note: During initial configuration of the access point, you must change the default system mode of the access point from AP mode to Router mode.

For information about accessing the access point for initial configuration, see Connect to the access point for initial configuration on page 24. After initial configuration, change the default system mode of the access point from AP mode to Router mode (see Change the system mode to Router mode or AP mode on page 138).

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 connect to the access point by using the NETGEAR Insight mobile app on an iOS or Android mobile device, by accessing the Insight Cloud Portal, or by using the local browser interface. You cannot use Insight access with the local browser interface. These types of access are mutually exclusive.

The Insight mobile app and the Insight Cloud Portal provide ease of access and let you configure most features that are available on the access point. The local browser interface lets you configure all features that are available on the access point.

If you use the Insight mobile app or the Insight Cloud Portal to connect to the access point, see one of the following sections:

- Connect over WiFi using the NETGEAR Insight Mobile App on an iOS or Android mobile device on page 25
- Connect over the Internet using the NETGEAR Insight Cloud Portal on page 26

If you use the local browser interface to connect to the access point, follow the procedure in *one* of these sections:

- Connect over WiFi using a WiFi-enabled computer or mobile device on page 27
- Connect over Ethernet using a computer connected to the same network on page 31
- Connect over Ethernet using a directly connected computer on page 34

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 the NETGEAR Insight Mobile App on an iOS or Android mobile device

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

For more information about the Insight mobile app, visit insight.netgear.com and see the NETGEAR knowledge base at netgear.com/support/product/insight.aspx.

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 Insight mobile app and log in to your NETGEAR account or create a new account to log in with.
3. Follow the prompts in the Insight mobile 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 connected to the Internet, you can use the Insight mobile app to configure the access point by connecting to its 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 the Internet using the NETGEAR Insight Cloud Portal

The Insight Cloud Portal is available for Insight Premium or Insight Pro subscribers. To use the NETGEAR Insight Cloud Portal to configure and manage the access point, the access point must already be connected to the Internet.

For more information about the Insight Cloud Portal and the configuration and management options that are available through the Insight Cloud Portal, visit insight.netgear.com and see the NETGEAR knowledge base at netgear.com/support/product/insight.aspx.

To connect to the access point over the Internet through the Insight Cloud Portal:

1. Visit https://insight.netgear.com/#/login.
   The Insight Cloud Portal web page displays.
2. Select **Login**.
   The NETGEAR Account Sign-In page displays.
3. Enter your Insight email address and password.
   If you do not own an Insight account, visit insight.netgear.com.
4. Click the **NETGEAR Sign In** button.
   You can now add the access point to an Insight network location so that you configure and manage the access point.

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 mobile 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**).

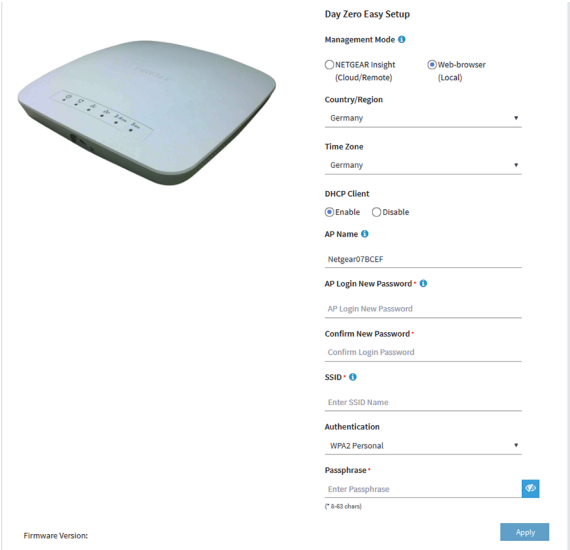
   Note: You can use www.routerlogin.net (and www.aplogin.net) only during initial setup of the access point.

   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 **Web-browser** radio 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.

(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	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.) 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.
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 Personal**. 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. • **WPA2 Personal Mixed**. 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. After you complete the setup process, you can set up WPA2 Enterprise security with RADIUS servers. For more information, see Set up an open or secure WiFi network on page 41.
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 and you are disconnected from the access point.
   If you changed the default country, the access point restarts.
7. 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.
8. 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.
9. 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

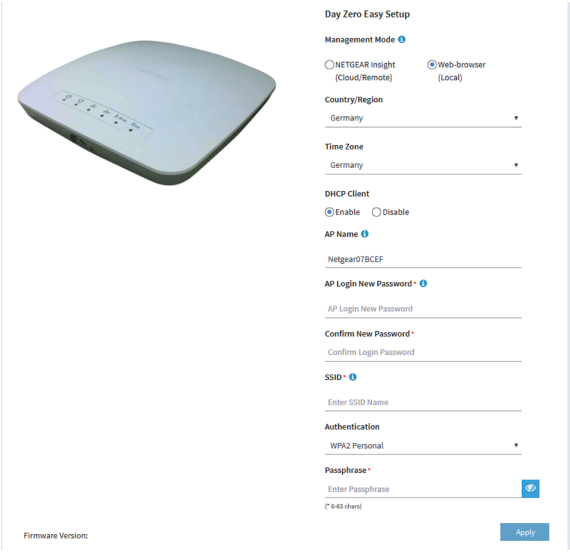
The following procedure assumes that your network includes a DHCP server (or router that functions as a DHCP server) and that the access point and the computer are on the same network. By default, the access point functions as a DHCP client. If you want to set up the access point with a static (fixed) IP address, see Connect over Ethernet using a directly connected computer on page 34.

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 **Web-browser** radio 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.

4. 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	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.) 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.

(Continued)

Setting	Description
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 (\).
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 Personal**. 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. • **WPA2 Personal Mixed**. 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. After you complete the setup process, you can set up WPA2 Enterprise security with RADIUS servers. For more information, see Set up an open or secure WiFi network on page 41.
Passphrase	Unless you select **Open** from the **Authentication Type** menu, enter a new passphrase (network key or WiFi password) for the WiFi network.

5. 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.

6. 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.

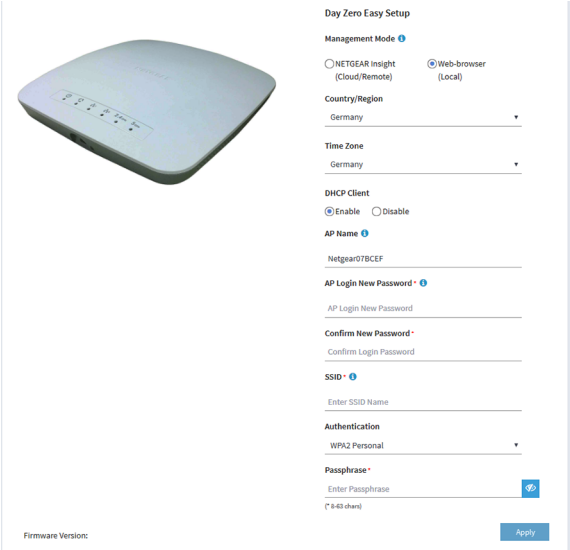
   (You can actually use any IP address in the 192.168.0.2–192.168.0.254 range, with the exception of IP address 192.168.0.100, which is the default IP address of the access point.)

   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 **Web-browser** radio 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.
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	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.) 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.
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 Personal**. 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. • **WPA2 Personal Mixed**. 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. After you complete the setup process, you can set up WPA2 Enterprise security with RADIUS servers. For more information, see Set up an open or secure WiFi network on page 41.
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. 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.
9. 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.
10. 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.

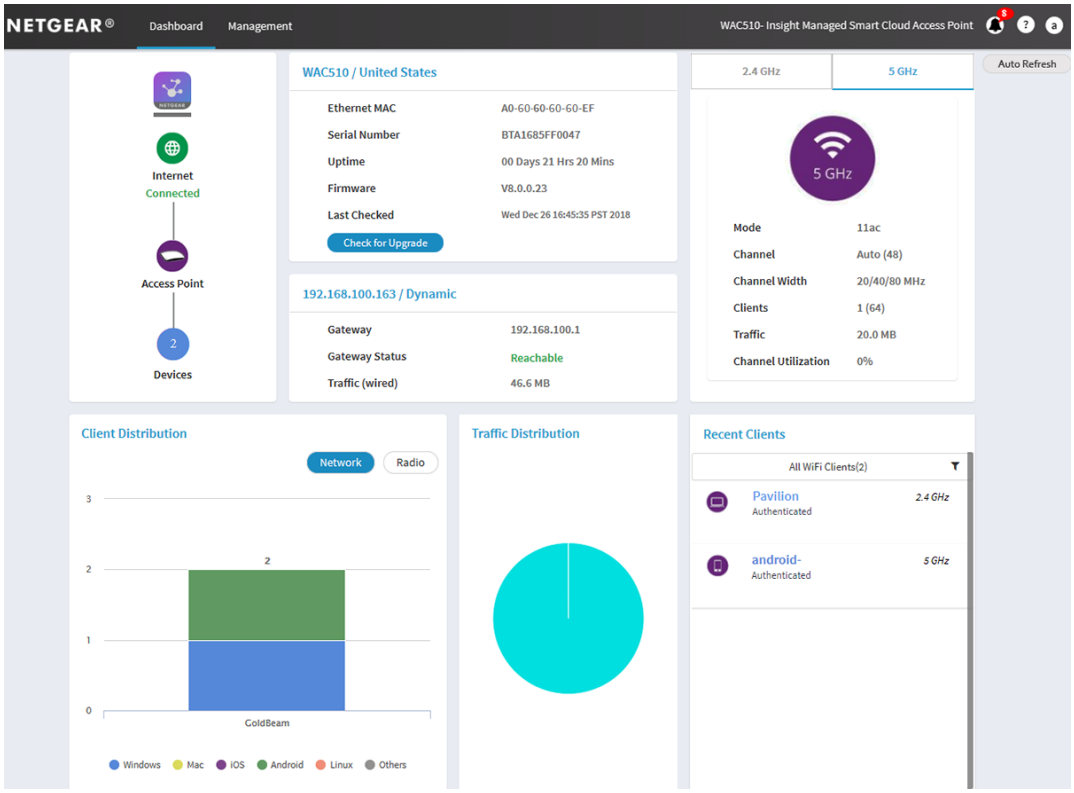
To log in to the access point's local browser interface:

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 161.

3

Manage the Basic WiFi and Radio Features

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 76.

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 in the 2.4 GHz radio band and four in the 5 GHz radio band), 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
- View or change the settings of a WiFi network
- Disable or enable a WiFi network or set up a WiFi activity schedule
- Remove a WiFi network
- Enable or disable client isolation for a WiFi network
- Hide or broadcast the SSID for a WiFi network
- Enable or disable band steering with 802.11k RRM and 802.11v WiFi network management
- Change the VLAN ID for a WiFi network
- Enable or disable PMF for a WiFi network
- Enable or disable URL tracking for a WiFi network
- Select a MAC ACL for a WiFi network
- Set bandwidth rate limits for a WiFi network
- Register and configure Facebook Wi-Fi for the access point
- Set up a captive portal for a WiFi network
- Unregister the access point from Facebook Wi-Fi

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 stands for service set identifier, which is the WiFi network name. When you create a new SSID, you are 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 109).

To set up a WiFi network:

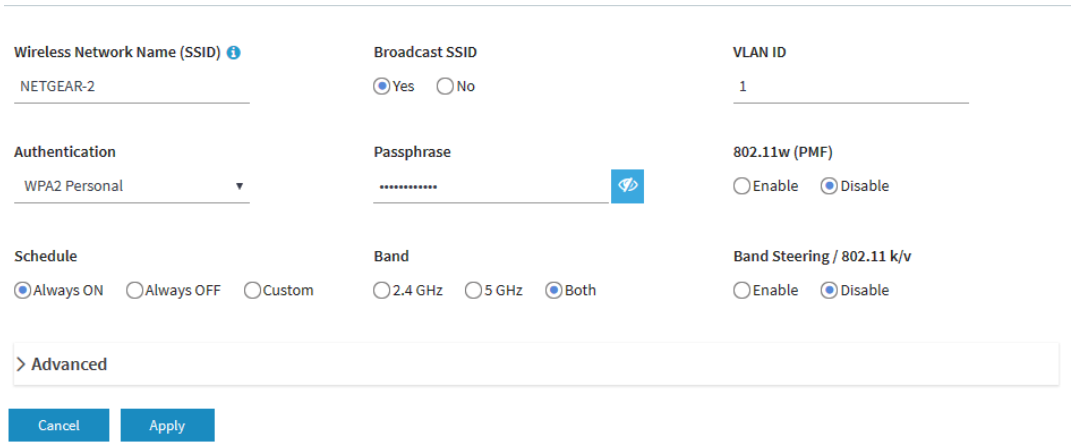
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   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. Specify the WiFi network name (SSID), select whether the SSID is broadcast, and specify the VLAN ID as described in the following table.

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.
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 120). If the access point functions in Router mode, you can use the VLAN ID to assign a particular DHCP server to the clients on the WiFi network (see Add a DHCP server for a WiFi network on page 129).

7. Specify the WiFi security by selecting an option from the **Authentication** menu and, if applicable, by specifying a passphrase in the **Passphrase** field or selecting an option from the **Encryption** menu, as described in the following table.

Setting	Description
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 Personal	This option, which is the same as WPA2-PSK, 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 sharedsecret. 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, **WPA2 Personal Mixed**. 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.

(Continued)

Setting	Description
WPA2 Personal Mixed	This mixed mode security, which is the same as WPA-PSK / WPA2-PSK, 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 109). From the **Data Encryption** menu, select the data encryption 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.

8. Optionally, disable the WiFi broadcast or set up a WiFi activity schedule by selecting one of the following radio buttons:

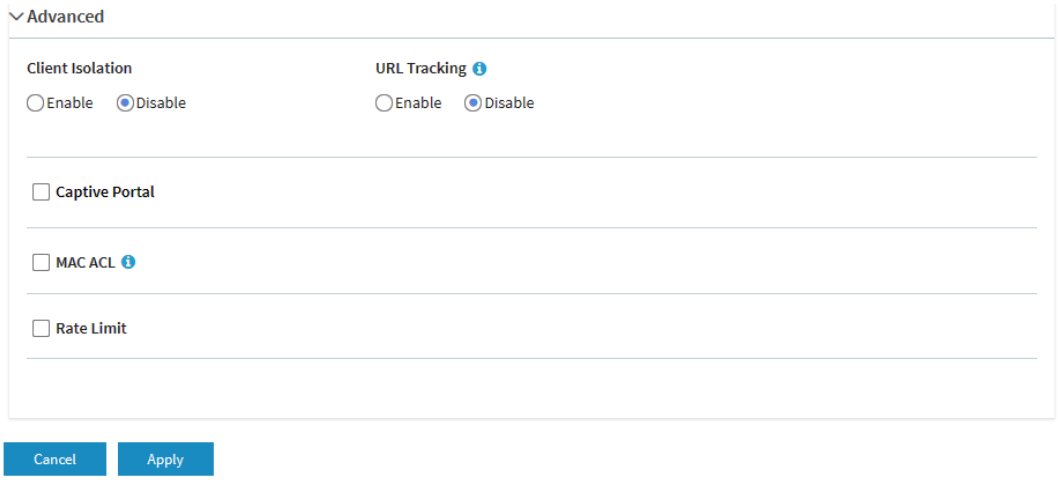
   - **Always ON**. When you set up an SSID, you are creating a new virtual access point (VAP). By default, the new VAP is enabled and the **Always ON** radio button is selected.
   - **Always OFF**. Select this radio button to set up the SSID but temporarily disable the VAP.
   - **Custom**. Select this radio button to set up a broadcast schedule. An icon displays to the right of the radio button. Do the following:
     a. Click the icon next to the radio button.
        A pop-up window opens.
     b. Either select a predefined time from the **Preset** menu or select custom time blocks by clicking the time blocks.
        A blue color for a time block indicates that the VAP will be enabled (on). A gray color for a time block indicates that the VAP will be disabled (off).
     c. Click the **Done** button.
        The pop-up window closes.

For each SSID and each day (from 12:00 a.m. to 11:59 p.m.), you can create three schedules to disable the VAP.

9. Optionally, enable 802.11w Protected Management Frames (PMF), select a single radio band only, enable band steering with 802.11k radio resource management (RRM) and 802.11v WiFi network management, or do all of this, as described in the following table.

Setting	Description
802.11w (PMF)	Protected Management Frames (PMF), according to the 802.11w standard, is a security feature that protects unicast and multicast management frames from being intercepted and changed for malicious purposes. This feature is disabled by default, but you can enable it.
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.
Band Steering / 802.11 k/v	By default, band steering with 802.11k RRM and 802.11v WiFi network management is disabled for the VAP. To enable band steering with 802.11k RRM and 802.11v WiFi network management, select the **Enable** radio button. Doing so allows the access point, under certain channel conditions, to steer WiFi devices that are dual-band capable to the 2.4 GHz or 5 GHz band of the VAP. Compared to the 2.4 GHz band, generally more channels and bandwidth are available in the 5 GHz band, causing less interference and allowing for a better user experience. 802.11k RRM and 802.11v WiFi network management affect the network in the following ways: • **802.11k RRM**. This feature lets the access point and 802.11k-aware clients dynamically measure the available radio resources. 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. • **802.11v WiFi network management**. This feature lets the access point steer its WiFi clients to the 2.4 GHz or 5 GHz band, based on the access point's channel load. The access point sets the received signal strength indicator (RSSI) threshold automatically. (That is, you cannot configure the RSSI threshold manually.)

10. Optionally, to configure client isolation, URL tracking, or both for the WiFi network, click the **> Advanced** tab.



11. Configure the client isolation and URL tracking settings as described in the following table.

Setting	Description
Client Isolation	By default, client isolation is disabled for the VAP. To block communication between WiFi clients that are associated with the same SSID or different SSIDs on the access point, select the **Enable** radio button. If you want to enable client isolation for an SSID and the access point functions in Router Mode, you must disable inter-VLAN routing for the VLAN that is associated with the SSID (see Enable or disable inter-VLAN routing on page 134).
URL Tracking	By default, URL tracking is disabled, and the **Disable** radio button is selected. To enable URL tracking for all URLs that are requested by WiFi clients that are connected to the SSID, select the **Enable** radio button. For information about how to view the tracked URLs per SSID or per WiFi client, see View or download tracked URLs on page 175.

Although you could also configure a captive portal, a MAC ACL, and bandwidth rate limits while you set up a WiFi network, these features are described separately and in detail in the following sections:

- Manage local MAC access control lists on page 94 and Select a MAC ACL for a WiFi network on page 55
- Set bandwidth rate limits for a WiFi network on page 57
- Set up a captive portal for a WiFi network on page 60

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

13. 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 169.) 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 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. 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 41.

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 169.) 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 or set up a WiFi activity schedule

You can temporarily disable a WiFi network (SSID or VAP), you can reenable the WiFi network, or you can set up a schedule that specifies when the WiFi network is active.

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

For each WiFi network and each day (from 12:00 a.m. to 11:59 p.m.), you can create three schedules.

