NETGEAR®

User Manual

AX1800 Dual Band PoE WiFi 6 Access Point

WAX210

September 2024
202-12726-02

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.

Applicable to 6 GHz devices only: Only use the device indoors. The operation of 6 GHz devices is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-12726-02	September 2024	First publication.

Contents

Chapter 1 Hardware Overview

Chapter 2 Installation and Initial Login

Chapter 3 Manage the Wired Network Settings

Chapter 4 Manage Basic WiFi Settings

Chapter 5 Manage Advanced WiFi Settings

Chapter 6 Manage the WiFi Radio Settings

Chapter 7 Maintain the AP

1

Hardware Overview

This manual is for the NETGEAR AX1800 Dual Band PoE WiFi 6 Access Point Model WAX210.

In this manual, we refer to this indoor, standalone model as the AP.

The AP provides 802.11ax high-performance WiFi connectivity for a small office/home office. It 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 AP to a PoE (802.3af) switch. If you use a regular switch, the AP requires a power adapter, which is supplied with a WAX210PA SKU. (If you purchased a WAX210 SKU without an included power adapter, you can purchase one separately.)

The chapter contains the following sections:

- Additional documentation
- Unpack the AP
- Top panel with LED
- Hardware interfaces
- Label

ⓘ **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/. Enter your model number to 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.

Additional documentation

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

- Installation guide
- Datasheet

Unpack the AP

The package contains the following items:

- WAX210 AP
- 2 T-bar hooks for mounting the AP to a ceiling with a T-bar
- 2 small screws for attaching the T-bar hooks to the AP
- 2 large screws and anchors for mounting the AP to a wall
- Installation guide

! **NOTE:** You power up the AP by connecting it to a PoE switch. A power adapter is included only with a WAX210PA SKU. (The cable of the power adapter varies by region.) 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 the installation guide, which you can download by visiting netgear.com/support/download/.

Top panel with LED

The LED that provides the status of the AP is located on the top panel of the AP.

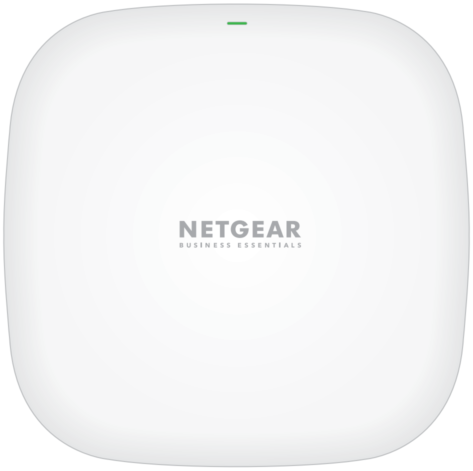

Figure 1. Top panel with LED

LED Color and Behavior	Description
▬	**Solid amber**: The AP is starting.
▬	**Slow blinking amber**: The AP is in the process of getting an IP address. If the LED remains slow blinking amber, the AP cannot get an IP address or the AP does not detect an Ethernet link (see LED remains slow blinking amber on page 122).
▬	**Fast blinking amber**: The firmware is being updated or the AP is in the process of being reset to factory defaults because someone pressed the **Reset** button or used the device UI to reset the AP. **Note**: If you press the **Reset** button or use the device UI to reset the AP, the LED lights as follows: 1. Solid amber for 5 seconds 2. Slow blinking amber for 5 to 10 seconds 3. Fast blinking amber during the remainder of the reset process

(Continued)

LED Color and Behavior	Description
🟩	**Solid green**: The AP is functioning with Internet connectivity but no WiFi client is connected
🟩	**Blinking green**: The AP is functioning with Internet connectivity and at least one WiFi client is connected and sending or receiving traffic.

ⓘ **NOTE:** For information about troubleshooting with the LED, see Troubleshoot with the LED on page 120.

Hardware interfaces

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

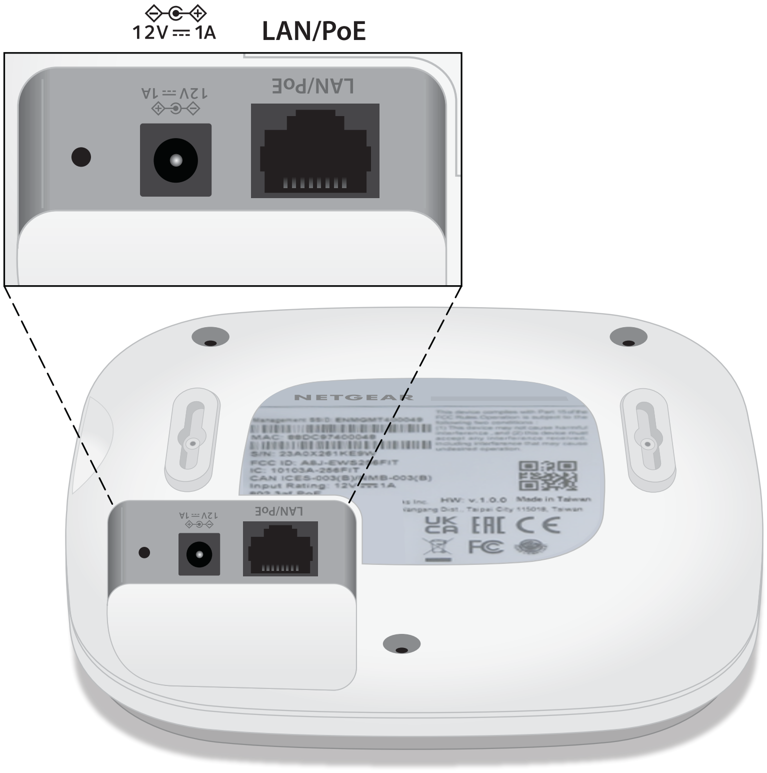

Figure 2. Hardware interfaces

The bottom panel contains the following components:

- **Reset button**. You can use the **Reset** button to restart the AP or to reset the AP to its factory default settings. To restart the AP, press the **Reset** button for two seconds. Pressing the **Reset** button for at least 11 seconds resets the AP to factory default settings.
- **DC power connector**. If you do not use a Power over Ethernet (PoE) switch to provide power to the AP, connect the power adapter to the DC power connector.
- **LAN/PoE port**. Connect the LAN/PoE Gigabit Ethernet RJ-45 port to a PoE switch, or if you use a power adapter, to a non-PoE switch (that is, a common switch).

  The LAN/PoE port supports Ethernet speeds up to 1 Gbps.

  ! **NOTE:** If you do not use a power adapter, use a PoE (803.2.af) switch.

Label

The AP label shows the serial number, MAC address, default WiFi network name (SSID) for the management WiFi network, and the associated passphrase (also referred to as network key or WiFi password) for the *management WiFi network*.

The management WiFi network (see Management WiFi network on page 45) provides access to the device user interface (UI) only. That is, the WiFi network is not intended for general WiFi clients access. The *user WiFi networks* (see User WiFi networks on page 36) are intended for general WiFi clients access. During initial login to the AP's device UI, you must set up a user WiFi network.

2

Installation and Initial Login

This chapter describes how you can install and access the AP in your network and go through the initial login process.

NOTE: When you log in to the AP, you connect to its device UI.

The chapter contains the following sections:

- Set up the AP in your network
- Initial login process
- When to use aplogin.net and when to use the assigned IP address
- Find the IP address of the AP
- Log in to the AP after you complete the initial login process
- Change the language
- Join a user WiFi network on the AP

⚠ **CAUTION:** This device must be professionally installed. It is the installer's responsibility to follow local country regulations, including operations within legal frequency channels, output power, and DFS requirements. The vendor, reseller, or distributor is not responsible for illegal wireless operations. For more details, see the device's terms and conditions.

Set up the AP in your network

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

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

- Set up the AP with a PoE network connection
- Set up the AP with a non-PoE network connection

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

Set up the AP with a PoE network connection

You can connect the AP to a Power over Ethernet (PoE) switch in your network. The switch must be capable of providing PoE (802.3af) power and must be connected to a network router that is connected to the Internet. If you use a PoE connection, the AP does not require a power adapter.

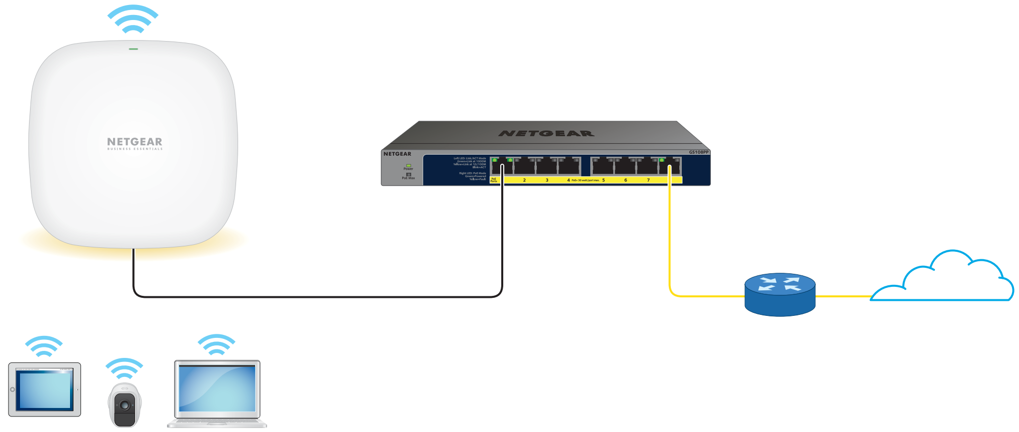

Figure 3. Set up the AP with a PoE connection to your network

NOTE: The LAN/PoE port supports Ethernet speeds up to 1 Gbps. Most switches support speeds of 1 Gbps or higher.

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

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

   Connect the cable to a PoE port on a PoE (802.3af) switch.
3. Check to see that the LED lights.

LED Color and Behavior	Description
🟧	**Solid amber**: The AP is starting.
🟧	**Slow blinking amber**: The AP is in the process of getting an IP address. If the LED remains slow blinking amber, the AP cannot get an IP address or the AP does not detect an Ethernet link (see LED remains slow blinking amber on page 122).
🟧	**Fast blinking amber**: The firmware is being updated.
🟩	**Solid green**: The AP is functioning with Internet connectivity but no WiFi client is connected
🟩	**Blinking green**: The AP is functioning with Internet connectivity and at least one WiFi client is connected and sending or receiving traffic.

You can now access the AP for initial configuration (see Initial login process on page 15).

Set up the AP with a non-PoE network connection

You can connect the AP to a regular switch, that is, a non–Power over Ethernet (PoE) switch in your network. The switch must be connected to a network router that is connected to the Internet. If you use a regular switch, the AP requires a power adapter, which is supplied for model WAX210PA. (For modelWAX210, a power adapter is an option that you can purchase.)

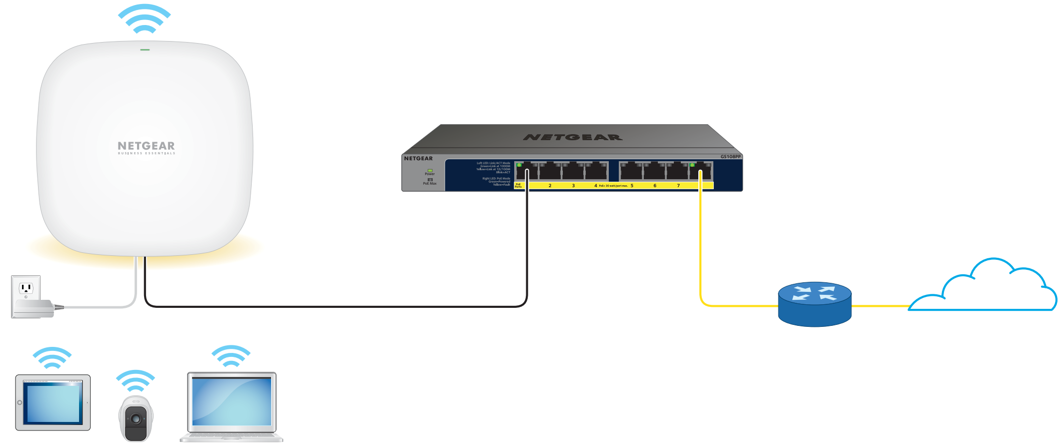

Figure 4. Set up the AP with a non-PoE connection to your network

NOTE: The LAN/PoE port supports Ethernet speeds up to 1 Gbps. Most switches support speeds of 1 Gbps or higher.

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

1. Connect an Ethernet cable to the LAN/PoE port on the AP.
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 AP and plug it into an electrical outlet.
4. Check to see that the LED lights.

LED Color and Behavior	Description
▬	**Solid amber**: The AP is starting.
✺	**Slow blinking amber**: The AP is in the process of getting an IP address. If the LED remains slow blinking amber, the AP cannot get an IP address or the AP does not detect an Ethernet link (see LED remains slow blinking amber on page 122).
✹	**Fast blinking amber**: The firmware is being updated.

(Continued)

LED Color and Behavior	Description
🟩	**Solid green**: The AP is functioning with Internet connectivity but no WiFi client is connected
🟩	**Blinking green**: The AP is functioning with Internet connectivity and at least one WiFi client is connected and sending or receiving traffic.

