NETGEAR®

User Manual

WiFi 6 AX1800/AX3600 Dual Band PoE/PoE+ Access Points

Models
WAX214
WAX218

January 2022
202-12175-02

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

Support and Community

Visit netgear.com/support to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/download/.

(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/download/.)

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.

For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.

By using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions. If you do not agree, return the device to your place of purchase within your return period.

Do not use this device outdoors. The PoE source is intended for intra building connection only.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-12175-02	January 2022	Removed incorrect information from the topic introduction that implied that the device might be managed remotely in Reboot the access point from the local browser UI on page 91.
202-12175-01	December 2020	First publication.

Contents

Chapter 5 Manage the Wired Network Settings

Chapter 6 Manage the Basic Radio and WiFi Settings

Chapter 7 Manage the Advanced WiFi and Radio Settings

Chapter 8 Maintain the access point

Appendix A Factory Default Settings and Technical Specifications

Appendix B Mount Model WAX214 to a Wall or Ceiling

Appendix C Mount Model WAX218 to a Wall or Ceiling

1

Introduction

This manual is for the following NETGEAR WiFi 6 Dual Band Access Point models:

- **WAX214**: NETGEAR WiFi 6 AX1800 Dual Band PoE Access Point.
- **WAX218**: NETGEAR WiFi 6 AX3600 Dual Band PoE+ Access Point.

Models WAX214 and WAX218, in this manual referred to as the access point, provide 802.11ax high-performance WiFi connectivity for a small office/home office and supports dual-band concurrent WiFi 6 operations at 2.4 GHz and 5 GHz.

This chapter contains the following sections:

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

Note: Firmware updates with new features and bug fixes are made available from time to time at 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 manual, *WiFi network* means the same as SSID (service set identifier or WiFi network name). That is, when we refer to a WiFi network we mean an individual SSID.

Unique features for each model

The following table shows the main differences between model WAX214 and model WAX218:

Table 1. Model WAX214 and model WAX218 main differences

Feature	Model WAX214	Model WAX218
Approximate combined throughput	1800 Mbps total: 600 Mbps at 2.4 GHz 1200 Mbps at 5 GHz	3600 Mbps total: 1200 Mbps at 2.4 GHz 2400 Mbps at 5 GHz.
Power over Ethernet[1]	PoE (802.af)	PoE+ (802.at)
Maximum speed LAN port	1 Gbps	2.5 Gbps
Form factor (L x W x H):	6.33 x 6.33 x 1.31 in. (160.9 x 160.9 x 33.3 mm)	8.0 x 8.0 x 1.37 in. (205.7 x 205.7 x 35.8 mm)

[1] *If used without a power adapter.*

Additional documentation

The following documents are available at netgear.com/support/download/:

- Installation guides
- Data sheets

Safety instructions and warnings for an indoor access point

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. Note the following:
  - For more information about the environment in which this product must operate, see the environmental specifications in the appendix or the data sheet.
  - If you want to connect the product over an Ethernet cable to a device located outdoors, the outdoor device must be properly grounded and surge protected, and you must install an Ethernet surge protector inline between the indoor product and the outdoor device. Failure to do so can damage the product.
  - Before connecting the product to outdoor cables or wired outdoor devices, see https://kb.netgear.com/000057103 for additional safety and warranty information.

  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.
- Do not service the product except as explained in your product documentation. Some devices should never be opened.
- If any of the following conditions occur, unplug the product from its power source, and then replace the part or contact your trained service provider:
  - Depending on your product, the power adapter, power adapter cable, power adapter plug, or PoE Ethernet cable 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 the product away from radiators and heat sources. Also, do not block cooling vents.

- Do not spill food or liquids on your product components, and never operate the product in a wet environment. If the product 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 product. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- If applicable to your product, allow the product to cool before removing covers or touching internal components.
- Be sure that devices that are attached over Ethernet cables are electrically rated to operate with the power available in your location.
- Depending on your product, use only the supplied power adapter or an Ethernet cable that provides PoE.
  If your product 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.
- To help prevent electric shock, plug any system and peripheral power cables into properly grounded power outlets.
- If applicable to your product, 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, and PoE Ethernet 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, or plugs. Consult a licensed electrician or your power company for site modifications.
- Always follow your local and national wiring rules.

2

Hardware Overview Model WAX214

The NETGEAR WiFi 6 AX1800 Dual Band PoE Access Point Model WAX214 is an indoor, standalone access point.

The access point provides 802.11ax high-performance WiFi connectivity for a small office/home office and supports dual-band concurrent WiFi 6 operations at 2.4 GHz and 5 GHz with a combined throughput of 1.8 Gbps (about 600 Mbps at 2.4 GHz and 1200 Mbps at 5 GHz).

A single Gigabit PoE LAN port lets you connect the access point to a PoE (802.3af) switch. If you use a regular switch, the access point requires a power adapter, which is supplied for model WAX214PA. (For model WAX214, a power adapter is an option that you can purchase.)

The chapter contains the following sections:

Unpack model WAX214

The package contains the following items:

- WAX214 access point
- Mounting bracket with screw holes for mounting to a solid ceiling or 15/16 in. (23.8 mm) T-bar
- Two screws and anchors for ceiling mounting or wall-mounting
- Installation guide

Note: You power up the access point by connecting it to a PoE switch. Depending on the product ordered, the package might also include a power adapter. If you ordered a package without a power adapter, you can still order a power adapter as an option.

For information about the mounting options, see Mount Model WAX214 to a Wall or Ceiling on page 141.

Top panel with LEDs for model WAX214

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 for model WAX214

Table 2. LED descriptions model WAX214

LED Icon	Description
5 GHz WLAN LED 	**Solid blue**: The 5 GHz radio is operating without clients.
	Blinking blue: The 5 GHz radio is transmitting or receiving data.
	Off: The 5 GHz WiFi radio is off.
2.4 GHz WLAN LED 	**Solid blue**: The 2.4 GHz radio is operating without clients.
	Blinking blue: The 2.4 GHz radio is transmitting or receiving data.
	Off: The 2.4 GHz WiFi radio is off.
LAN LED 	**Solid blue**: The LAN/PoE port detects a link with a powered-on device.
	Blinking blue: The LAN/PoE port is transmitting or receiving data.
	Off: Either no powered-on Ethernet device is connected to the LAN/PoE port, or, if a powered-on Ethernet device is connected, no Ethernet link is detected.
Power LED 	**Solid amber**: The access point is powered on.
	Off: No power is supplied to the access point.

Note: For information about troubleshooting with the LEDs, see Troubleshoot with the LEDs on page 126.

Hardware interfaces model WAX214

The bottom panel of the access point has a LAN/PoE port, Reset button, and DC power connector for an optional power adapter.

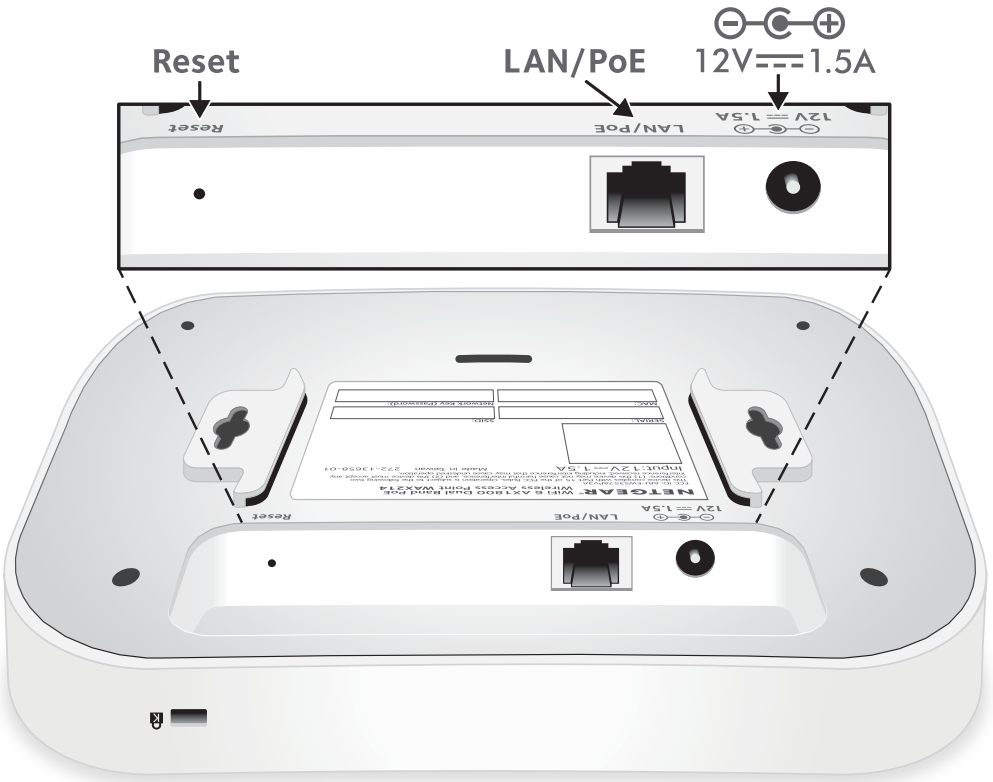


Figure 2. Hardware interfaces of model WAX214

The bottom panel contains the following components:

- **Reset button**. You can use the **Reset** button to restart the access point or to reset the access point to its factory default settings. To restart the access point, press the **Reset** button for about two seconds. Pressing the **Reset** for 10 seconds or longer resets the access point to factory default settings.
- **LAN/PoE port**. You can use the LAN/PoE Gigabit Ethernet RJ-45 port to connect the access point to a PoE switch, or if you use a power adapter, to a non-PoE switch. The LAN/PoE port supports Ethernet speeds up to 1 Gbps.
- **DC power connector**. If you do not use a PoE switch to provide power to the access point, connect an optional power adapter to the DC power connector.

Note: The back panel provides a Kensington lock slot for an optional security cable.

Label model WAX214

The access point label shows the serial number, MAC address, default WiFi network name (SSID) for the 2.4 GHz management SSID, and network key (WiFi password) for the management SSID. The management SSID provides access to the local browser interface (UI) only. That is, the management SSID is not intended for general WiFi clients access.

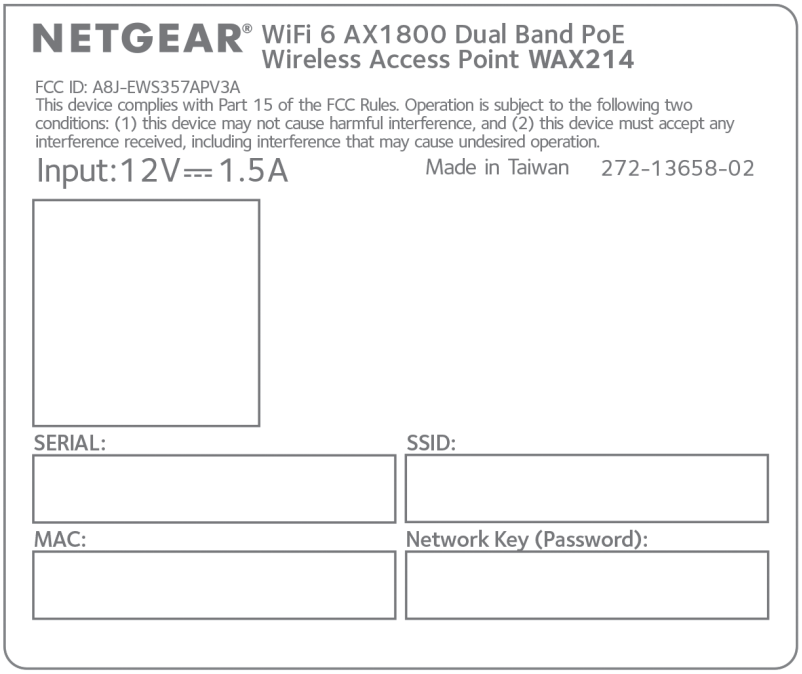


Figure 3. Product label model WAX214

3

Hardware Overview Model WAX218

The NETGEAR WiFi 6 AX3600 Dual Band PoE Access Point Model WAX218 is an indoor, standalone access point.

The access point provides 802.11ax high-performance WiFi connectivity for a small office/home office and supports dual-band concurrent WiFi 6 operations at 2.4 GHz and 5 GHz with a combined throughput of 3.6 Gbps (about 1200 Mbps at 2.4 GHz and 2400 Mbps at 5 GHz).

A single 2.5 Gbps PoE LAN port lets you connect the access point to a PoE+ (802.3at) switch. If you use a regular switch, the access point requires a power adapter, which is supplied for model WAX218PA. (For model WAX218, a power adapter is an option that you can purchase.)

The chapter contains the following sections:

Unpack model WAX218

The package contains the following items:

- WAX218 access point
- Mounting bracket with screw holes for mounting to a solid ceiling or 15/16 in. (23.8 mm) T-bar
- Two screws and anchors for ceiling mounting or wall-mounting
- Installation guide

Note: You power up the access point by connecting it to a PoE+ switch. Depending on the product ordered, the package might also include a power adapter. If you ordered a package without a power adapter, you can still order a power adapter as an option.

For information about the mounting options, see Mount Model WAX218 to a Wall or Ceiling on page 147.

Top panel with LEDs for model WAX218

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

Figure 4. Top panel with LEDs for model WAX218

Table 3. LED descriptions model WAX218

LED Icon	Description
5 GHz WLAN LED 	**Solid blue**: The 5 GHz radio is operating without clients.
	Blinking blue: The 5 GHz radio is transmitting or receiving data.
	Off: The 5 GHz WiFi radio is off.
2.4 GHz WLAN LED 	**Solid blue**: The 2.4 GHz radio is operating without clients.
	Blinking blue: The 2.4 GHz radio is transmitting or receiving data.
	Off: The 2.4 GHz WiFi radio is off.
LAN LED 	**Solid blue**: The LAN/PoE+ port detects a link with a powered-on device.
	Blinking blue: The LAN/PoE+ port is transmitting or receiving data.
	Off: Either no powered-on Ethernet device is connected to the LAN/PoE+ port, or, if a powered-on Ethernet device is connected, no Ethernet link is detected.
Power LED 	**Solid amber**: The access point is powered on.
	Off: No power is supplied to the access point.

Note: For information about troubleshooting with the LEDs, see Troubleshoot with the LEDs on page 126.

Hardware interfaces model WAX218

The bottom panel of the access point has a LAN/PoE+ port, Reset button, and DC power connector for an optional power adapter.

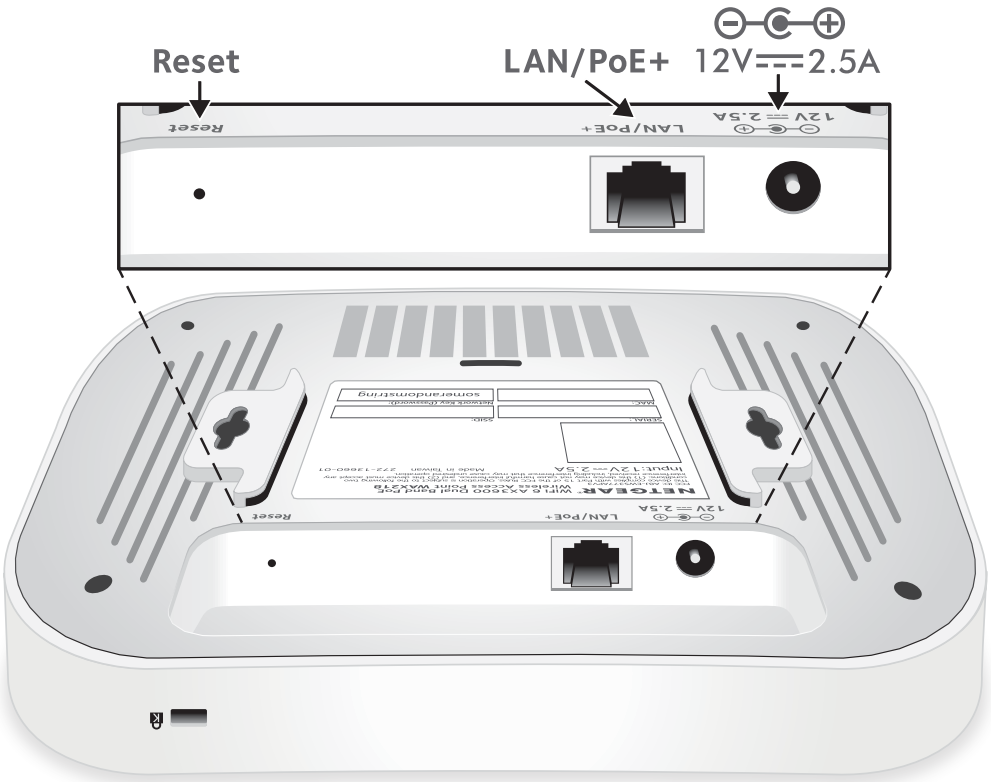


Figure 5. Hardware interfaces of model WAX218

The bottom panel contains the following components:

- **Reset button**. You can use the **Reset** button to restart the access point or to reset the access point to its factory default settings. To restart the access point, press the **Reset** button for about two seconds. Pressing the **Reset** for 10 seconds or longer resets the access point to factory default settings.
- **LAN/PoE+ port**. You can use the LAN/PoE+ Gigabit Ethernet RJ-45 port to connect the access point to a PoE+ switch, or if you use a power adapter, to a non-PoE switch. The LAN/PoE+ port supports Ethernet speeds up to 2.5 Gbps.

  Note: If you do not use a power adapter, use a PoE+ (803.2.at) switch. If you use a PoE (803.2.af) switch, the access point might not receive sufficient power for normal operation.

- **DC power connector**. If you do not use a PoE+ switch to provide power to the access point, connect an optional power adapter to the DC power connector.

Note: The back panel provides a Kensington lock slot for an optional security cable.

Label model WAX218

The access point label shows the serial number, MAC address, default WiFi network name (SSID) for the 2.4 GHz management SSID, and network key (WiFi password) for the management SSID. The management SSID provides access to the local browser interface (UI) only. That is, the management SSID is not intended for general WiFi clients access.

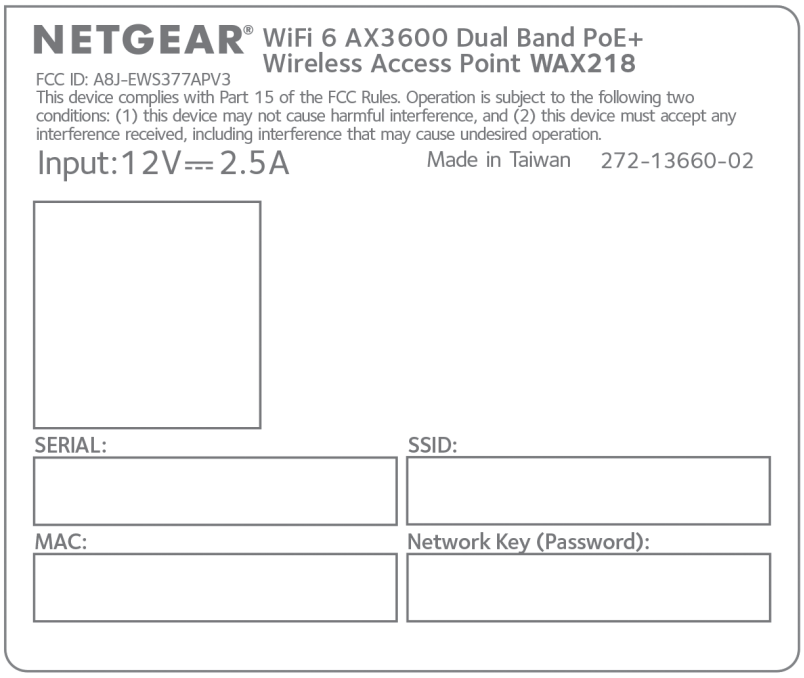


Figure 6. Product label model WAX218

4

Installation and Initial Log-in

This chapter describes how you can install and access the access point in your network and go through the initial log-in process.

Note: When you log in to the access point, you connect to the local browser UI.

The chapter contains the following sections:

Set up the access point in your network

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

The following sections describe how you can set up the access point in your network:

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

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

Set up the access point with a PoE or PoE+ network connection

You can connect the access point to a Power over Ethernet (PoE) switch in your network. The type of PoE switch depends on the access point model (see below). 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.