To disable or enable a WiFi network or set up a WiFi activity 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**.
   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 Schedule, select one of the following radio buttons:
   - **Always ON**. The WiFi network is enabled.
   - **Always OFF**. The WiFi network is disabled.
   - **Custom**. The WiFi network is enabled or disabled according to a schedule that you must set up.
     An icon displays to the right of the radio button.
7. If you select **Custom** in the previous step, do the following:
   a. Click the icon next to the radio button.
      A pop-up window opens.
   b. Either select a predefined time from the **Preset** menu or select custom time blocks by clicking the time blocks.
      A blue color for a time block indicates that the WiFi network will be enabled (on).
      A gray color for a time block indicates that the WiFi network will be disabled (off).
   c. Click the **Done** button.
      The pop-up window closes.
8. 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.

   A pop-up warning window opens.

6. Click the **Delete** button.

   The pop-window closes and the WiFi network is removed.

Enable or disable client isolation for a WiFi network

By default, client isolation is disabled for a WiFi network (SSID or VAP), allowing communication between WiFi clients that are associated with the same or different WiFi networks on the access point. For additional security, you can enable client isolation so that clients that are associated with the same or different WiFi networks *cannot* communicate with each other, except for communication over the Internet, which remains possible.

To enable or disable client isolation 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. Click the **> Advanced** tab.

The page expands.

7. Under Client Isolation, select one of the following radio buttons:
   - **Enable**. Client isolation is enabled for the WiFi network.
   - **Disable**. Client isolation is disabled for the WiFi network.
8. 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 87), 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 band steering with 802.11k RRM and 802.11v WiFi network management

Band steering lets the access point identify the WiFi devices that are dual-band capable and steer those devices to the 2.4 GHz or 5 GHz band of a WiFi network (SSID or VAP). Compared to the 2.4 GHz band, generally more channels and bandwidth are available in the 5 GHz band, causing less interference and allowing for a better user experience. Band steering includes 802.11k radio resource management (RRM) and 802.11v WiFi network management. By default, band steering is disabled.

802.11k RRM and 802.11v WiFi network management affect the network in the following ways:

- **802.11k RRM**. This feature lets the access point and 802.11k-aware clients dynamically measure the available radio resources. 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.
- **802.11v WiFi network management**. This feature lets the access point steer its WiFi clients to the 2.4 GHz or 5 GHz band, based on the access point's channel load. In an environment with multiple access points, 802.11v WiFi network management helps WiFi clients that are roaming to select the best access point.

The access point sets the received signal strength indicator (RSSI) threshold automatically. (That is, you cannot configure the RSSI threshold manually.)

To enable or disable band steering with 802.11k RRM and 802.11v WiFi network management 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 / 802.11 k/v, select one of the following radio buttons:
   - **Disable**. Band steering is disabled for the VAP. This is the default setting.
   - **Enabled**. Under certain channel conditions, the access point steers WiFi devices that are dual-band capable to the 2.4 GHz or 5 GHz band of the VAP.
7. Click the **Apply** button.
   Your settings are saved.

Change the VLAN ID for a WiFi network

If the access point functions in Router mode, you can use the VLAN ID to assign a particular DHCP server to the WiFi clients on the SSID (see Add a DHCP server for a WiFi network on page 129). By default, the VLAN ID for a WiFi network is 1.

The VLAN ID for a WiFi network 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 120).

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 ID (that is, a number).
   By default, the VLAN ID for a WiFi network is 1.
7. Click the **Apply** button.
   Your settings are saved.

Enable or disable PMF for a WiFi network

Protected Management Frames (PMF), according to the 802.11w standard, is a security feature that protects unicast and multicast management frames from being intercepted and changed for malicious purposes. This feature is disabled by default, but you can enable it.

To enable or disable PMF 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 802.11w (PMF), select one of the following radio buttons:
   - **Enable**. PMF is enabled for the WiFi network.
   - **Disable**. PMF is disabled for the WiFi network.
7. Click the **Apply** button.
   Your settings are saved.

Enable or disable URL tracking for a WiFi network

You can enable the access point to track all URLs that are requested by WiFi clients that are connected to a WiFi network (SSID or VAP). This feature is disabled by default, but you can enable it.

For information about how to view the tracked URLs per SSID or per WiFi client, see View or download tracked URLs on page 175.

To enable or disable URL tracking 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. Click the **> Advanced** tab.
   The page expands.
7. Under URL Tracking, select one of the following radio buttons:
   - **Enable**. URL Tracking is enabled for the WiFi network.
   - **Disable**. URL Tracking is disabled for the WiFi network.
8. 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 94), 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 109) 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 41).

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 displays lets you select an SSID.
5. Click the **>** button to the left the SSID.
   The settings for the selected SSID display.
6. Click the **> Advanced** tab.
   The page expands.
7. Select the **MAC ACL** check box.
8. 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.
     To change the MAC ACL policy, MAC addresses in the ACL, or both, click the link next to the group. For more information, see Manage local MAC access control lists on page 94.

- 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 109).

9. 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.

Note: Before you set bandwidth rate limits, check the Internet speed of the access point (see Check the Internet speed on page 186).

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 displays lets you select an SSID.
5. Click the **>** button to the left the SSID.
   The settings for the selected SSID display.
6. Click the **> Advanced** tab.
   The page expands.

7. Select the **Rate Limit** check box.
8. 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.
9. Click the **Apply** button.
   Your settings are saved.

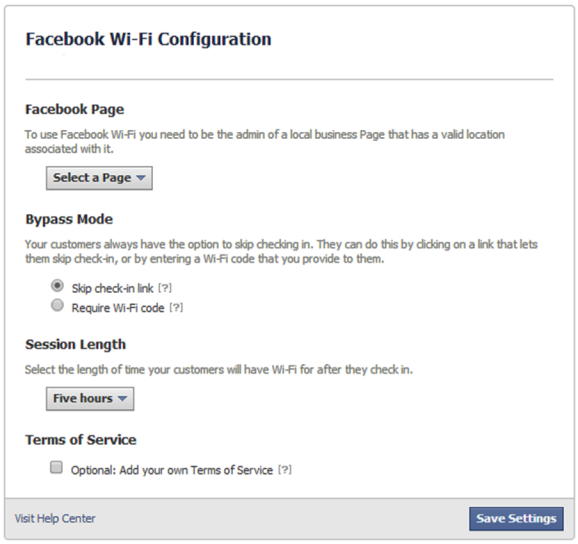
Register and configure Facebook Wi-Fi for the access point

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 60), you must register the access point with Facebook. By default, the capability to register is disabled.

To register and configure Facebook Wi-Fi for 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 > Configuration > Wireless > Basic > Facebook Wi-Fi**.
   The Facebook Wi-Fi page displays.
5. Select the Register with Facebook Wi-Fi **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.

14. To allow clients that are connected to the Facebook captive portal to establish a secure HTTP (HTTPS) session *before* the captive portal authentication occurs, select the Allow HTTPS **Enable** radio button.

By default, the Allow HTTPS **Disable** radio button is selected and clients that are connected to the Facebook captive portal cannot establish an HTTPS session until after the captive portal authentication occurs.

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

Set up a captive portal for a WiFi network

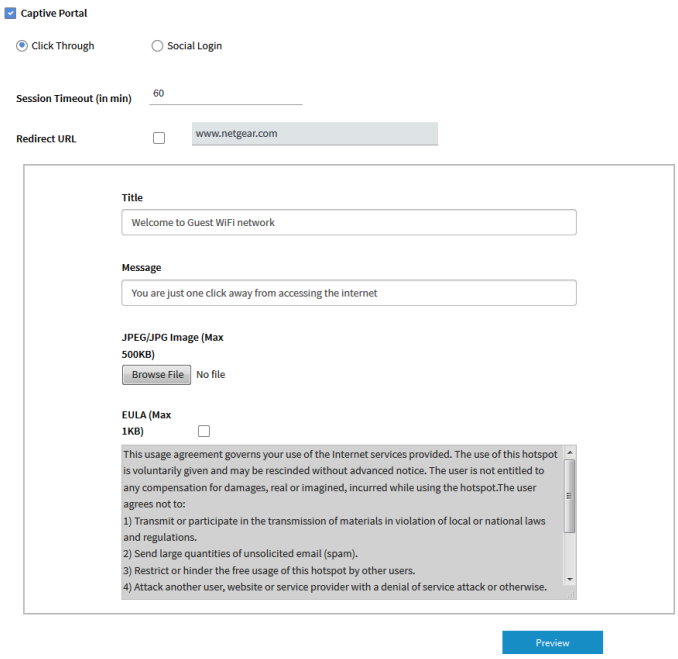
Use a captive portal to welcome or instruct WiFi users and limit their sessions. You can require users to agree to an end user license agreement (EULA) and redirect them a specific website. A captive portal is specific to an SSID.

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 and configure Facebook Wi-Fi for the access point on page 58).

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 displays lets you select an SSID.
5. Click the **>** button to the left the SSID.
   The settings for the selected SSID display.
6. Click the **> Advanced** tab.
   The page expands.

7. Select the **Captive Portal** check box.



8. 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 9.
   - **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 and configure Facebook Wi-Fi for the access point on page 58).
     If you select his option, you can skip Step 9.

9. 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.

(Continued)

Setting	Description
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.

10. 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).

11. Click the **Apply** button.
    Your settings are saved. WiFi clients attempting to connect to the SSID are presented with the captive portal login page.

Note: When you set up a captive portal with a social login (Facebook Wi-Fi), you can configure the option to allow clients that are connected to the Facebook captive portal to establish a secure HTTP (HTTPS) session *before* the captive portal authentication occurs (see Register and configure Facebook Wi-Fi for the access point on page 58). This option is not available when you set up a captive portal with a click-through login (that is, a local login), so an HTTPS session is blocked until after the captive portal authentication occurs.

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:

- Manage the basic settings for the radios
- Turn a radio on or off
- Change the WiFi mode for a radio
- Change the MCS index and data rate for a radio
- Change the channel width for a radio
- Change the output power for a radio
- Change the guard interval for a radio
- Change the channel for a radio
- Manage Quality of Service for a WiFi radio

For information about the advanced radio features, see Manage the advanced radio features on page 77.

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 77.

To manage the basic WiFi settings for the radios:

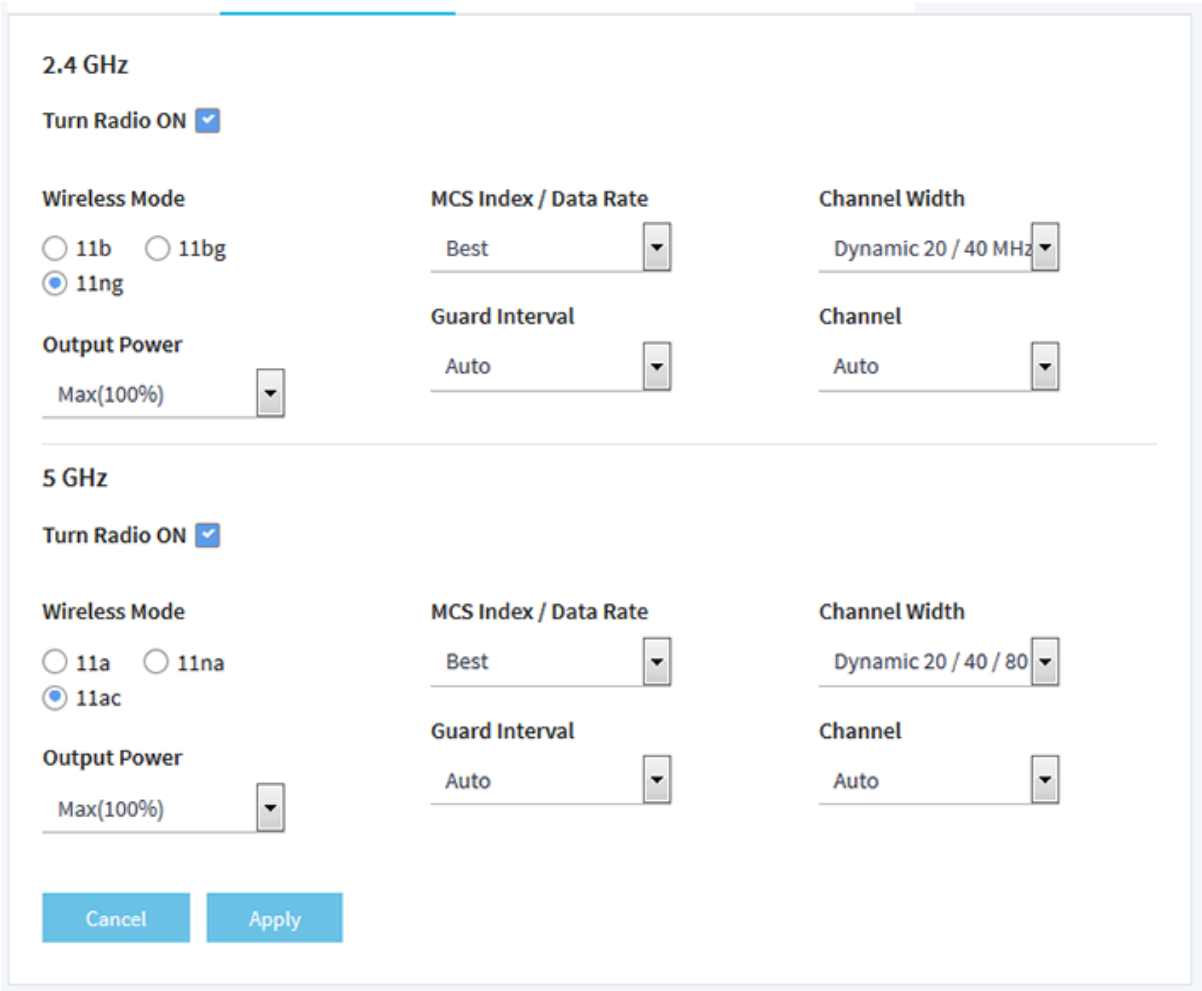
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   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.
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 802.11ac specification allows an 80 MHz–wide channel in addition to the 20 MHz and 40 MHz channels that are available with other modes. • The 40 MHz and 80 MHz channels enable higher data rates but leaves fewer channels available for use. The channel width and guard interval determine the available MCS index and data transmit rates.

(Continued)

Setting	Description
Output Power	From the menu, select the transmission power of the radio. You can select **100%(Max)**, **50%**, **25%**, **12.5%**, or **4%(Min)**. The default is 100%(Max). **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.
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.
   A pop-up warning window opens.
7. Click the **OK** button.
   The pop-up window closes and 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.
   A pop-up warning window opens.
7. Click the **OK** button.
   The pop-up window closes and your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

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.

   A pop-up warning window opens.

7. Click the **OK** button.

   The pop-up window closes and 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 70) and selected guard interval (see Change the guard interval for a radio on page 72).

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.
   A pop-up warning window opens.
7. Click the **OK** button.
   The pop-up window closes and 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 802.11ac specification allows an 80 MHz–wide channel in addition to the 20 MHz and 40 MHz channels that are available with other modes.
- The 40 MHz and 80 MHz channels enable higher data rates but leave fewer channels available for use.

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**.
   - **80 MHz**. This selection is available only for the 5 GHz radio.
   - **Dynamic 20 / 40 MHz**. This selection is available only for the 2.4 GHz radio and is the default setting for that 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.
   A pop-up warning window opens.
7. Click the **OK** button.
   The pop-up window closes and 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 **100%(Max)**, **50%**, **25%**, **12.5%**, or **4%(Min)**.
   The default is 100%(Max).
6. Click the **Apply** button.
   A pop-up warning window opens.
7. Click the **OK** button.
   The pop-up window closes and 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.
   A pop-up warning window opens.
7. Click the **OK** button.
   The pop-up window closes and 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.
   A pop-up warning window opens.
7. Click the **OK** button.
   The pop-up window closes and your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

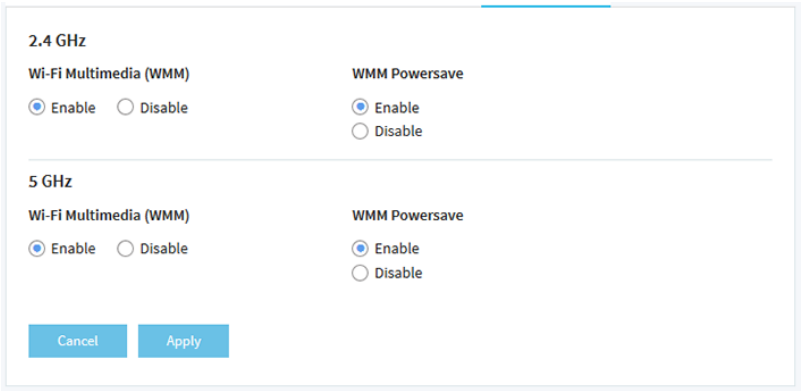
Manage Quality of Service for a WiFi radio

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 a WiFi 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 > 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.
   A pop-up warning window opens.

7. Click the **OK** button.
   The pop-up window closes and your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

4

Manage the Advanced WiFi and Radio Features

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 40.

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:

- Manage the advanced WiFi settings for the radios
- Manage the maximum number of clients for a radio
- Manage the broadcast and multicast settings for a radio
- Manage load balancing for the radios

For information about the basic radio features, see Manage the basic radio features on page 64.

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 64.

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 67.

To manage the advanced WiFi settings for the radios:

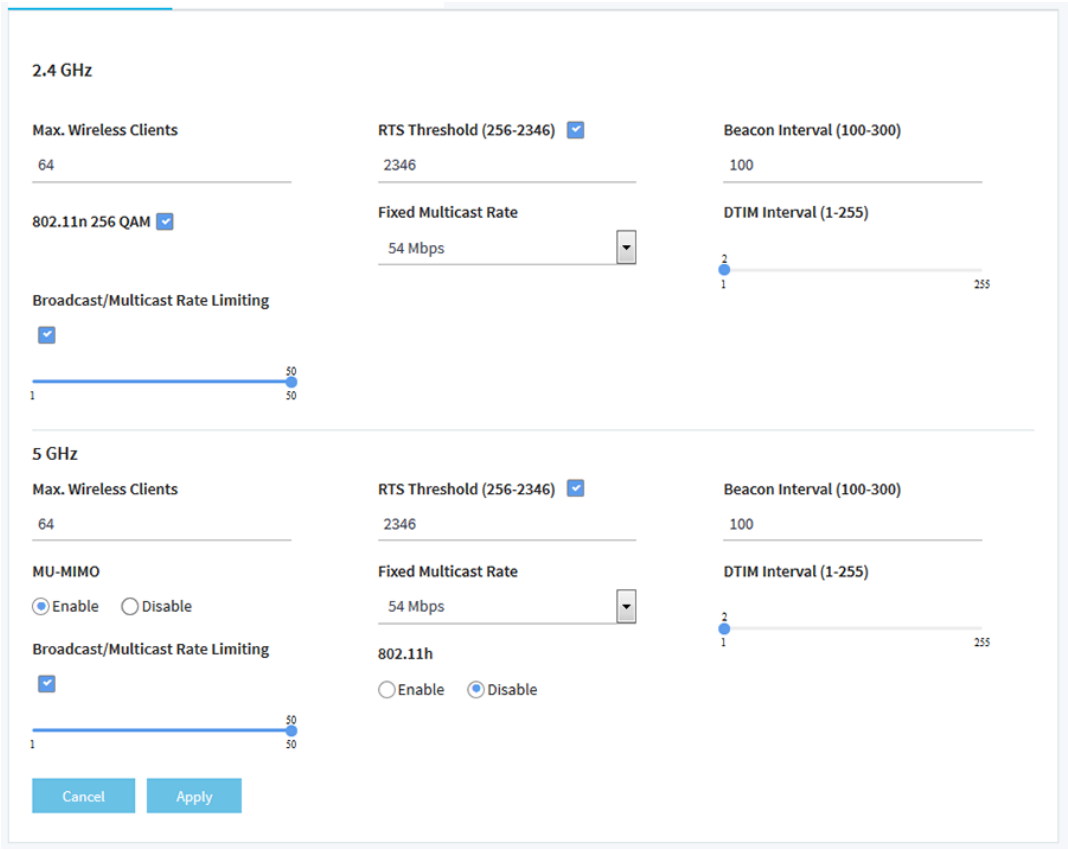
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   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. You can specify the radio settings for the 2.4 GHz and 5 GHz radios individually, but the 802.11n 256 QAM feature applies to the 2.4 GHz radio only and the MU-MIMO and 802.11h features apply to the 5 GHz radio only.

