NETGEAR®

User Manual

AX3000 Dual Band PoE WiFi 6 Access Point

WAX605

January 2026
202-12875-03

NETGEAR, Inc.
3553 N First Street
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.

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

This product is designed and warranted for indoor use only. Do not use this device outdoors. The PoE source is intended for intra building connection only.

Trademarks

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

Revision History

Publication Part Number	Publish Date	Comments
202-12875-03	January 2026	We revised the following sections: • Connect over WiFi to the local browser UI for initial configuration on page 21 • Connect over the LAN to the local browser UI for initial configuration on page 25 • Configure the offline using a directly connected computer on page 29
202-12875-02	December 2025	We added SNMPv3 configuration: • Enable SNMP and manage the SNMP settings on page 138 • Configure the SNMPv1/v2c settings on page 140 • Configure the SNMPv3 settings on page 141 We revised the following section: • Capture WiFi and Ethernet packets on page 195
202-12875-01	July 2025	We revised multiple sections throughout the document to remove Insight compatibility. We added the following section: • Manage the denial of service protection on page 101
202-12720-03	May 2025	We added the following sections: • You enter the wrong password and can no longer log in to the access point on page 203 We updated the following sections: • Top panel LED on page 12 • Set up an open or secure WiFi network on page 36 • Manage Quality of Service for a WiFi radio on page 71 • Set up an external captive portal for a WiFi network on page 77 • Set up RADIUS servers on page 88 • Manage neighbor AP detection on page 90 • Manage the syslog settings on page 123 • Display client distribution, connected clients, and client trends on page 152 • Display traffic volume, statistics, and channel utilization on page 155 We made other minor updates and corrections.
202-12720-02	May 2024	We added the option to test configured RADIUS servers in Set up RADIUS servers on page 88.
202-12720-01	February 2024	First publication.

Contents

Chapter 1 Introduction

Additional documentation..... 10

Chapter 2 Hardware Overview

Unpack the access point..... 12
Top panel LED..... 12
Hardware interfaces..... 14
Access point label..... 15
Safety instructions and warnings for an indoor access point..... 16

Chapter 3 Install the Access Point in Your Network and Access It for Initial Configuration

Position your access point for best performance..... 19
Set up and connect the access point to your network..... 20
Connect to the access point for initial configuration..... 21
Connect over WiFi to the local browser UI for initial configuration..... 21
Connect over the LAN to the local browser UI for initial configuration..... 25
Configure the offline using a directly connected computer.... 29
Log in to the access point after initial setup..... 33
What to do if you get a browser security warning..... 34

Chapter 4 Manage the Basic WiFi Features for a WiFi network

Set up an open or secure WiFi network..... 36
View or change the settings of a WiFi network..... 45
Remove a WiFi network..... 46
Hide or broadcast the SSID for a WiFi network..... 47
Change the VLAN ID for a WiFi network..... 48
Change the authentication and encryption for a WiFi network... 49
Enable or disable PMF for a WiFi network..... 53
Set up Multi PSK for a WiFi network..... 54
Disable or enable a WiFi network or set up a WiFi activity schedule..... 56
Enable or disable band steering with 802.11k RRM and 802.11v WiFi network management..... 58

Chapter 5 Manage the Basic Radio Features

Manage the basic WiFi settings for the radios..... 61

Turn a radio on or off..... 64
Change the WiFi mode for a radio..... 65
Change the channel width for a radio..... 67
Change the guard interval for a radio..... 68
Change the output power for a radio..... 69
Change the channel for a radio..... 70
Manage Quality of Service for a WiFi radio..... 71

Chapter 6 Set Up and Manage a Captive Portal

Set up a click-through captive portal for a WiFi network..... 75
Set up an external captive portal for a WiFi network..... 77