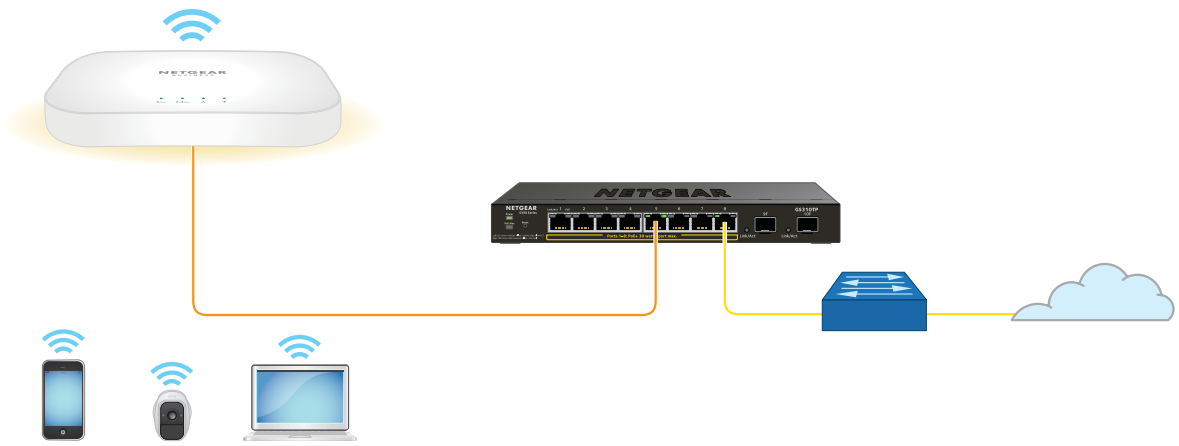


Figure 7. Set up model WAX214 with a PoE connection to your network

Note: The LAN/PoE port on model WAX214 supports Ethernet speeds up to 1 Gbps. Most switches support speeds of up to 1 Gbps.

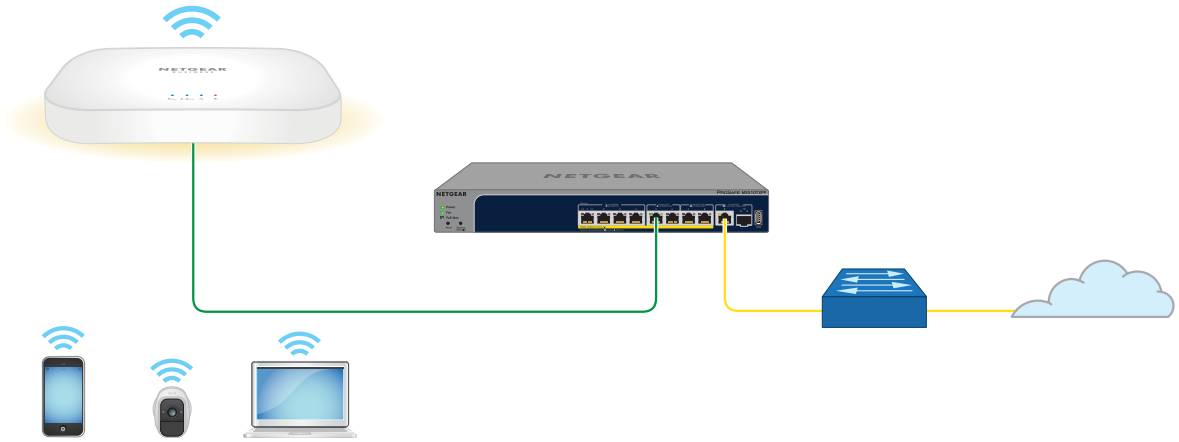


Figure 8. Set up model WAX218 with a PoE+ connection to your network

Note: The LAN/PoE+ port on model WAX218 supports Ethernet speeds up to 2.5 Gbps. The previous figure shows a NETGEAR MS510TXPP switch, which supports speeds of 2.5 Gbps and higher. However, if your Internet connection, modem, and switch support a speed of 1 Gbps (which is a common speed), the access point LAN connection functions at 1 Gbps.

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

1. Connect an Ethernet cable to the LAN/PoE (model WAX214) or LAN/PoE+ (model WAX218) port on the access point.
2. Connect the other end of the Ethernet cable to switch that is connected to your network and to the Internet.
   - **Model WAX214**: Connect the cable to a PoE port on a PoE (802.3af) switch. You can also use a PoE+ (802.3at) switch.
   - **Model WAX218**: Connect the cable to a PoE+ port on a PoE+ (802.3at) switch. We recommend that you do not use a PoE (803.2.af) switch because the provided power might be insufficient for this model.
3. Check to see that the LEDs light.

LED	Description
5 GHz WLAN	The 5 GHz WLAN LED lights solid blue or blinks blue.
2.4 GHz WLAN	The 2.4 GHz WLAN LED lights solid blue or blinks blue.
LAN	The LAN LED lights solid blue or blinks blue.
Power	The Power LED lights solid amber.

You can now access the access point for initial configuration (see Initial log-in process on page 26).

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 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 supplied for model WAX214PA and model WAX218PA. (For model WAX214 and model WAX218, a power adapter is an option that you can purchase.)

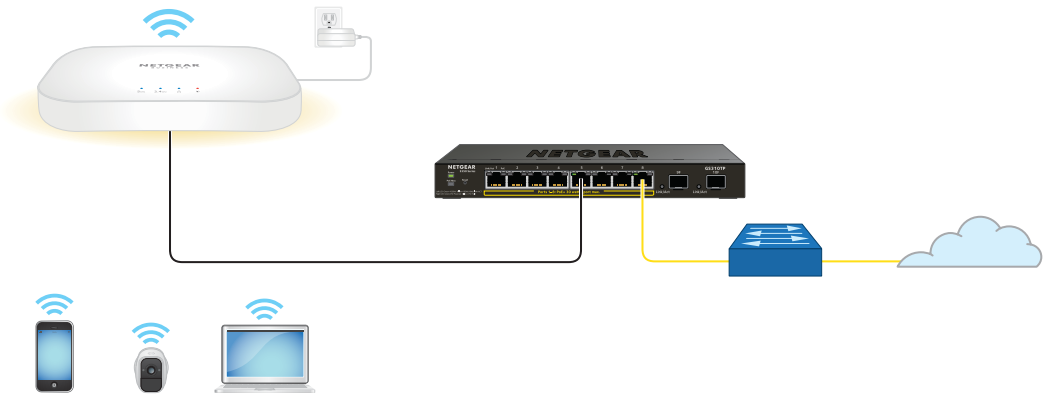


Figure 9. Set up model WAX214 with a non-PoE connection to your network

Note: The LAN/PoE port on model WAX214 supports Ethernet speeds up to 1 Gbps. Most switches support speeds of up to 1 Gbps.

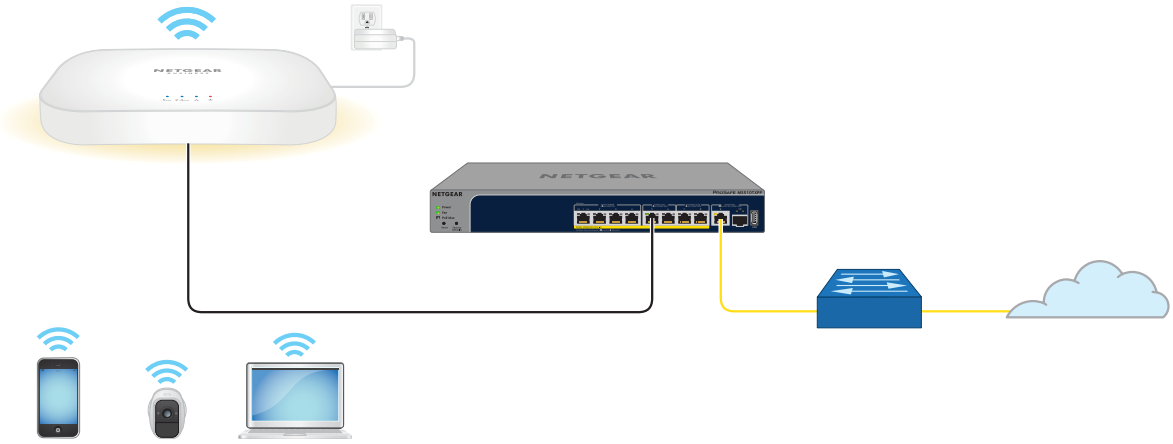


Figure 10. Set up model WAX218 with a non-PoE connection to your network

Note: The LAN/PoE+ port on model WAX218 supports Ethernet speeds up to 2.5 Gbps. The previous figure shows a NETGEAR MS510TXPP switch, which supports speeds of 2.5 Gbps and higher. However, if your Internet connection, modem, and switch support a speed of 1 Gbps (which is a common speed), the access point LAN connection functions at 1 Gbps.

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

1. Connect an Ethernet cable to the LAN/PoE (model WAX214) or LAN/PoE+ (model WAX218) 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.
4. Check to see that the LEDs light.

LED	Description
5 GHz WLAN 	The 5 GHz WLAN LED lights solid blue or blinks blue.
2.4 GHz WLAN 	The 2.4 GHz WLAN LED lights solid blue or blinks blue.

(Continued)

LED	Description
LAN 	The LAN LED lights solid blue or blinks blue.
Power 	The Power LED lights solid amber.

You can now access the access point for initial configuration (see Initial log-in process on page 26).

Initial log-in process

During the initial log-in process, the access point presents its Day Zero page. You must define a local device password that lets you access the local browser UI access point. You also must define a new WiFi network name (SSID) and associated WiFi passphrase (WiFi password).

After you complete the initial-log-in process and attempt to log in to the local browser UI, the access point no longer presents the Day Zero page but displays the regular login page that allows you to enter your local device password.

For more information about the initial log-in process, see one of the following sections:

- Connect directly to the access point over WiFi and log in for the first time on page 26
- Connect to the access point over the LAN and log in for the first time on page 29

Connect directly to the access point over WiFi and log in for the first time

This section describes how to connect a WiFi-enabled computer or mobile device over the 2.4 GHz management SSID to the access point for the first time and complete the initial configuration.

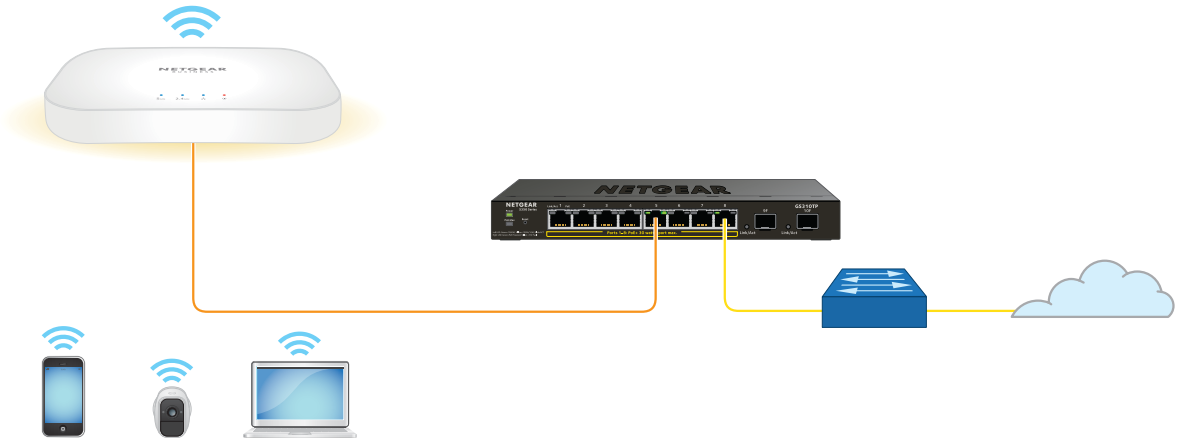


Figure 11. Connect directly to the access point over WiFi

The previous figure shows the access point (in this example, model WAX214) connected to a switch, which is connected to a router and the Internet. WiFi devices are directly connected to the access point.

To connect directly to the access point over WiFi and log in to the local browser UI for the first time:

1. On a WiFi-enabled computer or mobile device, find and connect to the access point's management SSID.

   The management SSID depends on the model and the MAC address. In the following examples, XXXXXX represents the last six digits of the MAC address of the LAN interface of the access point:

   - **WAX214**: WAX214XXXXXX-CONFIG-ONLY
   - **WAX218**: WAX218XXXXXX-CONFIG-ONLY

   In this manual, we also refer to this management SSID as the "CONFIG-ONLY" SSID. The default WiFi passphrase for the management SSID, which is a unique WiFi password, is printed on the access point label.

   If you cannot get a WiFi connection to the access point, see You cannot connect over the 2.4 GHz management SSID on page 130.

2. Launch a web browser and enter **https://www.aplogin.net** (which is the same as **https://192.168.0.100**) in the address field.

   The Day Zero login page displays. This page displays only the first time that you log in.

   IMPORTANT: If your browser does not display the Day Zero login page, see the following step.

3. If your browser displays a security message and does not let you proceed, do one of the following:

   - **Google Chrome**: If Google Chrome displays a *Your connection is not private* message, click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the IP address of the switch.
   - **Apple Safari**: If Apple Safari displays a *This connection is not private* message, click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window displays, click the **Visit Website** button. If another pop-up window displays to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.
   - **Mozilla Firefox**: If Mozilla Firefox displays a *Your connection is not secure* message, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
   - **Microsoft Internet Explorer**: If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message, click the **Continue to this website (not recommended)** link.
   - **Microsoft Edge**: If Microsoft Edge displays a *There is a problem with this website's security certificate* message or a similar warning, select **Details > Go on to the webpage**.

4. On the Day Zero page, configure the following settings:
   a. In the **AP Login New Password** field, specify a unique local login password, and confirm the password in the **Confirm New Password** field.
   We recommend that your password meets the following conditions:

      - Contains 8 to 32 characters
      - Contains no more than two identical characters in a row

      In addition, we recommend that your password meets at least three of the following four conditions:

      - At least one uppercase character
      - At least one lowercase character
      - At least one number
      - At least one special character, such as the following characters:
      @ # $ % ^ & * ( ) !

   b. In the **SSID** field, specify a WiFi network name for the main (first) WiFi network. This SSID does *not* replace the management SSID (depending on the model, WAX214XXXXXX-CONFIG-ONLY or WAX218XXXXXX-CONFIG-ONLY), which

you can continue to use to log in over a WiFi connection to the local browser UI of the access point.
In addition to the management SSID, the access point supports four WiFi networks. By default, only the main WiFi network is enabled.

c. In the **Passphrase** field, specify a passphrase (WiFi password) for the main WiFi network.
This passphrase must be a minimum of 8 characters and can be a maximum of 63 characters.
This passphrase does *not* replace the passphrase for the management SSID, which you can continue to use to log in over a WiFi connection to the local browser UI of the access point.

d. Select the check box to accept NETGEAR's terms and conditions and acknowledge that you read the privacy notice.

e. Click the **Apply** button.
Yous settings are saved. The access point restarts. After about two minutes, the login page displays.

5. If you are still connected to the management SSID but the login page does not display, in the address field of your web browser, enter **https://www.aplogin.net**.

   Note: If your browser displays a security message and does not let you proceed, see Step 3.

6. In the **Local Device Password** field, enter your new local device password, and click the **Login** button.

   The Device Status page displays. You can now configure the access point for your network and environment.

Connect to the access point over the LAN and log in for the first time

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 your computer are on the same LAN. By default, the access point functions as a DHCP client and receives an IP address from a DHCP server.

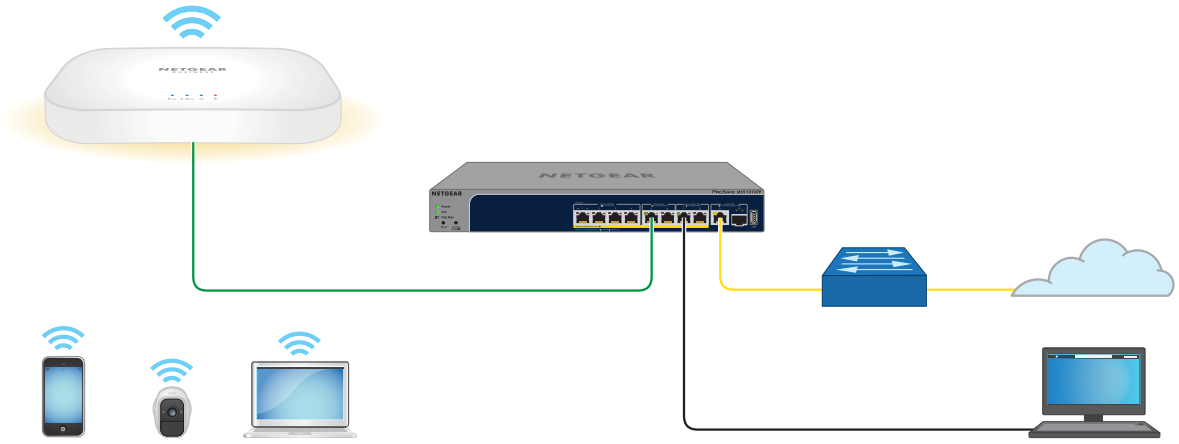


Figure 12. Connect to the access point over the LAN

The previous figure shows the access point (in this example, model WAX218) connected to a switch, which is connected to a router and the Internet. A computer is connected to the same switch as the access point. (The computer can connect to the LAN in a different way, but as long as the computer and the access point are on the same LAN, the following procedure is applicable.)

To connect to the access point over the LAN and log in for the first time:

1. Using an Ethernet cable, connect an Ethernet port on your computer to a LAN port on a switch or hub that is connected to your LAN.
2. If you do not yet know the IP address that is assigned to access point, use one of the following options, each of which is described in detail in Find the IP address of the access point on page 33):
   - Use the automatic device detection of a Windows-based computer.
   - Access your existing router or DHCP server.
   - Use the NETGEAR Insight mobile app.
   - Use a third-party IP scanner.
3. Launch a web browser and enter the IP address that is assigned to the access point in the address field.

   The Day Zero login page displays. This page displays only the first time that you log in.

   If your browser does not display the Day Zero login page but a security message, see Step 4. However, if you cannot get a LAN connection to the access point at all, see You cannot log in to the access point over a LAN connection on page 132.

4. If your browser displays a security message and does not let you proceed, do one of the following:

   - **Google Chrome**: If Google Chrome displays a *Your connection is not private* message, click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the IP address of the switch.
   - **Apple Safari**: If Apple Safari displays a *This connection is not private* message, click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window displays, click the **Visit Website** button. If another pop-up window displays to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.
   - **Mozilla Firefox**: If Mozilla Firefox displays a *Your connection is not secure* message, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
   - **Microsoft Internet Explorer**: If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message, click the **Continue to this website (not recommended)** link.
   - **Microsoft Edge**: If Microsoft Edge displays a *There is a problem with this website's security certificate* message or a similar warning, select **Details > Go on to the webpage**.

5. On the Day Zero page, configure the following settings:
   a. In the **AP Login New Password** field, specify a unique local login password, and confirm the password in the **Confirm New Password** field.
   We recommend that your password meets the following conditions:

      - Contains 8 to 32 characters
      - Contains no more than two identical characters in a row

      In addition, we recommend that your password meets at least three of the following four conditions:

      - At least one uppercase character
      - At least one lowercase character
      - At least one number
      - At least one special character, such as the following characters:
      @ # $ % ^ & * ( ) !

   b. In the **SSID** field, specify a WiFi network name for the main (first) WiFi network. This SSID does *not* replace the management SSID (depending on the model, WAX214XXXXXX-CONFIG-ONLY or WAX218XXXXXX-CONFIG-ONLY), which

you can continue to use to log in over a WiFi connection to the local browser UI of the access point.
In addition to the management SSID, the access point supports four WiFi networks. By default, only the main WiFi network is enabled.

c. In the **Passphrase** field, specify a passphrase (WiFi password) for the main WiFi network.
This passphrase must be a minimum of 8 characters and can be a maximum of 63 characters.
This passphrase does *not* replace the passphrase for the management SSID, which you can continue to use to log in over a WiFi connection to the local browser UI of the access point.

d. Select the check box to accept NETGEAR's terms and conditions and acknowledge that you read the privacy notice.

e. Click the **Apply** button.
Yous settings are saved. The access point restarts. After about two minutes, the login page displays.

6. If the login page does not display, in the address field of your web browser, enter the IP address that is assigned to the access point.

   Note: If your browser displays a security message and does not let you proceed, see Step 4.

7. In the **Local Device Password** field, enter your new local device password, and click the **Login** button.

   The Device Status page displays. You can now configure the access point for your network and environment.

When to use aplogin.net and when to use the assigned IP address

Use **https://www.aplogin.net** (which is the same as **https://192.168.0.100**) *only* when you connect to the access point over the 2.4 GHz management SSID, that is, over the "CONFIG-ONLY" SSID. For more information, see 2.4 GHz management SSID on page 58.

For all other types of connections, use the IP address that was assigned to the access point by your existing router or DHCP server during the setup process (see Initial log-in process on page 26) to log in to the local browser UI of the access point.

That means that you must use the assigned IP address in all following situations:

- Your mobile device is connected to one of the SSIDs on the access point but not to the "CONFIG-ONLY" SSID.
- Your wired computer is on the same network as the access point.
- Your mobile device is *not* directly connected to the access point network even if it is on the same network as the access point.
- Your mobile device *is* connected to the "CONFIG-ONLY" SSID, but the access point is set up with a static IP address.
- Your network includes another NETGEAR device that is also accessible by using **https://www.aplogin.net**. In such a situation, if you use **https://www.aplogin.net**, you might log in to the access point or you might log in to the other NETGEAR device, depending on your network situation.

If you do not know the IP address that was assigned to the access point, see Find the IP address of the access point on page 33.