You can now access the AP for initial configuration (see Initial login process on page 15).

Initial login process

During the initial login process, the AP presents a start page that lets you select the country or region in which you are using the AP, define the device password for the AP's device UI, create the first user WiFi network (SSID) with its associated passphrase (WiFi password), and accept NETGEAR's terms of use.

After you complete the initial-login process, if you want to log in to the device UI, the AP presents a regular login page that lets enter your device password.

For more information about the initial login process, see one of the following sections:

- Connect directly to the AP over WiFi and log in for the first time
- Connect to the AP over the LAN and log in for the first time

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

This section describes how to connect to the AP management WiFi network for the first time and complete the initial configuration. When you power up your AP, the management WiFi network becomes active. We recommend that you use a WiFi-enabled computer or tablet to connect to the management WiFi network for setup.

NOTE: For security reasons, the management WiFi network turns off when inactive for 15 minutes. If this happens *during setup*, press the **Reset** button for 2 seconds to restart the AP.

The AP supports two types of WiFi networks (SSIDs):

- **Management WiFi network**: The special purpose WiFi network that you use to access the AP's device UI to configure and manage the AP. You can use the QR code or WiFi network information on the AP label to connect to the management WiFi network. To protect your WiFi network security, the management WiFi network does *not* let you connect to the Internet. For more information, see Management WiFi network on page 45.
- **User WiFi network**: The WiFi network that provides general network access to authenticated users. During set up, you must configure the first user WiFi network. After you complete the initial setup process, you can configure up to three additional WiFi networks (see User WiFi networks on page 36).

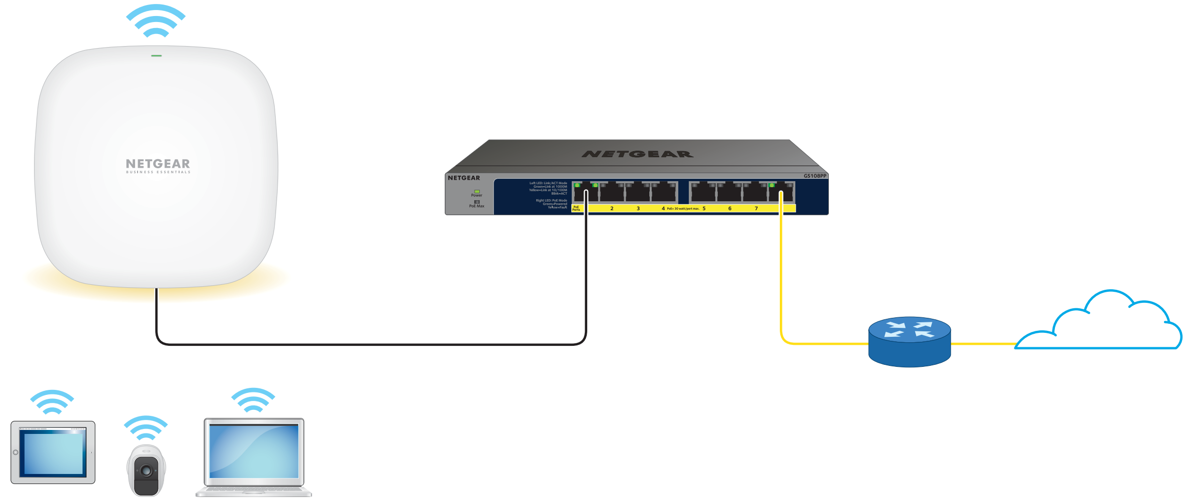

Figure 5. Connect directly to the AP over WiFi

The previous figure shows the AP connected to a switch, which is connected to a router and the Internet. WiFi devices are directly connected to the AP.

To connect directly to the AP over WiFi and log in to the device UI for the first time:

1. Connect your computer or tablet to the AP's management WiFi network (SSID) using one of the following methods:
    - **Scan the QR code**: Scan the QR code on the label to connect to the management WiFi network.
    - **Connect manually**: The default name of the management WiFi network is printed on the AP's label. The default network key (password) for WiFi access is also on the AP label.

      The management WiFi network name uses the format "WAX210XXXXXX-CONFIG-ONLY," in which XXXXXX represents the last six characters of the MAC address of the AP's LAN interface.

If you cannot get a WiFi connection to the AP, see You cannot connect to the management WiFi network on page 124.

2. Launch a web browser and enter **https://www.aplogin.net** in the address field.

   The start page for the setup process displays.

   If the start page does *not* display but instead a security warning or a NETGEAR page displays:

   - **Security warning**: Your browser might display a security warning because of the self-signed certificate on the AP, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
   - **NETGEAR page**: If your browser redirects to a www.netgear.com page, your computer or tablet is not connected to the AP's management WiFi network, and you must repeat the previous step.

3. Click the **Next** button.

   The page that displays lets you set a new password for the device UI and the first user WiFi network.

4. Configure the following settings:

   a. In the **AP Login New Password** field, set a unique password for access to the device UI, and confirm the password in the **Confirm AP Login New Password** field.

      Your password must meet the following conditions:

      - Contains 8 to 32 characters
      - 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 **Wireless Network (SSID)** field, set a WiFi network name for the first user WiFi network.

      This SSID does *not* replace the management WiFi network (WAX210XXXXXX-CONFIG-ONLY), which you can continue to use to log in over a WiFi connection to the device UI of the AP.

   c. In the **Network Key (Password)** field, set a WiFi password for the first user WiFi network.

      This WiFi password must be a minimum of 8 characters and can be a maximum of 63 characters.

This WiFi password does *not* replace the WiFi password for the management WiFi network, which you can continue to use to log in over a WiFi connection to the device UI of the AP.

d. From the **Country/Region** menu, select the country where you are using the AP.

   In some countries, the AP is sold with a preconfigured country or region setting and you cannot change it.

   ⓘ **NOTE:** In some countries, the is sold with a preconfigured country or region setting and you cannot change it.

   ⓘ **NOTE:** If you do not see your country or region listed in the menu, update the AP's firmware and check again. If you still do not see your country or region listed, contact NETGEAR support.

   ⓘ **NOTE:** Make sure that the country is set to the location where the device is operating. It might not be legal to operate the AP in a region other than the regions listed in the menu. You are responsible for complying with the local, regional, and national regulations that are set for channels, power levels, and frequency ranges.

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

f. Click the **Apply** button.

   Your settings are saved. A summary page displays and the AP restarts.

5. Wait two minutes until the AP completes its restart.

   You are done. The AP is connected to the network and ready to use. You can now connect a computer or mobile device to the user WiFi network that you just set up, using the WiFi password that you just defined.

6. (Optional) To continue to configure the AP for your network and environment, do the following

   a. Log in again to the management WiFi network.

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

      If your browser display a security warning, proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

   b. In the **Device Password** field, enter your new password for the device UI, and click the **Login** button.

      The Dashboard page displays.

      You can now configure the AP.

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

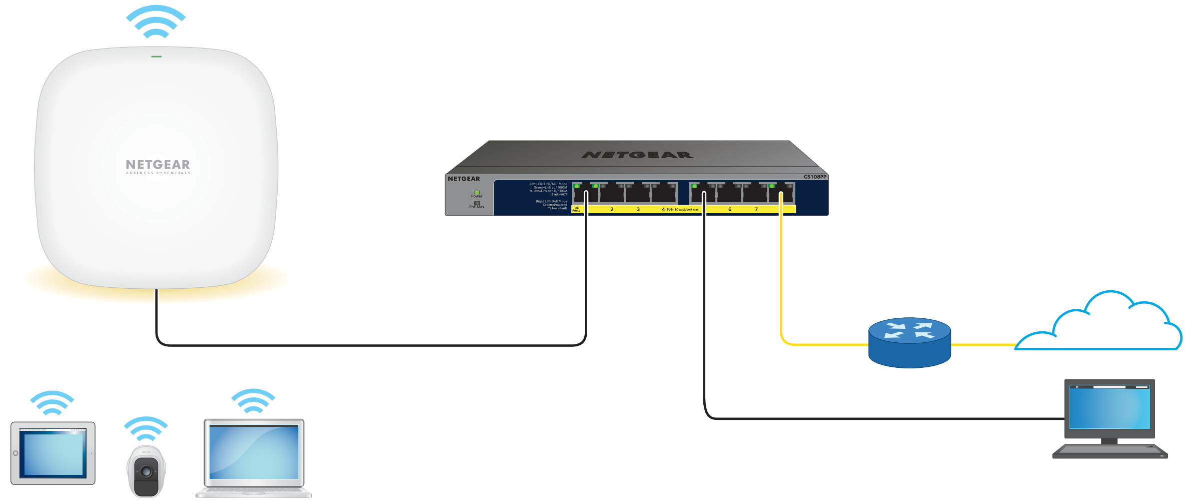

Figure 6. Connect to the AP over the LAN

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

To connect to the AP 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 by the DHCP server to the AP, use one of the following options, each of which is described in detail in Find the IP address of the AP on page 22:
   - Use the automatic device detection of a Windows-based computer.
   - Access your existing router or DHCP server.
   - Use a third-party IP scanner.
3. Launch a web browser and enter the IP address that is assigned to the AP in the address field.

   Use https, not http.

The start page for the setup process displays.

If the start page does *not* display but instead a security warning displays or you cannot get a LAN connection:

- **Security warning**: Your browser might display a security warning because of the self-signed certificate on the AP, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
- **No LAN connection**: If you cannot get a LAN connection to the AP at all, see You cannot log in to the AP over a LAN connection on page 125.

4. Click the **Next** button.

   The page that displays lets you set a new password for the device UI and the first user WiFi network.

5. Configure the following settings:

   a. In the **AP Login New Password** field, set a unique password for access to the device UI, and confirm the password in the **Confirm AP Login New Password** field.

   Your password must meet the following conditions:

   - Contains 8 to 32 characters
   - 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 **Wireless Network (SSID)** field, set a WiFi network name for the first user WiFi network.

   This SSID does *not* replace the management WiFi network (WAX210XXXXXX-CONFIG-ONLY), which you can continue to use to log in over a WiFi connection to the device UI of the AP.

   c. In the **Network Key (Password)** field, set a WiFi password for the first user WiFi network.

   This WiFi password must be a minimum of 8 characters and can be a maximum of 63 characters.

   This WiFi password does *not* replace the WiFi password for the management WiFi network, which you can continue to use to log in over a WiFi connection to the device UI of the AP.

   d. From the **Country/Region** menu, select the country where you are using the AP.

In some countries, the AP is sold with a preconfigured country or region setting and you cannot change it.

ⓘ **NOTE:** In some countries, the is sold with a preconfigured country or region setting and you cannot change it.

ⓘ **NOTE:** If you do not see your country or region listed in the menu, update the AP's firmware and check again. If you still do not see your country or region listed, contact NETGEAR support.

ⓘ **NOTE:** Make sure that the country is set to the location where the device is operating. It might not be legal to operate the AP in a region other than the regions listed in the menu. You are responsible for complying with the local, regional, and national regulations that are set for channels, power levels, and frequency ranges.

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

f. Click the **Apply** button.

   Your settings are saved. A summary page displays and the AP restarts.

6. Wait two minutes until the AP completes its restart.

   You are done. The AP is connected to the network and ready to use. You can now connect a computer or mobile device to the user WiFi network that you just set up, using the WiFi password that you just defined.

7. (Optional) To continue to configure the AP for your network and environment, do the following:

   a. Log in again.

      If your browser does not display the login page, enter the IP address that is assigned to the AP in the address field. Use https, not http.

      If your browser display a security warning, proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

   b. In the **Device Password** field, enter your new password for the device UI, and click the **Login** button.

      The Dashboard page displays.

      You can now configure the AP.

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

To log in to the device UI of the AP, use **https://www.aplogin.net** *only* when you connect to the AP over the management WiFi network. For more information, see Management WiFi network on page 45.

For all other types of connections, to log in to the device UI of the AP, use the IP address that was assigned to the AP by your existing router or DHCP server during the setup process (see Initial login process on page 15) .

That means that you must use the assigned IP address to log in to the device UI in all following situations:

- Your WiFi-enabled computer or tablet is connected to one of the user WiFi networks on the AP but not to the management WiFi network.
- Your wired computer is on the same network as the AP.
- Your WiFi-enabled computer or tablet is *not* directly connected to the AP network even if it is on the same network as the AP.
- Your WiFi-enabled computer or tablet *is* connected to the WiFi management network, but the AP 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 AP 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 AP, see Find the IP address of the AP on page 22.

Find the IP address of the AP

By default, the IP address of the AP is **https://192.168.0.100** (which is the same as **https://www.aplogin.net**). When you connect the AP to a network with a DHCP server (or a router that functions as a DHCP server), the AP is assigned a new IP address.

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

- **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 AP device icon, and select **Properties**.

      The AP IP address displays.

- **Option 2: Temporarily connect a computer or tablet directly over WiFi and log in**.

  If you already completed the initial login, temporarily connect a computer or tablet directly to the AP over WiFi and do the following:

  1. Open a web browser from the computer or tablet, which must be directly connected to the AP's management WiFi network.
  2. Enter **https://www.aplogin.net** in the address field.

     A login page displays.