Chapter 7 Manage Access and Security

Manage user accounts..... 82
Add a user account..... 82
Change the time-out period for a user session..... 83
Change the settings for a user account..... 84
Remove a user account..... 85
Block specific URLs and keywords for Internet access..... 86
Set up RADIUS servers..... 88
Manage neighbor AP detection..... 90
Enable neighbor access point detection and move access points to the Known AP List..... 91
Import an existing neighbor ACL in the Known AP List..... 92
Manage MAC ACLs for WiFi clients..... 94
Manually set up a MAC ACL for WiFi clients..... 95
Import an existing MAC ACL for WiFi clients..... 97
Enable L2 security..... 100
Manage the denial of service protection..... 101

Chapter 8 Manage the Local Area Network and IP Settings

Disable the DHCP client and specify a fixed IP address..... 104
Enable the DHCP client..... 105
Set the 802.1Q VLAN and management VLAN..... 106
Set an existing domain name..... 108
Enable or disable Spanning Tree Protocol..... 109
Enable or disable the network integrity check function..... 110
Enable or disable IGMP snooping..... 111
Enable or disable Ethernet LLDP..... 112
Enable or disable UPnP..... 113
Manage the multicast DNS gateway..... 113
Enable the multicast DNS gateway and add a policy..... 114
Change or remove a multicast DNS policy..... 116

Chapter 9 Manage and Maintain the Access Point

Change the country or region of operation..... 119
Change the admin user account password..... 120
Change the system name..... 121
Specify a custom NTP server..... 122
Set the time zone..... 123
Manage the syslog settings..... 123
Manage the firmware of the access point..... 125
Check for new firmware and update the firmware on the access point..... 126
Manually download firmware and update the access point.. 127
Revert to the backup firmware..... 129
Use an SFTP server to update the access point..... 130
Manage the configuration file of the access point..... 131
Back up the access point configuration..... 131
Restore the access point configuration..... 132
Reboot the access point from the local browser UI..... 134
Schedule the access point to reboot..... 135
Return the access point to its factory default settings..... 136
Use the Reset button to reset the access point..... 136
Use the local browser UI to reset the access point..... 137
Enable SNMP and manage the SNMP settings..... 138
Configure the SNMPv1/v2c settings..... 140
Configure the SNMPv3 settings..... 141
Manage the LED..... 143
Manage the Energy Efficiency Mode..... 144

Chapter 10 Monitor the Access Point and the Network

Display the access point Internet, IP, and system settings..... 147
Display the WiFi radio settings..... 149
Display unknown and known neighbor access points..... 151
Display client distribution, connected clients, and client trends. 152
Display traffic volume, statistics, and channel utilization..... 155
Display or download tracked URLs..... 157
Display, save, download, or clear the logs..... 159
Display a WiFi bridge connection..... 160
Display alarms and notifications..... 161

Chapter 11 Manage the Advanced WiFi Features for a WiFi network

Set NAT mode or Bridge mode for addressing and traffic..... 163
Enable or disable client isolation for a WiFi network..... 164
Enable or disable URL tracking for a WiFi network..... 166

Change the format of the DHCP offer messages in a WiFi network..... 167
Select a MAC ACL for WiFi clients in a WiFi network..... 168
Set bandwidth rate limits for a WiFi network..... 170
Configure advanced rate selection for a WiFi network..... 171
Assign host names to WiFi clients and manage the host name list..... 175

Chapter 12 Set up a WiFi Bridge

WiFi base station, WiFi repeater, and WiFi bridge requirements. 178
Set up a WiFi bridge between access points..... 179

Chapter 13 Manage the Advanced Radio Features

Manage the advanced WiFi settings for the radios..... 183
Manage the maximum number of clients for a radio..... 186
Manage the broadcast and multicast settings for a radio..... 187
Manage load balancing for the radios..... 188
Manage sticky clients..... 190
Manage the ARP proxy..... 191

Chapter 14 Diagnostics and Troubleshooting

Perform a ping test..... 194
Capture WiFi and Ethernet packets..... 195
Quick tips for WiFi troubleshooting..... 197
Troubleshoot with the LED..... 198
LED remains off..... 198
LED remains solid amber..... 199
LED is blinking amber slowly, continuously..... 199
Troubleshoot WiFi connectivity for a WiFi client device..... 200
Troubleshoot Internet browsing..... 201
You cannot log in to the access point over a LAN connection.. 201
Changes are not saved..... 202
You enter the wrong password and can no longer log in to the access point..... 203
Troubleshoot your network using the ping utility..... 203
Test the LAN path to your access point..... 203
Test the path from your computer to a remote device..... 204