Find the IP address of the access point

If you do not know the IP address that was assigned to the access point, use *one* of the following options to find the IP address of the access point:

- **Option 1: Use the automatic device detection of a Windows-based computer**.
  1. Launch File Explorer (or Windows Explorer).
  2. Select **Network** from the Navigation pane.
  3. Right-click the access point device icon, and select **Properties**.
     The access point IP address displays.

- **Option 2: Temporarily connect directly over WiFi and log in**. If you already completed the initial log-in, temporarily connect a mobile device directly to the access pointover WiFi and do the following:
  1. Open a web browser from the mobile device that is directly connected to the access point network.
  2. Enter **https://www.aplogin.net** in the address field.
     The Login page displays.
  3. Enter your local device password and click the **Login** button.
     The Device Status page displays.
     In the LAN Information - IPv4 section, the IP Address field displays the IP address that is assigned to the access point.

- **Option 3: Temporarily connect directly over WiFi and ping the access point.** If you already completed the initial log-in, temporarily connect a mobile device directly over WiFi to the access point and send a ping to **https://www.aplogin.net**.
  How to send a ping depends on mobile device.
  On your mobile device, the field with the ping results displays the IP address that is assigned to the access point.
- **Option 4: Use the NETGEAR Insight mobile app**. To use the NETGEAR Insight mobile app to discover the IP address of the access point in your network, do the following:
  1. On your iOS or Android mobile device, go to the app store, search for NETGEAR Insight, and download and install the app.
  2. Connect your mobile device to the access point WiFi network.
  3. Open the NETGEAR Insight mobile app.
  4. Tap **LOG IN** to log in to your NETGEAR account.
     After you log in to your account, the IP address of the access point displays in the device list.
- **Option 5: Access your existing router or DHCP server**. Access the DHCP server information of your existing router, modem (if the modem functions as a DHCP server), or dedicated DHCP server to see the devices that are connected to it, including the access point. The IP address that is assigned to the access point is listed.
- **Option 6: Use a third-party IP scanner**. Use an IP scanner application (they are available free of charge on the Internet) in the network of your existing router. The IP scanner results include the IP address that is assigned to the access point.

If you made a direct connection to the access point, you can now terminate that connection. Connect your computer or mobile device to the same network as the access point, and use the discovered IP address to log in to the access point.

Find the IP address of the access point with the NETGEAR Insight mobile app

The NETGEAR Insight mobile app lets you discover the access point in your network.

Note: Although you can use the NETGEAR Insight mobile app to register the access point, the access point is already registered automatically after the initial log-in process.

To use the NETGEAR Insight mobile app to discover the access point in your network:

1. On your iOS or Android mobile device, go to the app store, search for NETGEAR Insight, and download and install the app.
2. Connect your mobile device to the access point WiFi network.
3. Open the NETGEAR Insight mobile app.
4. Tap **LOG IN** to log in to your existing NETGEAR account, which is the same account that you logged into or created during the initial log-in process.

   After you log in to your account, the IP address of the access point displays in the device list.
5. Save the IP address for future use.

Log in to the access point after you complete the initial log-in process

After you complete the initial log-in process, the access point is ready for use and you can change the settings and monitor the traffic.

Depending on how you connect to the access point, when you enter **https://www.aplogin.net** or the IP address that is assigned to the access point and you use http, the browser automatically redirects your request to https. If you did not yet install the access point's security certificate, your browser might display a security message. You can either ignore this message or install the security certificate. Consider the following examples:

- **Google Chrome**: If Google Chrome displays a *Your connection is not private* message, click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the IP address of the switch.
- **Apple Safari**: If Apple Safari displays a *This connection is not private* message, click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window displays, click the **Visit Website** button. If another pop-up window displays to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.
- **Mozilla Firefox**: If Mozilla Firefox displays a *Your connection is not secure* message, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
- **Microsoft Internet Explorer**: If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message, click the **Continue to this website (not recommended)** link.

- **Microsoft Edge**: If Microsoft Edge displays a *There is a problem with this website's security certificate* message or a similar warning, select **Details > Go on to the webpage**.

To log in to the access point's local browser UI after you complete the initial log-in process:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message, see the information in the introduction to this task.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

The Device Status page displays various panes that let you see the status of your access point at a glance. You can now configure and monitor the access point.

Change the language

By default, the language of the local browser UI is set as Auto. You can change the language.

To change the language:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. In the upper right corner, select a language from the menu.

   The page refreshes with the language that you selected.

Join a WiFi network on the access point

You can manually add a WiFi device such as a WiFi-enabled computer, tablet, or smartphone to a WiFi network of the access point.

On the WiFi device that you want to connect to the access point, use the software application that manages your WiFi connections.

Note: By default, the access point's main (first) WiFi network is enabled but the second, third, and fourth WiFi networks are disabled. These WiFi networks differ from the management SSID, which you can use to log in over a WiFi connection to the local browser UI of the access point.

To connect a device to a WiFi network on the access point:

1. Make sure that the access point is receiving power (its Power LED is lit) and is connected to the Internet (its LAN LED is lit), and that the WiFi radios are on (its WLAN LEDs are lit).
2. On the WiFi device, open the software application that manages your WiFi connections.

   This application scans for all WiFi networks in your area.

3. Look for one of the access point's WiFi networks and select it.

   For the main WiFi network, you had to specify the SSID during the initial log-in process. To connect to the main WiFi network, look for *that* SSID.

4. Enter the WiFi password for WiFi access.

For the main WiFi network, you had to specify the WiFi passphrase (WiFi password) during the initial log-in process. To connect to the main WiFi network, enter *that* WiFi passphrase.

5. Click the **Connect** button.

   The device connects to the WiFi network of the access point.

5

Manage the Wired Network Settings

This chapter describes how you can manage the wired network settings of the access point.

The chapter includes the following sections:

Specify a static IPv4 address

By default, the DHCP client of the access point is enabled, allowing a DHCP server (usually, a router) in your network to assign an IPv4 address to the access point. You can disable the DHCP client and specify static (fixed) IP address settings for the access point.

To specify static IPv4 address settings for the access point:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Basic**.

   The page that displays shows the IPv4 Settings, IPv6 Settings, and Spanning Tree Protocol (STP) Settings sections.

5. In the IPv4 Settings section, select the **Static IP** radio button.

   The IPv4 address fields display.

6. Specify the static IPv4 address, subnet mask, gateway IPv4 address, and primary and secondary DNS addresses.
7. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window displays. The window shows the number of changes to be applied.

8. In the pop-up window, click the **Apply** button.

Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Note: To log back in to the access point, you now must use the static IP address that you assigned.

Specify a link-local IPv6 address

By default, the DHCP client of the access point is enabled, allowing a DHCPv6 server (usually, a router) in your network to assign an IPv6 address to the access point. You can disable the DHCP client and specify link-local IPv6 address settings for the access point. A link-local IPv6 address is an automatically generated IPv6 address that uses the IPv4 address in the interface portion of its address.

To specify link-local IPv6 address settings for the access point:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Basic**.

   The page that displays shows the IPv4 Settings, IPv6 Settings, and Spanning Tree Protocol (STP) Settings sections.

5. In the IPv4 Settings section, select the **Static IP** radio button.

   The **Link-local Address** check box becomes available.

6. In the IPv6 Settings section, clear the **Link-local Address** check box.
   The IPv6 address fields display.
7. Specify the static IPv6 address, subnet prefix length, IPv6 gateway address, and primary and secondary DNS addresses.
8. Click the **Save** button.
   Your settings are saved but not yet applied.
   A pop-up window displays. The window shows the number of changes to be applied.
9. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Note: To log back in to the access point, you now must use the IPv6 address that you assigned.

Reenable the DHCP client of the access point

If you disabled the DHCP client of the access point, you can reenable it, which affects both the IPv4 and IPv6 settings.

To reenable the DHCP client of the access point:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.
   A login window displays.
   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.
   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.
   The Device Status page displays.

4. Under Network, select **Basic**.

   The page that displays shows the IPv4 Settings, IPv6 Settings, and Spanning Tree Protocol (STP) Settings sections.

5. In the IPv4 Settings section, select the **DHCP** radio button.

   The IPv4 address fields no longer display, the **Link-local Address** check box is automatically selected, and the IPv6 address fields are masked out.

6. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window displays. The window shows the number of changes to be applied.

7. In the pop-up window, click the **Apply** button.

   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Note: To log back in to the access point, you now must use the IP address that is assigned by the DHCP (or DHCPv6) server in your network.
To determine the IP address that the DHCP server assigned to the access point, use one of the following methods:

- **Windows-based computer**: If you use a Windows-based computer, open Windows Explorer, and click the **Network** link. If prompted, enable the Network Discovery feature. Under Network Infrastructure, locate and click the access point device name (assuming that you did not change the device name).
- **DHCP server**: Access the DHCP server in your network and open the page that shows the network connections.
- **NETGEAR Insight app**: Use the NETGEAR Insight app to discover the IP address that is assigned to the access point. For more information, see Find the IP address of the access point with the NETGEAR Insight mobile app on page 34.
- **IP network scanner**: Use a third-party IP network scanner to scan for the IP address that is assigned to the access point.

Manage the STP settings

By default, Spanning Tree Protocol (STP) is enabled on the access point.

You can change the settings for STP, or disabled it entirely. However, we recommend that you keep STP enabled because it helps to prevent network loops.

To manage the STP settings:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.
4. Under Network, select **Basic**.

   The page that displays shows the IPv4 Settings, IPv6 Settings, and Spanning Tree Protocol (STP) Settings sections.
5. In the Spanning Tree Protocol (STP) Settings section, specify the settings that are described in the following table:

Setting	Description
Status	Select one of the following radio buttons: • **Enable**: STP is enabled. This is the default setting. • **Disable**: STP is disabled.
Hello Time	The interval in seconds between handshake packets the access point sends to communicate information about the topology throughout the entire bridged LAN. The range is 1–10 seconds. The default is 2 seconds.
Max Age	The period in seconds within which the access point must receive a hello packet from another device in the spanning tree before the access point assumes that the device is inactive. The range is 6–40 seconds. The default is 20 seconds.

(Continued)

Setting	Description
Forward Delay	The period in seconds that a device spends in each of the listening and learning states before entering the forwarding state. This delay is provided so that when a new device enters a busy network, the device analyzes data traffic before participating in the network. The range is 4–30 seconds. The default is 15 seconds.
Priority	The priority of the access point in the spanning tree. A smaller number means a higher priority. The range is 0–65535. The default is 32768.

6. Click the **Save** button.
   Your settings are saved but not yet applied.

   A pop-up window displays. The window shows the number of changes to be applied.

7. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

6

Manage the Basic Radio and WiFi Settings

This chapter describes how you can manage the basic radio and WiFi settings of the access point. For information about advanced WiFi and radio settings, see Manage the Advanced WiFi and Radio Settings on page 63.

The chapter includes the following sections:

Change the device name

The device name is also referred to as the AP name or system name. It is the access point name that displays in the network. By default, the device name is the access point's model number. You can change this name.

To change the device name of the access point:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.
4. Under Network, select **Wireless**.

   The Wireless Settings page displays.
5. In the **AP Name** field, enter a new name.

   The name must contain alphanumeric characters, cannot be longer than 15 characters, and cannot contains spaces. The name *can* contain hyphens, but cannot start or end with a hyphen.
6. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window displays. The window shows the number of changes to be applied.
7. In the pop-up window, click the **Apply** button.

   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Change the country and region of operation

After initial configuration, you can change the country and region of operation of the access point.

WARNING: 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.

WARNING: 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.

To change the country and region of operation of the access point:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.

   The Wireless Settings page displays.

5. From the **Country / Region** menu, select the country and region in which the access point is operating.
6. Click the **Save** button.

   Your settings are saved but not yet applied.

A pop-up window displays. The window shows the number of changes to be applied.

7. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security

When you performed the initial configuration on the Day Zero page, you were required to change the name and WiFi passphrase of the main (first) WiFi network (SSID) for WiFi clients. (By default, this SSID is configured for WPA2 personal security.)

The access point supports up to four SSIDs that can broadcast on either a single or both radios. (These four SSIDs are in addition to the 2.4 GHz management SSID.) By default, the access point's first SSID is enabled and the second, third, and fourth SSIDs are disabled. You can enable or disable an SSID, change the settings and WiFi security for an SSID, and perform other configuration tasks.

The type of WPA personal security (WPA2, WPA3, or a combination of both) that you select must depend on the types of devices in your WiFi network and the level of security that your environment requires. All types of WPA personal security function with a WiFi passphrase. A WiFi client can only access the WiFi network with the correct WiFi passphrase.

To change the settings for an active SSID or enable and configure an SSID that is open or secured with WPA2 or WAP3 personal security:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.
   The Wireless Settings page displays.

5. Go to the Wireless Settings - Access Point section.
   The following information displays:

   - Up to four SSIDs are available.
   - The **Enabled** check box is selected for the enabled SSIDs and cleared for the disabled SSIDs. You can either enable or disable SSIDs.
     By default, the main (first) SSID is enabled for both the 2.4 GHz and 5 GHz radios, but the second, third, and fourth SSIDs are disabled.
   - The SSID fields shows the names for the WiFi networks to which WiFi clients can connect. You can change the SSID names.
   - The Security fields show the types of WiFi security that are enabled for the SSID. By default, the type of WiFi security is WPA2-Personal.

6. Do one of the following:

   - **Enabled SSID**: To change the settings for a previously enabled SSID, click the **Edit** button for the SSID.
   - **Disabled SSID**: To enable and then change the settings for an SSID that is not yet enabled, select the **Enabled** check box for the SSID, and then click the **Edit** button for the SSID.

   A new page displays.

   Note: To allow you to focus on the essential SSID settings, the tables in the following steps do not include information about band steering, RADIUS settings (other than RADIUS settings for enterprise security), RADIUS accounting, the WiFi MAC filter, and WiFi traffic shaping. For more information about these advanced settings, see Manage the Advanced WiFi and Radio Settings on page 63.

7. In the Wireless Setting - Access Point 2.4GHz/5GHz section, specify the radio band, SSID name, and isolation security settings, as described in the following table.

Setting	Description
Enable	To enable the SSID to broadcast on both the 2.4 GHz radio and the 5 GHz radio, select the **2.4G** and **5G** check boxes. If you clear a check box, the SSID is not broadcast on the radio.
SSID	The SSID is the WiFi network name. Specify 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 (\).
Hidden SSID	To hide the WiFi network name and prevent it from displaying in the scanning list of a WiFi client, select the **Enable** radio button. To connect to the WiFi network, a user must know the WiFi network name. By default, this option is disabled.
Client Isolation	To prevent WiFi clients that are associated with the same or different WiFi networks on the access point from communicating with each other, select the **Enable** radio button. By default, this option is disabled. If you enable client isolation, WiFi clients can still communicate with each other over the Internet. **Note**: If L2 isolation is enabled, the **Client Isolation** radio buttons are disabled.
VLAN Isolation	To prevent clients on different VLANs from communicating with each other, select the **Enable** radio button, and enter the VLAN ID in the **ID** field. By default, this option is disabled. For the first SSID, the default VLAN ID is 1, for the second SSID, the default VLAN ID 2, for the third SSID, the VLAN ID is 3, and for the fourth SSID, the VLAN ID is 4. The range is from 1 to 4094. If you enable VLAN isolation, clients can still communicate with each other over the Internet.
L2 Isolation	To prevent WiFi and LAN clients on the same access point from communicating with each other, select the **Enable** radio button. By default, this option is disabled. If you enable L2 isolation, clients can still communicate with each other over the Internet. If you enable L2 isolation, to exclude a device from L2 isolation, enter the MAC address of the device in a **Whitelist** field. You can exclude up to three devices.

8. In the Wireless Security section, specify the WiFi security by selecting an option from the **Security Mode** menu, as described in the following table.

Setting	Description
None	A legacy open WiFi network does not provide any security. Any WiFi device can join the network. Clients are not authenticated and traffic is not encrypted. We recommend that you do *not* use a legacy open WiFi network without any security but configure WiFi security. However, a legacy open network might be appropriate for a WiFi hotspot.
OWE	The WiFi network can only accept clients that support the WiFi enhanced open feature, which is based on opportunistic wireless encryption (OWE). Select this option only if all the clients in the WiFi network support OWE.
WPA2-Personal	This option, which is the same as WPA2-PSK, is the default setting. This type of security enables only WiFi devices that support WPA2 to join the SSID.
WPA3-Personal	This option, which is the same as WPA3-PSK, is the most secure personal authentication option. WPA3 enables only WiFi devices that support WPA3 to join the SSID. If your network also includes WPA2 devices, select **WPA3/WPA2-Personal** security.
WPA2/WPA3-Personal	This option, which is the same as WPA3-PSK/WPA2-PSK, enables WiFi devices that support either WPA2 or WPA3 to join the SSID. WPA2 is less secure than WPA3.

9. If you select **WPA2-Personal**, **WAP3-Personal**, or **WPA2/WPA3-Personal** from the **Security Mode** menu, configure the following settings:
   a. **Passphrase**: Specify a phrase of 8 to 63 characters. To join the SSID, a user must enter this passphrase.
   b. **Group Key Update Interval**: Specify a period from 30 to 3600 seconds, which is the period after which the WiFi network group key changes in the background. (Connected users are not affected.) The default period is 3600 seconds. To disable group key changes, specify 0.

10. To enable fast roaming for WPA2-Personal security, in the Fast Roaming section, select the **Enable** radio button.

    For WPA personal security, fast roaming is available only if you select **WPA2-Personal** from the **Security Mode** menu. By default, fast roaming is disabled for these types of WiFi security. If your network includes WiFi clients that must be able to roam from one access point to another, enable fast roaming so that certain client applications can quickly reassociate with the new access point.

    Note: For information about band steering, RADIUS settings (other than RADIUS settings for enterprise security), RADIUS accounting, the WiFi MAC filter, and WiFi traffic shaping, see Manage the Advanced WiFi and Radio Settings on page 63.

11. Click the **Save** button.

    Your settings are saved but not yet applied.

    A pop-up window displays. The window shows the number of changes to be applied.

12. In the pop-up window, click the **Apply** button.

    Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security

When you performed the initial configuration on the Day Zero page, you were required to change the name and WiFi passphrase of the main (first) WiFi network (SSID) for WiFi clients. (By default, this SSID is configured for WPA2 personal security.)

The access point supports up to four SSIDs that can broadcast on either a single or both radios. (These four SSIDs are in addition to the 2.4 GHz management SSID.) By default, the access point's first SSID is enabled and the second, third, and fourth SSIDs are disabled. You can enable or disable an SSID, change the settings and WiFi security for an SSID, and perform other configuration tasks.

WPA2 or WPA3 enterprise-level security (or a combination thereof) uses RADIUS for centralized Authentication, Authorization, and Accounting (AAA) management. The following procedure includes the steps to configure a RADIUS server.

The type of WPA enterprise security (WPA2, WPA3, or a combination of both) that you select must depend on the types of devices in your WiFi network and the level of security that your environment requires. All types of WPA enterprise security function with a shared key (a WiFi password) that is also defined on the RADIUS server. A WiFi client can only access the WiFi network with the correct shared key.

To change the settings for an active SSID or enable and configure an SSID that is secured with WPA2 or WAP3 enterprise security:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.
   The Wireless Settings page displays.

5. Go to the Wireless Settings - Access Point section.
   The following information displays:

   - Up to four SSIDs are available.
   - The **Enabled** check box is selected for the enabled SSIDs and cleared for the disabled SSIDs. You can either enable or disable SSIDs.
     By default, the main (first) SSID is enabled for both the 2.4 GHz and 5 GHz radios, but the second, third, and fourth SSIDs are disabled.
   - The SSID fields shows the names for the WiFi networks to which WiFi clients can connect. You can change the SSID names.
   - The Security fields show the types of WiFi security that are enabled for the SSID. By default, the type of WiFi security is WPA2-Personal.

6. Do one of the following:

   - **Enabled SSID**: To change the settings for a previously enabled SSID, click the **Edit** button for the SSID.
   - **Disabled SSID**: To enable and then change the settings for an SSID that is not yet enabled, select the **Enabled** check box for the SSID, and then click the **Edit** button for the SSID.

   A new page displays.

   Note: To allow you to focus on the essential SSID settings, the tables in the following steps do not include information about band steering, RADIUS settings (other than RADIUS settings for enterprise security), RADIUS accounting, the WiFi MAC filter, and WiFi traffic shaping. For more information about these advanced settings, see Manage the Advanced WiFi and Radio Settings on page 63.

7. In the Wireless Setting - Access Point 2.4GHz/5GHz section, specify the radio band, SSID name, and isolation security settings, as described in the following table.