  3. Enter your device password and click the **Login** button.

     The Dashboard page displays.

     In the LAN Information - IPv4 section, the IP Address field displays the IP address that is assigned to the AP.

- **Option 3: Temporarily connect a computer directly over WiFi and ping the AP**.

  If you already completed the initial login, temporarily connect a WiFi-enabled computer directly to the AP's management WiFi network and send a ping to **https://www.aplogin.net**.

  How you can send a ping depends on your computer.

  On your computer, the field with the ping results displays the IP address that is assigned to the AP.

- **Option 4: 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 AP. The IP address that is assigned to the AP is listed.

- **Option 5: 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 AP.

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

Log in to the AP after you complete the initial login process

After you complete the initial login process, the AP is ready for use and you can change the settings and monitor the traffic.

Depending on how you connect to the AP, when you enter **https://www.aplogin.net** or the IP address that is assigned to the AP and you use http, the browser automatically redirects your request to https.

To log in to the AP's device UI after you complete the initial login process:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

The Dashboard page displays various panes that let you see the status of your AP at a glance. You can now configure and monitor the AP.

Change the language

By default, the language of the device UI is automatically detected. You can change the language.

To change the language:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard 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 user WiFi network on the AP

You can manually add a WiFi device such as a WiFi-enabled computer, tablet, or smartphone to a user WiFi network on the AP.

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

NOTE: By default, the AP’s first user WiFi network is enabled but the second, third, and fourth user WiFi networks are disabled. These user WiFi networks differ from the management WiFi network, which you can use only to log in over a WiFi connection to the AP’s device UI.

To connect a device to a user WiFi network on the AP:

1. Make sure that the AP is receiving power and is connected to the Internet (the LED is green or blinking green).
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 AP’s user WiFi networks and select it.

   For the first user WiFi network, you had to specify the WiFi network name (SSID) and associated passphrase (WiFi password) during the initial login process. To connect to the first user WiFi network, look for *that* SSID. If you did not add any additional user WiFi networks, the first user WiFi network is the only user WiFi network that is active on the AP.

   ⓘ **NOTE:** Do not select the AP’s management WiFi network because it does not provide access to the Internet.

4. Enter the WiFi password for WiFi access.

   For the first user WiFi network, you had to specify the passphrase (WiFi password) during the initial login process. To connect to the first user WiFi network, enter *that* WiFi password.

5. Click the **Connect** button.

   The device connects to the user WiFi network of the AP.

3

Manage the Wired Network Settings

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

The chapter includes the following sections:

- Set a static IPv4 address
- Reenable the DHCP client of the AP
- Use an existing management VLAN
- Specify a link-local IPv6 address for the AP
- Manage the STP settings

Set a static IPv4 address

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

To set a static IPv4 address for the AP:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Basic**.

   The page that displays shows the IPv4 Settings, IPv6 Settings, and Spanning Tree Protocol (STP) Settings sections.
5. Select the **Static IP** radio button.

   The IPv4 address fields display.
6. Set 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 opens. 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 AP is back online.

ⓘ **NOTE:** To log back in to the AP, you now must use the static IP address that you assigned.

Reenable the DHCP client of the AP

If you disabled the DHCP client of the AP by assigning a static IP address, you can reenable the DHCP client.

To reenable the DHCP client of the AP:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Basic**.

   The page that displays shows the IPv4 Settings, IPv6 Settings, and Spanning Tree Protocol (STP) Settings sections.
5. Select the **DHCP** radio button.

   The IPv4 address fields no longer display.
6. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window opens. 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 AP is back online.

ⓘ **NOTE:** To log back in to the AP, you now must use the IP address that is assigned by the DHCP server in your network.

To determine the IP address that the DHCP server assigned to the AP, 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 AP 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.
- **IP network scanner**: Use a third-party IP network scanner to scan for the IP address that is assigned to the AP.

Use an existing management VLAN

By default, you can access the device UI from any virtual local area network (VLAN), and management traffic such as traffic from a DHCP server can reach the AP from any VLAN. That is, management traffic is untagged.

If you are familiar with VLANs and you are using them in your network, you can increase the security in your network by specifying an *existing* management VLAN ID so that you can access the device UI from this VLAN only and management traffic can reach the AP over this VLAN only. That is, the management traffic is tagged with the VLAN ID.

⚠ **CAUTION:** The VLAN must already be defined on your network, and the DHCP server (if any), switch (if any), and router to which the AP is connected must be able to reach the AP over this VLAN. Otherwise, when you change the VLAN, connectivity problems might occur, and you might be locked out from the device UI.

To specify an existing management VLAN for the AP:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. Scroll down 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.

   By default, the management VLAN is VLAN ID 1.

8. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window opens. 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 AP is back online.

Specify a link-local IPv6 address for the AP

By default, the DHCP client of the AP is enabled, allowing a device that functions as a DHCPv6 server (usually, a router) in your network to assign an IPv6 address to the AP. You can disable the DHCP client and specify link-local IPv6 address settings for the AP.

To specify link-local IPv6 address settings for the AP:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > 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. 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 opens. 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 AP is back online.

NOTE: To log back in to the AP, you now must use the IPv6 address that you assigned.

Manage the STP settings

By default, Spanning Tree Protocol (STP) is disabled on the AP. You can enable STP and change the settings for STP.

STP can help to prevent a network loop, which can happen in the following situations:

- A network device (such as the AP) is connected to itself, either directly or indirectly.

For example, the AP is connected to switch 1, which is connected to switch 2, which is connected back to the AP.

- Two network devices are connected to each other by more than one path.

  For example, the AP is connected to switch 1; the AP is also connected to switch 2, which is connected to switch 1.

Broadcast storms caused by loops can slow or stop traffic on your network, but STP can prevent loops by ensuring that only one path between each set of network devices is active.

To manage the STP settings:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > 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 following settings:
   - **Status**: Select one of the following radio buttons:
     - **Enable**: STP is enabled.
     - **Disable**: STP is disabled. This is the default setting.
   - **Hello Time**: Enter the interval in seconds between handshake packets that the AP sends to communicate information about the topology throughout the entire bridged LAN.

     The range is from 1–10 seconds. The default is 2 seconds.

- **Max Age**: Enter the period in seconds within which the AP must receive a hello packet from another device in the spanning tree before the AP assumes that the device is inactive.

  The range is from 6–40 seconds. The default is 20 seconds.
- **Forward Delay**: Enter the period in seconds that the AP 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 can analyze data traffic before participating in the network.

  The range is from 4–30 seconds. The default is 15 seconds.
- **Priority**: Enter the priority of the AP in the spanning tree. A smaller number means a higher priority.

  The range is from 0–65535. The default is 32768.

6. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window opens. 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 AP is back online.

4

Manage Basic WiFi Settings

This chapter describes how you can manage basic WiFi settings of the AP. For information about advanced WiFi settings, see Manage Advanced WiFi Settings on page 51.

The chapter includes the following sections:

- User WiFi networks
- Management WiFi network
- Change the AP's device name

! **NOTE:** When you apply changes to the WiFi settings, existing WiFi clients might be temporarily disconnected. For some WiFi clients, users might need to manually reconnect.

User WiFi networks

The AP supports four user WiFi networks that can broadcast on a single band or both radio bands. These four networks are *in addition* to the management WiFi network.

The first time that you logged in to the AP, you were required to set up the name and associated passphrase (WiFi password) of the first user WiFi network. At that time, the AP enabled the first user WiFi network.

The second, third, and fourth user WiFi networks remain disabled until you manually enable and configure them.

Set up or change a user WiFi network with WPA2 or WPA3 personal security

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 password. A WiFi client can only access the WiFi network with the correct WiFi password.

By default, the WiFi security option for a user WiFi network is WPA2/WPA3 personal security. This is also the default security option for the first user WiFi network.

To change the settings for an active user WiFi network or enable and configure a user WiFi network that is secured with WPA2 or WPA3 personal security:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

   If the WiFi network is already enabled, go to Step 8. Otherwise, follow the next two steps.

6. To enable the settings for a disabled WiFi network, select the **Enabled** check box for the WiFi network.

   The options become available.

7. For a new WiFi network (one that was disabled), set the WiFi network name (SSID) and select the radio bands:

   - **SSID**: Set a name for the WiFi network with a maximum of 32 characters. You can use a combination of alphanumeric and special characters.
   - **2.4GHz**: To enable the network to broadcast in the 2.4 GHz radio band, select the **2.4GHz** check box. If you clear the check box, the network does not broadcast in the 2.4 GHz radio band.
   - **5GHz**: To enable the network to broadcast in the 5 GHz radio band, select the **5GHz** check box. If you clear the check box, the network does not broadcast in the 5 GHz radio band.

8. Click the **Edit** button for the WiFi network.

   A new page opens. The page shows more settings for the WiFi network, many of which are described in Manage Advanced WiFi Settings on page 51.

9. In the Wireless Security section, select a WPA personal option from the **Security Mode** menu:

   - **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 with the 802.11ax (Wi-Fi 6) standard to join the SSID. If your network also includes WPA2 devices that do not support the 802.11ax (Wi-Fi 6) standard, 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.

   ! **NOTE:** For these security options, the encryption is always AES.

10. Configure the following settings:
    - **Passphrase**: Set a WiFi password of 8 to 63 characters. To join the SSID, a user must enter this WiFi password.
    - **Group Key Update Interval**: Set 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, set the value to 0.
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 opens. 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 AP is back online.

Set up or change an open user WiFi network

An open network might be appropriate for a WiFi hotspot, or for guest users.

The AP supports a legacy open network that does not provide any security or encryption at all and an opportunistic wireless encryption (OWE) network that does not provide security but does provide encryption if the WiFi device also supports OWE.

To change the settings for an active user WiFi network or enable and configure a user WiFi network that is open or uses OWE:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

   If the WiFi network is already enabled, go to Step 8. Otherwise, follow the next two steps.

6. To enable the settings for a disabled WiFi network, select the **Enabled** check box for the WiFi network.

   The options become available.

7. For a new WiFi network (one that was disabled), set the WiFi network name (SSID) and select the radio bands:

   - **SSID**: Set a name for the WiFi network with a maximum of 32 characters. You can use a combination of alphanumeric and special characters.
   - **2.4GHz**: To enable the network to broadcast in the 2.4 GHz radio band, select the **2.4GHz** check box. If you clear the check box, the network does not broadcast in the 2.4 GHz radio band.
   - **5GHz**: To enable the network to broadcast in the 5 GHz radio band, select the **5GHz** check box. If you clear the check box, the network does not broadcast in the 5 GHz radio band.

8. Click the **Edit** button for the WiFi network.

   A new page opens. The page shows more settings for the WiFi network, many of which are described in Manage Advanced WiFi Settings on page 51.

9. In the Wireless Security section, select the open or OWE option from the **Security Mode** menu:

   - **None**: A legacy open WiFi network does not provide any security. Any WiFi device can join the network. WiFi devices are not authenticated and traffic is not encrypted. We recommend that you do *not* use a legacy open WiFi network without any security. However, a legacy open network might be appropriate for a WiFi hotspot.
   - **OWE**: The WiFi network can only accept WiFi devices that support the WiFi enhanced open feature, which is based on opportunistic wireless encryption (OWE). Select this option only if all the WiFi devices in the WiFi network support OWE. (With this option, WiFi devices that do not support OWE cannot connect.)

10. 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 opens. The window shows the number of changes to be applied.

11. 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 AP is back online.

Set up or change a user WiFi network with WPA2 or WPA3 enterprise security

WPA2 or WPA3 *enterprise-level* security 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 or WPA3) 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.

If a user WiFi network uses WPA2 or WPA3 enterprise-level security, you can also set up a network access server (NAS) that functions with RADIUS and a RADIUS accounting server. For more information, see:

- Set up a network access server for RADIUS for a user WiFi network on page 66
- Set up a RADIUS accounting server for a user WiFi network on page 67

To change the settings for an active user WiFi network or enable and configure a user WiFi network that is secured with WPA2 or WPA3 enterprise security:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

   If the WiFi network is already enabled, go to Step 8. Otherwise, follow the next two steps.

6. To enable the settings for a disabled WiFi network, select the **Enabled** check box for the WiFi network.

   The options become available.

7. For a new WiFi network, set the WiFi network name (SSID) and select the radio bands:

   - **SSID**: Set a name for the WiFi network with a maximum of 32 characters. You can use a combination of alphanumeric and special characters.
   - **2.4GHz**: To enable the network to broadcast in the 2.4 GHz radio band, select the **2.4GHz** check box. If you clear the check box, the network does not broadcast in the 2.4 GHz radio band.
   - **5GHz**: To enable the network to broadcast in the 5 GHz radio band, select the **5GHz** check box. If you clear the check box, the network does not broadcast in the 5 GHz radio band.

8. Click the **Edit** button for the WiFi network.

   A new page opens. The page shows more settings for the WiFi network, many of which are described in Manage Advanced WiFi Settings on page 51.