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 200. The default is 64 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.

(Continued)

Setting	Description
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.
802.11n 256 QAM	Select the **802.11n 256 QAM** check box to enable the 2.4 GHz radio to function over 256-quadrature amplitude modulation (QAM), which can increase the 2.4 GHz radio throughput. By default, 256-QAM is disabled for the 2.4 GHz radio, that is, the check box is cleared. By default, 256-QAM is enabled for the 5 GHz radio and you cannot disable it (the page does not provide a check box for the 5 GHz radio).
Fixed Multicast Rate	From the menu, select the multicast traffic transmission rate for the radio. The default is Auto, which lets the access point automatically adjust the multicast traffic transmission rate.
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 2.
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.

(Continued)

Setting	Description
MU-MIMO	By default, the MU-MIMO **Enable** radio button is selected and multiuser MIMO (MU-MIMO) is enabled. To disable MU-MIMO, select the MU-MIMO **Disable** radio button. 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.
802.11h	Select the 802.11h **Enable** radio button to enable 802.11h-capable WiFi clients to automatically switch to a new channel without disconnecting from the access point and without losing any data when the access point changes to another channel. By default, the 802.11h **Disable** radio button is selected and 802.11h is disabled. You can enable or disable 802.11h for the 5 GHz radio but not for the 2.4 GHz radio.

6. Click the **Apply** button.
   A pop-up warning window opens.
7. Click the **OK** button.
   The pop-up window closes and 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, one radio allows up to 64 client associations. You can specify a lower or higher number of clients, up to 200 clients for one radio. If the number of associated clients exceeds the maximum number that you specify, the radio rejects new client associations until the number drops below that maximum 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 200 for the radio. The default is 64 WiFi clients for the radio.
6. Click the **Apply** button.
   A pop-up warning window opens.
7. Click the **OK** button.
   The pop-up window closes and 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 Auto, which lets the access point automatically adjust the multicast traffic transmission rate. You can specify a fixed 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 Auto.
7. Click the **Apply** button.
   A pop-up warning window opens.
8. Click the **OK** button.
   The pop-up window closes and 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 each radio 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.

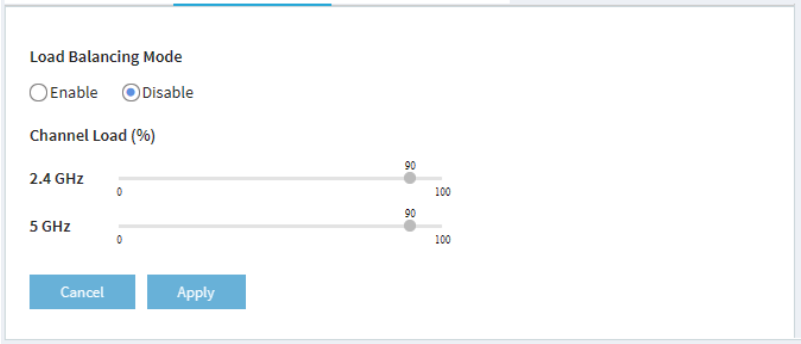
To manage load balancing for the radios:

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 the radios, select the Load Balancing Mode **Enable** radio button.

   By default, load balancing is disabled.

   The page provides a slider for each radio.
6. For each radio, move the associated slider to specify the percentage of network bandwidth utilization that is allowed on the radio before it stops accepting new client associations.

   The default is 90%, which specifies that all new associations are allowed up to 90 percent of the utilization rate of the radio.
7. Click the **Apply** button.

   A pop-up warning window opens.
8. Click the **OK** button.

   The pop-up window closes and your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Set a data volume limit for the access point

You can set a total monthly data volume limit that applies to all WiFi networks that you configure on the access point, that is, it applies to all SSIDs (or VAPs) collectively. A typical use of this feature is to restrict guest user data consumption.

For each SSID, you can define a percentage of the monthly data volume limit, in which case must allocate a data volume in MB to each WiFi client of that SSID. In relation to settings percentages for SSIDs, note the following:

- To make sure that each SSID receives its exact share of the total monthly data volume limit, make sure that the percentages for all SSIDs together do not exceed 100 percent.
- To set a less restrictive policy, the percentages for all SSIDs together do not need to add up to 100 percent. For example, if you set 60 percent for one SSID and 60 percent for another SSIDs, you are providing an equal chance to each SSID to consume 60 percent of the total monthly data volume limit. If one SSID actually consumes 60 percent, only 40 percent is available for the other SSID.
- If you do not set a data volume limit for any SSIDs, all SSIDs are allowed 100 percent of the total monthly data volume limit, and data is consumed on a *first come, first served* basis, up to the total monthly data volume limit.

You can specify when the monthly counter resets or manually reset the counter.

If the consumed data reaches a definable percentage of the profile data volume limit for an SSID, either the data is dropped for all WiFi clients of the SSID or those WiFi clients are disconnected.

To set a data volume limit for 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.

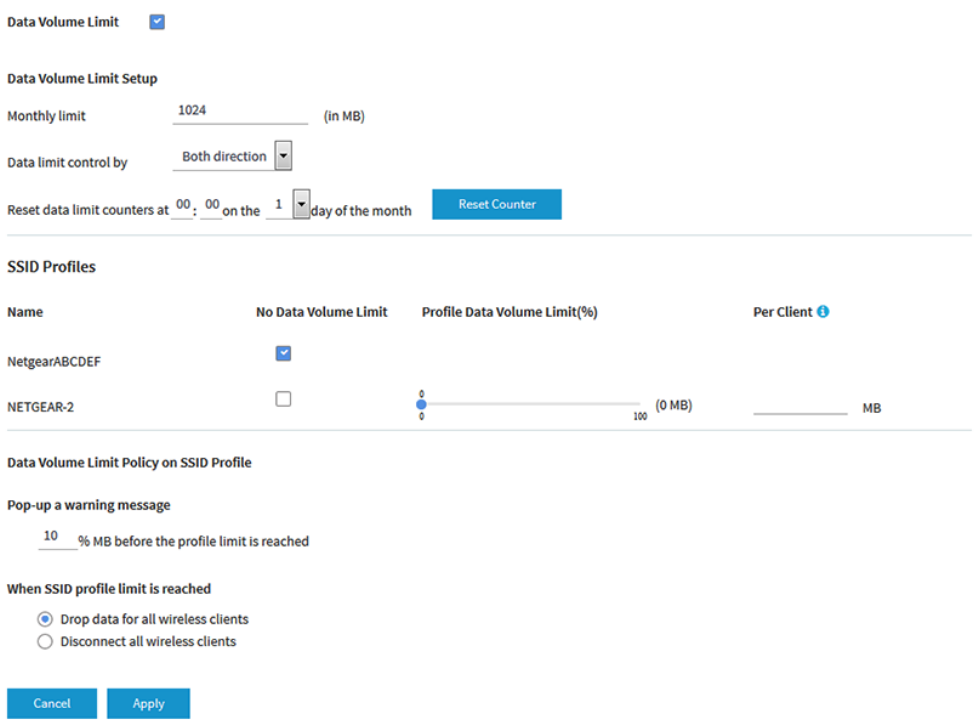
   A login window opens.
3. Enter the access point user name and password.

   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 > Configuration > Wireless > Advanced > Data Volume Limit**.

   The Data Volume Limit page displays.

5. Select the **Data Volume Limit** check box.



6. In the Data Volume Limit Setup section, specify the following settings, which apply to SSIDs collectively, whether or not you set a data volume limit for an SSID in Step 7:

   a. **Monthly limit**. Enter the total monthly data volume limit in MB for the access point, that is, for all SSIDs collectively.
   For example, if you enter 500000, a data volume limit of 500 GB applies to all SSIDs collectively.
   The default value is 1024 MB (1 GB). The maximum that you can enter is 100 TB (100000 GB).

   b. **Data limit control by**. From the menu, select if the data volume limit applies to downloaded data, to uploaded data, or to both combined.

   c. **Reset data limit counters**. Specify the day and time of the month when the counter is reset and the data volume usage for all SSIDs is reset to zero.
   To immediately reset the counter to zero, click the **Reset Counter** button and confirm your action by clicking the **OK** button.

7. In the SSID Profiles section, specify the following settings for any individual SSID for which you want to set a percentage of the total monthly data volume limit:
   a. **No Data Volume Limit**. To specify that the data volume limit applies to the SSID, clear the **No Data Volume Limit** check box for the SSID.
      If you leave the check box selected, no data volume limit applies to the SSID, which means that the SSID is assigned 100 percent. (If you do not set a data volume limit for any SSID, each SSID is assigned 100 percent.)
   b. **Profile Data Volume Limit (%)**. To set a percentage of the monthly data volume limit that you specified in Step 6, move the slider to the percentage that you want to set.
      For example, if the monthly data volume limit is 500000 MB and you move the slider to 60 percent, the volume limit for the SSID is 300000 MB (300 GB). That means that the SSID cannot consume more data than 300 GB. However, the actual available data volume for the SSID might be less than 300 GB if the data consumption on other SSIDs causes the total monthly data volume limit to be reached before the SSID consumes 300 GB.
   c. **Per Client**. If you set a percentage for an SSID, set a monthly data volume limit that applies to each WiFi client of the SSID by entering the monthly data volume limit in MB per WiFi client.
      Take the total monthly data volume limit and the percentage that you set for the SSID into account. For example, if the total monthly data volume limit is 500000 MB, the percentage for the SSID is 60 percent, and you expect about 30 clients to connect to the SSID, you could set a data volume of 10000 MB (10 GB) per WiFi client of the SSID.

      Note: When the remaining data volume reaches 10 percent of the monthly data volume limit for a WiFi client, the data rate for that WiFi client is restricted to 256 Kbps. However, the WiFi client can continue to consume data as long as the volume limit for the SSID is not yet reached.

8. In the Data Volume Limit Policy on SSID Profile section, specify the following settings that apply to each individual SSID for which you set a profile data volume limit in Step 7:
   a. **Pop-up a warning message**. Specify the percentage of the profile data volume limit for an SSID that, if exceeded, causes a pop-up message to be displayed. By default, if 10 percent of the remaining profile data volume limit for an SSID is exceeded, a pop-up warning message is displayed on the Data Volume Limit page.
   b. **When SSID profile limit is reached**. Select one of the following radio buttons to specify the action that occurs if the profile data volume limit for an SSID is exceeded:
      - **Drop data for all wireless clients**. The data for all WiFi clients of the SSID is dropped but the WiFi clients are not disconnected from the SSID.
      - **Disconnect all wireless clients**. All WiFi clients are disconnected from the SSID.

9. Click the **Apply** button.
   Your settings are saved.
   For information about monitoring the consumed data volume for each SSID for which you enabled a data volume limit, see View the data volume consumption on page 179.

Set up a WiFi bridge between access points

If the access point functions in AP mode, 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. WDS does not function if the AP functions in Router mode.

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.

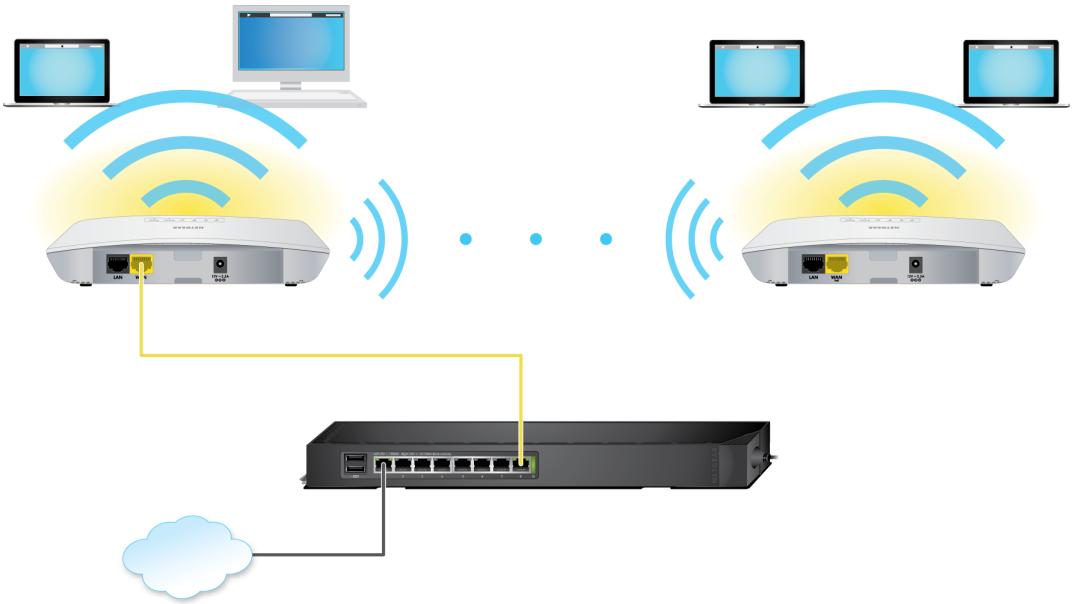


Figure 8. WiFi bridge configuration between two access points

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 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.

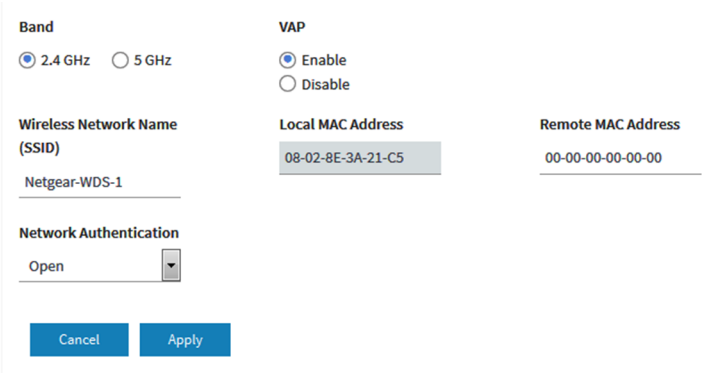
   The Dashboard page displays.
4. Select **Management > Configuration > Wireless Bridge**.

   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, in which case authentication and data encryption are not applicable. To secure the WDS connection, select **WPA2 Personal** and specify the following settings: • **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.
10. Configure the WiFi bridge settings on the access point at the other end of the WiFi bridge and restart that access point.
    If the access point at the other end of the WiFi bridge is a model WAC505, WAC510, or WAC540 access point, you do not need to restart it.
    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.

5

Manage Access and Security

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

The chapter includes the following sections:

- Block specific URLs and keywords for Internet access
- Manage local MAC access control lists
- Manage user accounts
- Manage neighbor AP detection
- Set up RADIUS servers

Note: For information about essential WiFi security (network authentication and encryption), see Set up an open or secure WiFi network on page 41.

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:

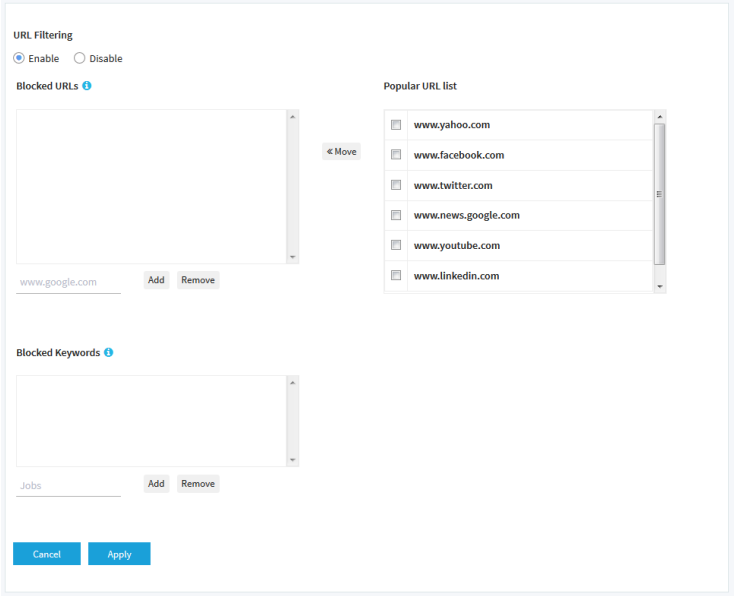
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   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 eight local access control lists (ACLs) that are based on MAC addresses. Each local MAC ACL can contain a total number of 256 MAC addresses.

If you set up an ACL with a policy that allows access and you apply that ACL to a WiFi network (that is, to an SSID), the ACL functions as follows:

- A WiFi device for which you place the MAC address in the ACL is allowed access to the WiFi network.
- All other WiFi devices are denied access to the WiFi network.

If you set up an ACL with a policy that denies access and you apply that ACL to a WiFi network (that is, to an SSID), the ACL functions as follows:

- A WiFi device for which you place the MAC address in the ACL is denied access to the WiFi network.
- All other WiFi devices are allowed access to the WiFi network.

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 55. 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
- Import an existing MAC access control list

Manually set up a MAC access control List

You can compose up to eight access control lists (ACLs) that are each based on up to 256 MAC addresses. The access point includes MAC ACLs with the following default group names and settings, which you can change:

- **Management**. If enabled, allows access to trusted stations by default.
- **Guest**. If enabled, allows access to trusted stations by default.
- **Guest1**. If enabled, denies access to untrusted stations by default.
- **Custom**. If enabled, denies access to untrusted stations by default.
- **Custom 1**. If enabled, allows access to trusted stations by default.
- **Custom 2**. If enabled, allows access to trusted stations by default.
- **Custom 3**. If enabled, allows access to trusted stations by default.
- **Custom 4**. If enabled, allows access to trusted stations by default.

By default, these MAC ACLs are disabled and do not include any stations. You can manually add devices, import devices (see Import an existing MAC access control list on page 98), or do both.