Appendix A Factory Default Settings and Technical Specifications

Factory default settings..... 206
Technical specifications..... 210

Appendix B Mount the Access Point to a Wall or Ceiling

Mount the access point to a solid wall or ceiling..... 213

Mount the access point to a T-bar..... 215
Unmount the access point..... 216

1

Introduction

This manual is for the NETGEAR AX3000 Dual Band PoE WiFi 6 Access Point model WAX605.

Model WAX605, in this manual referred to as the access point, supports IEEE 802.11ax, four (2+2) streams of WiFi 6, and dual-band concurrent operation at 2.4 GHz and 5 GHz with a combined throughput of 3000 Mbps (600 Mbps at 2.4 GHz and 2400 Mbps at 5 GHz). The 5 GHz radio supports 160 MHz bandwidth.

The access point functions as a Power over Ethernet (PoE) powered device (PD) in an existing network connected to a PoE switch. Model WAX605 supports an optional power adapter for connection to a regular switch or router. The PoE Ethernet port supports a speed of 1 Gbps.

This chapter contains the following sections:

- Additional documentation

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

Note: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download/. You can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this manual, you might need to update the firmware.

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

Additional documentation

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

- Installation guide
- Data sheet

2

Hardware Overview

The NETGEAR AX3000 Dual Band PoE WiFi 6 Access Point model WAX605 is an indoor access point that supports the 2.4 GHz and 5 GHz WiFi bands.

The chapter contains the following sections:

- Unpack the access point
- Top panel LED
- Hardware interfaces
- Access point label
- Safety instructions and warnings for an indoor access point

Unpack the access point

The package contains the following items:

- NETGEAR WAX605 access point
- Mounting bracket for a solid wall or ceiling, or 15/16 in. (23.8 mm) T-bar
- Mounting bracket for a 9/16 in. (14.3 mm) T-bar
- Two screws, spacers, and anchors for ceiling or wall mounting
- Installation guide

Note: Model WAX605 ships without a power adapter. Model WAX605AP ships *with* a power adapter (the type of power adapter varies by region). If you ordered model WAX605 but prefer to use the access point without a PoE connection, you can order a power adapter separately.

For information about the mounting options, see Mount the Access Point to a Wall or Ceiling on page 212.

Top panel LED

The single LED that provide the status of the access point is located on the top panel of the access point.

Figure 1. Top panel with single LED

Table 1. LED descriptions

LED Color	Description
	Off: No power is supplied to the access point.
	Solid amber, temporarily: The access point is starting or the Reset button was pressed.
	Solid magenta: The access point is initializing.
	Blinking magenta, slowly: The access point continues to initialize.
	Blinking amber fast, temporarily: The access point is updating firmware or is being reset to factory default settings. In the following problem situations, fast blinking amber might also occur: • The access point does not detect and Ethernet link. • In a wireless distribution system (WDS, see Set up a WiFi Bridge on page 177), the link between the WiFi repeater and the WiFi base station has failed.
	Solid green: The access point functions as a standalone access point.
	Blinking blue: At least one WiFi client is connected to the access point. The speed of blinking depends on the transmit and receive data rate of connected clients.
	Blinking green: At least one WiFi client is connected while the access point functions as a standalone access point. Blinking green might also occur in a wireless distribution system (WDS), when a connection is established between the WiFi base station and the WiFi repeater.
	Blinking amber slowly, continuously: The access point did not receive an IP address from a DHCP server.
	Solid amber, continuously: A boot error occurred or the AP is malfunctioning.

Note: For information about troubleshooting with the LED, see Troubleshoot with the LED on page 198.