9. In the Wireless Security section, select an enterprise option from the **Security Mode** menu:

   - **WPA2-Enterprise**: Clients that support WPA2-Enterprise can join the WiFi network but clients that support WPA3-Enterprise *only* cannot join the WiFi network. Clients that support both WPA2-Enterprise and WPA3-Enterprise can join the WiFi network.
   - **WPA3-Enterprise**: Clients that support WPA3-Enterprise can join the WiFi network but clients that support WPA2-Enterprise *only* cannot join the WiFi network. Clients that support both WPA2 and WPA3 can join the WiFi network.
   - **WPA2/WPA3-Enterprise**: This option, enables WiFi devices that support either WPA2-Enterprise or WPA3-Enterprise to join the WiFi network. WPA2-Enterprise is less secure than WPA3-Enterprise.

10. Configure the following RADIUS authentication server settings:

- **SuiteB 192bits** (WPA3-Enterprise only): Select the **Enable** or **Disable** radio button to enable or disable SuiteB 192bits encryption. By default, this option is disabled.

  For the other enterprise security options, you cannot set the encryption.
- **Group Key Update Interval**: Set 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, set the value to 0.
- **Radius Server**: Set the IPv4 address of the RADIUS authentication server. The AP must be able to reach this IP address.
- **Radius Port**: Set the port number that the AP uses to access the RADIUS authentication server. The default port number is 1812.
- **Radius Secret**: Specify the shared key (WiFi password) that is used between the AP and the RADIUS authentication server during the authentication process.

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 opens. 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 AP is back online.

Set up or change a guest WiFi network

The AP supports a total of four user WiFi networks. Each user WiFi network can function either as regular user WiFi network or a *guest* user WiFi network. The essential difference between a regular WiFi network and a guest network is the pool of IP addresses that the network assigns to its WiFi clients.

By default, and regardless of which user WiFi network functions as a guest network, 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 71.

To set up or change a guest WiFi network:

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

If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

   If the WiFi network is already enabled, go to Step 9. Otherwise, follow the next two steps.

6. To enable the settings for a disabled WiFi network, select the **Enabled** check box for the WiFi network.

   The options become available.

7. For a new WiFi network (one that was disabled), set the WiFi network name (SSID) and select the radio bands:

   - **SSID**: Set a name for the WiFi network with a maximum of 32 characters. You can use a combination of alphanumeric and special characters.
   - **2.4GHz**: To enable the network to broadcast in the 2.4 GHz radio band, select the **2.4GHz** check box. If you clear the check box, the network does not broadcast in the 2.4 GHz radio band.
   - **5GHz**: To enable the network to broadcast in the 5 GHz radio band, select the **5GHz** check box. If you clear the check box, the network does not broadcast in the 5 GHz radio band.

8. Select the **Guest Network** check box for the WiFi network.

9. Click the **Edit** button for the WiFi network.

   A new page opens. The page shows more settings for the WiFi network, many of which are described in Manage Advanced WiFi Settings on page 51.

10. In the Wireless Security section, select the open or OWE option, a WPA personal option, or a WPA enterprise from the **Security Mode** menu:

    - **Open**: A legacy open WiFi network does not provide any security. Any WiFi device can join the network. WiFi devices are not authenticated and traffic is not encrypted. We recommend that you do *not* use a legacy open WiFi network without any security. However, a legacy open network might be appropriate for a WiFi hotspot.
    - **OWE**: The WiFi network can only accept WiFi devices that support the WiFi enhanced open feature, which is based on opportunistic wireless encryption (OWE). Select this option only if all the WiFi devices in the WiFi network support OWE. (With this option, WiFi devices that do not support OWE cannot connect.)
    - **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 with the 802.11ax (Wi-Fi 6) standard to join the SSID. If your network also includes WPA2 devices that do not support the 802.11ax (Wi-Fi 6) standard, 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.
    - **WPA2-Enterprise**: Clients that support WPA2-Enterprise can join the WiFi network but clients that support WPA3-Enterprise *only* cannot join the WiFi network. Clients that support both WPA2-Enterprise and WPA3-Enterprise can join the WiFi network.
    - **WPA3-Enterprise**: Clients that support WPA3-Enterprise can join the WiFi network but clients that support WPA2-Enterprise *only* cannot join the WiFi network. Clients that support both WPA2 and WPA3 can join the WiFi network.
    - **WPA2/WPA3-Enterprise**: This option, enables WiFi devices that support either WPA2-Enterprise or WPA3-Enterprise to join the WiFi network. WPA2-Enterprise is less secure than WPA3-Enterprise.

11. If you select a WPA personal option from the **Security Mode** menu, configure the following settings:

    - **Passphrase**: Set a WiFi password of 8 to 63 characters. To join the SSID, a user must enter this WiFi password.
    - **Group Key Update Interval**: Set 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, set the value to 0.

12. If you select a WPA enterprise option from the **Security Mode** menu, configure the following settings:
    - **SuiteB 192bits** (WPA3-Enterprise only): Select the Enable or Disable radio button to enable or disable SuiteB 192bits encryption. By default, this option is disabled.

      For the other enterprise security options, you cannot set the encryption.
    - **Group Key Update Interval**: Set 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, set the value to 0.
    - **Radius Server**: Set the IPv4 address of the RADIUS authentication server. The AP must be able to reach this IP address.
    - **Radius Port**: Set the port number that the AP uses to access the RADIUS authentication server. The default port number is 1812.
    - **Radius Secret**: Specify the shared key (WiFi password) that is used between the AP and the RADIUS authentication server during the authentication process.
13. 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 opens. The window shows the number of changes to be applied.
14. 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 AP is back online.

Management WiFi network

You can use the *management* WiFi network *only* to access the device UI of the AP from a WiFi device for management purposes. That is, you do not get an Internet connection over this WiFi network. (This is a security feature.)

NOTE: The device UI calls the management WiFi network the *Management Interface*.

Only if you are connected to the management WiFi network, you can use **https://www.aplogin.net** to access to the device UI. For more information, see When to use aplogin.net and when to use the assigned IP address on page 22.

NOTE: By default, the idle time-out for the management WiFi network is 15 minutes. That is, if no WiFi client is connected to the management WiFi network for 15 minutes, the management WiFi network is turned off. Only after you restart the AP can you reconnect to the management WiFi network. However, you can disable the idle time-out so that the management WiFi network always stays on (see Disable the management WiFi network on page 48).

The management WiFi network cannot be used for regular WiFi client connections to the AP. For these types of connections, use one of the *user* WiFi networks (see User WiFi networks on page 36).

The name of the management WiFi network is derived from the last six digits of the AP's MAC address. In the following example, XXXXXX represents the MAC address:

WAX210XXXXXX-CONFIG-ONLY

You cannot change this name.

The default WiFi password for the management WiFi network is printed on the AP label. You *can* change this WiFi password and we recommend that you do so for greater security (see Change the password for the management WiFi network on page 46).

Change the password for the management WiFi network

You can change the WiFi password (network key) for the management WiFi network. You cannot change the type of WiFi security.

To change the password for the management WiFi network:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. In the Management Interface section, click the **Edit** button.

   A new page opens. The page shows the Wireless Security section for the management WiFi network.

6. In the **Passphrase** field, enter a new WiFi password for the management WiFi network.

   The length of the password must be from 8 to 63 characters.

   Use this new WiFi password when you connect to the management WiFi network to access the device UI.

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 opens. 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 AP is back online.

Disable the idle time-out for the management WiFi network

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

Only after you restart the AP can you reconnect to the management WiFi network. However, you can disable the idle time-out so that the management WiFi network stays always on.

To disable the idle time-out for the management WiFi network:

1. Launch a web browser from a computer or tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.

2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. In the Management Interface 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 opens. 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 AP is back online.

Disable the management WiFi network

As a security measure, you can entirely disable the management WiFi network. If you do so, you can still reach the AP’s device UI over a wired LAN connection or over one of the user WiFi networks, as long as the WiFi network is in default VLAN 1 and the management VLAN setting is disabled. (These are the default VLAN settings for any WiFi network on the AP.)

To disable the management WiFi network:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. In the Management Interface section, clear the **Enabled** check box.

   By default, this check box is selected.

6. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window opens. 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 AP is back online.

Change the AP's device name

The device name is also referred to as the AP name or system name. It is the AP name that displays in the network. By default, the device name is NETGEARXXXXXX, in which XXXXXX represents the last six characters of the MAC address of the AP's LAN interface. You can change this name.

To change the AP's device name:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. In the **AP Name** field, enter a new name.

   The name can be from 1 to 15 characters, must start and end with alphanumeric characters, cannot contains spaces, and cannot contain symbols, except for a hyphen (-).

6. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window opens. 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 AP is back online.

5

Manage Advanced WiFi Settings

This chapter describes how you can manage advanced WiFi settings of the AP. For information about basic WiFi settings, see Manage Basic WiFi Settings on page 35.

The chapter includes the following sections:

- Hide the name of a user WiFi network
- Isolate clients of a user WiFi network
- Enable L2 isolation for a user WiFi network and optionally set exceptions
- Enable VLAN isolation for a user WiFi network and set a VLAN ID
- Configure band steering for a user WiFi network
- Enable fast roaming for a user WiFi network
- Configure traffic shaping for a user WiFi network
- Manage access to a user WiFi network based on a client's MAC address
- Manually block a WiFi client from a user WiFi network
- Remove a WiFi client from an access control list
- Set up a network access server for RADIUS for a user WiFi network
- Set up a RADIUS accounting server for a user WiFi network
- Set up a WiFi on/off schedule for a user WiFi network
- Change the DHCP server settings for guest WiFi networks

NOTE: When you apply changes to the WiFi settings, existing WiFi clients might be temporarily disconnected. For some WiFi clients, users might need to manually reconnect.

Hide the name of a user WiFi network

By default, a user WiFi network broadcasts its network name (also called the SSID) so that users can detect the WiFi network in the scanned network list of their WiFi device. For additional security, you can turn off the broadcast of the network name and hide it so that users must know the network name to be able to join the user WiFi network.

To hide the name of a user WiFi network:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The Wireless Settings page displays.
5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.
6. Click the **Edit** button for the user WiFi network.

   A new page opens. The page shows more settings for the WiFi network.
7. In the Wireless Setting - Access Point’s SSID section, select the Hidden SSID **Enable** radio button.

   To connect to the WiFi network, a user must know the WiFi network name. By default, this option is disabled and the AP broadcasts the name.
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 opens. 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 AP is back online.

Isolate clients of a user WiFi network

By default, client isolation is disabled for a user WiFi network, allowing communication between WiFi clients that are associated with the same or different user WiFi networks on the AP.

For additional security, you can enable client isolation for a user WiFi network, preventing communication between WiFi clients of the user WiFi network and communication between WiFi clients of the user WiFi network and *another* user WiFi network on the AP. However, if you enable client isolation, WiFi clients can still communicate with each other over the Internet.

To isolate clients of a user WiFi networks on the AP:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The Wireless Settings page displays.
5. Go to the Wireless Settings - Access Point section.

The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

6. Click the **Edit** button for the user WiFi network.

   A new page opens. The page shows more settings for the WiFi network.

7. In the Wireless Setting - Access Point SSID's section, select the Client Isolation **Enable** radio button.

   By default, this option is disabled.

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 opens. 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 AP is back online.

Enable L2 isolation for a user WiFi network and optionally set exceptions

To prevent WiFi clients on a user WiFi network from communicating with each other, with WiFi clients on other user WiFi networks on the AP, and with any LAN (wired) clients that are connected to the AP, enable layer 2 (L2) isolation. By default, this option is disabled.

Optionally, you can set exceptions for up to three clients, based on the MAC addresses of the clients.

A client for which you set an exception can still communicate with another client, provided that you also set an exception for *that* client. However, even clients for which you do not set exceptions can still communicate with each other over the Internet.

To enable L2 isolation and optionally set exceptions:

1. Launch a web browser from a computer or tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.

2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The Wireless Settings page displays.

5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

6. Click the **Edit** button for the user WiFi network.

   A new page opens. The page shows more settings for the WiFi network.

7. In the Wireless Setting - Access Point’s SSID section, select the L2 Isolation **Enable** radio button.

   By default, this option is disabled.

8. To set an exception for a WiFi or wired client, enter the MAC address of the wired or WiFi client in the **Whitelist 1**, **Whitelist 2**, or **Whitelist 3** field.

   In each MAC address field, you can enter a single MAC addresses, so you can set exceptions for a total of three wired and WiFi clients.

   A wired or WiFi client for which you set an exception *can* communicate with another wired or WiFi client on the same user WiFi network, provided that you also set an exception for *that* client.

9. To set an exception for another wired or WiFi client, repeat the previous step but use another MAC address field.

10. 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 opens. The window shows the number of changes to be applied.

11. 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 AP is back online.

Enable VLAN isolation for a user WiFi network and set a VLAN ID

If you are familiar with virtual local area networks (VLANs) and you are using them in your network, you can assign a VLAN ID to a user WiFi network so that all traffic from the network is tagged with the VLAN ID.

WiFi clients on the VLAN can communicate with each other but not with WiFi clients on different VLANs, and the other way around. If you set different VLAN IDs for two user WiFi network, the clients of these different WiFi network cannot communicate with each other. In this way, you are providing extra security for your user WiFi networks.

If you enable VLAN isolation, clients can still communicate with each other over the Internet.

ⓘ **NOTE:** The VLAN that you assign to the user WiFi network must already be defined on your local area network (LAN).