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

To manually set up a MAC ACL:

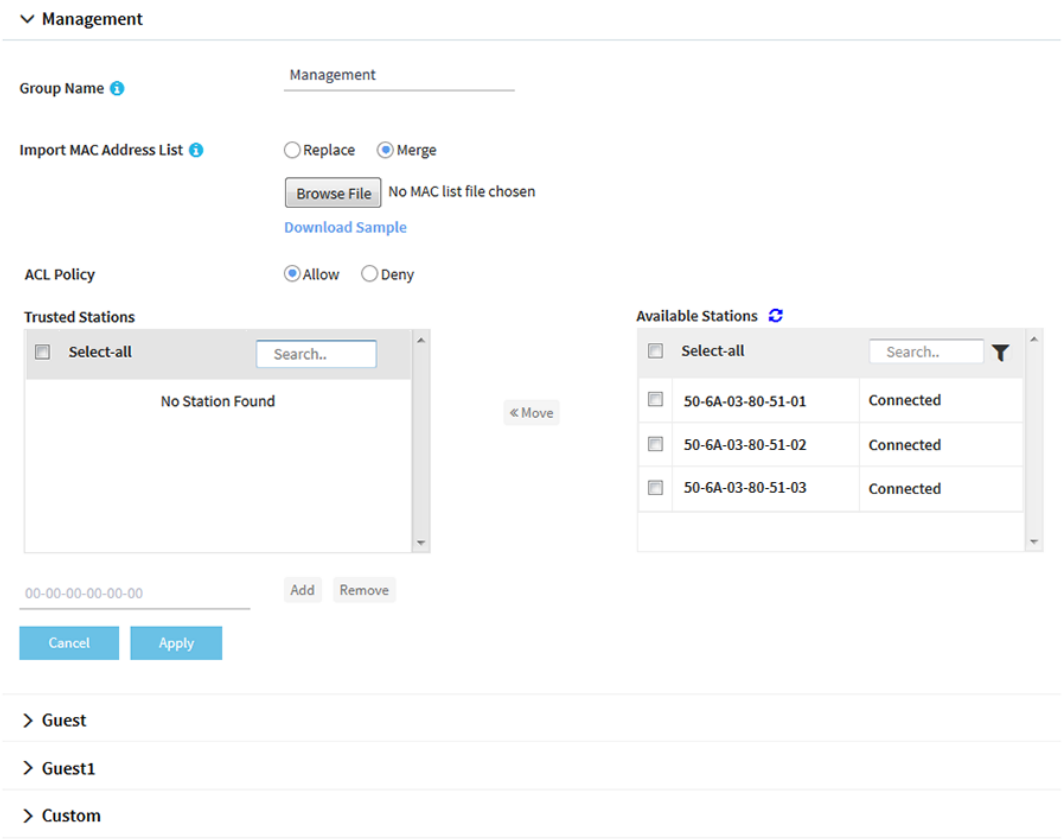
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   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**.
5. Click the group name for the MAC ACL that you want to set up.



The previous figure shows some examples. Devices in the Available Stations table are automatically detected by the access point and are common to all MAC ACLs, which allows you to add a device to more than one MAC ACL. A neighboring station displays as Neighbor and a connected station displays as connected.

6. To change the group name, enter a new name in the **Group Name** field.

   The default group names for the eight MAC ACLs are Management, Guest, Guest1, Custom, Custom 1, Custom 2, Custom 3, and Custom 4.

7. Select the ACL Policy **Allow** or **Deny** radio button.

   If you select the **Allow** radio button, a WiFi device for which you place the MAC address in the ACL is allowed access to the WiFi network, but all other WiFi devices are denied access to the WiFi network.

   If you select the **Deny** radio button, a WiFi device for which you place the MAC address in the ACL is denied access to the WiFi network, but all other WiFi devices are allowed access to the WiFi network.

8. Compose the ACL in the following way:

   - For an ACL for which you selected the **Allow** radio button in Step 7, do the following:

     - To manually add a device to the Trusted Stations table, enter the MAC address in the format 00-00-00-00-00-00 in the field below the Trusted Stations table, and click the **Add** button.
       The device is added to the Trusted Stations table.
     - 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.
       You can search the Available Stations table. You can also filter devices in the Available Stations table by clicking the **filter** icon.
     - To remove a device from the Trusted Stations table, select the check box for the device and click the **Remove** button.
       You can search the Trusted Stations table.
       When you remove a device from the Trusted Stations table, after the access point redetects the device, the device is once again placed in the Available Stations table.

   - For an ACL for which you selected the **Deny** radio button in Step 7, do the following:

     - To manually add a device to the Untrusted Stations table, enter the MAC address in the format 00-00-00-00-00-00 in the field below the Untrusted Stations table, and click the **Add** button.
       The device is added to the Untrusted Stations table.
     - To move a device from the Available Stations table to the Untrusted Stations table, select the check box for the device and click the **<< Move** button.
       You can search the Available Stations table. You can also filter devices in the Available Stations table by clicking the **filter** icon.
     - To remove a device from the Untrusted Stations table, select the check box for the device and click the **Remove** button.
       You can search the Untrusted Stations table.
       When you remove a device from the Untrusted Stations table, after the access point redetects the device, the device is once again placed in the Available Stations table.

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

   For more information about applying an ACL to a WiFi network, see Select a MAC ACL for a WiFi network on page 55.

WiFi devices in the Trusted Stations table can access the WiFi network to which you apply the ACL. WiFi devices in the Untrusted Stations table cannot access the WiFi network to which you apply the ACL.

Import an existing MAC access control list

You can import an existing access control list (ACL) that is based on up to 256 MAC addresses. You can import the list into any MAC ACL, but the MAC addresses on the list are available only for the MAC ACL into which you import the list. That is, if you want to use the same list in another MAC ACL, you must also import the list into that MAC ACL.

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:

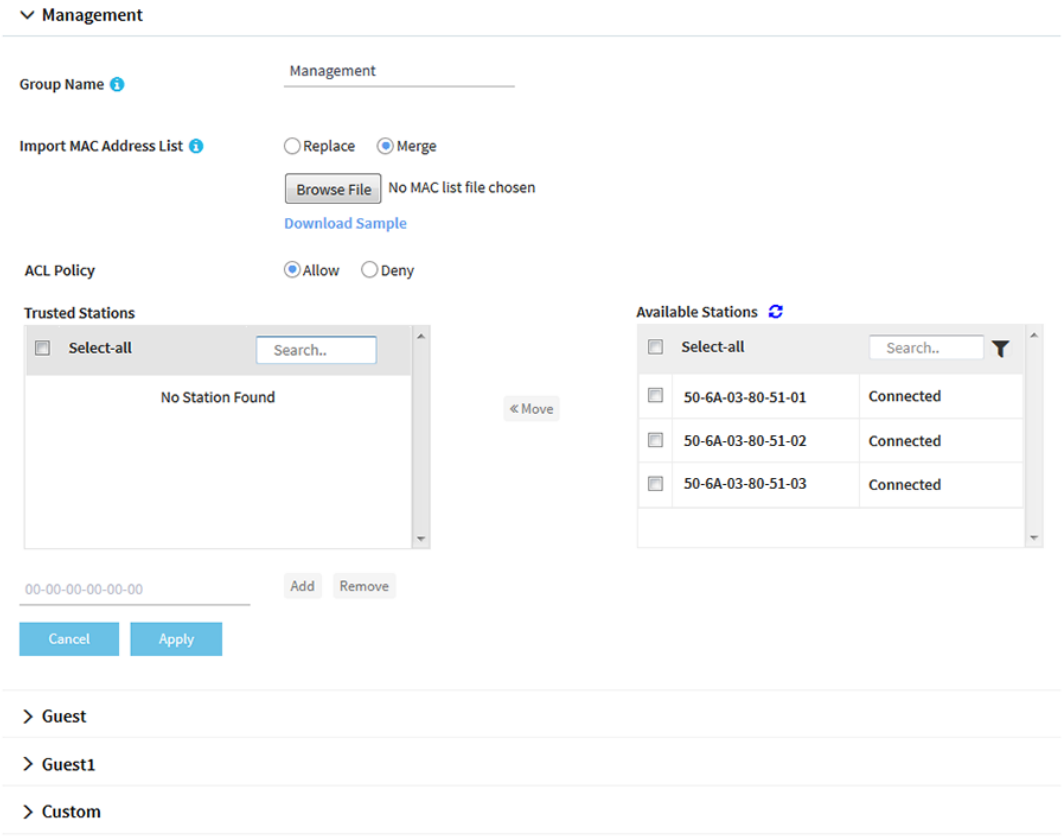
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   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**.

5. Click the group name for the MAC ACL that you want to set up.



The previous figure shows some examples. Devices in the Available Stations table are automatically detected by the access point and are common to all MAC ACLs, which allows you to add a device to more than one MAC ACL. A neighboring station displays as Neighbor and a connected station displays as connected.

6. To change the group name, enter a new name in the **Group Name** field.

   The default group names for the eight MAC ACLs are Management, Guest, Guest1, Custom, Custom 1, Custom 2, Custom 3, and Custom 4.

7. Select the ACL Policy **Allow** or **Deny** radio button.

   If you select the **Allow** radio button, a WiFi device for which you import the MAC address into the ACL is allowed access to the WiFi network, but all other WiFi devices are denied access to the WiFi network.

   If you select the **Deny** radio button, a WiFi device for which you import the MAC address into the ACL is denied access to the WiFi network, but all other WiFi devices are allowed access to the WiFi network.

8. To download a sample of a MAC ACL in the format that is required for importing, click the **Download Sample** link.

9. Import and compose the ACL in the following way:

   - For an ACL for which you selected the **Allow** radio button in Step 7, do the following:
     a. Replace or merge the MAC addresses in the import list with the MAC addresses in the Trusted Stations table (if any are already in the 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.
        You can search the Trusted Stations table.
        When you remove a device from the Trusted Stations table, after the access point redetects the device, the device is once again placed in the Available Stations table.

   - For an ACL for which you selected the **Deny** radio button in Step 7, do the following:
     a. Replace or merge the MAC addresses in the import list with the MAC addresses in the Untrusted Stations table (if any are already in the table) by selecting one of the following radio buttons:
        - **Replace**. MAC addresses in the Untrusted Stations table are replaced with the ones in the import list.
        - **Merge**. MAC addresses in the Untrusted 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 Untrusted Stations table.
     c. To remove a MAC address from the Untrusted Stations table, select the MAC address and click the **Remove** button.
        You can search the Untrusted Stations table.
        When you remove a device from the Untrusted Stations table, after the access point redetects the device, the device is once again placed in the Available Stations table.

10. Click the **Apply** button.

    Your settings are saved. For information about manually adding MAC addresses to those in the Trusted Stations table or Untrusted Stations table, see Manually set up a MAC access control List on page 95.

    For more information about applying an ACL to a WiFi network, see Select a MAC ACL for a WiFi network on page 55.

    WiFi devices in the Trusted Stations table can access the WiFi network to which you apply the ACL. WiFi devices in the Untrusted Stations table cannot access the WiFi network to which you apply the ACL.

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:

- Add a user account
- Change the settings for a user account
- Remove a user account

For information about changing the password for the default admin user account, see Change the admin user account password on page 141.

Add a user account

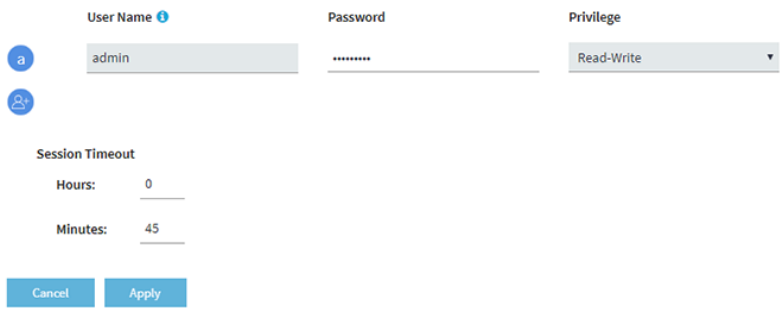
To add a user account:

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 6 and 64 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**.
   - **Session Timeout**. Use the **Hours** and **Minutes** fields to specify the period after which a session automatically expires and the user must log in again.
     By default, a session expires after 45 minutes.
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 6 and 64 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**.
   - **Session Timeout**. Use the **Hours** and **Minutes** fields to specify the period after which a session automatically expires and the user must log in again. By default, a session expires after 45 minutes.
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.
   A pop-up warning window opens.
6. Click the **Delete** button.
   The pop-up windows closes and 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 point detection and move access points to the Known AP List
- Import an existing neighbor access point list in the Known AP List

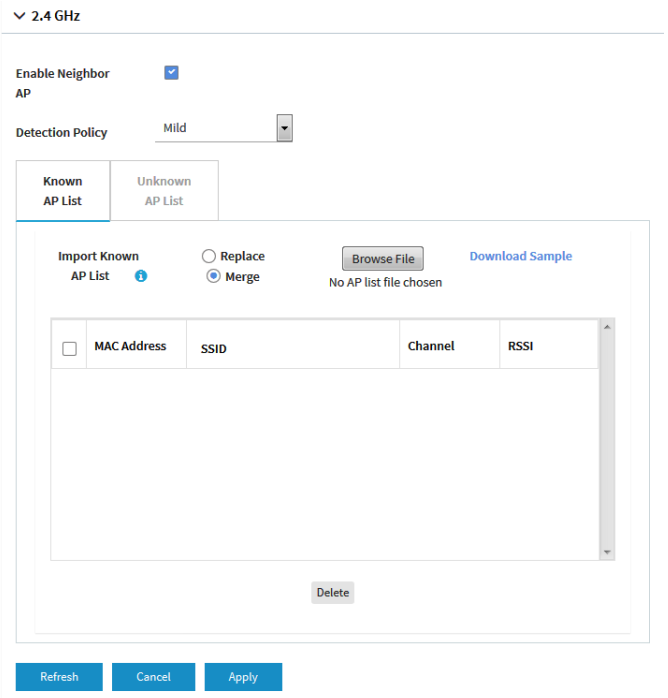
Enable neighbor access point detection and move access points to the Known AP List

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.

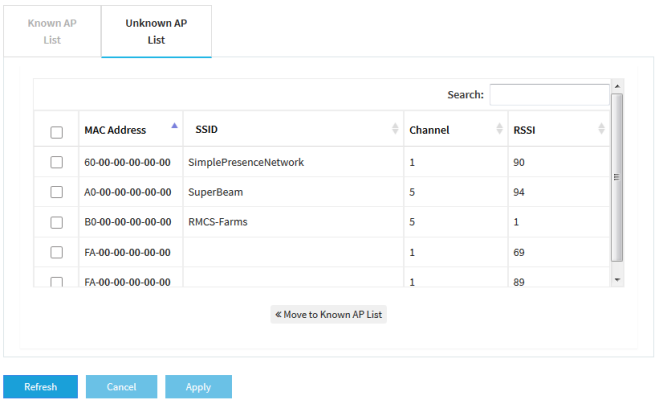
To enable neighbor access point detection and move detected access points to the Known AP List:

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:

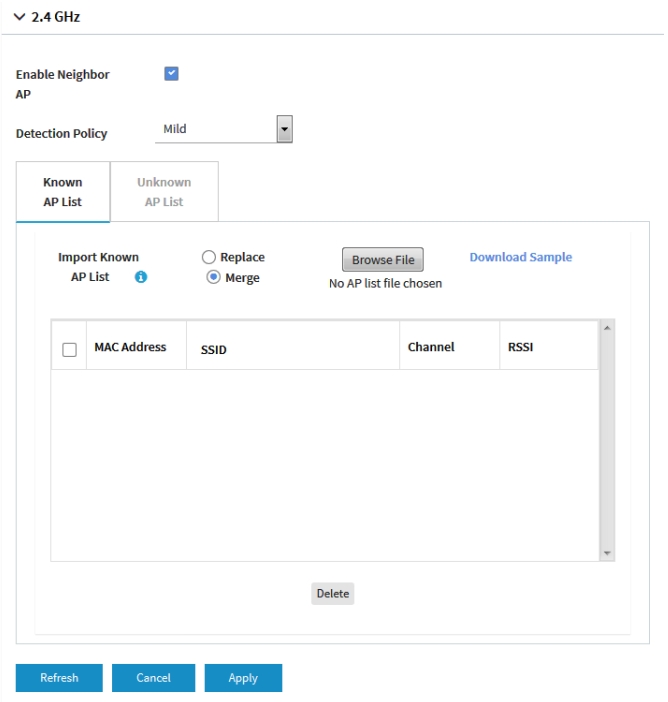
- Entries in the file must be MAC addresses only in hexadecimal format with each octet separated by a hyphen, for example 00-11-22-33-44-55.
- You must separate entries with a comma.
- The file must be in text format (that is, with a `.txt` or `.cfg` extension).

For information about enabling neighbor AP detection, see Enable neighbor access point detection and move access points to the Known AP List on page 104.

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 an AP list in the format that is required for importing in the Known AP List, 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 a device from the Known AP List, after the access point redetects the device, the device is once again placed in the Known 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 41) 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 41). 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 94).

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:

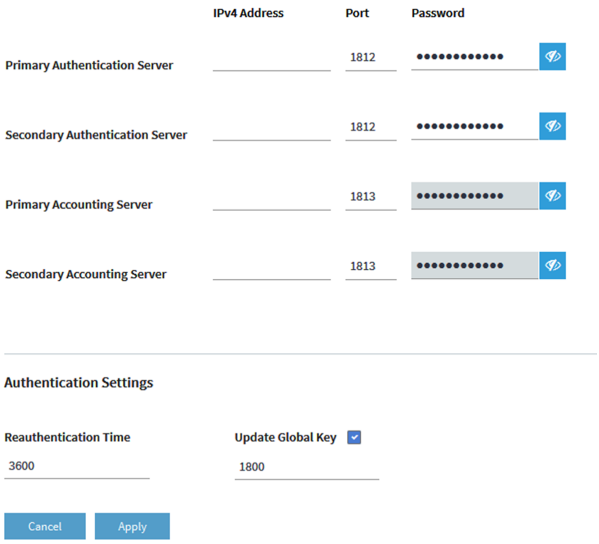
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   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.

6

Manage the Local Area Network and IP Settings

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 configure a LAN or WAN 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 in your network.

How your access point receives its IP address depends on whether it functions in AP mode (which is the default system mode) or Router mode:

- **AP mode**. The access point receives a LAN 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) LAN IP address, disable the DHCP client of the access point.
- **Router mode**. The access point receives a WAN IP address from your Internet provider. Although it is highly unlikely that you must disable the DHCP client when the access point functions in Router mode, you can do so and specify either a fixed (static) WAN IP address or a PPPoE WAN IP address for the WAN PoE port.

For more information, see the following sections:

- AP mode: Disable the DHCP client and specify a fixed IP address
- Router mode: Disable the DHCP client and specify a fixed WAN IP address
- Router mode: Specify WAN Point-to-Point Protocol over Ethernet settings

AP mode: Disable the DHCP client and specify a fixed IP address

To disable the DHCP client and specify a fixed IP address if the access point functions in AP 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.