Hardware interfaces

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

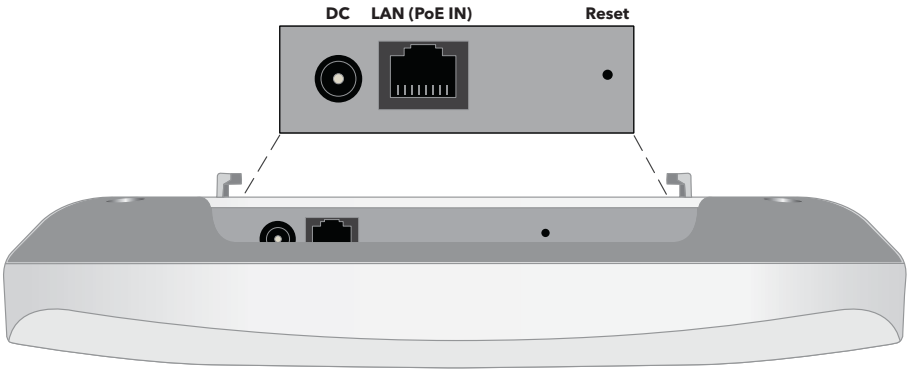


Figure 2. Hardware interfaces

The bottom panel contains the following components:

- **DC power connector**: If you do not use a PoE switch to provide power to the access point, connect an optional power adapter to the DC power connector.
- **LAN (PoE IN) port**: Use the LAN/PoE Gigabit Ethernet RJ-45 LAN port to connect the access point to a PoE switch that supports 802.3af power (PoE, with a 15.4W capacity per port), or if you use an optional power adapter, to a non-PoE switch.

  For more information about the LAN/PoE port connection, see Set up and connect the access point to your network on page 20.
- **Reset button**: You can use the **Reset** button to restart the access point or to reset the access point to its factory default settings. To restart the access point, press the **Reset** button for about two seconds. To reset the access point to factory default settings, press the **Reset** button for 10 seconds or longer.

  For more information, see Use the Reset button to reset the access point on page 136.

Access point label

The access point label on the bottom panel shows the QR code, serial number, MAC address, setup WiFi network name (SSID), and network key (password) of the access point.