To enable VLAN isolation for a user WiFi network and set a VLAN ID:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The Wireless Settings page displays.
5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

6. Click the **Edit** button for the user WiFi network.

   A new page opens. The page shows more settings for the WiFi network.

7. In the Wireless Setting - Access Point’s SSID section, select the VLAN Isolation **Enable** radio button.

   By default, VLAN isolation is disabled.

8. In the **VLAN ID** field, enter the VLAN ID for the user WiFi network.

   The range is from 1 to 4094. The VLAN ID must be one that you are already using in your LAN.

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 opens. 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 AP is back online.

Configure band steering for a user WiFi network

Band steering lets the AP identify the WiFi devices that are dual-band capable and steer those devices to the 2.4 GHz or 5 GHz band of a user WiFi network. 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.

To configure band steering for a user WiFi network:

1. Launch a web browser from a computer or tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.

2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

6. Click the **Edit** button for the user WiFi network.

   A new page opens. The page shows more settings for the WiFi network.

7. Scroll down to the Band Steering section.

8. Select the Status **Enable** radio button.

   By default, the Status Disable radio button is selected and band steering is disabled.

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 opens. 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 AP is back online.

Enable fast roaming for a user WiFi network

ⓘ **NOTE:** Fast roaming applies only to user WiFi networks for which you set the security option to WPA2-Personal or WPA2-Enterprise at a location that includes two APs that broadcast the same user WiFi network.

Fast roaming helps to improve the performance of mobile devices that are roaming in a user WiFi network, including power consumption and portability. Fast roaming reduces the delay in the connection when WiFi clients roam from one AP to another AP that broadcasts the same user WiFi network at your location.

To enable fast roaming for a user WiFi network:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The Wireless Settings page displays.
5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.
6. Click the **Edit** button for the user WiFi network.

   A new page opens. The page shows more settings for the WiFi network.

   ! **NOTE:** The Fast Roaming section displays on the page only if the security option is WPA2-Personal or WPA2-Enterprise.
7. In the Fast Roaming section, select the **Enable** radio button.

   By default, fast roaming is disabled.
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 opens. 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 AP is back online.

Configure traffic shaping for a user WiFi network

By default, the AP applies no bandwidth limitations for downloading and uploading traffic to any user WiFi network or any WiFi client.

The user WiFi networks are allocated the same amount of bandwidth for downloading and uploading traffic. By shaping the traffic for each user WiFi network, you can control the total bandwidth usage on the AP, or you can control the way the bandwidth is allocated between the user WiFi networks.

Similarly, within a single user WiFi network, all WiFi clients are allocated the same amount of bandwidth for downloading and uploading traffic. By shaping the traffic for the WiFi clients in a user WiFi network, you can control how much bandwidth is allowed for each WiFi client in the user WiFi network.

To configure traffic shaping for a user WiFi network:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.
5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.
6. Click the **Edit** button for the user WiFi network.

A new page opens. The page shows more settings for the WiFi network.

7. Scroll down to the Wireless Traffic Shaping section.
8. Select the Status **Enable** radio button.

   By default, the Status Disable radio button is selected and traffic shaping is disabled (the fields are masked).
9. In the **Download Limit** field, enter the limit, and select **Kbps** or **Mbps** from the associated menu.

   You can enter a limit from 1 Kbps to 999 Mbps.
10. In the **Upload Limit** field, enter the limit, and select **Kbps** or **Mbps** from the associated menu.

    You can enter a limit from 1 Kbps to 999 Mbps.
11. To limit the configured limits to each individual WiFi client (each individual user) of the user WiFi network, select the **Per User** check box.

    If the user WiFi network must provide a WiFi connection to multiple individual users, this option is useful to control the bandwidth usage of individual users.
12. 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 opens. The window shows the number of changes to be applied.
13. 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 AP is back online.

Manage access to a user WiFi network based on a client’s MAC address

By default, the AP does not restrict access to a user WiFi network based on a client’s MAC address.

For each user WiFi network, 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 user WiFi network. An ACL provides added security to ensure that only authorized WiFi devices connect to the user WiFi network:

- **Allow MAC addresses in the list**: 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 user WiFi network.
    - All other WiFi devices are denied a connection to the user WiFi network.
- **Deny MAC addresses in the list**: 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 user WiFi network.
    - All other WiFi devices are allowed to connect to the user WiFi network.

! **NOTE:** If you manually block a WiFi client (see Manually block a WiFi client from a user WiFi network on page 63), an ACL that denies the MAC address of the client is automatically added to the user WiFi network 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 user WiFi network.

The ACL does not apply to the computer or tablet that you use to access the device UI over the *management* WiFi network or over a LAN connection.

To set up a MAC filter for a user WiFi network:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The Wireless Settings page displays.

5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

6. Click the **Edit** button for the user WiFi network.

   A new page opens. The page shows more settings for the WiFi network.

7. Scroll down to the Wireless MAC Filter section.

   By default, the MAC filter is disabled and **Disabled** is selected from the **ACL Mode** menu, allowing all MAC addresses.

8. From the **ACL Mode** menu, select one of the following:

   - **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.
   - **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.

9. To add a 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.

10. 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 opens. The window shows the number of changes to be applied.

11. 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 AP is back online.

Manually block a WiFi client from a user WiFi network

You can manually block a WiFi client or connection from a user WiFi network.

If you do so, an ACL that denies the MAC address of the client is automatically added to the user WiFi network from which you blocked the client. That ACL denies access to the client but allows access to all other clients. You can manually delete the client from the ACL, after which the client is no longer denied access to the user WiFi network. For more information, see Manage access to a user WiFi network based on a client's MAC address on page 61.

To manually block a WiFi client or connection from a user WiFi network:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Overview > Connections**.

   The page that displays shows the Connection List - 2.4GHz table and the Connection List - 5GHz table.
5. To block a connected WiFi device, do the following:
   a. Click the associated **Block** 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 user WiFi network from which you blocked the WiFi device. This ACL denies the WiFi device access to the user WiFi network but allows access to all other WiFi devices. (For more information, see Manage access to a user WiFi network based on a client's MAC address on page 61.)

Remove a WiFi client from an access control list

Removing the MAC address of a WiFi client from an access control list (ACL) can either provide access or block access to the user WiFi network, depending on the type of ACL:

- **Removing allows access**: This applies in the following two situations:
  - You manually blocked a WiFi client or connection from a user WiFi network.
  - You set up an ACL that denies all WiFi clients in the ACL access to the user WiFi network.

  Removing the MAC address from the ACL allows the client access to the user WiFi network.
- **Removing blocks access**: You set up an ACL that allows all WiFi clients in the ACL access to the user WiFi network. Removing the MAC address from the ACL denies the client access to the user WiFi network.

To remove a WiFi client from an ACL for a user WiFi network:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The Wireless Settings page displays.
5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

6. Click the **Edit** button for the user WiFi network.

   A new page opens. The page shows more settings for the WiFi network.

7. Scroll down to the Wireless MAC Filter section, and next to the MAC address of the WiFi client that you want to remove from the ACL, click the **Delete** button.

   The MAC address is removed from the ACL.

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 opens. 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 AP is back online.

Set up a network access server for RADIUS for a user WiFi network

If you use WPA enterprise security (WPA2-Enterprise, WPA3-Enterprise, or WPA2/WPA3-Entertprise) for a user WiFi network and the LAN to which the AP connects includes a RADIUS network access server (NAS) that passes authentication information on to a RADIUS server, you can define the NAS settings for the WiFi user network.

For information about the RADIUS authentication server settings, see .Set up or change a user WiFi network with WPA2 or WPA3 enterprise security on page 40.

To define a RADIUS NAS for a user WiFi network:

1. Launch a web browser from a computer or tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.

2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.

6. Click the **Edit** button for the user WiFi network.

   A new page opens. The page shows more settings for the WiFi network.

7. Scroll down to the Radius Settings section.

   ⓘ **NOTE:** The Radius Settings section display only if the security for the user WiFi network is WPA2-Enterprise, WPA3-Enterprise, or WPA2/WPA3-Entertprise.

8. Configure the following settings:

   a. **NAS-ID**: Select the check box, and enter the ID of the NAS.

   b. **NAS-PORT**: Select the check box, and enter the port number of the NAS.

   c. **NAS-IP**: Select the check box, and enter the IP address of the NAS.

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 opens. 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 AP is back online.

Set up a RADIUS accounting server for a user WiFi network

If you use WPA enterprise security (WPA2-Enterprise, WPA3-Enterprise, or WPA2/WPA3-Entertprise) for a user WiFi network, you can also set up a RADIUS accounting server for the user WiFi network. (You can use WPA enterprise security without using a RADIUS accounting server.)

To set up a RADIUS accounting server for a user WiFi network:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.
5. Go to the Wireless Settings - Access Point section.

   The section shows four WiFi networks. The Enabled check box is selected for enabled WiFi networks and cleared for disabled WiFi networks.
6. Click the **Edit** button for the user WiFi network.

   A new page opens. The page shows more settings for the WiFi network.
7. Scroll down to the Radius Accounting section.

   ⓘ **NOTE:** The Radius Accounting section display only if the security for the user WiFi network is WPA2-Enterprise, WPA3-Enterprise, or WPA2/WPA3-Entertprise.
8. Select the Radius Accounting **Enable** radio button.

   By default, the Disable radio button is selected. and the fields are masked.
9. Configure the following settings:
   a. **Radius Accounting Server**: Enter the IPv4 address of the RADIUS accounting server. The AP must be able to reach this IP address.
   b. **Radius Accounting Port**: Enter the number of the UDP port on the AP that is used to access the RADIUS accounting server. The default port number is 1813.

c. **Radius Accounting Secret**: Enter the password (shared key) that is used between the AP and the accounting RADIUS server during the authentication process.

d. **Interim Accounting Interval**: Enter the period in seconds between each accounting update message that the AP sends to the RADIUS accounting server. The default period is 600 seconds.

10. 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 opens. The window shows the number of changes to be applied.

11. 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 AP is back online.

Set up a WiFi on/off schedule for a user WiFi network

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

You can use a predefined template for a schedule, refine such a schedule, or set a custom schedule. Depending on the schedule settings, WiFi is either turned off or on during the time that you set for a specific day.

ⓘ **NOTE:** 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 91.

To set up a WiFi on/off schedule for a user WiFi network:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Management > WiFi Scheduler**.

   The page that displays shows the Auto Reboot Setting section and the Wi-Fi Scheduler section.

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

   a. **Status**: Select the **Enable** radio button.

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

   b. **SSID Selection**: From the **SSID Selection** menu, select the user WiFi network to which the WiFi on/off schedule applies.

   c. **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 define a custom schedule or refine the settings for another type of schedule, do the following as needed in the Schedule Table:

   a. For each day, from the **Available** menu, select **available** or **unavailable**:

      - **available**: WiFi is turned *on* during the hours that you specify in the **Duration** fields for the selected day.
      - **unavailable**: WiFi is turned *off* during the hours that you specify in the **Duration** fields for the selected day.

   b. For each day, in the **Duration** fields, specify the start hour and minutes and the end hour 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.

   A pop-up window opens. 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 AP is back online.

Change the DHCP server settings for guest WiFi networks

A WiFi client that connects to a guest network (see Set up or change a guest WiFi network on page 42) is assigned an IP address in a different address range than a regular WiFi client. By default, the IP address range for guest WiFi clients is from 192.168.200.100 to 192.168.200.199.

If the DHCP address range in your network conflicts with the default IP address range for guest WiFi clients, you can change the DHCP IP address and subnet mask for guest WiFi clients, as well as the automatic DHCP server address assignment settings for guest WiFi clients. These settings apply to all WiFi guest networks on the AP.

You can change the DHCP server settings for a guest network only if you enable at least one guest network on a user WiFi network (see Set up or change a guest WiFi network on page 42).

To change the DHCP server settings for all guest WiFi networks:

1. Launch a web browser from a computer or tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.

2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

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 enable the guest network capability on a user WiFi network. Otherwise, the fields are masked.

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 192.168.200.199.
WINS Server IP	The IP address of the server that provides Windows Internet Name Service (WINS).

7. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window opens. 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 AP is back online.

6

Manage the WiFi Radio Settings

This chapter describes how you can manage the WiFi radio settings, which affect all user WiFi networks on the AP.

The chapter includes the following sections:

- Change the country and region of operation
- Manage the channel high throughput mode
- Manage the WiFi channels
- Manage the radio transmit power
- Change the minimum bit rate
- Manage client limits

NOTE: When you apply changes to the WiFi radio settings, existing WiFi clients might be temporarily disconnected. For some WiFi clients, users might need to manually reconnect.

Change the country and region of operation

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

- In some countries, the AP is sold with a preconfigured country or region setting and you cannot change it.
- If you do not see your country or region listed in the menu, update the AP's firmware and check again. If you still do not see your country or region listed, contact NETGEAR support.
- Make sure that the country is set to the location where the device is operating. It might not be legal to operate the AP in a region other than the regions listed in the menu. You are responsible for complying with the local, regional, and national regulations that are set for channels, power levels, and frequency ranges.

To change the country and region of operation of the AP:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.
5. From the **Country / Region** menu, select the country and region in which the AP is operating.
6. Click the **Save** button.