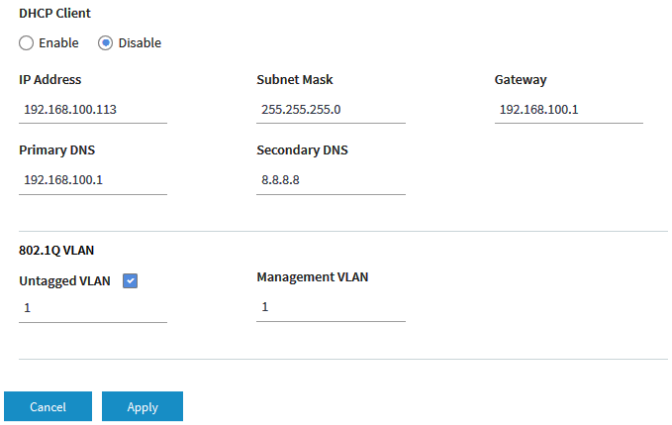
   A login window opens.
3. Enter the access point user name and password.

   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 > 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.
Subnet Mask	The subnet mask must be compatible with your LAN. (The subnet mask is usually 255.255.255.0).
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.

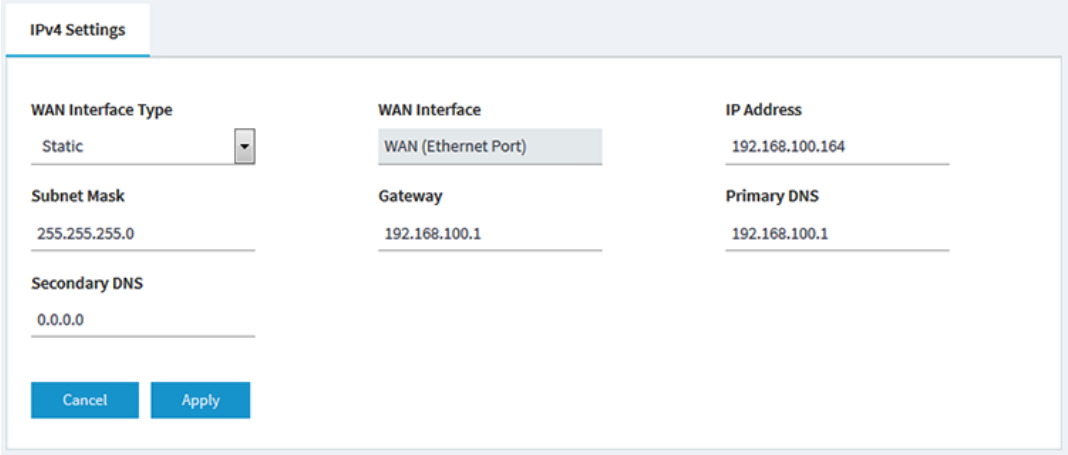
7. Click the **Apply** button.
   Your settings are saved. The access point restarts with the new IP settings.

Router mode: Disable the DHCP client and specify a fixed WAN IP address

To configure a fixed (static) IP address connection, you need the IP address information that your Internet service provider (ISP) gave you when you signed up for the Internet service.

To disable the DHCP client and specify a fixed WAN IP address if the access point functions in Router 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 > IP > WAN**.
   The page that displays lets you specify the WAN settings.
5. From the **WAN Interface Type** menu, select **Static**.



   The page also displays the WAN Interface field, which is fixed at WAN (Ethernet Port).
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 Internet modem.
Subnet Mask	The subnet mask must be compatible with your Internet modem. (The subnet mask is usually 255.255.255.0.)
Gateway	IP address of the gateway that is used by your Internet modem.

(Continued)

Setting	Description
Primary DNS	IP address of the primary DNS server that is used by your Internet modem.
Secondary DNS	IP address of the secondary DNS server that is used by your Internet modem, or leave this field blank.

7. Click the **Apply** button.
   Your settings are saved. The access point restarts with the new IP settings and establishes a connection with your ISP. This process might take a while.

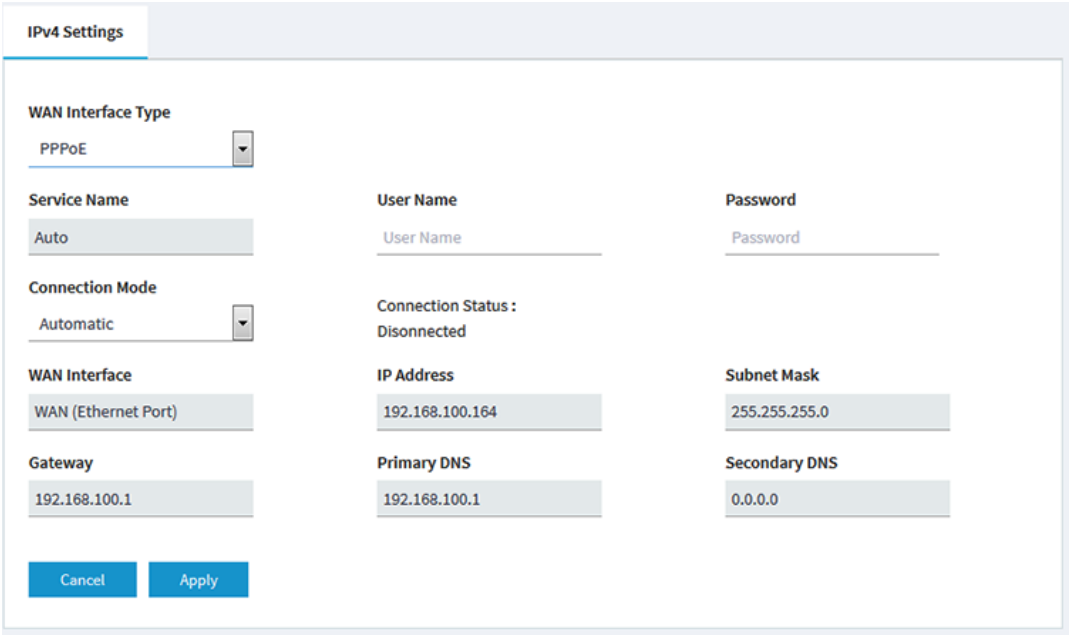
Router mode: Specify WAN Point-to-Point Protocol over Ethernet settings

To configure a WAN Point-to-Point Protocol over Ethernet (PPPoE) connection, you need the PPPoE login information that your Internet service provider (ISP) gave you when you signed up for the Internet service.

To specify the WAN PPPoE settings if the access point functions in Router 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 > IP > WAN**.
   The page that displays lets you specify the WAN settings.

5. From the **WAN Interface Type** menu, select **PPPoE**.



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

Setting	Description
User Name	The user name that your ISP gave you for the PPPoE connection or that you personalized.
Password	The password that your ISP gave you for the PPPoE connection or that you personalized.
Connection Mode	From the **Connection Mode** menu, select one of the following options: • **Automatic**. After you click the **Apply** button, the access point automatically establishes a PPPoE connection with the ISP. • **Manual**. After you click the **Apply** button, you must manually establish the PPPoE connection with the ISP by clicking the **Connect** button. When the connection is established, to terminate the PPPoE connection, you must click the **Disconnect** button.

Note: Whether you select the automatic or manual connection mode, all other fields are automatically populated when the access point obtains an IP address from your ISP. That is, the ISP assigns the IP address and all other all related PPPoE settings. However, the WAN Interface field is fixed at WAN (Ethernet Port).

7. Click the **Apply** button.

Your settings are saved.

If you specified an automatic connection mode, the access point establishes a PPPoE connection with the ISP, obtains a WAN IP address from the ISP.

8. If you specified a manual connection mode, click the **Connect** button.
   The access point establishes a PPPoE connection with the ISP and obtains a WAN IP address from the ISP. This process It might take a while.
   After the access point obtains a WAN IP address, the **Connect** button changes to the **Disconnect** button to enable you to manually terminate the PPPoE connection.

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.

How your access point receives its IP address depends on whether it functions in AP mode (which is the default system mode) or Router mode:

- If the access point functions in its default system mode (AP mode), it receives an IP address from a DHCP server (or a router that functions as a DHCP server) in your network.
- If the access point functions in Router mode, it receives an IP address from your Internet modem.

If you disabled the DHCP client, you can reenable it, which is described in the following sections:

- AP mode: Enable the DHCP client
- Router mode: Enable the DHCP client and let the access point obtain a WAN IP address

AP mode: Enable the DHCP client

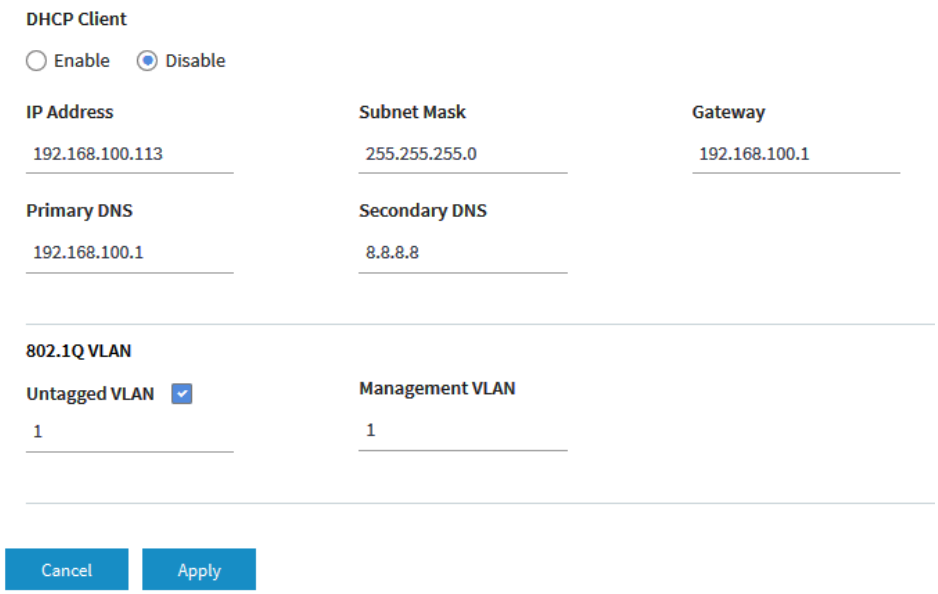
To enable the DHCP client if the access point functions in AP mode:

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 > 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.

Router mode: Enable the DHCP client and let the access point obtain a WAN IP address

If your Internet service provider (ISP) assigns IP addresses automatically through their DHCP server and you enable the DHCP client of the access point if the access point functions in Router mode, the access point can automatically obtain an IP address from your ISP. (This is the default setting if the access point functions in Router mode.)

To enable the DHCP client if the access point functions in Router mode:

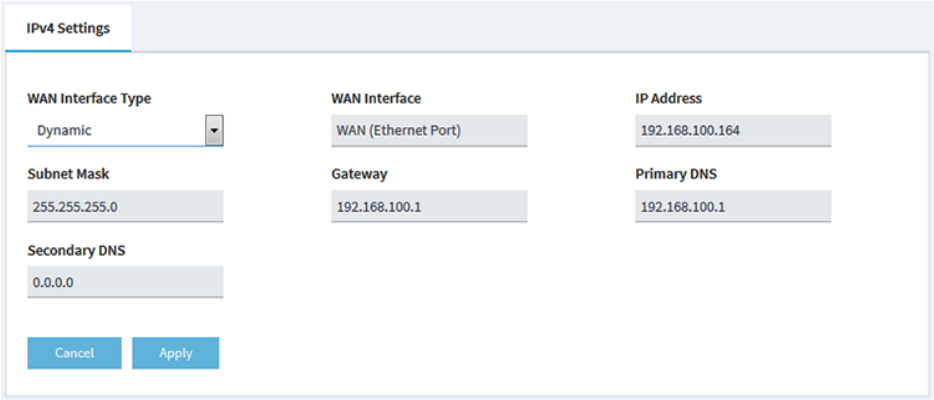
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   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 > IP > WAN**.

   The page that displays lets you specify the WAN settings.
5. From the **WAN Interface Type** menu, select **Dynamic**.



   Note: All fields are automatically populated when the access point obtains an IP address from your Internet service provider (ISP). That is, the ISP assigns the IP address and all other all related settings. However, the WAN Interface field is fixed at WAN (Ethernet Port).
6. Click the **Apply** button.

   Your settings are saved. The access point restarts with the new IP settings, establishes a connection with the ISP, and obtains a WAN IP address from the DHCP server of your ISP. This process might take a while.

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.

The following sections describe how you can set up the 802.1Q VLAN and management VLAN:

- AP mode: Set the 802.1Q VLAN and management VLAN
- Router mode: Set the 802.1Q VLAN and management VLAN

AP mode: Set the 802.1Q VLAN and management VLAN

To set the 802.1Q VLAN and management VLAN when the access point functions in AP mode:

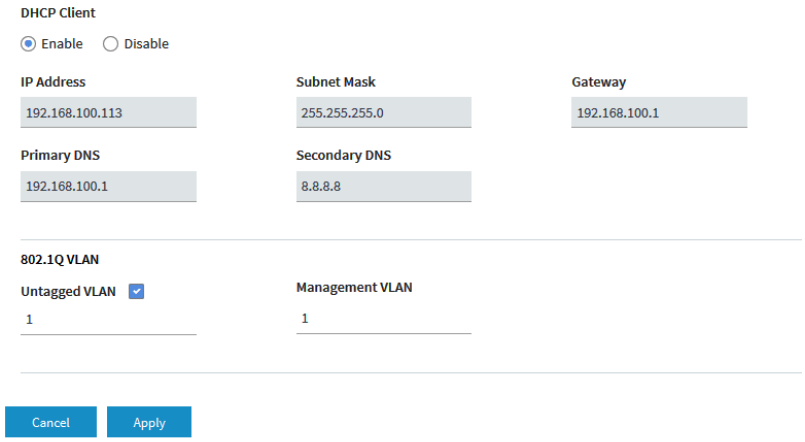
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   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 > 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.

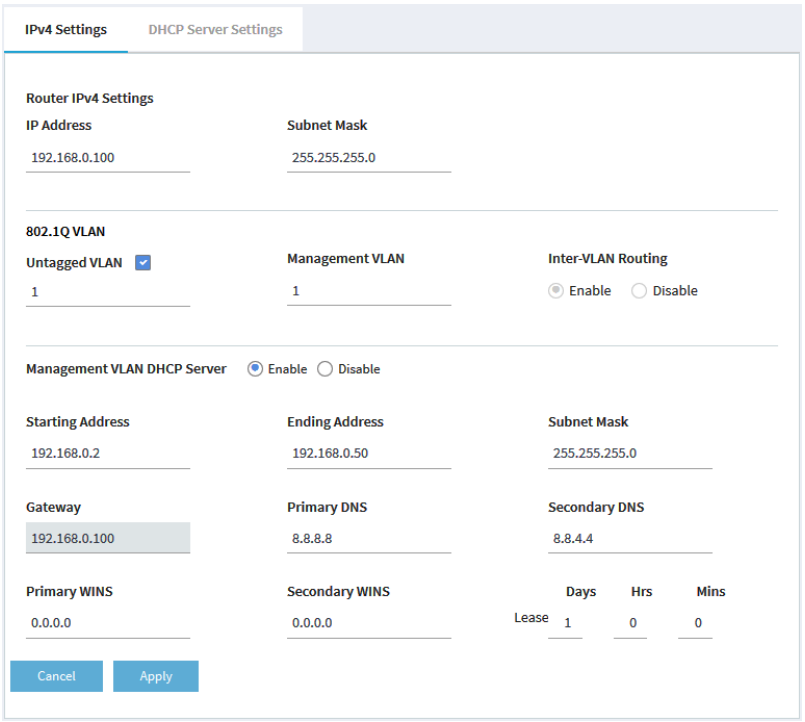
7. Click the **Apply** button.

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

Router mode: Set the 802.1Q VLAN and management VLAN

To set the 802.1Q VLAN and management VLAN when the access point functions in Router 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 > 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 the network integrity check function

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.

Router mode only: Manage DHCP servers

When the system mode of the access point is Router mode (see Change the system mode to Router mode or AP mode on page 138), you can add up to seven Dynamic Host Configuration Protocol (DHCP) servers in addition to the default DHCP server. (The access point can support a total of eight DHCP servers.) Each DHCP server can issue IP addresses from a unique address pool to the clients of a WiFi network with a unique VLAN ID. Each DHCP server corresponds to a unique VLAN ID.

The access point delivers the following settings to any WiFi device that requests DHCP:

- An IP address from the range that you define
- Subnet mask
- Gateway IP address
- DNS server IP address
- WINS server IP address, if any

The following sections describe how you can manage DHCP servers:

Manage the default DHCP server

The information in this section applies only when the system mode of the access point is Router mode (see Change the system mode to Router mode or AP mode on page

138). If it is, the management VLAN DHCP server (the default DHCP server) of the access point is enabled and assigns IP addresses to clients of the default WiFi network.

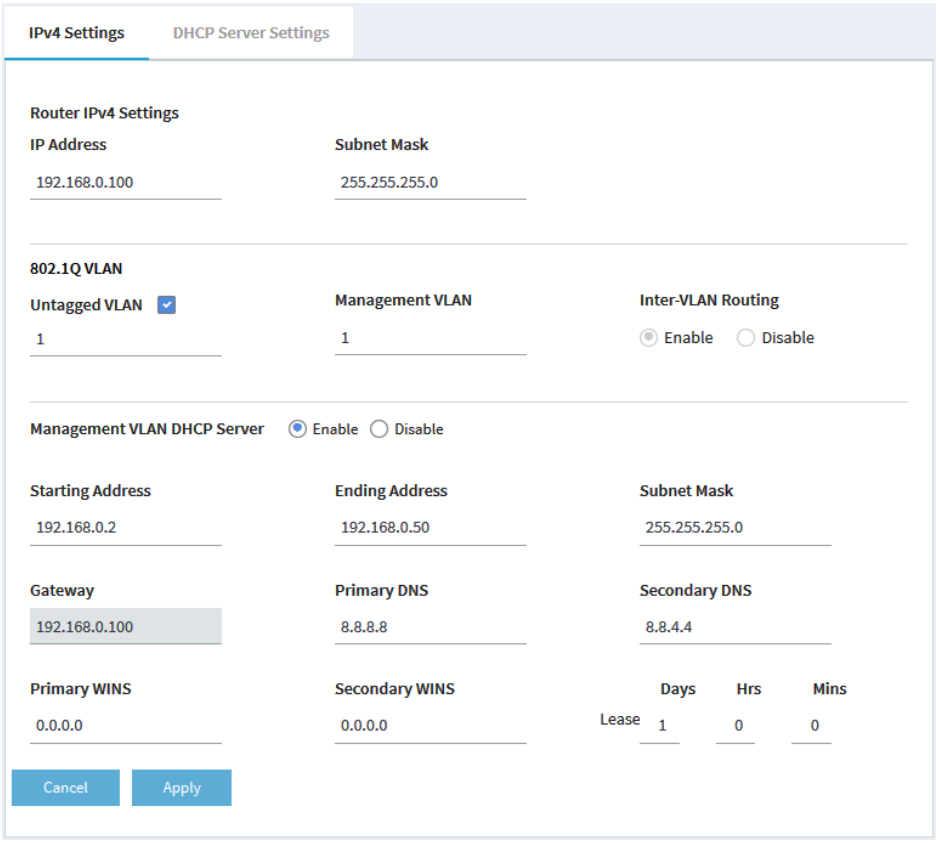
To manage the default DHCP server:

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 > IP > LAN**.