Setting	Description
Enable	To enable the SSID to broadcast on both the 2.4 GHz radio and the 5 GHz radio, select the **2.4G** and **5G** check boxes. If you clear a check box, the SSID is not broadcast on the radio.
SSID	The SSID is the WiFi network name. Specify 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 (\).
Hidden SSID	To hide the WiFi network name and prevent it from displaying in the scanning list of a WiFi client, select the **Enable** radio button. To connect to the WiFi network, a user must know the WiFi network name. By default, this option is disabled.
Client Isolation	To prevent WiFi clients that are associated with the same or different WiFi networks on the access point from communicating with each other, select the **Enable** radio button. By default, this option is disabled. If you enable client isolation, WiFi clients can still communicate with each other over the Internet. **Note**: If L2 isolation is enabled, the **Client Isolation** radio buttons are disabled.
VLAN Isolation	To prevent clients on different VLANs from communicating with each other, select the **Enable** radio button, and enter the VLAN ID in the **ID** field. By default, this option is disabled. For the first SSID, the default VLAN ID is 1, for the second SSID, the default VLAN ID 2, for the third SSID, the VLAN ID is 3, and for the fourth SSID, the VLAN ID is 4. The range is from 1 to 4094. If you enable VLAN isolation, clients can still communicate with each other over the Internet.
L2 Isolation	To prevent WiFi and LAN clients on the same access point from communicating with each other, select the **Enable** radio button. By default, this option is disabled. If you enable L2 isolation, clients can still communicate with each other over the Internet. If you enable L2 isolation, to exclude a device from L2 isolation, enter the MAC address of the device in a **Whitelist** field. You can exclude up to three devices.

8. In the Wireless Security section, specify WiFi enterprise security by selecting an option from the **Security Mode** menu, as described in the following table.

Setting	Description
WPA2-Enterprise	This option enables only WiFi devices that support WPA2 to join the SSID.
WPA3-Enterprise	This option enables only WiFi devices that support WPA3 to join the SSID. If your network also includes WPA2 devices, select **WPA3/WPA2-Enterprise** security.
WPA2/WPA3-Enterprise	This option enables WiFi devices that support either WPA2 or WPA3 to join the SSID. WPA2 is less secure than WPA3.

9. Configure the following RADIUS authentication server settings:
   a. **SuiteB 192bits**: (This setting applies to WPA3-Enterprise only.) To enable the equivalent of 192-bit cryptographic strength for WPA3, select the **Enable** button. By default, this options is disabled.
   b. **Group Key Update Interval**: Specify a period from 30 to 3600 seconds, which is the period after which the WiFi network group key changes in the background. (Connected users are not affected.) The default period is 3600 seconds. To disable group key changes, specify 0.
   c. **Radius Server**: Specify the IPv4 address of the RADIUS authentication server. The access point must be able to reach this IP address.
   d. **Radius Port**: Specify the number of the UDP port on the access point that is used to access the RADIUS authentication server. The default port number is 1812.
   e. **Radius Secret**: Specify the shared key (WiFi password) that is used between the access point and the RADIUS authentication server during the authentication process.

10. To enable fast roaming for WPA2-Enterprise security, in the Fast Roaming section, select the **Enable** radio button.

    For enterprise security, fast roaming is available only if you select **WPA2-Enterprise** from the **Security Mode** menu. By default, fast roaming is disabled for this type of WiFi security. If your network includes WiFi clients that must be able to roam from one access point to another, enable fast roaming so that certain client applications can quickly reassociate with the new access point.

    Note: For information about band steering, RADIUS settings (other than RADIUS settings for enterprise security), RADIUS accounting, the WiFi MAC filter, and WiFi traffic shaping, see Manage the Advanced WiFi and Radio Settings on page 63.

11. Click the **Save** button.

    Your settings are saved but not yet applied.

    A pop-up window displays. The window shows the number of changes to be applied.

12. In the pop-up window, click the **Apply** button.

    Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Configure a guest network on an SSID

You can configure one or more SSIDs as guest networks.

By default, and irrespective of which SSIDs function as guest networks, guest WiFi devices are assigned an IP address in the range from 192.168.200.100 to 192.168.200.200. You can change these automatically assigned IP addresses by changing the DHCP server settings for the guest networks. For more information, see Change the DHCP server settings for guest WiFi networks on page 87.

To configure a guest network:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.

   The Wireless Settings page displays.

5. In the Wireless Settings - Access Point section, do one of the following:

   - To change an existing SSID (one that is already enabled and configured) into a guest network, select the **Guest Network** check box for the SSID.

- To enable and configure a new SSID as a guest network, do the following:
  a. Select the **Enabled** check box for the SSID.
  b. Select the **Guest Network** check box for the SSID.
  c. Click the **Edit** button for the SSID.
     A new page opens.
  d. Configure the settings for the SSID.
     For more information, see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page 49.
  e. Click the **Save** button.
     Your settings are saved but not yet applied. The page closes. The Wireless Settings page displays again.

A pop-up window displays. The window shows the number of changes to be applied.

6. Click the **Apply** button.
   Your settings are saved and applied. The WiFi connection is reestablished. The page displays the number of seconds before the access point is back online.

2.4 GHz management SSID

You can use the 2.4 GHz management SSID *only* to access the local browser UI of the access point from a WiFi device for management purposes. That is, you might not get an Internet connection over this SSID. Furthermore, only if you are connected to the management SSID, you can use **https://www.aplogin.net** to access to the local browser UI. For more information about **https://www.aplogin.net**, see When to use aplogin.net and when to use the assigned IP address on page 32.

IMPORTANT: By default, the idle time-out for the management SSID is 15 minutes. That is, if no WiFi client is connected to the management SSID for 15 minutes, the management SSID is turned off. Only after you reboot the access point can you reconnect to the management SSID. However, you can disable the idle time-out so that the management SSID always stays on (see Disable the idle time-out for the 2.4 GHz management SSID on page 60).

The management SSID cannot be used for regular WiFi client connections to the access point. For these types of connections, use one of the regular SSIDs (see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page

49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53).

The name of the management SSID depends on the model and the MAC address. In the following examples, XXXXXX represents the last six digits of the MAC address of the LAN interface of the access point:

- **WAX214**: WAX214XXXXXX-CONFIG-ONLY
- **WAX218**: WAX218XXXXXX-CONFIG-ONLY

In this manual, we also refer to this management SSID as the "CONFIG-ONLY" SSID.

You cannot change the name of the management SSID. The default WiFi passphrase for the management SSID is printed on the access point label. You *can* change this WiFi passphrase and we recommend that you do so.

Change the passphrase for the 2.4 GHz management SSID

You can change the passphrase (WiFi password or network key) for the 2.4 GHz management SSID. (You cannot change the name of the management SSID.)

To change the passphrase for the management SSID:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.

   The Wireless Settings page displays.

5. In the Management Interface - 2.4G section, click the **Edit** button.
   A new page opens.
6. In the **Passphrase** field, enter a new passphrase (network key or WiFi password) that you must enter to connect to local browser UI of the access point.
   The length of the passphrase must be from 8 to 63 characters.
7. Click the **Save** button.
   Your settings are saved but not yet applied.

   A pop-up window displays. The window shows the number of changes to be applied.
8. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Disable the idle time-out for the 2.4 GHz management SSID

By default, the idle time-out for the 2.4 GHz management SSID is 15 minutes. That is, if no WiFi client is connected to the management SSID for 15 minutes, the management SSID is turned off.

Only after you reboot the access point can you reconnect to the management SSID. However, you can disable the idle time-out so that the management SSID stays always on.

To disable the idle time-out for the management SSID:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

The Device Status page displays.

4. Under Network, select **Wireless**.
   The Wireless Settings page displays.
5. In the Management Interface - 2.4G section, select the **Always on** radio button.
   By default, the **Turn off if idle in 15 minutes** radio button is selected.
6. Click the **Save** button.
   Your settings are saved but not yet applied.

   A pop-up window displays. The window shows the number of changes to be applied.
7. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Disable the 2.4 GHz management SSID

As a security measure, you can entirely disable the 2.4 GHz management SSID. If you do so, you can still reach the access point local browser UI over a wired LAN connection or over one of the other SSIDs, as long as the SSID is in default VLAN 1 and the management VLAN setting is disabled. (These are the default VLAN settings for any SSID on the access point.)

To disable the management SSID:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

The Device Status page displays.

4. Under Network, select **Wireless**.
   The Wireless Settings page displays.
5. In the Management Interface - 2.4G section, clear the **Enabled** check box.
6. Click the **Save** button.
   Your settings are saved but not yet applied.

   A pop-up window displays. The window shows the number of changes to be applied.
7. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

7

Manage the Advanced WiFi and Radio Settings

This chapter describes how you can manage the advanced WiFi and radio settings of the access point. For information about the basic WiFi and radio settings, see Manage the Basic Radio and WiFi Settings on page 46.

The chapter includes the following sections:

Manage the channel high throughput mode

The channel high throughput (HT) mode is also referred to as the channel width.

The default channel widths are as follows:

- **2.4 GHz radio**: 20MHz
- **5 GHz radio**: 80 MHz

The wider the channel, the better the performance (that is, the greater the transmission quality and speed), but the fewer channels are available for use. Before you change the channel width, consider your network conditions and the applications that must be supported. Use the following guidelines:

- A wider channel improves the performance (no or minimal interference and better data rates).
- 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 and 802.11ax specifications allow 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.

To manage the channel HT mode:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.
   The Wireless Settings page displays.
5. To change the channel HT mode for the 2.4 GHz radio, from the **Channel HT Mode** menu in the 2.4GHz (ax/n/g/b) column, select **20MHz** (the default setting), **40MHz**, or **20MHz/40MHz**.
6. To change the channel HT mode for the 5 GHz radio, from the **Channel HT Mode** menu in the 5GHz (ax/ac/n/a) column, select **20MHz**, **40MHz** , or **80MHz** (the default setting).
7. Click the **Save** button.
   Your settings are saved but not yet applied.
   A pop-up window displays. The window shows the number of changes to be applied.
8. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Manage the channel or channels

By default, a WiFi channel is automatically assigned for a radio on the access point. The channels that are available depend on the country and region that you selected for the access point.

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

If you use multiple access points, you can reduce interference by selecting different channels for adjacent access points. We recommend a channel spacing of four channels between adjacent access points (for example, for 5 GHz radios, use channels 44 and 60, or 112 and 128).

WARNING: Make sure that the country is set to the location where the device is operating (see Change the country and region of operation on page 48). You are responsible for complying with the local, regional, and national regulations that are set for channels, power levels, and frequency ranges.

To manage the channels:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

A login window displays.

If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.

   The Wireless Settings page displays.

5. Click the Channel **Configuration** button.

   A new page opens.

6. To reset all channels for a radio *before* you select one or more specific channels in the next step, click the **None** button for a radio.
7. Do one of the following:

   - **Specific channel for a radio**: To select a specific channel for a radio, click the button for the channel and frequency. The available channels depend on the country and region that you selected for the access point.
   - **Groups of channels for the 2.4 GHz radio**: To select a specific group of channels for the 2.4 GHz radio, select a button that displays a group of channels, for example, the **1,6,11** button or the **1,5,9** button.
   - **Groups of channels for the 5 GHz radio**: To select a specific group of channels for the 5 GHz radio, select a U-NII button, for example, the **U-NII-1** button or the **U-NII-3** button.
   - **Automatic channel allocation for a radio**: To enable automatic channel allocation for a radio, click the **All** button for the radio.

8. Click the **Save** button.

   Your settings are saved but not yet applied. The page closes. The Wireless Settings page displays again.

   A pop-up window displays. The window shows the number of changes to be applied.

9. In the pop-up window, click the **Apply** button.

   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Manage the radio transmit power

By default, the transmit power for the radios on the access point is automatically assigned.

You can disable automatic power assignment and set a specific transmit power. However, note the following:

- If you set the transmit power too high, the access point might not be able to connect to another WiFi device.
- If you set the transmit power too low, WiFi clients might not be able to connect to the access point.

IMPORTANT: Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.

WARNING: Make sure that the country is set to the location where the device is operating (see Change the country and region of operation on page 48). You are responsible for complying with the local, regional, and national regulations that are set for channels, power levels, and frequency ranges.

To manage the radio transmit power:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

The local device password is the one that you specified. The password is case-sensitive.

The Device Status page displays.

4. Under Network, select **Wireless**.
   The Wireless Settings page displays.
5. Do one of the following:
   - Clear the **Auto RF** radio button.
     Automatic transmit power (Auto) is disabled. The **Transmit Power** menu becomes available and you can specify a specific transmit power (see the next step).
   - Select the **Auto RF** button.
     Automatic transmit power (Auto) is enabled. This is the default setting. The **Transmit Power** menu is masked out.
6. If you cleared the Auto RF radio button in the previous step, from the **Transmit Power** menu, select the transmit power for a radio.
   The transmit power is expressed in dBm. You can select different transmit powers for the radios.
7. Click the **Save** button.
   Your settings are saved but not yet applied.

   A pop-up window displays. The window shows the number of changes to be applied.
8. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Change the minimum bit rate

The access point automatically sends data at the lowest effective bit rate.

We recommend that you do not manually change the minimum bit rate. However, if you understand the consequences, you can manually select a higher bit rate. Client devices must either use the selected bit rate or a higher bit rate.

WARNING: Be careful changing the minimum bit rate. If you set the bit rate too high, some WiFi devices might no longer be able to connect to the access point.

To change the minimum bit rate:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.

   The Wireless Settings page displays.

5. Click the Bit Rate **Configuration** button.

   A new page opens.

6. As a precaution, write down the current minimum bit rate for each radio.

   After you change the bit rate, if WiFi devices can no longer connect to the access point, you can reset the bit rate to the old value.

7. On the blue bar for a radio, select a new minimum bit rate by clicking the white dot that represents the bit rate.

   The bit rate is expressed in Mbps.

8. Click the **Save** button.

   Your settings are saved but not yet applied. The page closes. The Wireless Settings page displays again.

   A pop-up window displays. The window shows the number of changes to be applied.

9. In the pop-up window, click the **Apply** button.

   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Manage client limits

By default, a maximum of 64 WiFi clients can associate with each radio on the access point.

For each radio, you can specify a lower number of maximum WiFi clients. The range is from 1 to 64. The maximum number applies to all clients connected to one radio, that is, to all active SSIDs on the radio. For example, if two SSIDs are active on the 2.4 GHz radio, the maximum number of 64 clients applies to the two SSIDs on the 2.4 GHz radio, that is, *together* these SSIDs cannot support more than 64 clients. You cannot set client limits for individual SSIDs.

For a radio, you can also disable client limits entirely, allowing an unlimited number of clients to associate with the radio. However, if too many clients simultaneously connect to the radio, the quality and throughput of the connection might decrease, or clients might not be able to connect.

To manage client limits:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.

   The Wireless Settings page displays.

5. Do one of the following:
   - **Set client limits for a radio**: Set client limits by doing the following:
     a. Select the Clients Limits **Enable** radio button for the radio.
        By default, client limits are enabled for both radios.
     b. In the **Client Limits** field for the radio, enter a number from 1 to 64.
        For each radio, the default is 64.
   - **Disable client limits for a radio**: Disable client limits for a radio by selecting the Clients Limits **Disable** radio button.
     By default, client limits are enabled.
6. Click the **Save** button.
   Your settings are saved but not yet applied.
   A pop-up window displays. The window shows the number of changes to be applied.
7. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Manage the multicast and unicast streams to WiFi clients

When a client tries to associate with a WiFi network and negotiates an IP address, the access point converts the multicast DHCP offer message from the DHCP server to a unicast message, and forwards it to the client. This is the default option. You can disable this option so that the access point does not convert the multicast DHCP offer messages to unicast messages. Multicast messages cause more overhead in a WiFi network, but situations might exist in which you prefer multicast over unicast messages in your network.

To manage the multicast and unicast streams to WiFi clients:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the “CONFIG-ONLY” SSID, you can enter **https://www.aplogin.net**.
   A login window displays.

If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.
   The Wireless Settings page displays.

5. Do one of the following:

   - **Change multicast streams to unicast streams**: Select the Multicast to Unicast Stream Conversion **Enable** radio button.
     The access point converts multicast DHCP offer messages to unicast messages. This is the default setting.
   - **Keep multicast streams**: Select the Multicast to Unicast Stream Conversion **Disable** radio button.
     The access point does not convert multicast DHCP offer messages to unicast messages.

6. Click the **Save** button.
   Your settings are saved but not yet applied.

   A pop-up window displays. The window shows the number of changes to be applied.

7. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Scan for neighboring access points and WiFi routers

Scanning for neighboring access points and WiFi routers is useful if you notice interference between your access point and other access points or WiFi routers. You

can then adjust the channels on which your access point broadcasts (see Manage the channel or channels on page 65).

To scan for neighboring access points and WiFi routers:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.
4. Under Network, select **Wireless**.

   The Wireless Settings page displays.
5. Click the AP Detection **Scan** button for one of the radios.

   A new page opens. After the access point completes its scan for neighboring access points and WiFi routers in the selected radio band, the page displays (for each detected access point) the information that is described in the following table.

Setting	Description
BSSID	The basic service set ID (BSSID) in the format of a MAC address. This is usually the MAC address of the radio on the device that broadcasts the SSID.
SSID	The service set ID (SSID), which is the name for the WiFi network that the access point detects.
Channel	The radio channel on which the SSID is being broadcast.
Signal Level	The strength of the WiFi signal that is being broadcast, expressed in –dBm. A lower value means a stronger signal. For example, –40 dBm indicates a stronger signal than –60 dBm.

(Continued)

Setting	Description
Type	The WiFi mode that is configured for the SSID (for example, 11a/n).
Security	The type of security, if any, that is configured for the SSID (for example, WPA2-PSK).
Mode	The operation mode of the detected device. This mode is always Master.

6. To repeat the scan for the radio band, click the **Repeat scan** button.
   The page refreshes with the most recent information.

Manage the 802.11ax mode for the 2.4 GHz radio

By default, the 802.11ax mode is enabled on the access point. WiFi 6 (802.11ax) is backward compatible with earlier WiFi standards. However, if your network includes many legacy devices that do not support WiFi 6, in some unlikely situations, compatibility problems could occur. To mitigate such situations, NETGEAR gives you the option to disable the 802.11ax mode for the 2.4 GHz radio.

To manage the 802.11ax mode for the 2.4 GHz radio:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

The Device Status page displays.

4. Under Network, select **Wireless**.
   The Wireless Settings page displays.
5. Do one of the following:
   - **Disable the 802.11ax mode for the 2.4 GHz radio**: Select the 11ax **Disable** radio button.
   - **Enable the 802.11ax mode for the 2.4 GHz radio**: Select the 11ax **Enable** radio button. This is the default mode.
6. Click the **Save** button.
   Your settings are saved but not yet applied.
   A pop-up window displays. The window shows the number of changes to be applied.
7. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Set up a WiFi on/off schedule for an SSID

You can set up a WiFi on/off schedule. Scheduling an SSID to be turned off is a green feature that allows you to turn off WiFi during scheduled vacations, office shutdowns, on evenings, or on weekends. You can set up and manage a WiFi on/off schedule for each SSID.

Before you enable and set up a WiFi on/off schedule, make sure that the time zone settings are synchronized with your local time. For more information, see Manage the date and time settings on page 97.

To set up a WiFi on/off schedule for an SSID:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.
   A login window displays.
   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Management, select **WiFi Scheduler**.

   A page displays the Auto Reboot Settings section and the Wi-Fi Scheduler section.

5. In the Wi-Fi Scheduler section, select the following:

   - **Status**: Select the **Enable** radio button.
     By default, the **Disable** button is selected, and the settings are masked out.
   - **SSID Selection**: From the **SSID Selection** menu, select the SSID to which the WiFi on/off schedule must apply.
   - **Schedule Templates**: From the **Schedule Templates** menu, select one of the following templates:
     - **Always available**.
     - **Available 8-17 daily**.
     - **Available 8-17 daily except weekends**.
     - **Custom schedule**.

     Based on your selection, the Schedule Table is preconfigured. You can refine the settings.

6. To refine the settings in the Schedule Table, do the following as needed:

   - For each day, from the **Available** menu, select **available** or **unavailable**:
     - **available**: WiFi is turned on during the hours that you must specify in the **Duration** fields for the selected day.
     - **unavailable**: WiFi is turned off during the hours that you must specify in the **Duration** fields for the selected day.
   - For each day, in the **Duration** fields, specify the start hour and minutes and the end hours and minutes.
     If you selected **available** from the **Available** menu, WiFi is turned on during the hours that you specify in the **Duration** fields for the selected day.

If you selected **unavailable** from the **Available** menu, WiFi is turned off during the hours that you specify in the **Duration** fields for the selected day.

7. Click the **Save** button.

   Your settings are saved but not yet applied. The page closes. The Wireless Settings page displays again.

   A pop-up window displays. The window shows the number of changes to be applied.

8. In the pop-up window, click the **Apply** button.

   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Set up band steering for an SSID

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 an SSID. 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. By default, band steering is disabled for an SSID.

IMPORTANT: For band steering to function correctly, you must configure the same SSID settings, including WiFi security settings, for the 2.4 GHz and 5 GHz bands of the SSID. For more information about the SSID settings, see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page 49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53.

To set up a band steering for an SSID:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.
   The Wireless Settings page displays.

5. In the Wireless Settings - Access Point section , click the **Edit** button for the SSID.
   A new page opens.

6. Scroll down to the Band Steering section.

7. Select the Status **Enable** radio button.
   By default, band steering is disabled and the Status **Disable** radio button is selected.