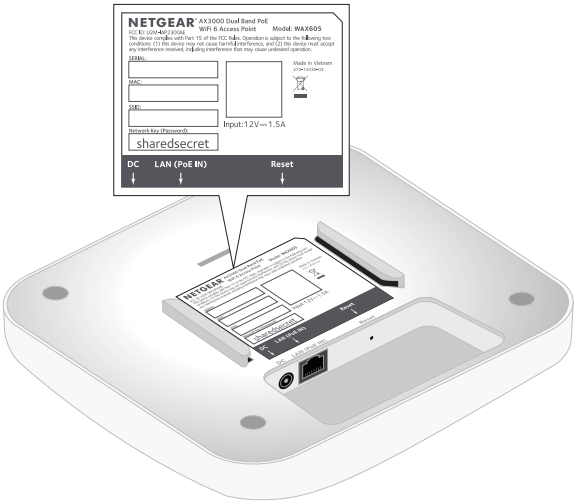


Figure 3. Access point label location

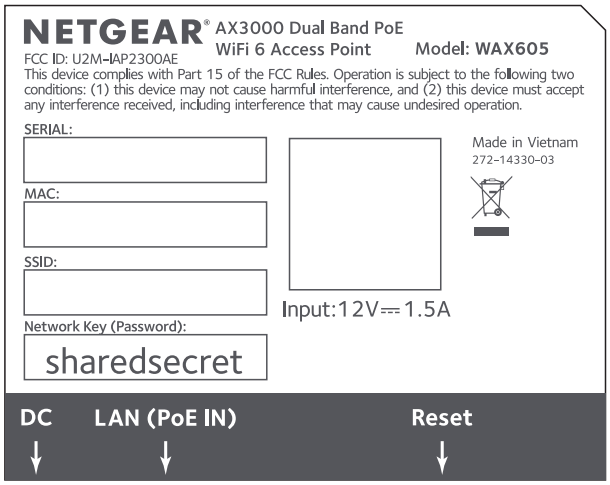


Figure 4. Access point label

Safety instructions and warnings for an indoor access point

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

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

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

  Failure to follow these guidelines can result in damage to your NETGEAR product, which might not be covered by NETGEAR's warranty, to the extent permissible by applicable law.
- Do not service the product except as explained in your product documentation. Some devices should never be opened.
- If any of the following conditions occur, unplug the product from its power source, and then replace the part or contact your trained service provider:
  - Depending on your product, the power adapter, power adapter cable, power adapter plug, or PoE Ethernet cable is damaged.
  - An object fell into the product.
  - The product was exposed to water.
  - The product was dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep the product away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your product components, and never operate the product in a wet environment. If the product gets wet, see the appropriate section in your troubleshooting guide, or contact your trained service provider.

- Do not push any objects into the openings of your product. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- If applicable to your product, allow the product to cool before removing covers or touching internal components.
- Be sure that devices that are attached over Ethernet cables are electrically rated to operate with the power available in your location.
- Depending on your product, use only the supplied power adapter or an Ethernet cable that provides PoE.

  If your product uses a power adapter:

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

3

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

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

The chapter contains the following sections:

- Position your access point for best performance
- Set up and connect the access point to your network
- Connect to the access point for initial configuration
- Log in to the access point after initial setup
- What to do if you get a browser security warning

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.

Note: During installation, if you do not see your country or region listed in the menu, update the access point's firmware and check again. If you still do not see your country or region listed, contact NETGEAR support.

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

Position your access point for best performance

Before you install and mount your access point as described in the installation guide or an appendix to this manual, consider how you can position the access point for best performance.

WiFi clients that are within the access point WiFi range can connect to the WiFi network. However, the WiFi range can vary significantly depending on the physical placement of your access point. For example, the thickness, density, and number of walls the WiFi signal passes through can limit the range.

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

Tips for positioning your access point:

- Place your access point near the center of the area where the WiFi clients operate.

  A line of sight between the access point and the WiFi clients is not required for good performance.
- Place the access point in an elevated location, minimizing the number of walls and ceilings between the access point and the WiFi clients.
- Place the access point away from electrical devices such as these:
  - Ceiling fans
  - Home security systems
  - Microwaves
  - Computers
  - Bases of cordless phones
  - 2.4 GHz and 5.8 GHz cordless phones
- Place the access point away from large metal surfaces, large glass surfaces, insulated walls, and items such as these:
  - Solid metal doors
  - Aluminum studs
  - Brick
  - Concrete

If you are using adjacent standalone access points, use non-overlapping radio frequency channels to reduce interference. For more information, see Change the channel for a radio on page 70.

Set up and connect the access point to your network

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

Note: Depending on the product ordered, the package might not include a power adapter. You power up the access point by connecting it to a PoE switch. If you ordered a package without a power adapter but do not want to use a PoE connection, you can still order a power adapter as an option.

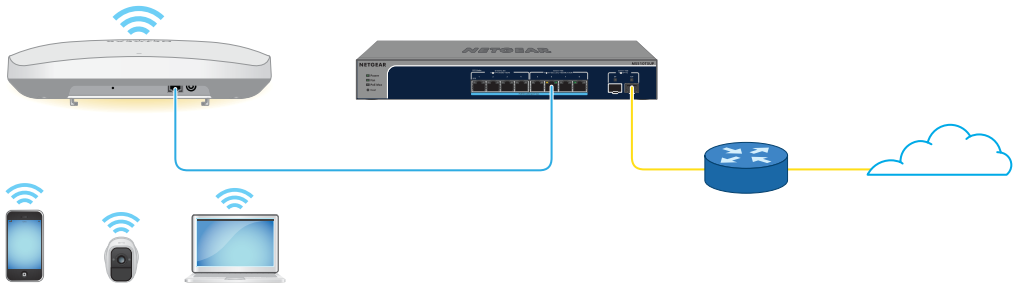


Figure 5. Set up the access point with a PoE connection to your network

To set up the access point with an Ethernet connection to your network:

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

   The access point requires 802.3af (PoE) input.