Your settings are saved but not yet applied.

A pop-up window opens. 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 AP is back online.

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**: 20 MHz
- **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.
- The 802.11ac and 802.11ax specifications allow an 80 MHz–wide channel and an 160 MHz–wide channel in addition to the 20 MHz and 40 MHz channels.
- The 40 MHz, 80 MHz, and 160 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 tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.
2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

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**, **80MHz** (the default setting), or **160MHz**.

7. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window opens. 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 AP is back online.

Manage the WiFi channels

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

! **NOTE:** You do not need to change the channel unless you experience interference, which can be indicated by lost connections.

If you use multiple access points, you can reduce interference by selecting non-overlapping 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 74). 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 WiFi channels:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.
5. Click the Channel **Configuration** button.

   A new page opens. The page shows the available channels for the 2.4 GHz radio band and 5 GHz radio band. The available channels depend on the country and region that you selected for the AP.
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:
   - **Automatic channel allocation for a radio**: To enable automatic channel allocation for a radio, click the **All** button for the radio.
   - **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.
- **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 AP.

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 opens. 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 AP is back online.

Manage the radio transmit power

By default, the AP's radios transmit at full power.

If you have several APs in your network, interference could occur at full power. You can set one or both radios to transmit at half or a quarter power. However, if you set the transmit power too low, WiFi clients might not be able to connect to the AP.

If the AP is the only AP in your network and your WiFi devices are all fairly close to the AP, you could use a lower radio transmit power, allowing you to save some energy.

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 74). 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 for a radio:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

5. From the **Transmit Power** menu for a radio, select **Full** (the default), **Half**, or **Quarter**.
6. Click the **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window opens. 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 AP is back online.

Change the minimum bit rate

The AP 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:** By default, 802.11b legacy clients cannot connect to the 2.4 GHz radio because the default bit rate is set too high for them. If your network includes 802.11b clients, lower the bit rate for the 2.4 GHz radio so that these clients too can connect to the AP.

To change the minimum bit rate:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.

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

   A new page opens. The page shows the bit rate settings.

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 AP, 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 a white dot that represents a 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 opens. 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 AP is back online.

Manage client limits

By default, a maximum of 64 WiFi clients can associate with each radio on the AP. (A WiFi client is the same as a WiFi device.) The AP can support a total of 128 WiFi clients.

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 user WiFi networks on the radio. For example, if two user WiFi networks are active on the 2.4 GHz radio band, the maximum number of 64 clients applies to the two networks on the 2.4 GHz radio band, that is, *together* these networks cannot support more than 64 clients on the 2.4 GHz radio band. You cannot set client limits for individual user WiFi networks.

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 for a radio:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.
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 opens. 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 AP is back online.

7

Maintain the AP

This chapter describes how you can maintain the AP.

The chapter includes the following sections:

- Update the AP firmware
- Back up or restore the configuration file
- Change the AP device password and idle session time-out period
- Manage the date and time settings
- Restart the AP from the device UI
- Schedule the AP to automatically restart
- Reset the AP to factory default settings using the device UI
- SNMPv1, SNMPv2, and SNMPv3
- Enable or disable UPnP

Update the AP firmware

You can log in to the AP and check if new firmware is available, you can configure the AP to automatically check for new firmware, and you can manually install a specific firmware version on your AP.

Check for new firmware and update the AP

The AP firmware (AP software) is stored in flash memory. If the automatic firmware upgrade check is enabled, you might see a message *A new firmware upgrade is available* at the top of the device UI pages when new firmware is available. You can respond to that message to update the firmware or you can check to see if new firmware is available and update your product.

To check for new firmware and update your AP:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **System Manager > Firmware**.

   The page that displays shows the Automatic Firmware Upgrade Check section and the Local Firmware Upgrade section.
5. Click the **Check for New Firmware** button.

The AP finds new firmware information. If any is available, the New Firmware Version field shows the version, the Release Date field shows when the firmware was released, and the Upgrade Firmware button displays.

6. Click the **Upgrade Firmware** button.

   The AP locates and downloads the firmware and begins the update.

   The page displays the update progress.

   ⚠ **WARNING:** To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not close the browser, click a link, or load a new page. Do not turn off the AP. Wait until the AP finishes.

   When the update is finished, you can log back into the AP. After you log in, the firmware version displays on the Dashboard page.

Manually update the AP firmware

You can visit the NETGEAR support website at netgear.com/support/download/ to determine if new firmware is available for the AP.

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

ⓘ **NOTE:** Before you update 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 AP after a firmware update.

To manually update the firmware on the AP:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

The Dashboard page displays.

4. Select **System Manager > Firmware**.

   The page that displays shows the Automatic Firmware Upgrade Check section and the Local Firmware Upgrade section.

5. Locate and select the firmware file on your computer by doing the following:

   a. In the Local Firmware Upgrade section, click the **Choose File** button.

   b. Navigate to the firmware file and select it.

6. Click the **Upload** button.

   The page displays the update progress.

   ⚠ **WARNING:** To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not close the browser, click a link, or load a new page. Do not turn off the AP. Wait until the AP finishes.

   When the update is finished, you can log back into the AP. After you log in, the firmware version displays on the Dashboard page.

Manage the firmware update settings

You can set the AP to automatically check for future firmware versions as they become available. If new firmware is available, the device UI displays a message *A new firmware upgrade is available*, and you can respond to that message to update the firmware.

To manage automatic updates for future firmware versions:

1. Launch a web browser from a computer or tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.

2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **System Manager > Firmware**.

   The page that displays shows the Automatic Firmware Upgrade Check section and the Local Firmware Upgrade section.

5. Select one of the following Status radio buttons.

   - **Enable**: The AP automatically checks for future firmware versions as they become available. We recommend that you select this setting so that you get the latest security and feature updates as soon as they are available.
   - **Disable**: The AP does not automatically update to future firmware versions. This is the default setting. You must manually check for and update to future firmware versions.

6. Click the **Apply** button.

   Your settings are saved and applied.

Back up or restore the configuration file

The configuration settings of the AP are stored within the AP 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 AP 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 AP's configuration settings:

1. Launch a web browser from a computer or tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.

2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **System Manager > Backup/Restore**.

   The page that displays shows the Backup/Restore Settings section.

5. Click the Backup Settings **Export** button.

   A pop-up window opens.

6. Choose a location to store the file on your computer.

   The default name of the backup file is `backup-NETGEARXXXXXX-yyyy-mm-dd.tar.gz`, in which XXXXXX are the last six digits of the MAC address of the LAN interface, yyyy is the year, mm is the month, and dd is the date. If you change the device name (see Change the AP's device name on page 49), *that* name is shown in the backup file.

   An example of a name of a backup file is `backup-NETGEAR123456_2024-05-05.tar.gz`.

7. Save the file.

Restore the AP configuration settings

If you backed up the configuration settings (see Back up the AP configuration settings on page 87), you can restore the configuration settings from the backup file.

To restore the AP's configuration settings from the backup file:

1. Launch a web browser from a computer or tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.

2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **System Manager > Backup/Restore**.

   The page that displays shows the Backup/Restore Settings section.

5. Click the Restore New Setting **Choose File** button and navigate to and select the saved configuration file (that is, the backup file).

   The default name of the backup file is `backup-NETGEARXXXXXX-yyyy-mm-dd.tar.gz`, in which XXXXXX are the last six digits of the MAC address of the LAN interface, yyyy is the year, mm is the month, and dd is the date. If you change the device name (see Change the AP’s device name on page 49), *that* name is shown in the backup file.

   An example of a name of a backup file is `backup-NETGEAR123456_2024-05-05.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 AP. Wait until the AP finishes.

   When the restoration is finished, the login page displays.

Change the AP device password and idle session time-out period

The device password is the password that lets you log in to the device UI of the AP.

The first time that you logged in to AP and set up the AP, you defined the device password. You can change it.

Your password must meet the following conditions:

- Contains 8 to 32 characters
- At least one uppercase character
- At least one lowercase character

- At least one number
- At least one special character, such as the following characters:

  @ # $ % ^ & * ( ) !

The idle session time-out period is the time after which you are automatically logged out from the device UI if no configuration activity is detected.

To change the device password and idle session time-out period:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **System Manager > Account**.

   The page that displays shows the Account Settings section and the Idle Session Timeout Settings section.

   You cannot change the administrator user name. It is always admin.
5. In the **Current Password** field, enter your current device password.
6. In the **New Password** and **Verify Password** fields, enter the new device password.
7. To change the idle session time-out period, from the **Hour** and **Minutes** menus, select a new time-out period.

   The minimum time-out period is 15 minutes.
8. Click the **Apply** button.

   Your settings are saved and applied.

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

Manage the date and time settings

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

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

To manage the date and time settings:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Management > 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:
     - o 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 device UI of the AP by clicking the **Synchronize with PC** button.

- **Automatically Get Date and Time**: The AP 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.
7. To enable the daylight saving time adjustment, select the **Enable Daylight Saving** check box and set the start and end dates and times for the daylight saving time.
8. Click the **Apply** button.

   Your settings are saved and applied.

Restart the AP from the device UI

You can use the device UI to restart the AP. This is useful if the AP is installed at a location that is not easy to reach. Restarting the AP takes two minutes.

To restart the AP from the device UI:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. In the top banner of the page, click the **Reboot/Reset** button.

A pop-up window displays.

5. Click the **Reboot the device** button.

   A pop-up window displays.

6. Click the **OK** button.

   The AP restarts. The page displays the progress.

   ⚠ **WARNING:** To avoid the risk of corrupting the firmware, do not interrupt the restart. For example, do not close the browser, click a link, or load a new page. Do not turn off the AP. Wait until the AP finishes, which takes two minutes.

   When the restart is finished, the login page displays.

Schedule the AP to automatically restart

You can schedule the AP to automatically restart 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 AP to automatically restart:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Management > WiFi Scheduler**.

The page that displays shows 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 AP to automatically restart.
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 **Apply** button.

   Your settings are saved and applied.

Reset the AP to factory default settings using the device UI

Under some circumstances (for example, if you lost track of the changes that you made to the configuration of the AP or you move the AP to a different network), you might want to erase the configuration and reset the AP to factory default settings (see Factory default settings on page 130). Resetting the AP to factory default settings takes ten minutes.

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

You can use either the physical **Reset** button on the AP (see Hardware interfaces on page 9) or the software **Reset** button in the device UI.

After you reset the AP to factory default settings, the default settings are as follows:

- The LAN IP address is https://192.168.0.100, which is the same as https://www.aplogin.net.
- The AP's DHCP client is enabled,
- The management WiFi network is shown in the format WAX210XXXXXX-CONFIG-ONLY, where XXXXXX is customized to every device (based on the last six digits of the MAC address).
- The default password for WiFi access to the management WiFi network is a unique WiFi password that is printed on the AP label.

For a list of factory default settings, see Factory default settings on page 130.

⚠ **CAUTION:** Resetting to factory defaults erases all settings that you configured in the AP.

To reset the AP to factory default settings using the device UI:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **System Manager > Backup/Restore**.

   The page that displays shows the Backup/Restore Settings section.
5. Click the Reset to Default **Reset** button.

   A pop-up window displays.
6. Click the **OK** button.

   The page displays the reset progress.

   If you can see the LED of the AP, the LED lights as follows:

   a. Solid amber for 5 seconds

   b. Slow blinking amber for 5 to 10 seconds

   c. Fast blinking amber during the remainder of the reset process

   ⚠ **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 AP. Wait until the AP finishes, which takes ten minutes.

   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 AP and the same as www.aplogin.net.
7. If your AP 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.

The start page for the setup process displays. This page lets you select the country or region in which you are using the AP, define the device password for the AP's device UI, create the first user WiFi network (SSID) with its associated passphrase (WiFi password), and accept NETGEAR's terms of use.

If the start page does not display, you might need to enter another IP address. Note the following:

- If you do not know the IP address, see Find the IP address of the AP on page 22.
- Use https, not http.
- Your browser might display a security warning because of the self-signed certificate on the AP, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

SNMPv1, SNMPv2, and SNMPv3

The AP supports Simple Network Management Protocol (SNMP), which lets SNMP network management software access and manage the access point by using the SNMPv1, SNMPv2, or SNMPv3 protocol. By default, SNMP is disabled on the AP.

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 AP:

To enable SNMPv1 and SNMPv2 and manage the settings:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Management > Advanced**.

   The page displays the SNMP Settings section and the Email Alert section.

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:

   - **Contact**: Enter the contact name for SNMP management.

     This is an optional field for information only.

   - **Location**: Enter the location for SNMP management.

     This is an optional field for information only.

   - **Community Name (Read Only)**: Enter the community string that enables the SNMP management station to read the AP’s MIB objects.

     The default is public. We recommend that you change the community string to a secure (complex) string.

   - **Community Name (Read Write)**: Enter the community string that enables the SNMP management station to read and write the AP’s MIB objects.

     The default is private. We recommend that you change the community string to a secure (complex) string.

   - **Port**: Enter the port number at which the SNMP management station must receive traps.

     The default is port number 162.

   - **IP Address**: Enter the IP address of the SNMP management station that must receive traps.

   - **Community Name**: Enter the community name that is associated with the IP address that must receive traps.