8. From the **Band Steering** menu, select one of the following options (which apply only to dual-band capable WiFi devices) and specify the associated minimum received signal strength indicator (RSSI) value in decibel milliwatts (dBm):

   - **Prefer 5GHz**: In the **5GHz RSSI** field, specify the RSSI value of the dual-band capable WiFi device below which the device is not steered to the 5 GHz band. We recommend that you set an RSSI value between –60 and –80. A device that cannot connect to the 5 GHz band because its RSSI value is too low can still connect to the 2.4 GHz band.
   - **Force 5GHz**: All dual-band capable WiFi devices are forced to associate with the 5 GHz band. A device that is already connected to the 2.4 GHz band is not disassociated. An RSSI value does not apply to this option.
   - **Band Balance**:
     - **5GHz RSSI**: Specify the RSSI value of the dual-band capable WiFi device below which the device is not steered to the 5 GHz band. We recommend that you set an RSSI value between –60 and –80. A device that cannot connect to the 5 GHz band because its RSSI value is too low can still connect to the 2.4 GHz band.
     - **Percent of clients on 5GHz radio**: Specify the percentage of newly connecting, dual-band capable WiFi devices that are steered to the 5 GHz band. The RSSI value of these devices must be within the the threshold that you specify in the **5GHz RSSI** field. For example, a percentage of 75 specifies that 75 percent of newly connecting, dual-band capable WiFi devices for which the RSSI value is within the the threshold are steered to the 5 GHz band, while 25 percent of newly connecting, dual-band capable WiFi devices are associated with the 2.4 GHz band.

9. Click the **Save** button.

   Your settings are saved but not yet applied. The page closes. The Wireless Settings page displays again.

   A pop-up window displays. The window shows the number of changes to be applied.

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

    Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Set up a RADIUS accounting server

You can set up a RADIUS accounting server without using enterprise security, which requires setting up a RADIUS *authentication* server (see Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53).

To set up a RADIUS accounting server:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.

   The Wireless Settings page displays.

5. In the Wireless Settings - Access Point section, do one of the following:
   - To configure a RADIUS accounting server for an existing SSID (one that is already enabled and configured), click the **Edit** button for the SSID.
   - To enable an SSID that is still disabled and configure a RADIUS accounting server for the SSID, select the **Enabled** check box for the SSID, and then click the **Edit** button for the SSID.

   A new page opens.
6. In the Radius Accounting section, configure the settings as described in the following table.

Setting	Description
Radius Accounting	To enable RADIUS accounting, select the **Enable** radio button. By default, the **Disable** radio button is selected.
Radius Accounting Server	Enter the IPv4 address of the RADIUS accounting server. The access point must be able to reach this IP address.
Radius Accounting Port	Enter the number of the UDP port on the access point that is used to access the RADIUS accounting server. The default port number is 1813.
Radius Accounting Secret	Enter the password (shared key) that is used between the access point and the accounting RADIUS server during the authentication process.
Interim Accounting Interval	Enter the period in seconds between each accounting update message that the access point sends to the RADIUS accounting server. The default period is 600 seconds.

7. Click the **Save** button.

   Your settings are saved but not yet applied. The page closes. The Wireless Settings page displays again.

   A pop-up window displays. The window shows the number of changes to be applied.
8. In the pop-up window, click the **Apply** button.

   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Configure Network Access Server settings

If your network includes a Network Access Server (NAS) that functions as the gateway to a RADIUS server, you can set up NAS settings for the SSID that requires its clients to

authenticate over RADIUS (see Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53) or for which you set up RADIUS accounting (see Set up a RADIUS accounting server on page 79).

To configure Network Access Server settings:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Network, select **Wireless**.

   The Wireless Settings page displays.

5. In the Wireless Settings - Access Point section, do one of the following:

   - To configure the NAS settings for an existing SSID (one that is already enabled and configured), click the **Edit** button for the SSID.
   - To enable an SSID that is still disabled and configure the NAS settings for the SSID, select the **Enabled** check box for the SSID, and then click the **Edit** button for the SSID.

   A new page opens.

6. In the Radius Settings section, configure the settings as described in the following table.

Setting	Description
NAS-ID	To enable and configure this option, select the check box and specify an ID for the SSID, which enables the NAS to identify traffic from the SSID.
NAS-PORT	To enable and configure this option, select the check box and specify the number of the port on the NAS.
NAS-IP	To enable and configure this option, select the check box and specify the IPv4 address of the NAS. The access point must be able to reach this IP address.

7. Click the **Save** button.
   Your settings are saved but not yet applied. The page closes. The Wireless Settings page displays again.
   A pop-up window displays. The window shows the number of changes to be applied.
8. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Configure traffic shaping

In a configuration with multiple SSIDs, the WiFi clients on all SSID are allocated the same amount of bandwidth for downloading and uploading traffic. By shaping the traffic for each SSID, you can control the total bandwidth usage on the access point, or you can control the way the bandwidth is allocated between the SSIDs.

For each SSID, you can shape the traffic by limiting the bandwidth for downloading traffic and the bandwidth for uploading traffic, either for the entire SSID or for each user (WiFi client) of the SSID.

To configure traffic shaping for a SSID:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.
   A login window displays.
   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.
   The Device Status page displays.
4. Under Network, select **Wireless**.
   The Wireless Settings page displays.
5. In the Wireless Settings - Access Point section, click the **Edit** button for the SSID.
   A new page opens.
6. Scroll down to the Wireless Traffic Shaping section.
7. Select the Status **Enable** radio button.
   By default, the Status **Disable** radio button is selected and traffic shaping is disabled for the SSID.
8. In the **Download Limit** field, enter the limit.
   You can enter a limit from 1 to 999 in either Kbps or Mbps. If you enable traffic shaping, do not enter 0. Otherwise downloading traffic is disabled entirely.
9. In the **Upload Limit** field, enter the limit.
   You can enter a limit from 1 to 999 in either Kbps or Mbps. If you enable traffic shaping, do not enter 0. Otherwise uploading traffic is disabled entirely.
10. To apply the configured limits to each individual user of the SSID, select the **Per User** check box.
    If you use the SSID to provide a WiFi connection to multiple individual users, this option is useful to the control the bandwidth usage of individual users.
11. Click the **Save** button.
    Your settings are saved but not yet applied. The page closes. The Wireless Settings page displays again.
    A pop-up window displays. The window shows the number of changes to be applied.
12. In the pop-up window, click the **Apply** button.
    Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Set up a MAC filter for an SSID

By default, the access point does not restrict access to an SSID based on a MAC address.

For each SSID, you can set up a MAC address filter, which is an access control list (ACL) that is based on MAC addresses of WiFi clients for which you want to either allow or deny access to the SSID. An ACL provides added security to ensure that only authorized WiFi devices connect to the SSID:

- **MAC address that allows access**: An ACL with a policy that allows access functions as follows:
  - A WiFi device for which you place the MAC address in the ACL is allowed to connect to the SSID.
  - All other WiFi devices are denied a connection to the SSID.
- **MAC address that denies access**: An ACL with a policy that denies access functions as follows:
  - A WiFi device for which you place the MAC address in the ACL is denied a connection to the SSID.
  - All other WiFi devices are allowed to connect to the SSID.

Note: If you manually block a WiFi client (that is, *kick* a client, see Manually block a WiFi client or connection from an SSID on page 86), an ACL that denies the MAC address of the client is automatically added to the SSID from which you blocked the client. That ACL denies access to the client but allows access all other clients. You can manually delete the client from the ACL, after which the client is no longer denied access to the SSID.

To set up a MAC filter for an SSID:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.
   The Device Status page displays.
4. Under Network, select **Wireless**.
   The Wireless Settings page displays.
5. In the Wireless Settings - Access Point section , click the **Edit** button for the SSID.
   A new page opens.
6. Scroll down to the Wireless MAC Filter section.
   By default, the MAC filter is disabled and the **Disabled** button is selected from the **ACL Mode** menu.
7. From the **ACL Mode** menu, select one of the following:
   - **Deny MAC in the List**: The MAC addresses that you add to the list are denied access but all other MAC address are allowed access.
   - **Allow MAC in the List**: The MAC addresses that you add to the list are allowed access but all other MAC address are denied access.

   By default, the selection is Disabled and all MAC addresses are allowed.
8. To add MAC addresses to the list, do the following:
   a. Enter the MAC address of a WiFi device in the fields.
   b. Click the **Add** button.
      The MAC address is added to the list. The address displays, together with an entry number, and a **Delete** button, allowing you to remove the MAC address from the list.
   c. To add another MAC address, repeat steps a and b.
9. Click the **Save** button.
   Your settings are saved but not yet applied. The page closes. The Wireless Settings page displays again.
   A pop-up window displays. The window shows the number of changes to be applied.
10. In the pop-up window, click the **Apply** button.

Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Manually block a WiFi client or connection from an SSID

You can manually block a WiFi client (that is, *kick* a client) or connection from an SSID.

If you do so, an ACL that denies the MAC address of the client is automatically added to the SSID from which you blocked the client. That ACL denies access to the client but allows access all other clients. You can manually delete the client from the ACL, after which the client is no longer denied access to the SSID. For more information, see Set up a MAC filter for an SSID on page 84.

To manually block a WiFi client or connection from an SSID:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Overview, select **Connections**.

   The page that displays shows the Connection List - 2.4GHz table and the Connection List - 5GHz table.

   For more information, see Display the WiFi connections on page 116.

5. To block a client or device, click the associated **Kick** button in the Block column on the right.

A pop-up window opens.

6. Click the **OK** button.
   The client no longer displays on the page, but the automatically created ACL is not yet saved.
   A pop-up window opens. The window shows the number of changes to be applied.
7. Click the **Apply** button.
   Your settings are saved and applied. The WiFi connection is reestablished. The page displays the number of seconds before the access point is back online.

Change the DHCP server settings for guest WiFi networks

By default, a WiFi client that connects to a guest network (see Configure a guest network on an SSID on page 57) is assigned an IP address in the range from 192.168.200.100 to 192.168.200.200. You can change this address range, which applies to all WiFi guest networks on the access point.

You can change the DHCP server settings for a guest network only if you enabled at least one guest network on an SSID.

To change the DHCP server settings for guest WiFi network:s

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.
   A login window displays.
   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.
   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.
   The Device Status page displays.

4. Under Network, select **Wireless**.
   The Wireless Settings page displays.
5. Scroll down to the Guest Network DHCP Server Settings section.
   You can change the DHCP server settings for a guest network only if you enabled at least one guest network on an SSID. Otherwise, the fields are masked out.
6. Configure the settings that are described in the following table, keeping in mind that the IP address, starting IP address, and ending IP address must be in the same range.
   The manual IP settings define the IP address and subnet mask for the DHCP server. The automatic DHCP server settings define the range of IP addresses from which the DHCP server automatically assigns an IP address.

Setting	Description
Manual IP Settings	
IP Address	The IP address for the guest network. The default IP address is 192.168.200.1.
Subnet Mask	The subnet mask associated with the IP address. The default subnet mask is 255.255.255.0.
Automatic DHCP Server Settings	
Starting IP Address	The starting IP address in the address range from which a WiFi client on a guest network can be assigned an IP address. The default starting IP address is 192.168.200.100.
Ending IP Address	The ending IP address in the address range from which a WiFi client on a guest network can be assigned an IP address. The default ending IP address is 192.168.200.200.
WINS Server IP	The IP address of an optional Windows Internet Name Service.

7. Click the **Save** button.
   Your settings are saved but not yet applied.
   A pop-up window displays. The window shows the number of changes to be applied.
8. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

8

Maintain the access point

This chapter describes how you can maintain the access point.

The chapter includes the following sections:

Upgrade the firmware

You can visit the NETGEAR support website to determine if new firmware is available for the access point.

If new firmware is available, download the firmware file to your computer. If needed, unzip the firmware file. Then, update the access point to the new firmware.

Note: Before you upgrade the firmware, we recommend that you read the firmware release notes, if available. Although it is highly unlikely, a situation might occur that requires you to reconfigure the access point after a firmware upgrade.

To upgrade the firmware on the access point:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under System Manager, select **Firmware**.

   The page displays the Firmware Upgrade section and the Backup/Restore Settings section.

   The current firmware version and the device version display.

5. Locate and select the firmware file on your computer by doing the following:
   a. In the Firmware Upgrade section, click the **Choose File** button.
   b. Navigate to the firmware file.
      The filename ends in `.bin`.

c. Select the firmware file.

6. Click the **Upload** button.
   The page displays the upgrade progress.

   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.

   When the upgrade is finished, the login page displays. The firmware version displays on the login page.

Reboot the access point from the local browser UI

You can use the local browser UI to reboot the access point. This is useful if the access point is installed at a location that is not easy to reach.

To reboot the access point from the local browser UI:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. At the top right of the page, select the **Reset** tab.

The page displays the Reboot the device section and the Restore the device to default settings section.

5. Click the **Reboot the device** button.
   The page displays the reboot progress.

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

   When the reboot is finished, the login page displays.

Schedule the access point to reboot

You can schedule the access point to automatically reboot at a time that is convenient for the network, for example, when you do not expect any WiFi traffic to be processed.

To schedule the access point to automatically reboot:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.
4. Under Management, select **WiFi Scheduler**.
   A page displays the Auto Reboot Settings section and the Wi-Fi Scheduler section.
5. In the Auto Reboot Settings section, select the Status **Enable** radio button.

6. Select one or more check boxes for the days on which you want the access point to automatically reboot.
7. In the fields under the days, use the 24-hour clock format to enter the hour in the left field (for example, enter **23** for 11 p.m.) and the minutes in the right field (for example, enter **30** for 11:30 p.m.).
8. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window displays. The window shows the number of changes to be applied.
9. In the pop-up window, click the **Apply** button.

   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Back up or restore the configuration file

The configuration settings of the access point are stored within the access point in a configuration file. You can back up (save) this file to your computer. After you do so, you can restore the configuration from the file.

Back up the access point configuration settings

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. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

The local device password is the one that you specified. The password is case-sensitive.

The Device Status page displays.

4. Under System Manager, select **Firmware**.
   The page displays the Firmware Upgrade section and the Backup/Restore Settings section.
5. In the Backup/Restore Settings section, click the Backup Settings **Export** button.
   A pop-up window opens.
6. Choose a location to store the file on your computer.
   The name of the backup file is `backup-NETGEARXXXXXX-yyyy-mm-dd.tar.gz`, in which XXXXXX represents the last six digits of the MAC address of the access point (unless you changed the AP name, which is also referred to as the device name), yyyy is the year, mm is the month, and dd is the date.

   An example of a name of a backup file is `backup-NETGEARFFFDB7-2020-11-16.tar.gz`.
7. Follow the directions of your browser to save the file.

Restore the access point configuration settings

If you backed up the configuration settings (see Back up the access point configuration settings on page 93), you can restore the configuration settings from the backup file.

To restore the access point's configuration settings from the backup file:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

The local device password is the one that you specified. The password is case-sensitive.

The Device Status page displays.

4. Under System Manager, select **Firmware**.
   The page displays the Firmware Upgrade section and the Backup/Restore Settings section.

5. In the Backup/Restore Settings section, click the Restore New Setting **Choose File** button and navigate to and select the saved configuration file (that is, the backup file).
   The name of the backup file is `backup-NETGEARXXXXXX-yyyy-mm-dd.tar.gz`, in which XXXXXX represents the last six digits of the MAC address of the access point (unless you changed the AP name, which is also referred to as the device name), yyyy is the year, mm is the month, and dd is the date.

   An example of a name of a backup file is `backup-NETGEARFFFDB7-2020-11-16.tar.gz`.

6. Click the **Import** button.
   The page displays the restoration progress.

   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.

   When the restoration is finished, the login page displays.

Reset the access point to factory default settings

Under some circumstances (for example, if you lost track of the changes that you made to the configuration of the access point 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 (see Factory default settings on page 137).

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

You can use either the physical **Reset** button on the back panel of the access point (see Hardware interfaces model WAX214 on page 13 or Hardware interfaces model WAX218 on page 18) or the software **Reset** button in the local browser UI.

After you reset the access point to factory default settings, the LAN IP address is https://192.168.0.100 (https://www.aplogin.net), the access point's DHCP client is enabled, the default management SSID is shown in the format WAX214XXXXXX-CONFIG-ONLY or WAX218XXXXXX-CONFIG-ONLY (in which XXXXXX represents the last six digits of the MAC address of the access point), and the default password for WiFi access is a unique WiFi password that is printed on the access point label. For a list of factory default settings, see Factory default settings on page 137.

To reset the access point to factory default settings using the local browser UI:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under System Manager, select **Firmware**.

   The page displays the Firmware Upgrade section and the Backup/Restore Settings section.

5. In the Backup/Restore Settings section, click the Reset to Default **Reset** button.

   The page displays the reset progress.

   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.

   When the reset is finished, the address bar of your web browser might display 192.168.0.100, which is the default IP address of the access point and the same as www.aplogin.net.

6. If your access point used a non-default IP address before you reset it to factory default settings (for example, an IP address assigned by the DHCP server in your network), enter *that* IP address in the address bar.

   If you do not know the IP address, see Find the IP address of the access point on page 33.

   The Day Zero page displays. You can now reconfigure the access point.

Manage the date and time settings

By default, the access point is configured to automatically get the date and time from an Network Time Protocol (NTP) server that is preconfigured.

You can also manually set the date and time, configure a time zone, and specify daylight saving time settings.

To manage the date and time settings:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Management, select **Time Zone**.

   The page that displays shows the Date and Time Settings section and the Time Zone section.

5. To configure the date and time, in the Date and Time Settings section, select one of the following radio buttons:
   - **Manually Set Date and Time**: Specify the date and time settings by doing *one* of the following:
     - Enter the setting manually by doing the following:
       a. In the **Date** fields, specify the year, month, and date.
       b. In the **Time** fields, specify the hour and minutes.
          Use 24-hour format.
     - Synchronize the date and time setting with the computer from which you log in to the local browser UI of the access point by clicking the **Synchronize with PC** button.
   - **Automatically Get Date and Time**: The access point automatically gets the date and time from the Network Time Protocol (NTP) server that is specified in the **NTP Server** field.
     This is the default setting. You can specify a different NTP server from the one that is preconfigured.
6. To configure a time zone, in the Time Zone section, select a time zone from the **Time Zone** menu.
   If you manually select a time zone, you can also manually configure daylight saving time settings (see the next step).
7. To manually enable and configure daylight saving time settings, in the Time Zone section, do the following:
   a. Select the **Enable Daylight Saving** check box.
   b. From the **Start** menus, select the month, day, and time that daylight saving time must start.
   c. From the **End** menus, select the month, day, and time that daylight saving time must end.
8. Click the **Apply** button.
   Your settings are saved and applied.

SNMPv1, SNMPv2, and SNMPv3

The access point supports Simple Network Management Protocol (SNMP), which lets SNMP network management software such as HP OpenView access and manage the

access point by using the SNMPv1, SNMPv2, or SNMPv3 protocol. By default, SNMP is disabled on the access point.

SNMPv1 and SNMPv2 support groups that can manage traps that the SNMP agent generates. SNMPv3 supports users that can do the same but can provide a higher level of security through authentication and encryption.

Enable SNMPv1 and SNMPv2 and manage the settings

You can enable SNMPv1 and SNMPv2 and manage the associated settings for the access point:

To enable SNMPv1 and SNMPv2 and manage the settings:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Management, select **Advanced**.

   The page displays the advanced settings with the Management Mode section at the top.

5. In the SNMP Settings section, select the Status **Enable** radio button.

   By default, the SNMP settings are masked out and the Status **Disable** radio button is selected.

6. Configure the SNMPv1 and SNNPv2 settings as described in the following table:

Setting	Description
Contact	The contact name for SNMP management. This is an optional field for information only.
Location	The location for SNMP management. This is an optional field for information only.
Community Name (Read Only)	The community string that enables the SNMP management station to read the access point's MIB objects. The default is public.
Community Name (Read Write)	The community string that enables the SNMP management station to read and write the access point's MIB objects. The default is private.
Port	The port number at which the SNMP management station must receive traps. The default is 162.
IP Address	The IP address of the SNMP management station that must receive traps.
Community Name	The community name that is associated with the IP address that must receive traps. The default is public.

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

Enable SNMPv3 and manage the settings

You can enable SNMPv3 and manage the associated settings for the access point:

To enable SNMPv3 and manage the settings:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

The local device password is the one that you specified. The password is case-sensitive.

The Device Status page displays.

4. Under Management, select **Advanced**.
   The page displays the advanced settings with the Management Mode section at the top.
5. In the SNMP Settings section, select the Status **Enable** radio button.
   By default, the SNMP settings are masked out and the Status **Disable** radio button is selected.
6. Scroll down to the SNMPv3 Settings section and select the Status **Enable** radio button.
   By default, even if you enabled the SNMP settings (see the previous step), the SNMPv3 settings are masked out and the Status **Disable** radio button is selected.
7. Configure the SNMPv3 settings as described in the following table:

Setting	Description
Username	Specify a name for the SNMPv3 user account. The name can be from 1 to 31 characters.
Authorized Protocol	From the **Authorized Protocol** menu, select one of the following options for authentication: • **MD5**: The MD5 message-digest algorithm is used for authentication. You must specify an authentication key for SNMPv3 access (see the Authorized Key). • **SHA**: Secure Hash Algorithms (SHA) is used for authentication. You must specify an authentication key for SNMPv3 access (see the Authorized Key). • **None**: A user cannot access SNMPv3 information from an SNMP browser.
Authorized Key	If you select **MD5** or **SHA** from the **Authorized Protocol** menu, specify an authorization key (password) in the **Authorized Key** field. The key can be from 8 to 32 characters.
Private Protocol	From the **Private Protocol** menu, select one of the following options for encryption: • **DES**: The information is encrypted with Data Encryption Standard (DES). You must specify an encryption key for the SNMP traffic. • **None**: The SNMP traffic is not encrypted.