   The settings of the default DHCP server apply to the management VLAN, which, by default, is VLAN 1. For information about setting the 802.1Q VLAN and the management VLAN, see Set the 802.1Q VLAN and management VLAN on page 120.

   By default, the Management VLAN DHCP Server **Enable** radio button is selected.

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

Setting	Description
Starting Address	Enter the starting IP address of the DHCP IP address range. By default, the address is 192.160.0.2.
Ending Address	Enter the ending IP address of the DHCP IP address range. By default, the address is 192.168.0.50.
Subnet Mask	Enter the subnet mask that is used for all IP addresses in the DHCP IP address range. By default, the mask is 255.255.255.0.
Gateway	The IP address of the gateway that is used by your Internet modem. By default, the address is 192.168.0.100.
Primary DNS	The IP address of the primary Domain Name System (DNS) server that is used by your Internet modem. By default, the address is 8.8.8.8.
Secondary DNS	The IP address of the secondary DNS server that is used by your Internet modem. By default, the address is 8.8.4.4.
Primary WNS	The IP address of the primary Windows Internet Name Service (WINS) server that is used by your Internet modem, if any.
Secondary WNS	The IP address of the secondary WINS server that is used by your Internet modem, if any.
Lease	From the menus, specify the duration of the IP address lease. By default, the lease expires after one day (24 hours), after which the WiFi client must renew the lease.

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

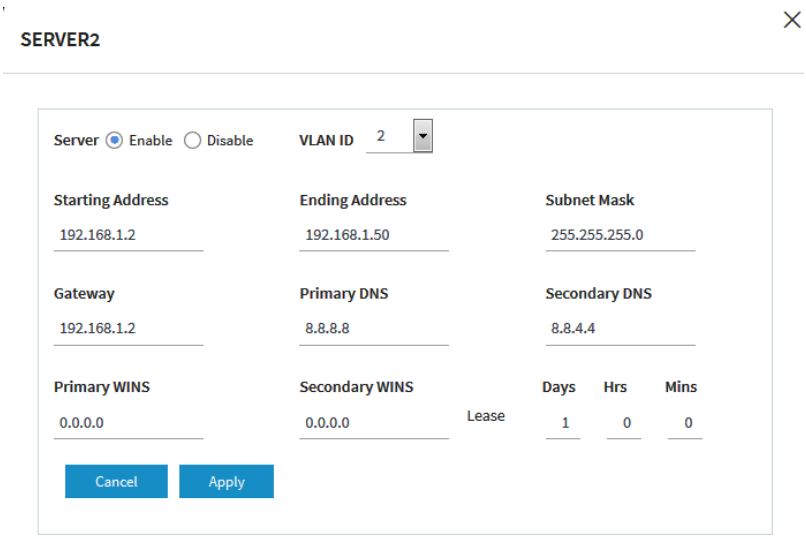
Add a DHCP server for a WiFi network

The information in this section applies only when the system mode of the access point is Router mode (see Change the system mode to Router mode or AP mode on page 138). If it is, the default DHCP server of the access point is enabled and you can also add up to seven additional DHCP servers for WiFi clients only.

IMPORTANT: You can add an additional DHCP server only after you set up a WiFi network with a unique VLAN ID that is not yet serviced by an existing DHCP server (see Set up an open or secure WiFi network on page 41).

To add a DHCP 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 > IP > LAN > DHCP Server Settings**.
   If you did not yet add any DHCP servers, only + Add Server displays.
5. Click the **+** button to the left of Add Server.



   Servers that you add are designated Server 2 through Server 7.
   By default, the **Enable** radio button is selected.
6. Specify the settings that are described in the following table.

Setting	Description
VLAN ID	From the **VLAN ID** menu, select the VLAN ID for the WiFi network (SSID) to which you assign the DHCP server. For information about assigning a VLAN ID to a WiFi network, see Change the VLAN ID for a WiFi network on page 53.
Starting Address	Enter the starting IP address of the DHCP IP address range.
Ending Address	Enter the ending IP address of the DHCP IP address range.
Subnet Mask	Enter the subnet mask that is used for all IP addresses in the DHCP IP address range.
Gateway	The IP address of the gateway that is used by your Internet modem.
Primary DNS	The IP address of the primary Domain Name System (DNS) server that is used by your Internet modem.
Secondary DNS	The IP address of the secondary DNS server that is used by your Internet modem. Or leave this field blank.
Primary WNS	The IP address of the primary Windows Internet Name Service (WINS) server that is used by your Internet modem, if any.
Secondary WNS	The IP address of the secondary WINS server that is used by your Internet modem. Or leave this field blank.
Lease	From the menus, specify the duration of the IP address lease. By default, the lease expires after one day (24 hours), after which the WiFi client must renew the lease.

7. Click the **Apply** button.
   Your settings are saved.
8. To view the SSIDs to which the DHCP server is assigned, click the **SSID** link just below the VLANID field at the top of the page.

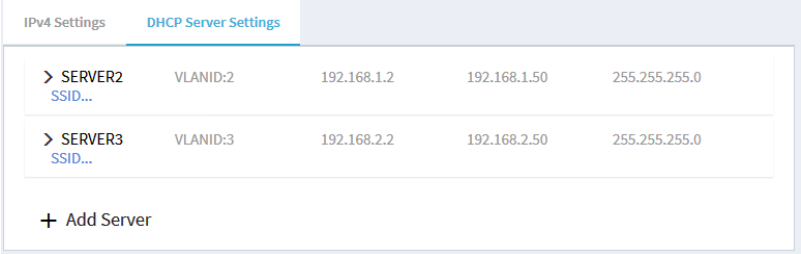
View or change the settings for a DHCP server

The information in this section applies only when the system mode of the access point is Router mode (see Change the system mode to Router mode or AP mode on page 138). If it is, the default DHCP server of the access point is enabled and you can also add up to seven additional DHCP servers for WiFi clients only.

You can view or change the setting of a DHCP server that you added. For information about the default DHCP server, see Manage the default DHCP server on page 127.

To view or change the setting of a DHCP 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 > IP > LAN > DHCP Server Settings**.



5. Click the **>** button to the left the DHCP server.
   The settings for the selected DHCP server display.
6. Change the settings for the DHCP server as needed.
   For detailed descriptions of the settings, see Add a DHCP server for a WiFi network on page 129.
7. If you made changes, click the **Apply** button.
   Your settings are saved.

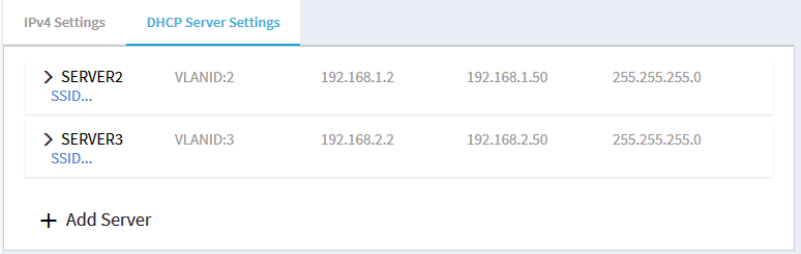
Disable a DHCP server

The information in this section applies only when the system mode of the access point is Router mode (see Change the system mode to Router mode or AP mode on page 138). If it is, the default DHCP server of the access point is enabled and you can also add up to seven additional DHCP servers for WiFi clients only.

You can temporarily disable a DHCP server.

To disable a DHCP 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 > IP > LAN > DHCP Server Settings**.



5. Click the **>** button to the left the DHCP server.
   The settings for the selected DHCP server display.
6. Select the Server **Disable** radio button.
7. Click the **Apply** button.
   Your settings are saved.

Remove a DHCP server

The information in this section applies only when the system mode of the access point is Router mode (see Change the system mode to Router mode or AP mode on page 138). If it is, the default DHCP server of the access point is enabled and you can also add up to seven additional DHCP servers for WiFi clients only.

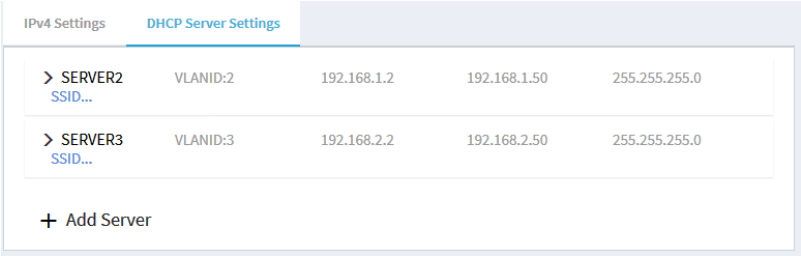
You can remove a DHCP server that you no longer need.

To remove a DHCP 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 > IP > LAN > DHCP Server Settings**.



5. Click the **>** button to the left the DHCP server.
   The settings for the selected DHCP server display.
6. Click the **Delete** button.
   A pop-up warning window opens.
7. Click the **Delete** button.
   The pop-up window closes and the DHCP server is removed.

Enable or disable inter-VLAN routing

The information in this section applies only when the system mode of the access point is Router mode (see Change the system mode to Router mode or AP mode on page 138).

By default, inter-VLAN routing is enabled and clients of different WiFi networks (each with a unique VLAN) can communicate with each other. You can select the VLANs that participate in inter-VLAN routing. For added security, you can disable inter-VLAN routing so that clients of different WiFi networks (each with a unique VLAN) cannot communicate with each other.

To enable or disable inter-VLAN routing:

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 > Inter VLAN Settings**.

   The inter-VLAN routing options displays.

5. Enable or disable inter-VLAN routing by doing the following:

   - To enable inter-VLAN routing, do the following:
     a. Select the **Enable** radio button.
        Inter-VLAN routing is enabled. This is the default setting.
     b. To specify the VLANs that must participate in inter-VLAN routing, select or clear the check boxes for the individual VLANs.
        If you did not create any VLANs, only the default VLAN (with ID 1) displays.

   - To disable inter-VLAN routing, select the **Disable** radio button.

6. Click the **Apply** button.

   Your settings are saved.

7

Manage and Maintain the Access Point

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

The chapter includes the following sections:

Change the management mode to NETGEAR Insight or Web-browser

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

- **NETGEAR Insight mode**. You can manage the access point remotely from a mobile device on which the NETGEAR Insight mobile app is installed or, if you are an Insight Premium or Insight Pro subscriber, through the Insight Cloud Portal. The NETGEAR Insight mode is the default setting. In this mode, you *can* connect to the access point over the local browser interface, but only a basic and limited local browser interface is available. For information about the Insight mobile app and Insight Cloud Portal, visit insight.netgear.com and see the NETGEAR knowledge base at netgear.com/support/product/insight.aspx.

  IMPORTANT: When you change the management mode from Web-browser mode to NETGEAR Insight 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**.

- **Web-browser mode**. You can manage the access point locally from a WiFi or wired device through the local browser interface. In this mode, the access point functions as a standalone device and is not connected to the Insight cloud-based management platform.

To change the management mode to NETGEAR Insight mode or Web-browser 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 > Management Mode**.

The Management Mode page displays.

5. Select one of the following radio buttons:

   - **NETGEAR Insight**. The access point functions in NETGEAR Insight management mode.
   - **Web-browser**. The access point functions in Web-browser management mode.

   WARNING: When you change the management mode from Web-browser mode to NETGEAR Insight 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**.

6. Click the **Apply** button.
   A pop-up warning window opens.

7. Click the **OK** button.
   The pop-up window closes and your settings are saved. The access point restarts in the new management mode.

Change the system mode to Router mode or AP mode

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

- **AP**. Select the **AP** radio button to let the access point function with its router functionality disabled. This is the default setting. When the access point is in AP mode, connect the WAN PoE port of the access point to your network.
- **Router**. Select the **Router** radio button to let the access point function with its router functionality enabled, including network address translation (NAT) and the option to enable and configure the DHCP server of the access point. When the access point is in Router mode, connect the WAN PoE port of the access point to a LAN port on the Internet modem.

  IMPORTANT: When you change the system mode, the access point is also reset to factory default settings with the exception of the IP address of the WAN PoE port, the host name, the country of operation, and the time zone.

For more information about how you can connect the access point to your network or Internet modem, see Set up and connect the access point to your network or Internet modem on page 21.

To change the system mode to AP mode or Router 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:

   - **AP**. The access point functions in AP mode. This is the default setting.
   - **Router**. The access point functions in Router mode.

   WARNING: The system mode changes and the access point is reset to factory default settings with the exception of the IP address of the WAN PoE port, the host name, the country of operation, and the time zone.
6. Click the **Apply** button.

   A pop-up warning window opens.
7. Click the **OK** button.

   The pop-up window closes and your settings are saved. The access point restarts in the new system mode.

Change the country or region of operation

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

- 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.
   A pop-up warning window opens.
7. Click the **OK** button.
   The pop-up window closes and 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 64 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.

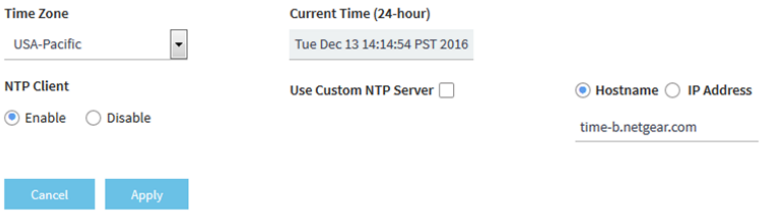
To specify a custom NTP server:

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 144.

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 142.

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.

Manage 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 secure FTP (SFTP)

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 management methods:

- Check for new firmware and upgrade the access point
- Manually download firmware and upgrade the access point
- Revert to the backup firmware
- Use an SFTP server to upgrade the access point

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 remains 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. After you upgrade the access point to new firmware, the old firmware is saved as backup firmware so that you can revert to it (see Revert to the backup firmware on page 148).

IMPORTANT: When you install an older firmware version (or the backup firmware version), that is, you downgrade rather than upgrade the firmware, 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 download firmware manually and upgrade your access point:

1. Visit netgear.com/support/download/, 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 `WAC505-510_V8.0.0.23_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.

Revert to the backup firmware

After you upgrade the access point to new firmware, the old firmware is saved as backup firmware so that you can revert to it.

IMPORTANT: When you revert to the backup firmware and the backup firmware is an earlier version than the firmware version that is running on the access point, 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 revert to the backup firmware on the access point:

1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable 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. The page shows both the current firmware version and the backup firmware version.

5. Click the **Bootup Backup Firmware** button.

   A pop-up warning window opens.

   IMPORTANT: When you revert to the backup firmware, 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 **Swap** button.

   The pop-up window closes, the firmware reversion process initiates, and the access point restarts.

   WARNING: To avoid the risk of corrupting the firmware, do not interrupt the reversion. 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.

7. Verify that the access point runs the backup firmware version by logging back in to the access point.

   The firmware version is stated on the Dashboard page.

Use an SFTP server to upgrade the access point

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

To upgrade the firmware of the access point from an SFTP 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 **SFTP**.
6. Specify the following server settings:
   - **Firmware File**. The name of the access point firmware file on the SFTP server.
   - **SFTP Server IP**. The IP address of the SFTP server on your network.
   - **User Name**. The user name that is required to access the SFTP server.
   - **Password**. The password that is required to access the SFTP 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 page displays.
5. Click the **Backup** button.
6. Choose a location to store the file on your computer.

   The name of the backup file is `WAC510-WAC510-dd-mm-yy_hh-mm-ss-config.tar`, in which 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 `WAC510-WAC510-02-15-19_18-56-53-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 page displays.
5. Click the **Browse** button and navigate to and select the saved configuration file.

   The name of the backup file is `WAC510-WAC510-dd-mm-yy_hh-mm-ss-config.tar`, in which 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 `WAC510-WAC510-02-15-19_18-56-53-config.tar`.
6. Click the **Restore** button.

   A pop-up warning window opens.
7. Click the **Restore** button.

   The pop-up window closes and 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.
   A pop-up warning window opens.
6. Click the **Reboot** button.
   The pop-up window closes and the access point reboots, which takes about one minute.

Schedule the access point to reboot

You can schedule the access point to reboot at a time that is more convenient for the network, for example, when you do not expect any WiFi clients (or only a few) to be connected to the access point.

To schedule the access point to reboot:

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 **Enable Scheduled Reboot** button so that the button displays blue.
   The scheduling controls display.
6. Select the check box for the day on which you want the access point to reboot.
   You can select multiple days.
7. Using the **Start Time** menus, specify the hour and minutes for the time at which the access point must reboot.
   Specify the hour in 24-hour format.
8. Click the **Apply** button.
   Your settings are saved.

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 197.

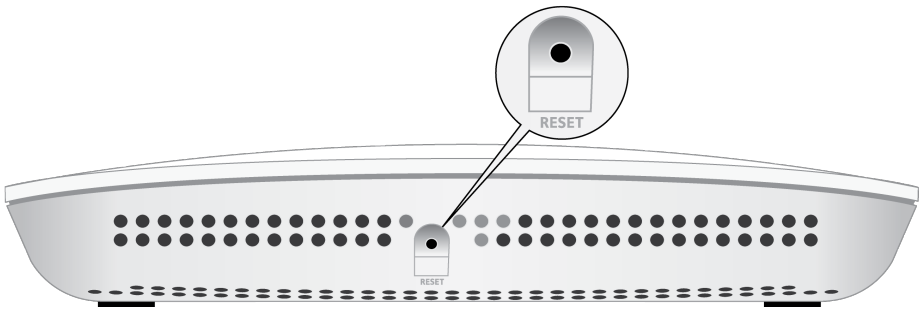
Use the Reset button

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 NETGEAR Insight network location, you must first use the Insight mobile app or Insight Cloud Portal to remove the access point from the Insight network location 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 left side of the access point, locate the recessed **Reset** button.



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. 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.
   A pop-up warning window opens.
6. Click the **Restore** button.
   The pop-up windows closes and 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.

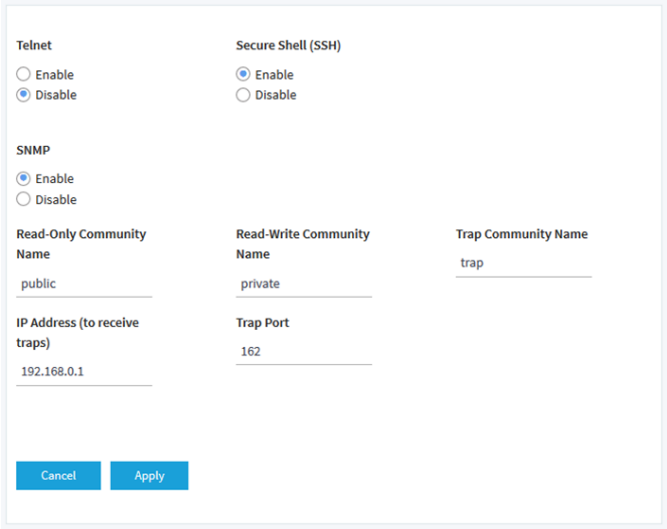
To enable SNMP and manage the SNMP settings:

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 13. 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.