     The default is public. We recommend that you change the community name to a secure (complex) name.

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 AP:

To enable SNMPv3 and manage the settings:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Management > Advanced**.

   The page displays the SNMP Settings section and the Email Alert section.
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 make sure that the Status **Enable** radio button is selected.
7. Configure the following SNMPv3 settings:
   - **Username**: Enter 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.

- **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**: Enter the unique ID that identifies the AP as an SNMP agent.

  You can also keep the default ID.

8. Click the **Apply** button.

   Your settings are saved and applied.

Enable or disable UPnP

Universal Plug and Play (UPnP) lets the AP be discovered by other devices in a network that support UPnP. For enhanced security, UPnP is disabled by default, but you can enable it.

To enable or disable UPnP:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Management > UPnP**.

   The page that displays shows the UPnP Settings section.

5. Select a Status radio button:

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

6. Click the **Apply** button.

   Your settings are saved and applied.

8

Monitor the AP and its Network Connections

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

The chapter includes the following sections:

- Display the AP device, memory, LAN, and WiFi status information
- Display the WiFi connections
- Display the CPU, user WiFi network, and LAN traffic loads
- Scan for neighboring access points and WiFi routers
- Set up email alerts
- Logs

Display the AP device, memory, LAN, and WiFi status information

You can display AP device information, memory information, Ethernet LAN information for IPv4, WiFi LAN information, and statistics.

To display the AP device status and other information:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

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

   The following tables describe the information on the page.

Table 1. Device Information section

Setting	Description
AP Name	The device name (system name). For more information, see Change the AP's device name on page 49.
Serial Number	The fixed serial number of the AP.
MAC Address LAN	The fixed MAC address of the LAN/PoE+ port.
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.

Table 1. Device Information section (Continued)

Setting	Description
Country/Region	The country and region that you set for the AP operation. For more information, see Change the country and region of operation on page 74.
Current Local Time	The time that the AP detected. For more information, see Manage the date and time settings on page 91.
Uptime	The period since that last time the AP started or rebooted.
Firmware Version	The firmware version. For more information, see Update the AP firmware on page 84.
Device Version	The device version.
Management VLAN ID	Shows whether management traffic is tagged or untagged. For more information, see Use an existing management VLAN on page 30.
LAN Speed	The speed of the LAN/PoE port.

Table 2. Memory Information section

Setting	Description
Total Available	The total memory in kB and the available memory in kB and percentage. **Note**: 1 kB = 1 kilobit = 1000 bits.
Free	The total memory in kB and the free memory in kB and percentage.
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 3. LAN Information - IPv4 section

Setting	Description
IP Address	The IPv4 address that is assigned to the LAN/PoE+ port of the AP. This is the IPv4 address over which you can reach the device UI. For more information, see Set a static IPv4 address on page 28.
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 AP is enabled (which it is by default). For more information, see Reenable the DHCP client of the AP on page 29.
Spanning Tree Protocol (STP)	Shows whether STP is enabled (which it is by default). For more information, see Manage the STP settings on page 32.

Table 4. LAN Information - IPv6 section

Setting	Description
IP Address	The IPv6 address that is assigned to the LAN port of the AP. This is the IPv6 address over which you can reach the local browser UI.
Link-Local Address	The link-local IPv6 address of the AP. For more information, see Specify a link-local IPv6 address for the AP on page 31.
Gateway	The IPv6 address of the gateway.
Primary DNS	The IPv6 address of the primary DNS server.
Secondary DNS	The IPv6 address of the secondary DNS server, if any.

Table 5. 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 75.
Channel	The WiFi channel. For for information, see Manage the WiFi channels on page 76.

Table 6. 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 75.
Channel	The WiFi channel. For for information, see Manage the WiFi channels on page 76.

Table 7. Statistics Access Point 2.4GHz/5GHz section

Setting	Description
Profile	The profile number from 1 to 4 for the user WiFi network.
SSID	The WiFi network name.
Security	The type of WiFi security on the SSID.
VID	The VLAN ID (VID), if any, that is configured for the SSID.
802.1Q	Shows whether VLAN isolation is enabled.
RX (Packets)	The amount of packets in B, MB, or GB and the number of packets that is received on the SSID.
TX (Packets)	The amount of packets in B, MB, or GB and the number of packets that is transmitted on the SSID.

Display the WiFi connections

You can display the WiFi connections (the list of connected devices) on each radio.

To display the WiFi connections:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Overview > Connections**.

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

   For each radio band, the total number of connections is shown.

Table 8. Connected WiFi device information

Setting	Description
Hostname	The device name of the connected WiFi device.
OS	The operating system that the connected WiFi device is using.
IP	The IP address that the AP assigned to the WiFi device. For WiFi devices that connect to a regular user WiFi network, the IP address is one from the address range that the DHCP server (or router) in your network assigns. For WiFi devices that connect to a *guest* user WiFi network, the IP address is from a different address range that you can customize (see Change the DHCP server settings for guest WiFi networks on page 71).
Mode	The WiFi mode that the connected WiFi device is using (for example, 802.11ac).
MAC Address	The unique MAC address of the connected WiFi device.

Table 8. Connected WiFi device information (Continued)

Setting	Description
SSID	The SSID (user WiFi network) on which the WiFi device is connected.
TX (KB)	The total amount of traffic in kilobyte (KB) that the WiFi device transmitted.
RX (KB)	The total amount of traffic in kilobyte (KB) that the WiFi device received.
RSSI (dBm)	The received signal strength indicator (RSSI) for the WiFi device. The RSSI is expressed in minus decibel-milliwatts (dBm). A higher value such as –35 means a stronger signal; a lower value such as –70 means a weaker signal.
Block	Whether the WiFi device is blocked from the user WiFi network. For more information, see the next step.

5. To block a connected WiFi device, do the following:
   a. Click the associated **Block** 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 user WiFi network from which you blocked the WiFi device. This ACL denies the WiFi device access to the user WiFi network but allows access to all other WiFi devices. (For more information, see Manage access to a user WiFi network based on a client's MAC address on page 61 and Remove a WiFi client from an access control list on page 65.)
6. To refresh the information on the page, click the **Refresh** button.

Display the CPU, user WiFi network, and LAN traffic loads

You can display the CPU, user WiFi network, and LAN traffic loads on the AP.

To display the CPU, user WiFi network, and LAN traffic loads:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **Overview > Resource Usage**.

   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 user WiFi network and for the LAN.

   If only one user WiFi network is active, the traffic information for the network displays (see the information in the next step).

6. To display the traffic information for a user WiFi network, select the tab for the network.

   The page displays traffic information for the network.

   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 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.

Scan for neighboring access points and WiFi routers

Scanning for neighboring access points and WiFi routers is useful if you notice interference between your AP and other APs or WiFi routers. You can then adjust the channels on which your AP broadcasts (see Manage the WiFi channels on page 76).

To scan for neighboring access points and WiFi routers:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Network > Wireless**.

   The page that displays shows the Wireless Settings section and other sections.
5. Click the AP Detection **Scan** button for one of the radios.

   A new page opens. After the AP completes its scan for neighboring access points and WiFi routers in the selected radio band, the page displays (for each detected AP) 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 AP detects.
Channel	The radio channel on which the SSID is being broadcast.

(Continued)

Setting	Description
Signal Level	The strength of the WiFi signal that is being broadcast, expressed in percentage. A higher percentage means a stronger signal.
Type	The WiFi mode that is configured for the SSID (for example, 11b/g/n).
Security	The type of security, if any, that is configured for the SSID (for example, WPA2-PSK).

6. To repeat the scan for the radio band, click the **Repeat scan** button.

   The page refreshes with the most recent information.

Set up email alerts

You can specify an email address to which the AP automatically can send an alert when the configuration of the AP is changed.

To set up email alerts:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Management > Advanced**.

   The page displays the SNMP Settings section and the Email Alert section.
5. In the Email Alert section, configure the following settings:

   a. Select the Status **Enable** check box.

The fields 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 default subject information is a combination of the AP model number and MAC address of the LAN interface, as shopwn in the following example:

[Email-Alert][WAX210][*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 AP 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 SMTP server does not use security. This is the default setting.
- **SSL/TLS**: The SMTP server uses the SSL or TLS security protocol
- **STARTTLS**: The SMTP 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 **Save** button.

   Your settings are saved but not yet applied.

   A pop-up window opens. 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 AP is back online.

Logs

The AP 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 AP 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.

Display 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 AP logs. You can also download the messages and clear the message log.

To display and manage the system log:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **System Manager > Log**.

   The page that displays shows the System Log section.
5. To manage the log capability, select one of the following Status radio buttons:
   - **Enable**: The AP logs messages.

     This is the default settings.
   - **Disable**: The AP does not log messages.
6. To select the event severity that the AP 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 events at the Error, Critical, Alert, and Emergency security levels.

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 AP send log messages to a remote log server, which is also referred to as a remote syslog host.

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

To set up a remote log server:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

A login page displays.

If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.

3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.

4. Select **System Manager > Log**.

   The page that displays shows the System Log section.

5. To manage the remote log server capability, select one of the following Remote Log radio buttons:

   - **Enable**: The AP sends log messages to a remote log server.

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

   - **Disable**: The AP 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 AP sends its traffic log to the remote log server.

   - **Disable**: The AP 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 AP 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.

9

Perform Diagnostics and Troubleshooting

This chapter describes how you can perform diagnostics and troubleshoot the AP and its network connections.

The chapter includes the following sections:

- Send a ping
- Send a traceroute request
- Send a name server lookup request
- Perform a speed test for the connection to a WiFi client
- Quick tips for WiFi troubleshooting
- Troubleshoot with the LED
- Troubleshoot the WiFi connectivity
- Troubleshoot Internet browsing
- You cannot log in to the AP over a LAN connection
- Changes are not saved in the device UI
- Troubleshoot your network using the ping utility of your computer

Send a ping

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

To send a ping:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Management > 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 AP 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 AP must send.

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

   The AP sends the ping. The results display on the page.

Send a traceroute request

The AP can send a traceroute request to an IPv4 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 tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.
2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Management > 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 AP sends the traceroute request. By default, the traceroute request consists of a 46-byte packet and can detect a maximum of 30 hops. The results display on the page.

Send a name server lookup request

The AP 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 tablet that is directly connected over WiFi to the AP or connected to the same network as the AP.
2. Enter the IP address that is assigned to the AP.

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Management > 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 AP sends the name server lookup request. The results display on the page.

Perform a speed test for the connection to a WiFi client

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

You can find the IP addresses of WiFi clients on the Connection page (see Display the WiFi connections on page 105).

To perform a speed test for the connection to a WiFi client:

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

   If you are directly connected to the management WiFi network, you can enter **https://www.aplogin.net**.

   A login page displays.

   If you do not know the IP address, see Find the IP address of the AP on page 22. For more information about the management WiFi network, see Management WiFi network on page 45.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
3. Enter the device password and click the **Login** button.

   The device password is the one that you specified the first time you logged in to the AP. The device password is case-sensitive.

   The Dashboard page displays.
4. Select **Management > 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** field, enter the IP address of the WiFi client.

   You can find the IP address of a WiFi client on the Connection page (see Display the WiFi connections on page 105).
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.

   ! **NOTE:** 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 AP 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, try power cycling your AP:

1. Unplug the Ethernet cable from the AP to your network switch.
2. If you use a power adapter, disconnect it from the AP.
3. Plug in the Ethernet cable from the AP to your network switch. Wait five minutes.
4. If you use a power adapter, connect it to the AP. Wait five minutes.

If someone cannot connect with a WiFi device to the AP, try the following:

- **Do the WiFi settings match?** Make sure that the WiFi settings in the WiFi device and AP 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 user WiFi network.

  The user WiFi network and WiFi security settings of the AP and WiFi device must match exactly. For more informations about these settings and the radio bands, see User WiFi networks on page 36.

- **Is the type of security supported?** Make sure that the WiFi device supports the authentication and encryption that is configured for the user WiFi network. For more information, see User WiFi networks on page 36.

  ! **NOTE:** If the AP’s WiFi authentication and encryption is set to WPA2/WPA3-Personal, make sure that the WiFi adapter device driver is updated to the latest version on the WiFi device.

- **Did the WiFi on/off schedule turn off the radios?** If you set up a WiFi on/off schedule, the schedule might be active and turned off broadcast of the user WiFi network. For more information, see Set up a WiFi on/off schedule for a user WiFi network on page 69.

- **Is the user WiFi network hidden?** If the AP’s user WiFi network 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 user WiFi network broadcast, see Hide the name of a user WiFi network on page 52.

- **Are both radios disabled for the user WiFi network?** Make sure that both radios are not disabled for the user WiFi network. If the radios are disabled, in the device UI, both the 2.4 GHz and 5 GHz check boxes are cleared for the user WiFi network. For more information, see User WiFi networks on page 36.
- **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 Manage access to a user WiFi network based on a client's MAC address on page 61).
- **Does the device functions as a DHCP client?** Make sure that the WiFi device does not use a static IP address but is configured as a DHCP client to receive an IP address automatically from the AP. (For most devices, DHCP is the default setting.)
- **Is the device at the wrong location?** Make sure that the WiFi device is not too far from the AP or too close. To see if the signal strength improves, move the WiFi device near the AP 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 AP and the WiFi device.