(Continued)

Setting	Description
Private Key	If you select **DES** from the **Private Protocol** menu, specify an encryption key (password) in the **Private Key** field. The key can be from 8 to 32 characters.
Engine ID	Specify the unique ID that identifies the SNMP management station.

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

Logs

The access point generates messages in response to events, faults, errors, changes in configuration, and other occurrences. The messages are stored locally. In addition, you can configure the access point to forward the messages to a remote server for monitoring purposes or long-term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on their severity.

View and manage the system log

The system log stores messages in memory based on the severity of an event. You can view these messages and specify the event severity that the access point logs. You can also download the messages and clear the message log.

To view and manage the system log:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under System Manager, select **Log**.
   The System Log page displays. You can view the log messages.

5. To manage the log capability, select one of the following Status radio buttons:

   - **Enable**: The access point log messages.
     This is the default settings.
   - **Disable**: The access point does not log messages.

6. To select the event severity that the access point logs, from the **Log type** menu, select one of the following severity levels:

   - **ALL**: All events are logged. This is the default setting. A large number of events might be logged.
   - **Debug**: Events that provide very detailed device information, down to the debugging level, are logged.
   - **Information**: Events that provide device information are logged.
   - **Notice**: Normal but significant device events are logged.
   - **Warning**: The lowest level of device warnings are logged.
   - **Error**: Device errors are logged. An example is a failure to request a device token.
   - **Critical**: The third-highest device warning level. An critical event is logged if a critical device malfunction occurs.
   - **Alert**: The second-highest warning level. An alert event is logged if a serious device malfunction occurs, such as all device features being down. Action must be taken immediately.
   - **Emergency**: The highest warning level. If the device is down, or not functioning properly, an emergency event is logged.

   Note: Events with the selected severity level and all events of greater severity are logged. For example, if you select Error, the logged events include Error, Critical, Alert, and Emergency.

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

8. To refresh the information on the page, click the **Refresh** button.
   The page refreshes and displays the most recent log messages.
9. To download the log file to your computer, click the **Download** button, and save the log file to a location on your computer.
10. To clear the log, click the **Clear** button.
    The pages refreshes and all log messages are cleared.

Set up a remote log server

You can let the access point send log messages to a remote log server, which is also referred to as a remote syslog host.

You can also let the access point send the traffic log to the remote log server. (The traffic log is too large to be stored locally on the access point.)

To set up a remote log server:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.
4. Under System Manager, select **Log**.
   The System Log page displays.
5. To manage the remote log server capability, select one of the following Remote Log radio buttons:
   - **Enable**: The access point sends log messages to a remote log server.

You must specify the IP address of the remote log server (see Step 7).

- **Disable**: The access point does not send log messages to a remote log server. This is the default settings.

6. If the remote log server capability is enabled, to manage whether the traffic log is sent to the remote log server, select one of the following Traffic Log radio buttons:
   - **Enable**: The access point sends its traffic log to the remote log server.
   - **Disable**: The access point does not send its traffic log to the remote log server. This is the default settings.
7. In the **Log Server IP Address** field, enter the IP address of the remote log server.
8. In the **Log Server Port** field, enter the port number that the access point uses to contact the remote log server.
   By default, the port number is 514.
9. Click the **Apply** button.
   Your settings are saved and applied.

Set up email alerts

You can specify an email address to which the access point automatically can send an alerts when the configuration of the access point is changed.

To set up email alerts:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.
   A login window displays.
   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.
   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

The local device password is the one that you specified. The password is case-sensitive.

The Device Status page displays.

4. Under Management, select **Advanced**.
   The page displays the advanced settings with the Management Mode section at the top.
5. In the Email Alert section, configure the following settings:
   a. Select the Status **Enable** check box.
      The field and menus become available.
   b. In the **From** field, enter the originating email address.
   c. In the **To** field, enter the email address of the recipient.
   d. In the **Subject** field, enter the subject information of the email or leave the default subject information.
      The subject information depends on the model and the MAC address, indicated in the following default subject information by [XX:XX:XX:XX:XX:XX]:
      - **WAX214**: *[Email-Alert][WAX214][XX:XX:XX:XX:XX:XX] Configuration Changed*
      - **WAX218**: *[Email-Alert][WAX218][XX:XX:XX:XX:XX:XX] Configuration Changed*.
   e. In the **Username** field, enter the user name to access the originating email account.
   f. In the **Password** field, enter the password to access the originating email account.
   g. In the **SMTP Server** field, enter the name of the outgoing email server name.
   h. In the **Port** field, enter the port number that the access point uses to contact the SMTP server.
      By default, the port number is 25.
   i. From the **Security Mode** menu, select one of the following options, depending on the security that the SMPT server uses:
      - **None**: The SMPT server does not use security. This is the default setting.
      - **SSL/TLS**: The SMPT server uses the SSL or TLS security protocol
      - **STARTTLS**: The SMPT server uses the STARTTLS security protocol.
6. To send a test email, click the **Send Test Mail** button.
7. Verify that the recipient receives the email.
8. Click the **Apply** button.
   Your settings are saved and applied.

Change the local device password

The local device password is the password that lets you log in to the local browser UI.

When you performed the initial configuration on the Day Zero page, you were required to change the local device password. You can change it again.

We recommend that your password meets the following conditions:

- Contains 8 to 32 characters
- Contains no more than two identical characters in a row

In addition, we recommend that your password meets at least three of the following four conditions:

- At least one uppercase character
- At least one lowercase character
- At least one number
- At least one special character, such as the following characters:
  @ # $ % ^ & * ( ) !

To change the local device password:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under System Manager, select **Account**.
   The Account Settings page displays.
5. In the **Current Password** field, enter your current local login password.
6. In the **New Password** and **Verify Password** fields, enter the new local login password.
7. Click the **Apply** button.
   Your settings are saved and applied.

You are logged out from the local browser UI. If you log in again, use your new local device password.

Specify an existing management VLAN

By default, you can access the local browser UI from any VLAN and management traffic such as traffic from a DHCP server can reach the access point from any VLAN. That is, management traffic is untagged.

For additional security, you can specify an existing management VLAN ID so that you can access the local browser UI from this VLAN only and management traffic can reach the access point over this VLAN only. That is, the management traffic is tagged with the VLAN ID.

CAUTION: The VLAN must be defined on your network, and the DHCP server, switch, and router to which the access point is connected must be able to reach the access point over this VLAN. Otherwise, when you change the VLAN, connectivity problems might occur, and you might be locked out from the local browser UI.

To specify an existing management VLAN for the access point:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.
   The Device Status page displays.
4. Under Network, select **Wireless**.
   The Wireless Settings page displays.
5. Scroll to the Management VLAN Setting section at the bottom of the page.
6. Click the Status **Enable** radio button.
7. In the field that becomes available, enter the ID of the management VLAN.
8. Click the **Save** button.
   Your settings are saved but not yet applied.
   A pop-up window displays. The window shows the number of changes to be applied.
9. In the pop-up window, click the **Apply** button.
   Your changes are applied. If the WiFi link must be reestablished, the page displays the number of seconds before the access point is back online.

Control the LEDs

By default, all LEDs are enabled and function as described in Top panel with LEDs for model WAX214 on page 12 or Top panel with LEDs for model WAX218 on page 17. You can manage whether the LEDs light at all. This function is useful if you want the access point to function in a dark environment.

To control the LEDs:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.
   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.
   A login window displays.

If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.
   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Management, select **Tools**.
   By default, the Ping tab is selected and the Ping Test Parameters page displays.

5. Select the **LED** tab.
   The LED Control page displays.

6. To control the Power LED, select one of the following Power radio buttons:
   - **Enable**: The Power LED is enabled. This is the default setting.
   - **Disable**: The Power LED is disabled and turned off.

7. To control the 5 GHz WLAN, 2.4 GHz WLAN, and LAN LEDs, select one of the following Other radio buttons:
   - **Enable**: The 5 GHz WLAN, 2.4 GHz WLAN, and LAN LEDs are enabled. This is the default setting.
   - **Disable**: The 5 GHz WLAN, 2.4 GHz WLAN, and LAN LEDs are disabled and turned off.

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

9

Monitor the access point and its Network Connections

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

The chapter includes the following sections:

Display the access point device, memory, LAN, and WiFi status information

You can display access point device information, memory information, Ethernet LAN information for IPv4 and IPv6, WiFi LAN information, and statistics.

To display the access point device status and other information:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.
4. To refresh the information on the page, click the **Refresh** button.

   The following tables describe the information on the page.

Table 4. Device Information section

Setting	Description
AP Name	The device name (system name). For more information, see Change the device name on page 47.
Serial Number	The fixed serial number of the access point.
MAC Address LAN	The fixed MAC address of the LAN/PoE (model WAX214) or LAN/PoE+ (model WAX218) port.

Table 4. Device Information section (Continued)

Setting	Description
MAC Address Wireless LAN - 2.4GHz	The fixed MAC address of the 2.4 GHz radio interface.
MAC Address Wireless LAN - 5GHz	The fixed MAC address of the 5 GHz radio interface.
Country	The country and region that you set for the access point operation. For more information, see Change the country and region of operation on page 48.
Current Local Time	The time that the access point detected. For more information, see Manage the date and time settings on page 97.
Uptime	The period since that last time the access point started or rebooted.
Firmware Version	The firmware version. For more information, see Upgrade the firmware on page 90.
Device Version	The device version.
Management VLAN ID	Shows whether management traffic is tagged or untagged. For more information, see Specify an existing management VLAN on page 108.
LAN Speed	The speed of the LAN/PoE (model WAX214) or LAN/PoE+ (model WAX218) port.

Table 5. Memory Information section

Setting	Description
Total Available	The total memory in kB and the available memory in kB and percentage. **Note**: 1 kB = 1 kilobyte = 1000 bytes.
Free	The total memory in kB and the free memory in kB and percentage.

Table 5. Memory Information section (Continued)

Setting	Description
Cached	The total memory in kB and the cached memory in kB and percentage.
Buffered	The total memory in kB and the buffered memory in kB and percentage.

Table 6. LAN Information - IPv4 section

Setting	Description
IP Address	The IPv4 address that is assigned to the LAN/PoE (model WAX214) or LAN/PoE+ (model WAX218) port of the access point. This is the IPv4 address over which you can reach the local browser UI. For more information, see Specify a static IPv4 address on page 40.
Subnet Mask	The subnet mask that is associated with the IPv4 address.
Gateway	The IPv4 address of the gateway.
Primary DNS	The IPv4 address of the primary DNS server.
Secondary DNS	The IPv4 address of the secondary DNS server, if any.
DHCP Client	Shows whether the DHCP client of the access point is enabled (which it is by default). For more information, see Reenable the DHCP client of the access point on page 42.
Spanning Tree Protocol (STP)	Shows whether STP is enabled. For more information, see Manage the STP settings on page 43.

Table 7. LAN Information - IPv6 section

Setting	Description
IP Address	The IPv6 address that is assigned to the LAN/PoE (model WAX214) or LAN/PoE+ (model WAX218) port of the access point. This is the IPv6 address over which you can reach the local browser UI.
Link-Local Address	The link-local IPv6 address of the access point. For more information, see Specify a link-local IPv6 address on page 41.
Gateway	The IPv6 address of the gateway.

Table 7. LAN Information - IPv6 section (Continued)

Setting	Description
Primary DNS	The IPv6 address of the primary DNS server.
Secondary DNS	The IPv6 address of the secondary DNS server, if any.

Table 8. Wireless LAN Information - 2.4GHz section

Setting	Description
Wireless Mode	The WiFi mode, which is fixed at 802.11 ax/n/g/b.
Channel Bandwidth	The WiFi channel bandwidth. For for information, see Manage the channel high throughput mode on page 64.
Channel	The WiFi channel. For for information, see Manage the channel or channels on page 65.

Table 9. Wireless LAN Information - 5GHz section

Setting	Description
Wireless Mode	The WiFi mode, which is fixed at 802.11 ax/ac/n/a.
Channel Bandwidth	The WiFi channel bandwidth. For for information, see Manage the channel high throughput mode on page 64.
Channel	The WiFi channel. For for information, see Manage the channel or channels on page 65.

Table 10. Statistics Access Point 2.4GHz/5GHz section

Setting	Description
Profile	The profile number from 1 to 5, including the 2.4 GHz management SSID.
SSID	The WiFi network name.
Security	The type of WiFi security on the SSID.
VID	The VLAN ID, if any, that is configured for the SSID.

Table 10. Statistics Access Point 2.4GHz/5GHz section (Continued)

Setting	Description
802.1Q	Shows whether VLAN isolation is enabled.
RX (Packets)	The amount of packets in Bytes and the number of packets that is received on the SSID.
TX (Packets)	The amount of packets in Bytes and the number of packets that is transmitted on the SSID.

Display the WiFi connections

You can display the WiFi connections on each radio.

To display the WiFi connections:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.
4. Under Overview, select **Connections**.

   The page that displays shows the Connection List - 2.4GHz table and the Connection List - 5GHz table.

Table 11. Connected WiFi device information

Setting	Description
SSID	The SSID to which the WiFi device is connected.
MAC Address	The MAC address of the connected WiFi device.
TX (KB)	The total amount of traffic in kilobytes that the WiFi device transmitted.
RX (KB)	The total amount of traffic in kilobytes that the WiFi device received.
RSSI (dBm)	The received signal strength indicator (RSSI) for the WiFi device. The RSSI is expressed in decibel-milliwatts (dBm).
Block	For more information, see Manually block a WiFi client or connection from an SSID on page 86.

5. To block (*kick*) a connected WiFi device, do the following:
   a. Click the associated **Kick** button in the Block column on the right.
      A pop-up window opens.
   b. Click the **OK** button.
      The WiFi device no longer displays on the page. An ACL that denies the MAC address of the WiFi device is automatically added to the SSID from which you blocked the WiFi device. This ACL denies access to the WiFi device but allows access all other WiFi devices. (For more information, see Set up a MAC filter for an SSID on page 84.)
      A pop-up window opens. The window shows the number of changes to be applied. (The automatically-created ACL is not saved until you click the **Apply** button.)
   c. Click the **Apply** button.
      Your settings are saved and applied. The WiFi connection is reestablished. The page displays the number of seconds before the access point is back online.
6. To refresh the information on the page, click the **Refresh** button.

Display the CPU, SSID, and LAN traffic loads

You can display the CPU, SSID, and LAN traffic loads on the access point.

To display the CPU, SSID, and LAN traffic loads:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.
4. Under Overview, select **Realtime**.

   The page that displays shows the CPU load, that is, by default, the Load tab is selected.

   The page displays the current, average, and peak CPU traffic load, each of which is expressed in a percentage, is updated every three seconds, and covers a maximum period of three minutes.
5. Select the **Traffic** tab.

   The page displays a tab for each active SSID and for the LAN.

   If only one SSID is active, the traffic information for the SSID displays (see the information in the next step).
6. To display the traffic information for an SSID, select the tab for the SSID.

   The page displays traffic information for the SSID.

   For each radio band (2.4 GHz and 5 GHz), a graph displays the traffic load, which is updated every three seconds and covers a maximum period of three minutes.

For each radio band, the page also displays the current inbound and outbound traffic loads, the average inbound and outbound traffic loads, and the peak inbound and outbound traffic loads, each of which is expressed in kilobytes per second (KB/s), is updated every three seconds, and covers a maximum period of three minutes.

7. To display the traffic information for the wired connection, select the **LAN** tab.

   The page displays traffic information for the LAN/PoE (model WAX214) or LAN/PoE+ (model WAX218) port, including the current inbound and outbound traffic loads, the average inbound and outbound traffic loads, and the peak inbound and outbound traffic loads, each of which is expressed in kilobytes per second (KB/s), is updated every three seconds, and covers a maximum period of three minutes.

10

Perform Diagnostics and Troubleshooting

This chapter describes how you can perform diagnostics and troubleshoot access point and its network connections.

The chapter includes the following sections:

Send a ping

The access point can ping the IPv4 or IPv6 address of a device or network location and display the results. You can use this option to check whether the access point can communicate with a particular IPv4 or IPv6 device or network location.

To send a ping:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.
4. Under Management, select **Tools**.

   By default, the Ping tab is selected and the Ping Test Parameters page displays.
5. In the **Target IP / Domain Name** field, enter the IP address that the access point must ping.
6. In the **Ping Packet Size** field, enter the size in bytes of the each ping packet.

   The default size is 64 bytes.
7. In the **Number of Pings** field, enter the number of ping packets that the access point must send.

   The default number is 4.
8. Click the **Start** button.

   The access point sends the ping. The results display on the page.

Send a traceroute request

The access point can send a traceroute request to an IPv4 or IPv6 address or host name and display the results. You can use this option to discover the paths that packets take to a remote destination.

To send a traceroute request:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.
3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.
4. Under Management, select **Tools**.

   By default, the Ping tab is selected and the Ping Test Parameters page displays.
5. Select the **Traceroute** tab.

   The Traceroute Test Parameters page displays.
6. In the **Target IP / Domain Name** field, enter the IP address or domain name for which you want to send a traceroute request.
7. Click the **Start** button.

   The access point sends the traceroute request. By default, the traceroute request consists of a 38-byte packet and can detect a maximum of 30 hops. The results display on the page.

Send a name server lookup request

The access point can send a domain name server lookup (nslookup) request to an IP address or host name and display the results. You can use this option to discover the domain name of an IP address or, the other way around, the IP address of a domain name.

To send a name server lookup request:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Management, select **Tools**.

   By default, the Ping tab is selected and the Ping Test Parameters page displays.

5. Select the **Nslookup** tab.

   The Nslookup Test Parameters page displays.

6. In the **Target IP / Domain Name** field, enter the IP address or domain name for which you want to send a name server lookup request.
7. Click the **Start** button.

   The access point sends the name server lookup request. The results display on the page.

Perform a speed test

You can perform a speed test for a point-to-point link between the access point and a WiFi client and display the results of the speed test. The maximum WiFi speed that the access point can measure is 100 Mbps. You can also use this option to determine the general WiFi network performance.

To perform a speed test:

1. Launch a web browser from a computer or mobile device that is directly connected over WiFi to the access point or connected to the same network as the access point.
2. Enter the IP address that is assigned to the access point.

   If you are directly connected to the "CONFIG-ONLY" SSID, you can enter **https://www.aplogin.net**.

   A login window displays.

   If you do not know the IP address, see Find the IP address of the access point on page 33. For more information about the "CONFIG-ONLY" SSID, see 2.4 GHz management SSID on page 58.

   If your browser does not display a login window but displays a security message and does not let you proceed, see Log in to the access point after you complete the initial log-in process on page 35.

3. Enter the access point local device password and click the **Login** button.

   The local device password is the one that you specified. The password is case-sensitive.

   The Device Status page displays.

4. Under Management, select **Tools**.

   By default, the Ping tab is selected and the Ping Test Parameters page displays.

5. Select the **Speed Test** tab.

   The Speed Test Parameters page displays.

6. In the **Target IP / Domain Name** field, enter the IP address or domain name for which you want to perform a speed test.
7. In the **Time Period** field, enter the duration in seconds of the entire speed test.

   The default is 20 seconds.

8. In the **Check Interval** field, enter the interval in seconds between the intermediate throughput results.

   The default is 5 seconds.

The **IPv4 Port** field is fixed at port number 5201. The **IPv6 Port** field is fixed at port number 60001.

9. Click the **Start** button.
   The access point performs the speed test. The results display on the page.

Quick tips for WiFi troubleshooting

If one or more WiFi networks do not function normally, consider to repower your access point:

1. Unplug the Ethernet cable from the access point to your network switch.
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. Wait two minutes.
4. If you use a power adapter, connect it to the access point. Wait two minutes.

If someone cannot connect with a WiFi device to the access point, try the following:

- **Is a WLAN LED off?** Make sure that one or both WLAN LEDs on the access point are on:
  - **Both WLAN LEDs are off**: If both WLAN LEDs are off and you did not disable the LEDs (see Control the LEDs on page 109), the WiFi radios are probably off too. For more information about enabling or disabling the WiFi radios, see Set up a WiFi on/off schedule for an SSID on page 75.
  - **One WLAN LED is off**: If only one WLAN LED is off, the associated radio band (2.4 GHz or 5 GHz) is probably disabled on all active WiFi networks (SSIDs). For example, if the 5 GHz WLAN LED is off but the 2.4 GHz WLAN LED is lighting, the 5 GHz radio band is probably disabled for each active SSID. For more information, see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page 49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53.

- **Do the WiFi settings match?** Make sure that the WiFi settings in the WiFi device and access point match exactly and that the radio band (2.4 GHz or 5 GHz) over which the device is trying to connect is broadcasting for the SSID.
  The SSID and WiFi security settings of the access point and WiFi device must match exactly. For more informations about these settings and the radio bands, see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page 49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53.