8

Monitor the Access Point and the Network

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

The chapter includes the following sections:

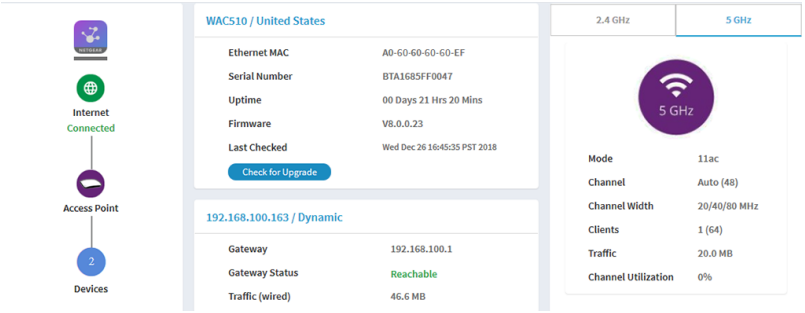
View the access point Internet, IP, and system settings

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.



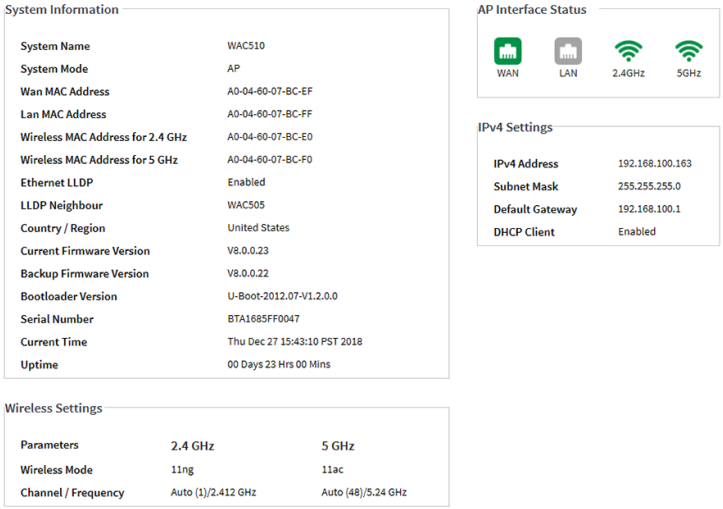
4. Look at the following panes:

   - **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 connection to the NETGEAR Insight cloud-based management platform, if any.
     - Status of the Internet connection.
     - Functioning mode of the 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.
  - The serial number.
  - Device uptime.
  - Firmware version.
  - The date and time that the access point itself or someone manually last checked if new firmware was available.

  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 146).
- **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 four sections:

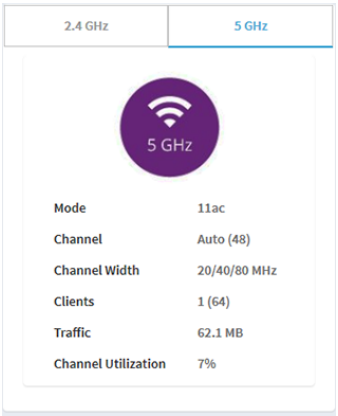
- **System Information section**. The following settings are displayed:
  - **System Name**. The access point NetBIOS name.
  - **System Mode**. The access point system mode (AP or Router).
  - **Wan MAC Address**. The MAC address of the WAN Ethernet port of the access point.
  - **Lan MAC Address**. The MAC address of the LAN 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).
  - **LLDP Neighbour**. The name of the LLDP neighbour, if any.
  - **Country / Region**. The country or region in which the access point operates or for which the access point is licensed.
  - **Current Firmware Version**. The version of the firmware that is running on the access point.
  - **Backup Firmware Version**. The version of the backup firmware on the access point.
  - **Bootloader Version**. The primary bootloader (U-Boot) version 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.
- **AP Interface Status**. A green icon indicates that the interface is in use. A gray icon indicates that the interface is not in use.
- **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).

- **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.

View the WiFi radio settings

To view the WiFi radio settings of the access point:

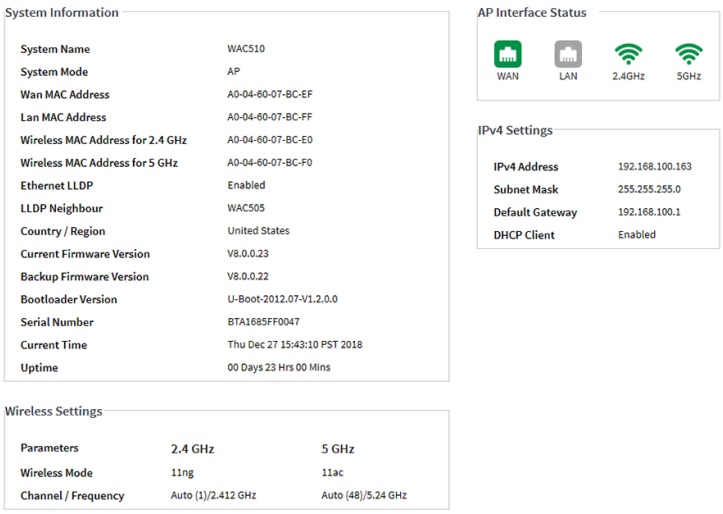
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.
   A login window opens.
3. Enter the access point user name and 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
   - 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 radio is shown.
6. To view more detailed information, select **Management > Monitoring > System**.



The page shows four sections:

- **System Information section**. The following settings are displayed:
  - **System Name**. The access point NetBIOS name.
  - **System Mode**. The access point system mode (AP or Router).
  - **Wan MAC Address**. The MAC address of the WAN Ethernet port of the access point.
  - **Lan MAC Address**. The MAC address of the LAN 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).
  - **LLDP Neighbour**. The name of the LLDP neighbour, if any.

  - **Country / Region**. The country or region in which the access point operates or for which the access point is licensed.
  - **Current Firmware Version**. The version of the firmware that is running on the access point.
  - **Backup Firmware Version**. The version of the backup firmware on the access point.
  - **Bootloader Version**. The primary bootloader (U-Boot) version 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.

- **AP Interface Status**. A green icon indicates that the interface is in use. A gray icon indicates that the interface is not in use.
- **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).

- **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.

View unknown and known neighbor access points

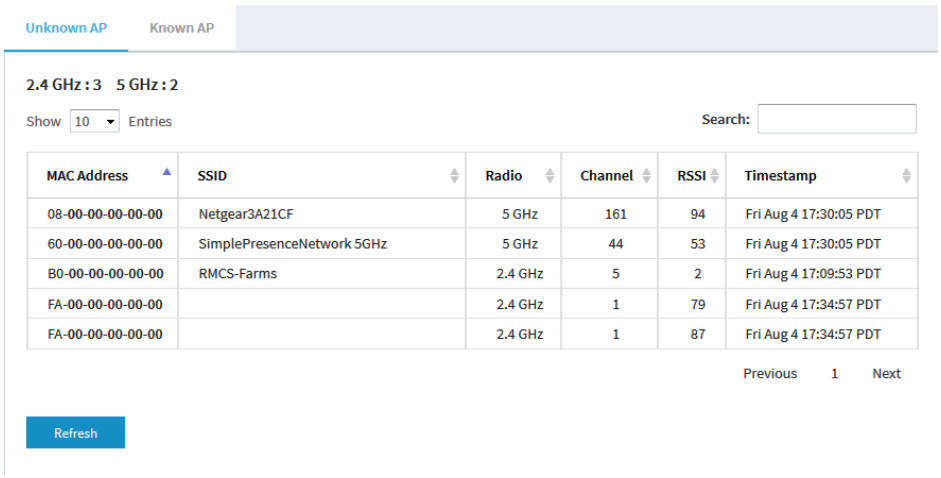
If you enabled neighbor access point (AP) detection (see Manage neighbor AP detection on page 104), you can view the unknown access points in the Unknown AP list and the known access points in the Known AP list.

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.

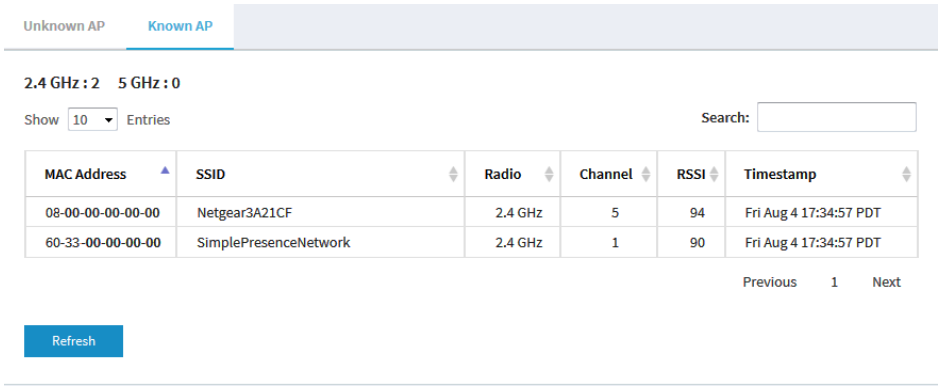
   A login window opens.
3. Enter the access point user name and password.

   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.

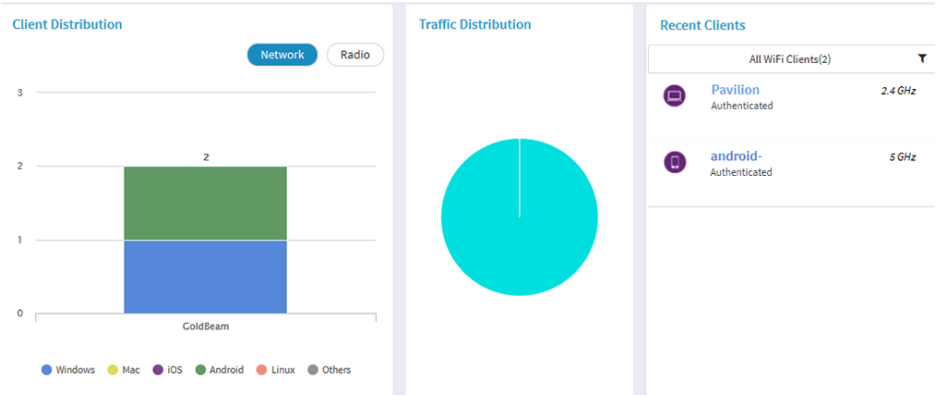
View client distribution, connected clients, and client trends

To view the clients that are connected to the access point, either over WiFi or through an Ethernet 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.



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 Recent Clients pane (shown on the right side in the previous figure) shows the top 5 recently connected clients list.

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.

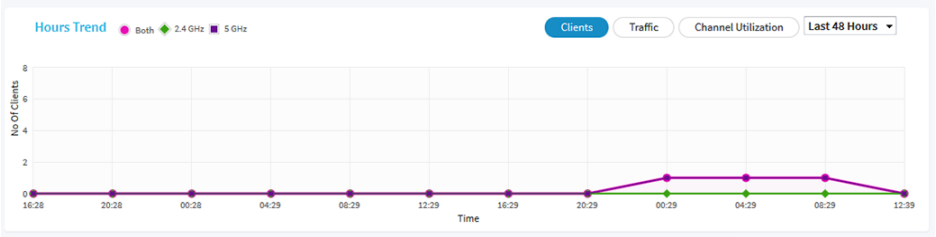
5. To see recent clients for all networks or a single network, in the Connected Clients pane, click the icon in the menu under Recent Clients, and select **All WiFi Clients**, the clients for a specific WiFi network (SSID), or **LAN Devices**.

   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 (WiFi clients only) 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.

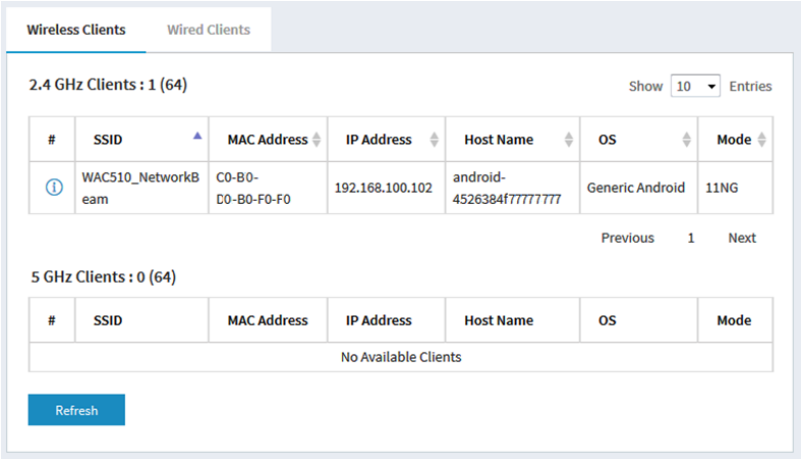


The Hours Trend pane shows a graph with the number of clients, the traffic in MB, or the channel utilization over a period that you can select. (The previous figure

shows the trend for the last 48 hours.) 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).

You can also click the **Traffic** button or the **Channel Utilization** button. For more information, see View WiFi and WAN traffic, traffic statistics, and channel utilization on page 173.

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 and wired clients, select **Management > Monitoring > Connected Clients**.



By default, the **Wireless Clients** tab is selected and the connected WiFi clients display. (For information about wired clients, see Step 12).

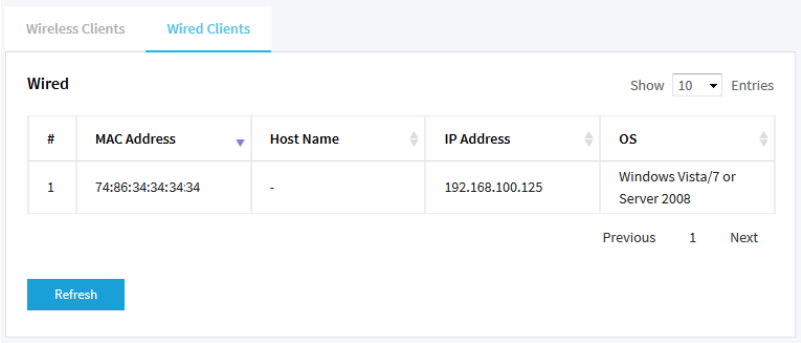
For each radio, the page displays the number of connected clients and the maximum number of supported clients.

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, do the following:
    a. 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.

    b. Click the **Close** button.
    The Detailed Client Information page closes.

12. To view information about the wired clients, click the **Wired Clients** tab.



For each wired client, the page displays the MAC address, host name, IP address, and operating system (OS).

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

View WiFi and WAN traffic, traffic statistics, and channel utilization

To view WiFi and WAN (wired) traffic, traffic statistics, and channel utilization:

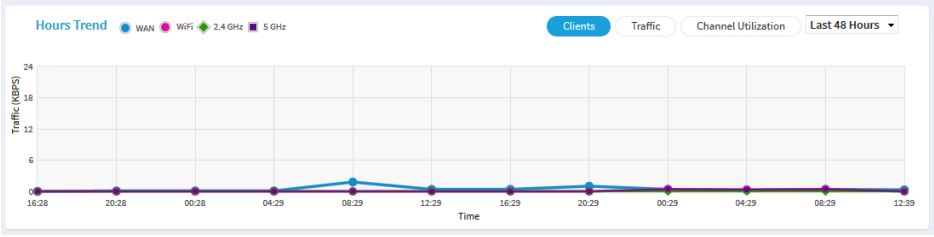
1. Open a web browser from a computer that is connected to the same network as the access point or to the access point directly through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   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.

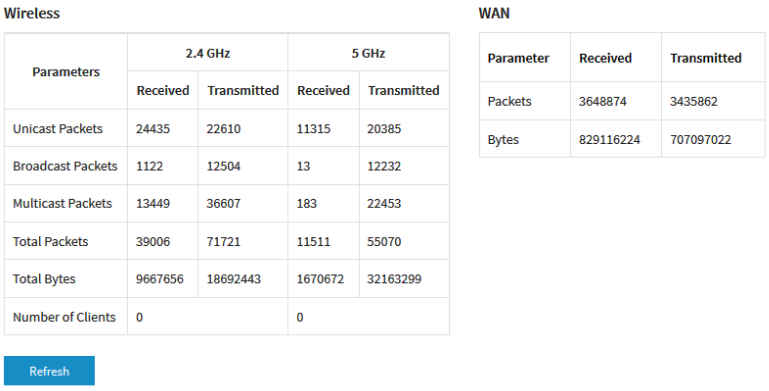
   By default, the **Clients** button is selected.



5. To view traffic information, do the following:
   a. Click the **Traffic** button.
      The graph shows the information for WAN (wired) 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	24435	22610	11315	20385
Broadcast Packets	1122	12504	13	12232
Multicast Packets	13449	36607	183	22453
Total Packets	39006	71721	11511	55070
Total Bytes	9667656	18692443	1670672	32163299
Number of Clients	0		0	

Refresh

WAN

Parameter	Received	Transmitted
Packets	3648874	3435862
Bytes	829116224	707097022

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.

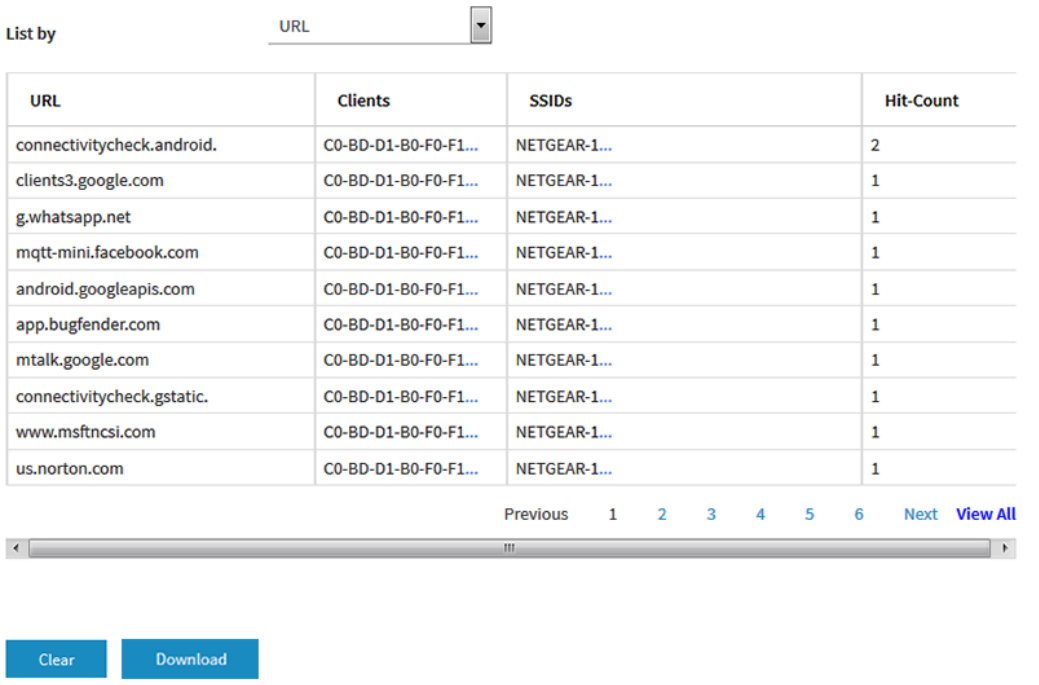
9. To display the most recent information, click the **Refresh** button.