Troubleshoot with the LED

For general information about the LED, see Top panel with LED on page 8.

When you connect the AP to a power source, the LED lights as described here:

1. **The LED lights solid amber**: The AP is receving power and starting.
2. **The LED lights slow blinking amber**: The Internet connection is in the process of being set up.
3. **The LED lights solid or blinking green**: The AP is functioning with Internet connectivity. If the LED is blinking green, at least one WiFi client is connected and sending or receiving traffic.

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

- LED remains off on page 121
- LED remains solid amber on page 121
- LED remains slow blinking amber on page 122

LED remains off

ⓘ **NOTE:** If you do not use a power adapter, the AP requires PoE (802.3af) power.

PoE connection: If you use a PoE connection and the LED remains off when you connect the Ethernet cable to a PoE switch, do the following:

- Make sure that the Ethernet cable between the AP and the PoE switch is correctly connected at both ends.
- Make sure that the other end of the Ethernet cable is plugged into a PoE port, not a regular (non-PoE) port.
- Make sure that the switch is actually receiving power.
- Make sure that the PoE power budget of the PoE switch is not oversubscribed so that the switch is capable of delivering PoE power to the AP. Most PoE switches have LEDs that indicate when they are providing PoE power on a port and an LED that indicates PoE oversubscription.

Power adapter: If you use a power adapter and the LED remains off when you provide power to the AP, do the following:

- Make sure that the power adapter is correctly connected to the AP, 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.

LED remains solid amber

If the LED remains solid amber five minutes after the AP started, a boot error occurred or the AP is malfunctioning.

Do the following:

- Make sure that you are using the correct Ethernet cable, that the cable is correctly inserted a both ends, and that the device at the other end is powered up.

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.

- If the LED remains solid amber, disconnect the AP from its power source, reconnect it, and wait five minutes to see if the startup procedure completes successfully.
- If the LED still remains solid amber after five minutes, use the **Reset** button (see Hardware interfaces on page 9) to return the AP to its factory default settings.

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.

LED remains slow blinking amber

During regular operation, the only time that the LED blinks amber temporarily is when firmware is being upgraded. Also, in that situation, the LED blinks amber quickly, not slowly. If the AP blinks amber slowly and continuously, the AP did not receive an IP address from a DHCP server, or the AP does not detect an Ethernet link.

Check to make sure that the DHCP client of the AP is enabled (it is enabled by default; otherwise see Reenable the DHCP client of the AP on page 29), that your network includes a DHCP server (or a router that functions as a DHCP server), and that the DHCP server can reach the AP (both must be on the same network).

In the unlikely situation that your network does not include a DHCP server, you might need to configure a fixed (static) IP address on the AP (see Set a static IPv4 address on page 28).

If the problems is not resolved, do the following:

- Make sure that you are using the correct Ethernet cable, that the cable is correctly inserted a both ends, and that the device at the other end is powered up.

  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.
- If the LED remains slow blinking amber, disconnect the AP from its power source, reconnect it, and wait five minutes to see if the AP can detect and Ethernet link.
- If the LED still remains slow blinking amber after five minutes, use the **Reset** button (see Hardware interfaces on page 9) to return the AP to its factory default settings.

Troubleshoot the WiFi connectivity

If you want to change the WiFi settings of the AP'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 AP

If a WiFi device cannot connect to the AP or the WiFi connectivity is not normal, try to isolate the problem:

- **Do the WiFi network name (SSID), WiFi security, and radio band settings match?** Make sure that the WiFi settings in the WiFi device and AP 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 user WiFi network.

  The SSID and WiFi security settings of the AP and WiFi device must match exactly. For more informations about these settings and the radio bands, see User WiFi networks on page 36.
- **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 user WiFi network. For more information, see User WiFi networks on page 36.

  ! **NOTE:** If the AP'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 AP?**
  - **Did the WiFi on/off schedule turn off the radios?** If you set up a WiFi on/off schedule, the schedule might be active and turned off broadcast of the user WiFi network. For more information, see Set up a WiFi on/off schedule for a user WiFi network on page 69.
  - **Is the user WiFi network hidden?** If the AP's user WiFi network 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 user WiFi network broadcast, see Hide the name of a user WiFi network on page 52.
- **Is the device at the wrong location?** Make sure that the WiFi device is not too far from the AP or too close. To see if the signal strength improves, move the WiFi device near the AP 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 AP 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 Manage access to a user WiFi network based on a client’s MAC address on page 61).
- **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 to the management WiFi network

You can use the management WiFi network only to access the device UI of the AP from a WiFi device for management purposes. The management WiFi network cannot be used for regular WiFi client connections to the AP. Regular WiFi clients must access a user WiFi network.

If you cannot connect over the management WiFi network, check the following:

- **Was the management WiFi network automatically turned off?** By default, the idle time-out for the management WiFi network is 15 minutes. That is, if no WiFi client is connected to the management WiFi network for 15 minutes, the management WiFi network is turned off. Only after you restart the AP can you reconnect to the management WiFi network. However, you can disable the idle time-out so that the management WiFi network stays always on. For more information, see Disable the idle time-out for the management WiFi network on page 47.
- **Are you using the correct SSID and password?** The management WiFi network is shown in the format WAX210XXXXXX-CONFIG-ONLY, where XXXXXX is customized to every device (based on the last six digits of the MAC address).

  You cannot change the name of the management WiFi network. The default password for WiFi access to the management WiFi network is a unique WiFi password that is printed on the AP label. You *can* change this WiFi password and we recommend that you do so (see Change the password for the management WiFi network on page 46).
- **Did you disable the management WiFi network?** If you disabled the management WiFi network, you can reach the AP device UI only over a wired LAN connection. For more information, see Disable the management WiFi network on page 48.

Troubleshoot Internet browsing

If a WiFi device is connected to the AP 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 AP (that is, the AP uses static IP address settings), restart the WiFi device and verify the DNS address.

- The WiFi device might not use the correct IP address (TCP/IP) settings.

  If the WiFi device obtains its information by DHCP, restart the WiFi device and verify that the address is in the correct IP address range that the AP assigns to WiFi clients:

  - For WiFi devices that connect to a regular user WiFi network, the IP address is one from the address range that the DHCP server (or router) in your network assigns.
  - For WiFi devices that connect to a *guest* user WiFi network, the IP address is from a different address range that you can customize (see Change the DHCP server settings for guest WiFi networks on page 71).

  For information about IP address problems, see Troubleshoot your network using the ping utility of your computer on page 126.

NOTE: If you are connected to the management WiFi to manage the AP, you cannot get an Internet connection. This is by design. For more information, see Management WiFi network on page 45.

You cannot log in to the AP over a LAN connection

If you are unable to log in to the AP from a computer on your local network and use the AP's device UI, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet cable between the computer and the AP.
- Make sure that the IP address of your computer is in the same subnet as the AP.

  If you disabled the AP's DHCP client and configured a fixed (static) IP address when you connected the AP to your network (see Set a static IPv4 address on page 28), change the IP address and subnet mask on your computer to so that the IP addresses of your computer and the AP are in the same IP subnet.

- If the AP 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 AP 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 AP device icon, and select **Properties**. The AP IP address displays. Assuming that you did not change the device name, the AP is shown as NETGEARXXXXXX, in which XXXXXX represents the last six characters of the MAC address of the AP's LAN interface.

  - **DHCP server**: Access the DHCP server in your network and open the page that shows the network connections.
  - **IP network scanner**: Use an IP network scanner to scan for the IP address that is assigned to the AP.

(!) **NOTE:** For more information, see Find the IP address of the AP on page 22.

- 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 device UI

If you are logged in to the AP's device UI and the AP 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

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 AP

You can ping the AP from a Windows-based computer to verify that the path to your AP is set up correctly. You can use a WiFi or wired connection to the AP.

To ping the AP 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 AP, 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 AP and your computer are correct. For more information, see Display the AP device, memory, LAN, and WiFi status information on page 102.
- Correct physical connections?

  If the AP 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 AP and computer.
- Correct software?

  If you are using a wired connection to the AP, 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 AP 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 AP on page 127.
3. If you do not receive replies, check the following:
   - Check to see that IP address of the AP 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 AP 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. This is the modem through which the router (to which the AP is connected) can reach the Internet
   - If your ISP assigned a host name to your registered computer, use that host name as the account name on the router that connects to your ISP.
   - 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 use the authorized computer’s MAC address. For information about how to do this, see your router’s documentation.

A

Factory Default Settings and Technical Specifications

This appendix includes the following sections:

- Factory default settings
- Technical specifications

Factory default settings

You can reset the AP to the factory default settings, which are shown in the following table.

For information about resetting the AP to its factory settings, see Reset the AP to factory default settings using the device UI on page 94.

Table 9. Factory default settings

Feature	Default Setting
Access	
Domain name	https://www.aplogin.net
Default IP address	https://192.168.0.100
DHCP client	Enabled. **Note**: If connected to a network, the AP receives an IP address from a DHCP server or router in the network.
Device password	No default password. The first time that you log in to the device UI, you must define a device password that applies only to device UI access of the AP.
Management VLAN	Disabled (untagged)
Management WiFi network	
SSID (WiFi network name)	WAX210XXXXXX-CONFIG-ONLY XXXXXX represents the last six characters of the MAC address of the AP’s LAN interface.
WiFi password for the management WiFi network	The unique WiFi password is printed on the AP label. The security is WPA2/WPA3-Personal.
Time-out period for the management WiFi network	Automatically turns off after15 minutes of being idle.
User WiFi networks	
SSID (WiFi network names)	By default, the first user WiFi network is enabled after you specify the name and WiFi password the first time that you log in to the device UI. The second, third, and fourth SSIDs are disabled by default: NETGEARXXXXXX_2 NETGEARXXXXXX_3 NETGEARXXXXXX_4 XXXXXX represents the last six characters of the MAC address of the AP’s LAN interface. When you enable one of these user WiFi networks, the default WiFi password is *sharedsecret* and the default security is WPA2/WPA3-Personal.
DHCP IP address range for WiFi client assignment	The address range is the same range from which the DHCP server (or router) in your network assigns addresses.

Table 9. Factory default settings (Continued)

Feature	Default Setting
DHCP IP address range for *guest* WiFi client assignment	The address range is derived from the range of the DHCP server (or router) in your network, but it is not the same range.
Settings for each individual user WiFi network	
Guest network	Disabled
Hidden SSID	Disabled
Client isolation	Disabled
VLAN isolation	Disabled
VLAN	Non assigned
L2 isolation	Disabled
Fast roaming	Disabled
Band steering	Disabled
Wireless MAC filter	Disabled
Wireless traffic shaping	Disabled
2.4 GHz and 5 GHz radios (These settings apply to all user WiFi networks.)	
Channel HT mode	2.4 GHz radio: 20 MHz 5 GHz radio: 80 MHz
Radio transmission power	Full
Channel	The available channels and the default channel depend on the configured region and country.
Bit rate	Automatic
Client limits	64 for each radio 128 for the AP
WiFi on/off schedule	None
System	
SNMPv1 and SNMPv2	Disabled
SNMPv3	Disabled
STP	Disabled
UPnP	Disabled
Date and time settings	Obtained automatically from the default NTP server

Table 9. Factory default settings (Continued)

Feature	Default Setting
Log	Enabled
Remote log	Disabled
Email alerts	Disabled
Automatic firmware upgrade check	Disabled

Technical specifications

The following table shows the technical specifications of the AP. For more information, see the product data sheet, which you can download by visiting netgear.com/support/download/.

Table 10. Technical specifications

Feature	Description
Power adapter	A power adapter is included for model WAX210PA but not for model WAX210. Both models can operate with PoE power. 12V, 1A (18W), the plug is localized to the country of sale. Maximum power consumption with a power adapter: 15.2W
Power over Ethernet	If you do not use a power adapter, the LAN/PoE port requires 802.3af (PoE) power. Maximum power consumption with PoE: 11W **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).
Dimensions (L x W x H)	4.53 x 4.53 x 1.2 in. (115 x 115 x 30.5 mm)
Weight	0.45 lb (203 g)
Operating temperature	32° to 104°F (0° to 40°C)
Operating humidity	5 to 95% maximum relative humidity, noncondensing
Storage temperature	–40° to 176°F (–40° to 80°C)
Storage humidity	up to 95% maximum relative humidity, noncondensing
LAN interface	One 10/100/1000 Mbps Ethernet (RJ-45) PoE port with Auto Uplink (Auto MDI-X)

Table 10. Technical specifications (Continued)

Feature	Description
WiFi interfaces	2.4 GHz radio 5 GHz radio The WiFi interfaces can operate concurrently.
Maximum theoretical throughput	2.4 GHz radio: about 600 Mbps 5 GHz radio: about 1200 Mbps
Maximum number of WiFi clients	128 (64 on the 2.4 GHz radio and 64 on the 5 GHz radio) The supported number of clients depends on the network and traffic conditions.
Operating frequency range 2.4 GHz band	2412 MHz – 2483.5 MHz The supported channels depend on the configured regulatory domain.
Operating frequency range 5 GHz band	US: 5150 MHz – 5895 MHz 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
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	CE