- **Is the type of security supported?** Make sure that the WiFi device supports the authentication and encryption that is configured for the SSID. For more information, see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page 49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53.

  Note: If the access point's WiFi authentication and encryption is set to WPA3 Personal, make sure that the WiFi adapter device driver is updated to the latest version on the WiFi device.

- **Is the device blocked in a MAC filter?** Make sure that the WiFi device is not on a MAC filter (access control list) that blocks access to the device (see Set up a MAC filter for an SSID on page 84).
- **Is the device at the wrong location?** Make sure that the WiFi device is not too far from the access point or too close. To see if the signal strength improves, move the WiFi device near the access point but at least 6 feet (1.8 meters) away.
- **Is the WiFi signal blocked?** Make sure that the WiFi signal is not blocked by objects between the access point and the WiFi device.
- **Is the SSID hidden?** If the access point's SSID broadcast is disabled, the WiFi network name is hidden and does not display in the WiFi device's scanning list.
  To connect to a hidden network, the user must know and enter both the network name and the WiFi password. For more information about the SSID broadcast, see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page 49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53.
- **Does the device functions as a DHCP client?** Make sure that the 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.)

Troubleshoot with the LEDs

For general information about the LEDs and LED icons, see Top panel with LEDs for model WAX214 on page 12 or Top panel with LEDs for model WAX218 on page 17.

When you connect the access point to a power source, if you did not disable the LEDs (see Control the LEDs on page 109), the LEDs light as described here:

1. The Power LED lights solid amber.
2. After about two minutes, the 5 GHz WLAN, 2.4 GHz WLAN, and LAN LEDs light solid blue or are blinking blue.

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

- Power LED remains off on page 127
- 2.4 GHz WLAN LED, 5 GHz WLAN LED, or both WLAN LEDs are off on page 128
- LAN LED is off in a setup with a power adapter on page 128

Power LED remains off

IMPORTANT: If you do not use a power adapter, model WAX214 requires PoE power, and model WAX218 requires PoE+ power.

PoE or PoE+ connection: If you use a PoE (model WAX214) or PoE+ (model WAX218) connection and the Power LED and other LEDs remain off when you connect the Ethernet cable to a PoE or PoE+ switch, do the following:

- Make sure that the LEDs are not disabled (see Control the LEDs on page 109).
- Make sure that the Ethernet cable between the access point and the PoE or PoE+ switch is correctly connected at both ends.
- Make sure that the other end of the Ethernet cable is plugged into a PoE or PoE+ port.
- Make sure that the switch is actually receiving power.
- Make sure that the PoE power budget of the PoE or PoE+ switch is not oversubscribed so that the switch is capable of delivering PoE or PoE+ power to the access point.

Power adapter: If you use a power adapter and the Power LED and other LEDs remain off when you provide power to the access point, do the following:

- Make sure that the LEDs are not disabled (see Control the LEDs on page 109).
- 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 plugged into 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 correct NETGEAR power adapter for this product. That is, do not use the power adapter for another NETGEAR product or a third-party power adapter.

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.

2.4 GHz WLAN LED, 5 GHz WLAN LED, or both WLAN LEDs are off

If the 2.4 GHz WLAN LED, 5 GHz WLAN LED , or both WLAN LEDs are off, do the following:

- **Both WLAN LEDs are off**: If both WLAN LEDs are off and you did not disable the LEDs (see Control the LEDs on page 109), the WiFi radios are probably off too. For more information about enabling or disabling the WiFi radios, see Set up a WiFi on/off schedule for an SSID on page 75.
- **One WLAN LED is off**: If only one WLAN LED is off, the associated radio band (2.4 GHz or 5 GHz) is probably disabled on all active WiFi networks (SSIDs). For example, if the 5 GHz WLAN LED is off but the 2.4 GHz WLAN LED is lighting, the 5 GHz radio band is probably disabled for each active SSID. For more information, see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page 49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53.

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

LAN LED is off in a setup with a power adapter

If the LAN LED is off when you use a power adapter to provide power to the access point and you did not disable the LEDs (see Control the LEDs on page 109), check the following:

- Make sure that the Ethernet cable connectors are securely plugged in at the access point LAN/PoE (model WAX214) or LAN/PoE+ (model WAX218) port 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.

Note: Unless you disabled the LEDs, both the Power LED and the LAN LED light when the access point receives power through its PoE port (model WAX214) or PoE+ port (model WAX218). If these LEDs do not light when you connect an Ethernet cable, see Power LED remains off on page 127.

Troubleshoot the WiFi connectivity

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

A WiFi device cannot connect to the access point

If a WiFi device cannot connect to the access point or the WiFi connectivity is not normal, try to isolate the problem:

- **Do the SSID, WiFi security, and radio band settings match?** Make sure that the WiFi settings in the WiFi device and access point match exactly and that the radio band (2.4 GHz or 5 GHz) over which the device is trying to connect is broadcasting for the SSID.
  The SSID and WiFi security settings of the access point and WiFi device must match exactly. For more informations about these settings and the radio bands, see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page 49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53.
- **Does the WiFi device support the type of security?** Make sure that the WiFi device supports the authentication and encryption that is configured for the SSID. For more information, see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page 49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53.

  Note: If the access point's WiFi authentication and encryption is set to WPA3 Personal, make sure that the WiFi adapter device driver is updated to the latest version on the WiFi device.

- **Can the WiFi device find the access point**?
  - **Are both WLAN LEDs off?** If both WLAN LEDs are off and you did not disable the LEDs (see Control the LEDs on page 109), the WiFi radios are probably off too. For more information about enabling or disabling the WiFi radios, see Set up a WiFi on/off schedule for an SSID on page 75.
  - **Is one WLAN LED off?** If only one WLAN LED is off, the associated radio band (2.4 GHz or 5 GHz) is probably disabled on all active WiFi networks (SSIDs). For example, if the 5 GHz WLAN LED is off but the 2.4 GHz WLAN LED is lighting, the 5 GHz radio band is probably disabled for each active SSID. For more information, see Configure a WiFi network that is open or secured with WPA2 or

WAP3 personal security on page 49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53.

- **Is the SSID hidden?** If the access point's SSID broadcast is disabled, the WiFi network name is hidden and does not display in the WiFi device's scanning list. To connect to a hidden network, the user must know and enter both the network name and the WiFi password. For more information about the SSID broadcast, see Configure a WiFi network that is open or secured with WPA2 or WAP3 personal security on page 49 or Configure a WiFi network that is secured with WPA2 or WAP3 enterprise security on page 53.

- **Does your network includes many legacy devices?** By default, the 802.11ax mode is enabled on the access point. WiFi 6 (802.11ax) is backward compatible with earlier WiFi standards. However, if your network includes many legacy devices that do not support WiFi 6, in some unlikely situations, compatibility problems could occur. To mitigate such situations, NETGEAR gives you the option to disable the 802.11ax mode for the 2.4 GHz radio. For more information, see Manage the 802.11ax mode for the 2.4 GHz radio on page 74.
- **Is the device at the wrong location?** Make sure that the WiFi device is not too far from the access point or too close. To see if the signal strength improves, move the WiFi device near the access point but at least 6 feet (1.8 meters) away.
- **Is the WiFi signal blocked?** Make sure that the WiFi signal is not blocked by objects between the access point and the WiFi device.
- **Is the device blocked in a MAC filter?** Make sure that the WiFi device is not on a MAC filter (access control list) that blocks access to the device (see Set up a MAC filter for an SSID on page 84).
- **Can the WiFi device receive an IP address?** Make sure that the 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.)

You cannot connect over the 2.4 GHz management SSID

You can use the 2.4 GHz management SSID only to access the local browser UI of the access point from a WiFi device for management purposes. The 2.4 GHz management SSID cannot be used for regular WiFi client connections to the access point.

If you cannot connect over the 2.4 GHz management SSID, check the following:

- **Was the 2.4 GHz management SSID automatically turned off?** By default, the idle time-out for the 2.4 GHz management SSID is 15 minutes. That is, if no WiFi client is connected to the 2.4 GHz management SSID for 15 minutes, the 2.4 GHz management SSID is turned off. Only after you reboot the access point can you reconnect to the 2.4 GHz management SSID. However, you can disable the idle

time-out so that the 2.4 GHz management SSID stays always on. For more information, see Disable the idle time-out for the 2.4 GHz management SSID on page 60.

- **Are you using the correct SSID and password?** The name of the 2.4 GHz management SSID depends on the model and the MAC address. In the following examples, XXXXXX represents the last six digits of the MAC address of the LAN interface of the access point:
  - **WAX214**: WAX214XXXXXX-CONFIG-ONLY
  - **WAX218**: WAX218XXXXXX-CONFIG-ONLY

  You cannot change the name of the 2.4 GHz management SSID. The default WiFi passphrase for the management SSID is printed on the access point label. You *can* change this WiFi passphrase and we recommend that you do so.
- **Did you disable the 2.4 GHz management SSID?** If you disabled the 2.4 GHz management SSID, you can reach the access point local browser UI only over a wired LAN connection. For more information, see Disable the 2.4 GHz management SSID on page 61.

Troubleshoot Internet browsing

If a 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:

- The WiFi device might not recognize any DNS server 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), restart the WiFi device and verify the DNS address.
- The WiFi device might not use the correct TCP/IP settings.
  If the WiFi device obtains its information by DHCP, reboot the WiFi device 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 of your computer or mobile device on page 133.

Note: If you are connected to the 2.4 GHz management SSID to manage the access point, you might not get an Internet connection. For more information, see 2.4 GHz management SSID on page 58.

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 UI, 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 your network (see Specify a static IPv4 address on page 40), 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 the access point is connected to a network with a DHCP server and you do not know the IP address, determine the IP address that the DHCP server assigned to the access point by using one of the following methods:
  - **Windows-based computer**: If you use a Windows-based computer, open Windows Explorer, and click the **Network** link. If prompted, enable the Network Discovery feature. Under Network Infrastructure, locate and right-click the access point device icon, and select **Properties**. The access point IP address displays. Assuming that you did not change the device name, the access point is shown as NETGEARXXXXXX, in which XXXXXX represents the last six digits of the MAC address of the LAN interface of the access point.
  - **DHCP server**: Access the DHCP server in your network and open the page the shows the network connections.
  - **NETGEAR Insight app**: Use the NETGEAR Insight app to discover the IP address that is assigned to the access point. For more information, see Find the IP address of the access point with the NETGEAR Insight mobile app on page 34.
  - **IP network scanner**: Use an IP network scanner to scan for the IP address that is assigned to the access point.

  Note: For more information, see Find the IP address of the access point on page 33.

- 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 in the local browser UI

If you are logged in to the access point's local browser UI 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 **Save** or **Apply** button before moving to another page or tab. If you clicked the **Save** button, when you are ready with entering configuration settings, click the **Apply** button to apply the configuration settings. Otherwise, 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 of your computer or mobile device

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 troubleshoot a network using the ping utility in your computer or mobile device

Test the LAN path from a Windows-based computer to the access point

You can ping the access point from a Windows-based computer to verify that the path to your access point is set up correctly. You can use a WiFi or wired connection to the access point.

To ping the access point from a Windows-based computer:

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

   ping www.aplogin.net

3. Click the **OK** button.

You see a message like this one:

```
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, check to see if the following is correct:

- Correct LAN subnet?
  Verify that the IP addresses and LAN subnet for the access point and your computer are correct. For more information, see Display the access point device, memory, LAN, and WiFi status information on page 112.
- Correct physical connections?
  If the access point and computer are connected through a switch or hub, make sure that the link LEDs are lit for the switch ports that are connected to the access point and computer.
- Correct software?
  If you are using a wired connection to the access point, verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

Test the path from a Windows-based computer to a remote device

To test the path from a Windows-based computer that is connected to the access point to a remote device:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the Windows Run window, type
   ping -n 10 *<IP address>*

   in which *<IP address>* is the IP address of a remote device such as your ISP DNS server.

   If the path is functioning correctly, messages display that are similar to those shown in Test the LAN path from a Windows-based computer to the access point on page 133.

3. If you do not receive replies, check the following:
   - Check to see that IP address of the access point is listed as the default gateway for your computer. If DHCP assigns the IP configuration of your computers, this information is not visible in your computer Network Control Panel. Verify that the IP address of the access point is listed as the default gateway.
   - Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.
   - Check to see that your modem is connected and functioning.
   - If your ISP assigned a host name to your registered computer, use that host name as the account name on your modem.
   - Your ISP might be rejecting the Ethernet MAC addresses of all but one of your computers.
     Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem. Some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If your ISP does this, configure your router to "clone" or "spoof" the MAC address from the authorized computer.

A

Factory Default Settings and Technical Specifications

This appendix includes the following sections:

Factory default settings

You can reset the access point to the factory default settings, which are shown in the following table.

For information about resetting the access point to its factory settings, see Reset the access point to factory default settings on page 95.

Table 12. Factory default settings model WAX214 and model WAX218

Feature	Default Setting
Access	
Default IP address	192.168.0.100 (aplogin.net)
DHCP client	Enabled. **Note**: If connected to a network, the access point receives an IP address from a DHCP server or router in the network.
Local device password	No default password. The first time that you log in to the local browser UI, you must define a local device password that applies only to local browser UI access.
2.4 GHz management SSID	
Model WAX214	WAX214XXXXXX-CONFIG-ONLY XXXXXX represents the last six digits of the MAC address of the LAN interface of the access point.
Model WAX21	WAX218XXXXXX-CONFIG-ONLY XXXXXX represents the last six digits of the MAC address of the LAN interface of the access point.
WiFi passphrase for management SSID	The unique WiFi password is printed on the access point label. The security is WPA2-Personal.
Management SSID time-out	Automatically turned off after15 minutes of being idle.
WiFi networks (SSIDs) for client connections	
5 GHz SSIDs	By default, the first SSID is enabled after you specify the name and WiFi passphrase the first time that you log in to the local browser UI. The second, third, and fourth SSIDs are disabled by default: NETGEARXXXXXX_2 NETGEARXXXXXX_3 NETGEARXXXXXX_4 XXXXXX represents the last six digits of the MAC address of the 2.4 GHz radio of the access point. When you enable one of these SSIDs, the default WiFi passphrase is sharedsecret and the default security is WPA2-Personal.
SSID (settings for each individual SSID)	
Guest network	Disabled

Table 12. Factory default settings model WAX214 and model WAX218 (Continued)

Feature	Default Setting
Hidden SSID	Disabled
Client isolation	Disabled
VLAN isolation	Disabled
L2 isolation	Disabled
Band steering	Disabled
Fast roaming	Disabled
WiFi MAC filter	Disabled
WiFi traffic shaping	Disabled
2.4 GHz and 5 GHz radios	
Channel HT mode	2.4 GHz radio: 20 MHz 5 GHz radio: 80 MHz
Radio transmission power	Automatic (Auto RF)
Channel	The available channels and the default channel depend on the configured region and country.
Bit rate	Automatic
Client limits	64 for each radio
Multicast to unicast stream conversion	Enabled
11ax mode	Enabled
Other	
Date and time settings	Obtained automatically from the default NTP server
STP	Disabled
Management VLAN	Disabled (untagged)
SNMP	Disabled

Technical specifications

The following table shows the technical specifications of the access point. For more information, see the product data sheet, which you can download by visiting netgear.com/support/download/.

Table 13. Technical specifications model WAX214 and model WAX218

Feature	Description
Power adapter	Model WAX214: 12V, 1.5A (18W) The plug is localized to the country of sale. A power adapter is included for model WAX214PA but not for model WAX214. Both models can operate with PoE power.
	Model WAX218: 12V, 2.5A (30W) The plug is localized to the country of sale. A power adapter is included for model WAX218PA but not for model WAX218. Both models can operate with PoE+ power.
Power over Ethernet **Note**: PoE might be considered a network environment 0 per IEC TR 62101, and thus the interconnected ITE circuits might be considered safety extra low voltage (SELV).	Model WAX214: If you do not use a power adapter, the LAN/PoE port requires 802.3af (PoE) power. Maximum power consumption with PoE: 12.5W
	Model WAX218: If you do not use a power adapter, the LAN/PoE+ port requires 802.3at (PoE+) power. Maximum power consumption with PoE: 19.5W
Dimensions (L x W x H)	Model WAX214: 6.33 x 6.33 x 1.31 in. (160.9 x 160.9 x 33.3 mm)
	Model WAX218: 8.0 x 8.0 x 1.37 in. (205.7 x 205.7 x 35.8 mm)
Weight	Model WAX214: 0.84 lb (380 g)
	Model WAX218: 1.73 lb (788 g)
Operating temperature	32° to 104°F (0° to 40°C)
Operating humidity	0 to 90% maximum relative humidity, noncondensing
Storage temperature	–22° to 176°F (–30° to 80°C)
Storage humidity	0 to 90% maximum relative humidity, noncondensing

Table 13. Technical specifications model WAX214 and model WAX218 (Continued)

Feature	Description
LAN interface	Model WAX214: One 10/100/1000 Mbps Ethernet (RJ-45) PoE port with Auto Uplink (Auto MDI-X)
	Model WAX218: One 10/100/1000/2500 Mbps Ethernet (RJ-45) PoE+ port with Auto Uplink (Auto MDI-X)
WiFi interfaces	2.4 GHz radio for WiFi devices and management access 5 GHz radio for WiFi devices The interfaces can operate concurrently.
Maximum theoretical throughput	Model WAX214: 2.4 GHz radio: 573.5 Mbps 5 GHz radio: 1201 Mbps
	Model WAX218: 2.4 GHz radio: 1147 Mbps 5 GHz radio: 2402 Mbps
Operating frequency range 2.4 GHz band	US: 2.412–2.462 GHz Europe: 2.412–2.472 GHz The supported channels depend on the configured regulatory domain.
Operating frequency range 5 GHz band	US: 5.180–5.240 + 5.745–5.825 GHz Europe: 5.180–5.700 GHz The supported channels depend on the configured regulatory domain.
Supported radio technologies	IEEE 802.11ax IEEE 802.11ac specification IEEE 802.11n 2.0 specification IEEE 802.11g IEEE 802.11b IEEE 802.11a
Maximum number of supported clients	128, of which 64 are on the 2.4 GHz radio and 64 are on the 5 GHz radio. The supported number of clients depends on the network and traffic conditions.
802.11 security	Opportunistic wireless encryption (OWE) WPA2-Personal WPA3-Personal WPA2/WPA3-Personal WPA2-Enterprise WPA3-Enterprise WPA2/WPA3-Enterprise **Note**: We recommend that you set up security. In certain situations, and if you are aware of the risks, you can select an open network without security.
Regulatory safety compliance	CB EN60950 EN62368

B

Mount Model WAX214 to a Wall or Ceiling

The access point package includes wall-mounting and ceiling-mounting components.

You can mount the access point to a solid surface (a wall or a ceiling) or to a ceiling with a 15/16 in. (23.8 mm) T-bar, or you can install the access point freestanding on a flat surface.

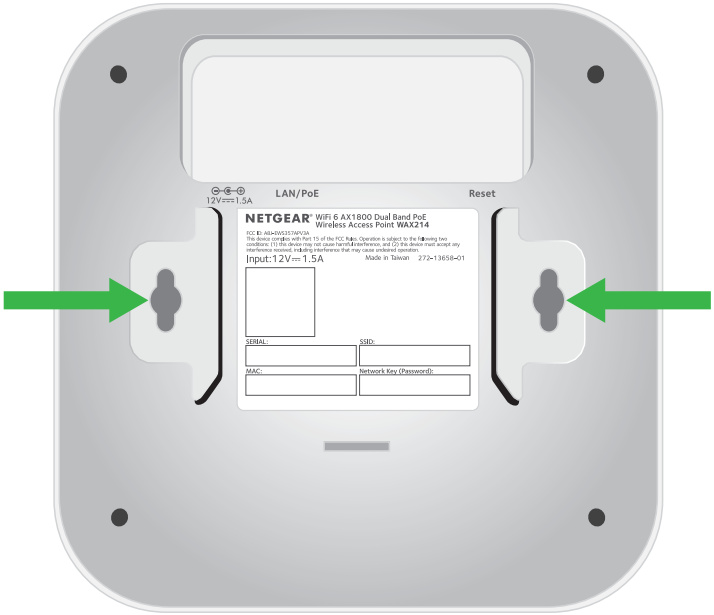
We recommend that you use a flat Ethernet cable so that the cable fits in the narrow space between the access point and the surface on which it is mounted or placed.

This appendix includes the following sections:

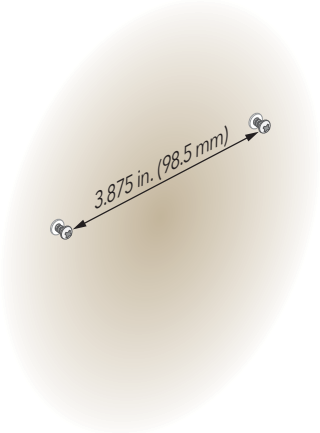
Mount model WAX214 to a wall

To mount the access point to a wall:

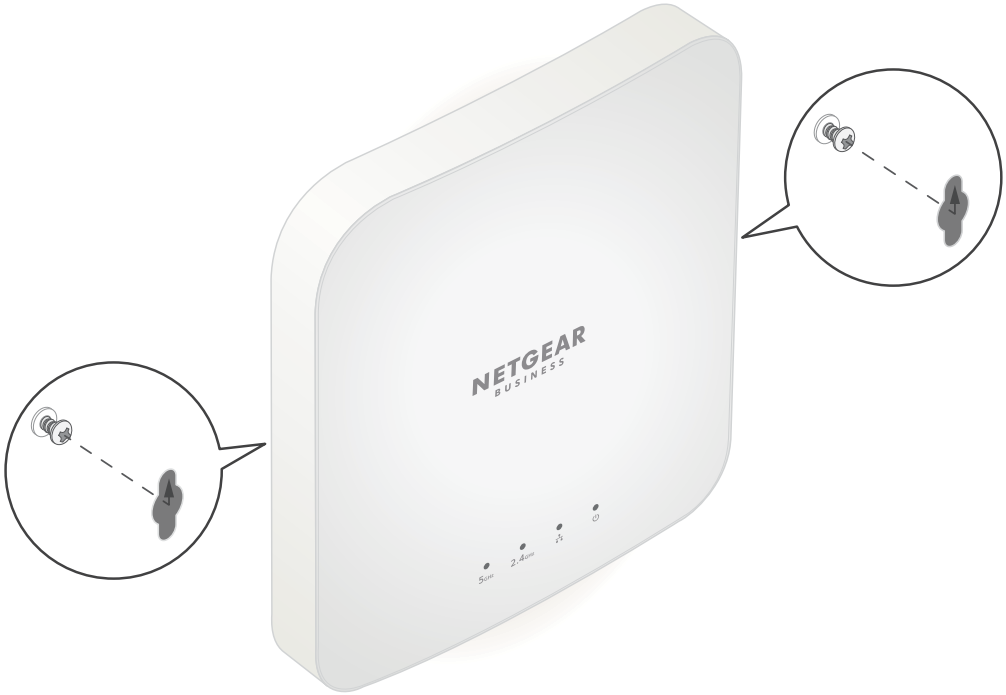
1. The bottom of the access point includes two holes that let you mount the access point on two screws inserted in a wall.



2. Mark the wall where you want to insert the provided anchors and screws, which must be 3.875 in. (98.5 mm) apart.
3. Insert the anchors and screws, but leave about 0.25 in. (6 mm) of each screw protruding from the wall so that you can insert the screws into the holes on the bottom of the access point.



4. Line up the holes on the bottom of the access point with the screws in the wall and mount the access point to the wall.

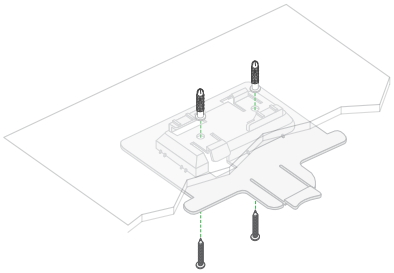


Mount model WAX214 to a solid ceiling

To mount the access point to a solid ceiling:

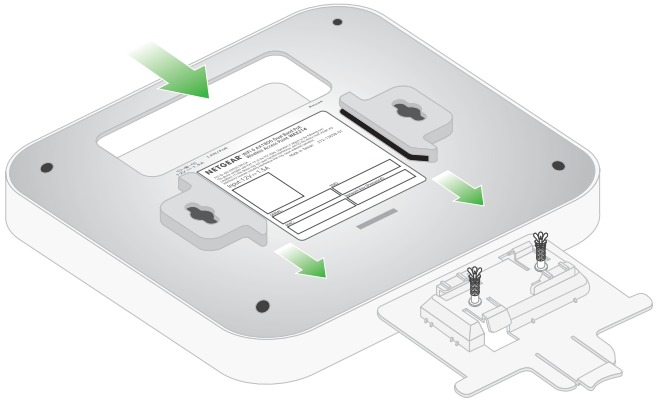
1. Using the anchors and screws provided, attach the 15/16 in. (23.8 mm) bracket with the screw holes to the ceiling.

   The rectangular protruding part of the bracket must be facing the ceiling.

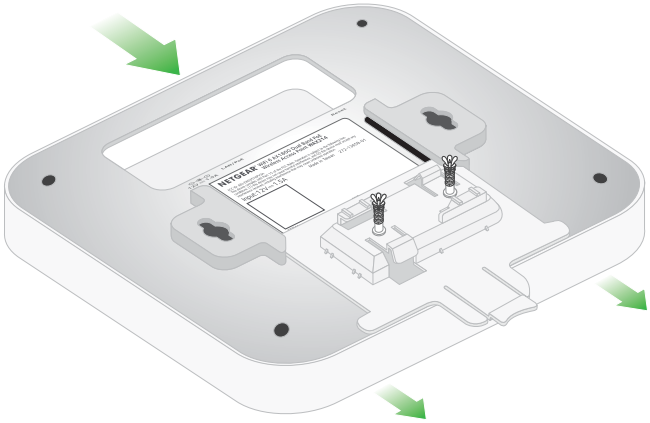


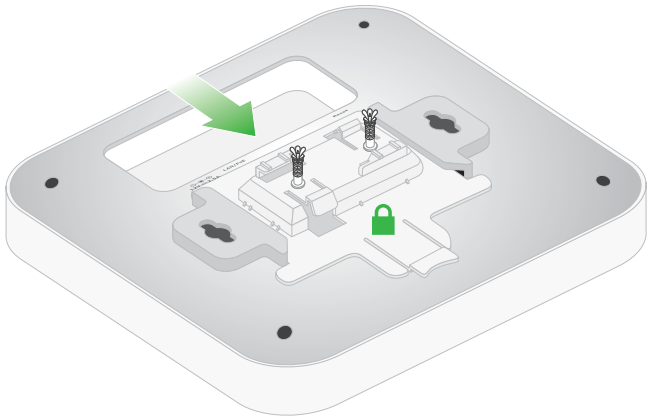
2. Hold the access point upside down with the front of the access point facing the bracket.

3. Line up the guides on the bottom of the access point with the bracket.

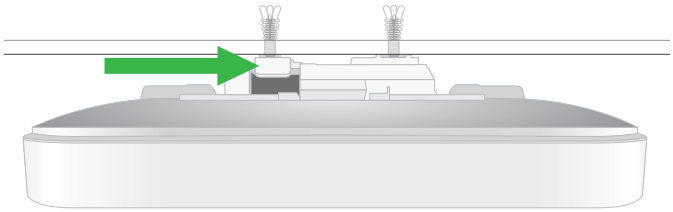


4. Slide the access point into the bracket until it locks in place.





Note: To unlock the access point, push the locking tab toward the ceiling and slide the access point out of the bracket. The following figure shows a side view of the access point attached to the ceiling. The green arrow indicates the locking tab.

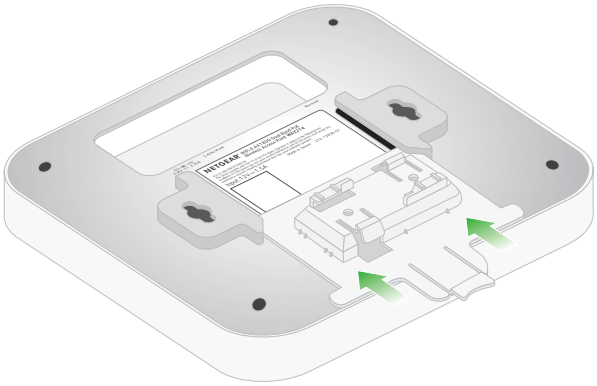


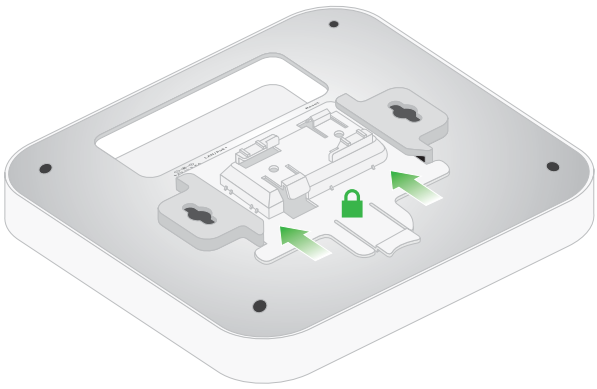
Mount model WAX214 to a T-bar

To mount the access point to a T-bar:

1. Slide the 15/16 in. (23.8 mm) bracket between the guides on the bottom the access point until it locks in place.

   The locking tab must be at the front of the access point.

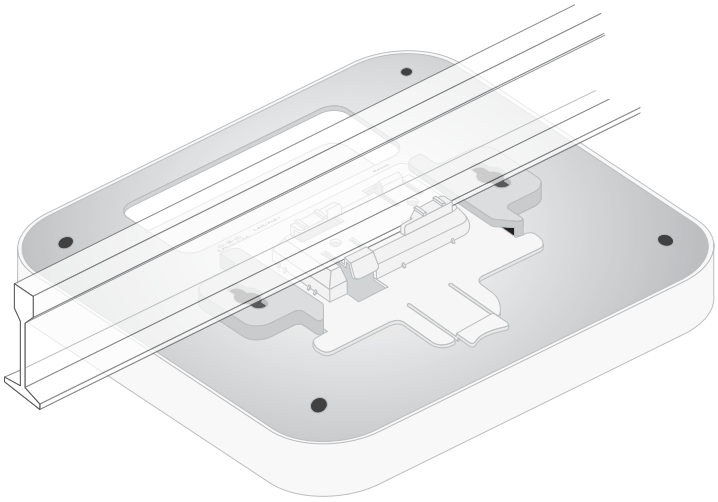




2. Hold the access point upside down.

Note: If you can reach behind the T-bar, hold the T-bar with one hand and the access point with your other hand.

3. Align the rectangular protruding part of the bracket with the T-bar.
4. Hook the bracket onto one side of the T-bar.
5. Hook the bracket onto the other side of the T-bar until the bracket locks onto the T-bar.



C

Mount Model WAX218 to a Wall or Ceiling

The access point package includes wall-mounting and ceiling-mounting components.

You can mount the access point to a solid surface (a wall or a ceiling) or to a ceiling with a 15/16 in. (23.8 mm) T-bar, or you can install the access point freestanding on a flat surface.

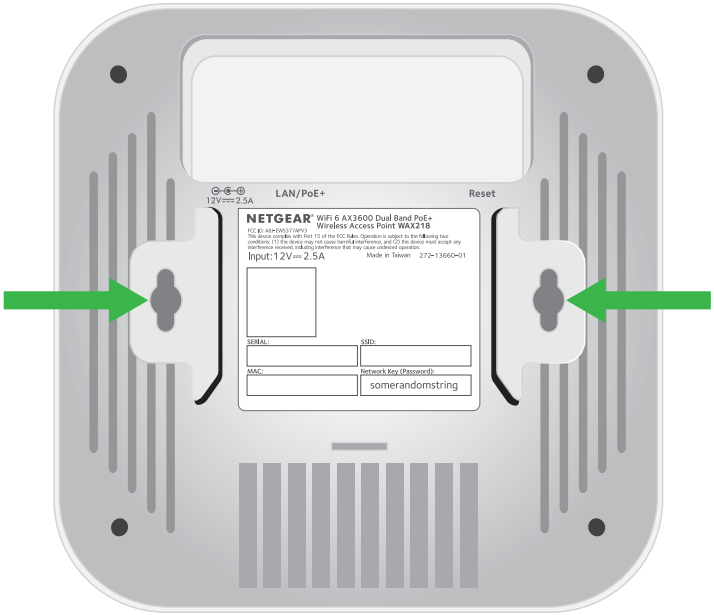
We recommend that you use a flat Ethernet cable so that the cable fits in the narrow space between the access point and the surface on which it is mounted or placed.

This appendix includes the following sections:

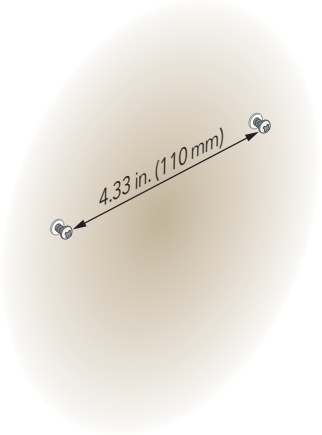
Mount model WAX218 to a wall

To mount the access point to a wall:

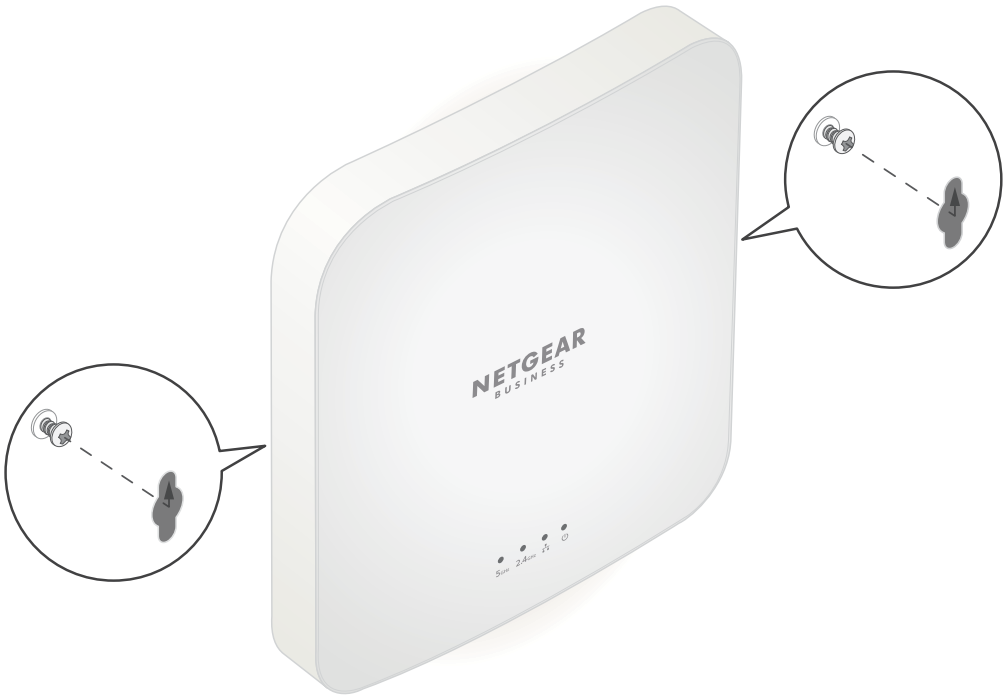
1. The bottom of the access point includes two holes that let you mount the access point on two screws inserted in a wall.



2. Mark the wall where you want to insert the provided anchors and screws, which must be 4.33 in. (110 mm) apart.
3. Insert the anchors and screws, but leave about 0.25 in. (6 mm) of each screw protruding from the wall so that you can insert the screws into the holes on the bottom of the access point.



4. Line up the holes on the bottom of the access point with the screws in the wall and mount the access point to the wall.

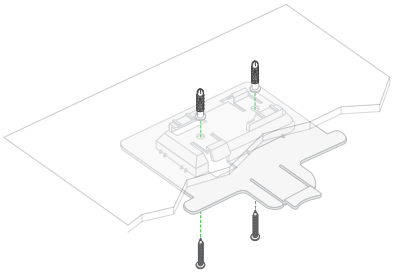


Mount model WAX218 to a solid ceiling

To mount the access point to a solid ceiling:

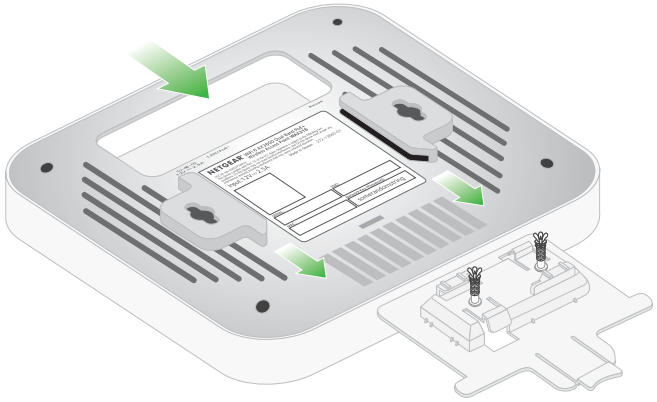
1. Using the anchors and screws provided, attach the 15/16 in. (23.8 mm) bracket with the screw holes to the ceiling.

   The rectangular protruding part of the bracket must be facing the ceiling.

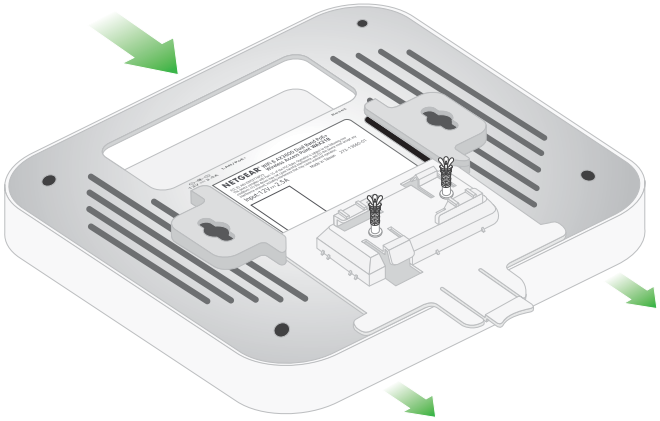


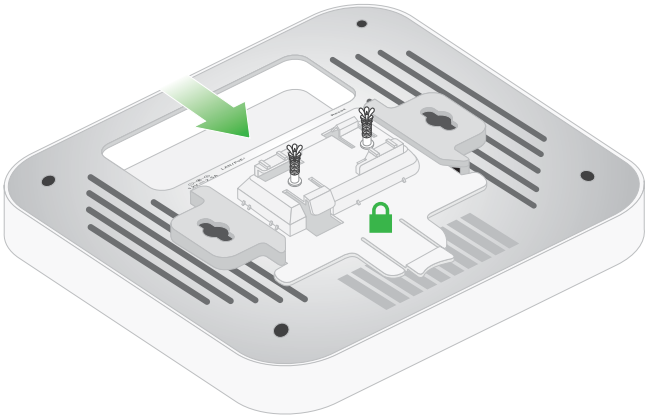
2. Hold the access point upside down with the front of the access point facing the bracket.

3. Line up the guides on the bottom of the access point with the bracket.

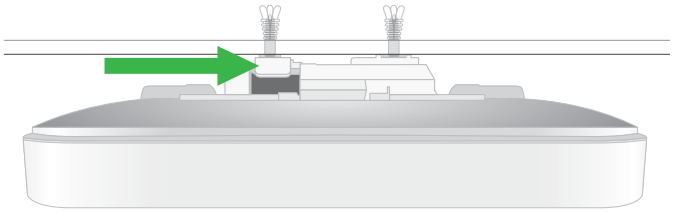


4. Slide the access point into the bracket until it locks in place.





Note: To unlock the access point, push the locking tab toward the ceiling and slide the access point out of the bracket. The following figure shows a side view of the access point attached to the ceiling. The green arrow indicates the locking tab.

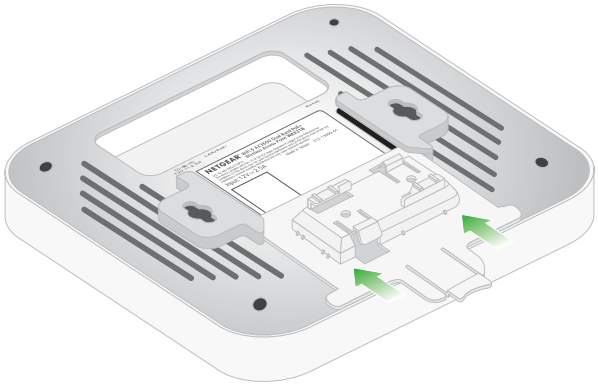


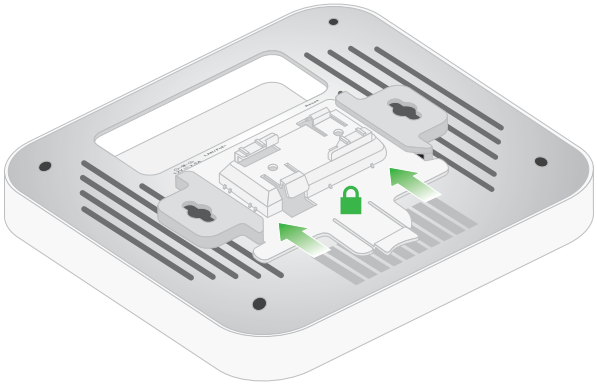
Mount model WAX218 to a T-bar

To mount the access point to a T-bar:

1. Slide the 15/16 in. (23.8 mm) bracket between the guides on the bottom the access point until it locks in place.

   The locking tab must be at the front of the access point.





2. Hold the access point upside down.

Note: If you can reach behind the T-bar, hold the T-bar with one hand and the access point with your other hand.

3. Align the rectangular protruding part of the bracket with the T-bar.
4. Hook the bracket onto one side of the T-bar.
5. Hook the bracket onto the other side of the T-bar until the bracket locks onto the T-bar.