View or download tracked URLs

If you enabled URL tracking for a WiFi network (see Enable or disable URL tracking for a WiFi network on page 55), you can view the tracked URLs by URL, WiFi client, and SSID. You can also download a URL tracking report as a `.csv` file.

To view or download tracked URLs:

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 > URL Tracking**.



By default, the table shows the URLs that were accessed, each with the MAC address of the WiFi client that accessed the URL, the associated SSID, and the number of times that the WiFi client accessed the URL.

5. To view additional information, click the **...** link to the right of a MAC address or SSID.
6. To view URL tracking information by WiFi client, do the following:
   a. From the menu, select **Client**.
      The table shows the MAC addresses of the WiFi clients, each with the client host name, and the first URL of the list of URLs that the client accessed.
   b. To view all URLs that a WiFi client accessed, click the **...** link to the right of the first URL.
      A pop-up window opens and displays all URLs that the WiFi client accessed.
   c. Click the **Close** button.
      The pop-up window closes.
7. To view URL tracking information by SSID, do the following:
   a. From the menu, select **SSID**.
      The table shows the SSIDs and the first URL of the list of URLs that were accessed on the SSID.
   b. To view all URLs that were accessed on the SSID, click the **...** link to the right of the first URL.
      A pop-up window opens and displays all URLs that the were accessed on the SSID.
   c. Click the **Close** button.
      The pop-up window closes.
8. To download a URL tracking report as a `.csv` file, click the **Download** button, and follow the directions of your browser.
9. To clear all URL tracking information, do the following:
   a. Click the **Clear** button.
      A pop-up warning window opens.
   b. Click the **OK** button.
      The pop-up window closes and the information is cleared.

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.

Note: If the access point functions in the NETGEAR Insight management mode, you can also view and manage the cloud activity logs, which show the connection of the access point to the Insight cloud-based management platform. If the access point functions in the NETGEAR Insight management mode, this is option is available from the Dashboard page by selecting **Management > Monitoring > Cloud Logs**.

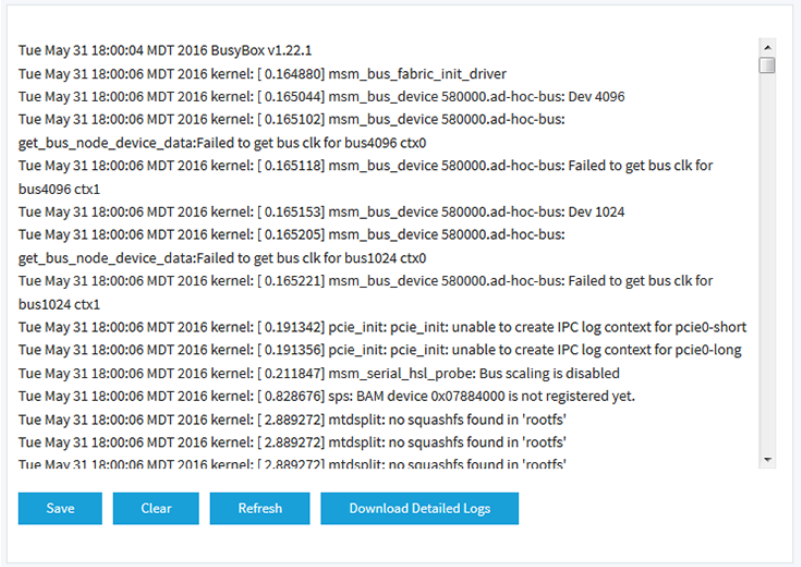
To view, save, download, or clear the logs:

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

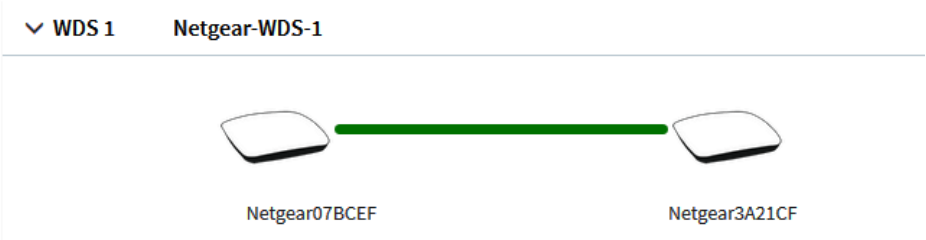
You can view whether a WiFi bridge is established and view the function (master or slave), MAC addresses, and IP addresses of the access points that form the WiFi bridge.

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 the data volume consumption

If you enabled data limits for one or more WiFi networks (see Set a data volume limit for the access point on page 84), you can view the data volume consumption and volume status details.

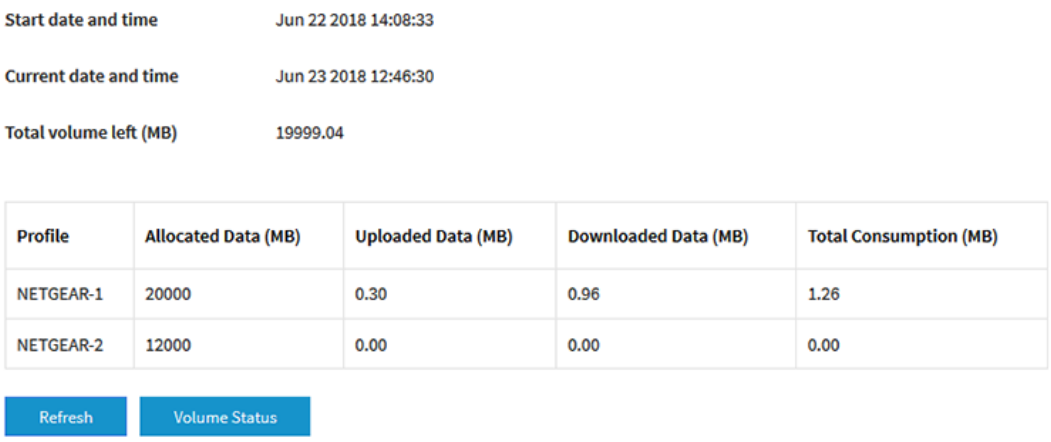
To view the data volume consumption and volume status details:

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 > Data Volume Limit**.



   At the top, the page states the start date and time of the data volume counter, the current date and time, and the total volume that is left in relation to the data volume limit that you set.

   For each SSID, the table shows the allocated data (which is the allocated SSID percentage of the total monthly data volume limit that you set), the uploaded and downloaded data, and the total data consumption.

5. To view details about the volume, do the following:
   a. Click the **Volume Status** button.
      A pop-up window opens and, for each SSID, displays details in a graphic.
   b. Click the **X** in the upper right corner.
      The pop-up window closes.

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

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.

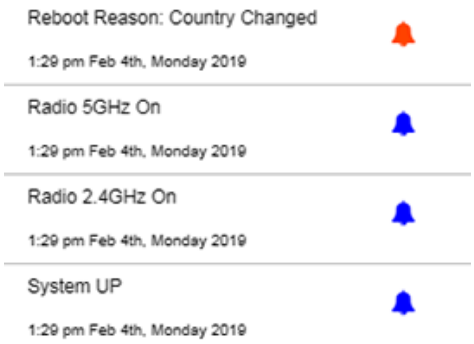
3. Enter the access point user name and password.

   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.

   The alarm bell icon at the top right of the page shows a number, indicating the total number of new alarms and notifications since the last time that you viewed alarms and notifications.

4. Click the alarm bell icon.



   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.

9

Diagnostics and Troubleshooting

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

The chapter includes the following sections:

Capture WiFi and Ethernet 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.

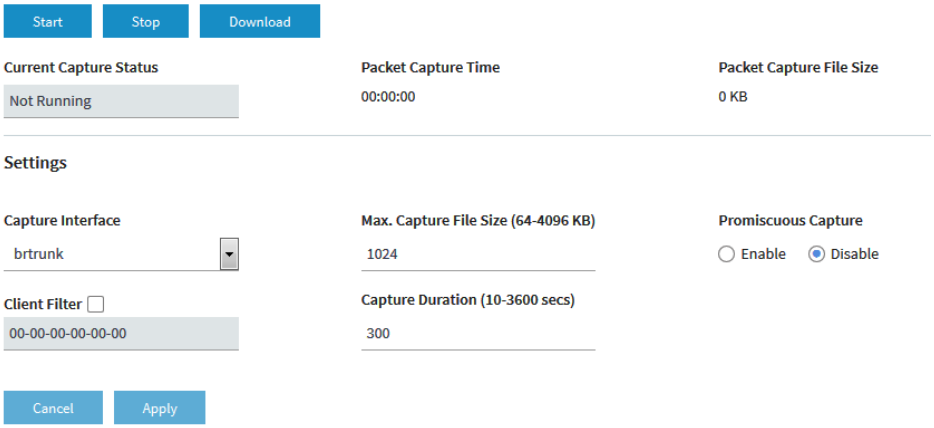
The packet capture capability can be useful for analyzing a WiFi deployment, monitoring a WiFi network, debugging protocols, determining WiFi network bottlenecks, and, in general, troubleshooting any irregularities in a WiFi network.

You can select to capture all packets or selected packets only.

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 > Diagnostics > 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 interfaces, 2.4 GHz radio, and 5 GHz radio. This is the default setting. • **Eth0**. Only packets on the WAN Ethernet interface are captured. • **Eth1**. Only packets on the LAN 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.

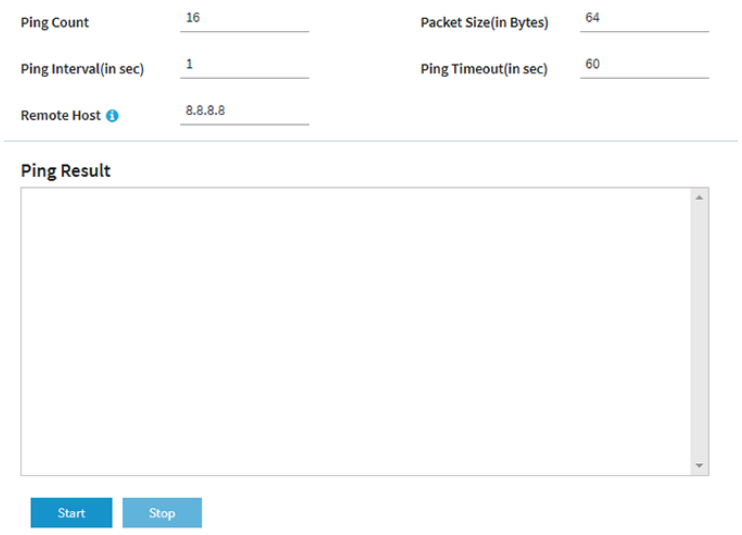
8. To download the file with captured packets, do the following:
   a. Click the **Download** button.
   b. Follow the directions of your browser to save the file to your computer.
9. To display the latest information on the page, click the **Refresh** button.

Perform a ping test

You can ping the IP address of a device or network location from the access point and view the results of the ping test.

To perform a ping test:

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 > Diagnostics > Ping Test**.



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

Setting	Description
Ping Count	The number of pings that the access point must send. The default number is 16.
Packet Size (in Bytes)	The size of each ping packet. The default size is 64 bytes.
Ping Interval (in sec)	The interval between pings. The default interval is 1 second.
Ping Timeout (in sec)	The period after which a ping times out. The default period is 60 seconds.
Remote Host	The IP address that the access point must ping.

6. To start the ping test, click the **Start** button.
   The results of the ping test display in the Ping Result field.
7. To stop the ping test before the ping count is reached or if the ping times out, click the **Stop** button.

Check the Internet speed

You can check the Internet speed of the access point. The results might be helpful if you want to set bandwidth rate limits (see Set bandwidth rate limits for a WiFi network on page 57).

To check the Internet speed:

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 > Diagnostics > Speed Check**.
   The Internet Speed Check page displays.
5. Click the **Test Speed** button.
   After a short delay, the page displays the measured latency in ms, download speed in Mbps, and upload speed in Mbps.

6. To view the test history, click the **View History** link.
   A table shows the results of previous tests.

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 67.
- 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 24.
- Make sure that your WiFi device supports the security that you are using for your WiFi network (WPA2 Personal or WPA2 Personal Mixed). For more information, see Set up and manage WiFi networks on page 41.
- 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 41.

- 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 WAN PoE LED lights solid amber or solid green.
   - The Insight LED lights solid blue or solid green (see Top panel with LEDs on page 13).
   - 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 189
- Power LED remains solid amber on page 189
- Power LED is blinking amber continuously on page 190
- Insight LED is off on page 190
- 2.4G or 5G WLAN LED is off on page 191
- WAN PoE LED or LAN LED is off while a device is connected on page 191

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.

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 155.

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 117), 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 configure a LAN or WAN IP address on page 112).

Insight LED is off

If the WAN PoE port of the access point is connected to a PoE switch, non-PoE switch, or Internet modem and the WAN PoE LED lights amber or green but the Insight LED is off, the access point functions either in the PC Web-browser mode or in the NETGEAR Insight App mode but is not connected to the Insight cloud-based management platform.

If the access point functions in the PC Web-browser mode, the Insight LED is off. This is normal LED behavior.

If the access point functions in the NETGEAR Insight App mode but the Insight LED is off, do the following:

1. Verify that the management mode of the access point is indeed the NETGEAR Insight App mode.

   For more information, see Change the management mode to NETGEAR Insight or Web-browser on page 137.

2. Make sure that the cable connections between the access point and your network are good.
3. Make sure that the access point is connected to the Internet and that the Internet connection is good.
4. Make sure that the access point is running the latest firmware.

   For more information, see Manage the firmware of the access point on page 145.

5. Restart the access point and wait five minutes to see if the Insight LED lights solid blue.

If you use a power adapter with the access point, disconnect and reconnect the power adapter and wait five minutes to see if the Insight LED lights solid blue.

6. Use the **Reset** button to return the access point to its factory default settings.
   For more information, see Use the Reset button on page 155.

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 67). 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.

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.

WAN PoE LED or LAN LED is off while a device is connected

When a powered-on network device such as a PoE switch, non-PoE switch, or Internet modem is connected to the WAN PoE port of the access point, the WAN PoE LED lights amber or green, depending on the speed of the connection. Similarly, when a network device such as a switch, hub, or computer 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 WAN PoE LED or 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 24.
- 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 67.
- 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 41.
- Does your WiFi device support the security that you are using for your WiFi network (WPA2 Personal or WPA2 Personal Mixed). For more information, see Set up and manage WiFi networks on page 41.

  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 194.

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 configure a LAN or WAN IP address on page 112), 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 155.
- 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 194 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.

A

Factory Default Settings and Technical Specifications

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 154.

Table 2. Access point factory default settings

Feature	Default Setting
Access point login	
Management mode	NETGEAR Insight management mode
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 By default, Router mode is disabled, including NAT and the DHCP server function.
DHCP client	Enabled so that the access point receives an IP address from a DHCP server in the network.
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.

Table 2. Access point factory default settings (Continued)

Feature	Default Setting
Security	WPA2 Personal (which is WPA2-PSK) WiFi password (network key): sharedsecret
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 isolation	Disabled
Broadcast SSID	Enabled
Band steering	Disabled Automatic band steering includes automatic 802.11k RRM and automatic 802.11v WiFi network management.
VLAN ID (for WiFi clients)	1
Network authentication	WPA2 Personal (which is WPA2-PSK)
Data encryption	AES
Passphrase	sharedsecret
802.11w (PMF)	Disabled
URL tracking	Disabled
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

Table 2. Access point factory default settings (Continued)

Feature	Default Setting
Wi-Fi Multimedia (WMM)	Enabled
WMM powersave	Enabled
Advanced WiFi settings for all WiFi networks (SSIDs or VAPs)	
Number of WiFi clients	Default: 64 per radio Maximum: 200 per radio
Beacon interval	100 millisec.
802.11n 256 QAM	Disabled for the 2.4 GHz radio (nonconfigurable for the 5 GHz radio)
RTS threshold	2346
DTIM interval	2 sec.
Broadcast/multicast rate limiting	Enabled with a limit of 50 packets per second
Fixed multicast rate	Auto
MU-MIMO	Enabled for the 5 GHz radio (nonconfigurable for the 2.4 GHz radio)
802.11h	Disabled for the 5 GHz radio (nonconfigurable for the 2.4 GHz radio)
Load balancing between radios	Disabled
Data volume limit	None
Wireless bridge	None configured
General security	
URL filtering	None
RADIUS servers	None configured
Neighbour AP detection	Disabled
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 1300 Mbps simultaneous throughput (400 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: 200 (200 per radio) Maximum number of 5 GHz WiFi clients: 200 (200 per radio) Maximum number of clients for the access point: 400 (2 radios)
WiFi standards	IEEE 802.11ac Wave 2 standard WiFi Multimedia Prioritization (WMM) Wireless distribution system (WDS)
802.11 security	WPA2 Personal, WPA2 Personal Mixed, 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 and DFS (5.25–5.35 + 5.50–5.70) • Australia: 5.18–5.24 + 5.745–5.825 GHz • Japan: 5.18–5.24 GHz and DFS (5.26–5.32 + 5.50–5.64)
Power over Ethernet	If you do not use a power adapter, the PoE port requires 802.3af (PoE) power. 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).
PoE consumption	9.3W
Power adapter (not included but can be ordered as an option)	12 VDC, 2.5A The plug is localized to the country of sale.

Table 3. Access point specifications (Continued)

Feature	Description
Hardware interfaces	One WAN PoE port and one regular (non-PoE) LAN port, both of which are 10/100/1000BASE-T RJ-45 ports with Auto Uplink (Auto MDI-X). If you do not use a power adapter, the PoE port requires 802.3af (PoE) power.
Dimensions (W x D x H)	7.75 x 7.75 x 1.45 in. (197.32 x 197.32 x 37 mm)
Weight	1.22 lb (555.5 g)
Operating temperature	32° to 104°F (0° to 40°C)
Operating humidity	10 to 90% maximum relative humidity, noncondensing
Storage temperature	–4° to 158°F (–20° to 70°C)
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 D03
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)
Regulatory compliance Europe	EN 55032:2012 + AC:2013/CISPR 32:2012 EN 61000-3-2:2014 EN 61000-3-3:2013 EN 55024:2010 EN 300 328 V1.9.1 (2015-02) EN 301 893 V1.8.1 (2015-03) EN 50385:2002 EN 50581.2012 EN 50564: 2011 EN 60950-1 2005 (ed.2) + A1:2009 + A2:2013 EN 60950-1:2006 + A11:2009 + A12:2011 + A2:2013
Regulatory compliance Australia	AS/NZS CISPR 32:2013, Class B AS/NZS 4268:2012 + A1:2013 AS/NZS 4268:2012 + A1:2013 AS/NZS 2772.2:2011