   While the access point is starting or in the process of getting an IP address from a DHCP server (or router functioning as a DHCP server) in your network, the LED initially lights solid amber, and then blinks amber slowly. After about two minutes, the LED turns solid green or solid blue and the access point is ready for you to perform the initial configuration.

For information about accessing the access point for initial configuration, see Connect to the access point for initial configuration on page 21.

Connect to the access point for initial configuration

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

For information about using the local browser UI, see one of the following sections:

- Connect over WiFi to the local browser UI for initial configuration on page 21
- Connect over the LAN to the local browser UI for initial configuration on page 25
- Configure the offline using a directly connected computer on page 29

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

Connect over WiFi to the local browser UI for initial configuration

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

To connect over WiFi to the local browser UI for initial configuration:

1. From your computer or mobile device, connect over WiFi to the access point's setup WiFi network using one of the following methods:
   - **Scan the QR code**: Scan the QR code on the access point label on the bottom of the access point to connect to the setup WiFi network.
   - **Connect manually**: The setup WiFi network is on the access point label and is shown in the format NETGEARxxxxxx-SETUP, where xxxxxx is the last six hexadecimal digits of the access point's MAC address. The default password is **sharedsecret**.
2. On the computer or mobile device, launch a web browser and, in the address bar, enter **http://aplogin.net**.

   Note: You can use **http://aplogin.net** only during initial setup of the access point.

Your browser might display a security warning because of the self-signed certificate on the access point, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and default password.

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

   The Day Zero Easy Setup page displays.

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

4. To let the access point check for the latest firmware, click the **Check for Upgrade** button.

   If new firmware is available for the access point, we recommend that you upgrade the firmware. After the firmware upgrade completes, the access point restarts. When the access point is ready, go back to Step 1 of this procedure.

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

Setting	Description
Country/Region	From the menu, select the country and region in which the access point is operating. **Note**: In some countries, the access point 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 access point'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 access point 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.
Time Zone	From the menu, select the time zone for the country and region in which the access point is operating.
DHCP Client	By default, the DHCP client of the access point allows the access point to receive an IP address from a DHCP server (or router that functions as a DHCP server) in your network. To set up the access point with a static (fixed) IP address, do the following: a. Select the **Disable** radio button. Additional fields display. b. Specify the IP address, IP subnet mask, IP address of the default gateway, and IP address of the DNS server.

(Continued)

Setting	Description
AP Name	As an option, enter a new name for the access point. The name must contain alphanumeric characters, must contain at least one alphabetical character, cannot be longer than 15 characters, and can contain hyphens but cannot start or end with a hyphen. By default, the access point name is Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address.
AP Login New Password	Enter a new admin password. This is the password that you must use to log in to the access point's local browser UI. (It is *not* the password that you use for WiFi access.) The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. Save the password for future use.
Confirm New Password	Enter exactly the same password that you entered in the **AP Login New Password** field.
SSID	You cannot use the setup SSID for regular operation. The setup SSID is for initial setup only. Enter a new name with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).

6. From the **Authentication** menu, select one of the following authentication types for the WiFi network:
   - **Open**: A legacy open WiFi network does not provide any security. Any WiFi device can join the network. We recommend that you do *not* use a legacy open WiFi network but configure WiFi security. However, a legacy open network might be appropriate for a WiFi hotspot.

     Note: You do not need to create a passphrase for an open network.

     If you select **Open** from the **Authentication** menu, the **Enhanced Open** check box displays.
     - **Enhanced Open check box cleared**: The WiFi network is a legacy open network without any security. This is the default option for an open network. Clients are not authenticated, traffic is not encrypted, and 802.11w (PMF) is automatically disabled.
     - **Enhanced Open check box selected**: The WiFi enhanced open feature is enabled. This feature is based on opportunistic wireless encryption (OWE). The encryption is set to CCM mode protocol (CCMP) and 802.11w (PMF) is automatically set to mandatory. If you select the **Enhanced Open** check box, the **Allow Devices to Connect with Open** check box displays.

       If you select the **Allow Devices to Connect with Open** check box, the WiFi network can accept both clients that support the WiFi enhanced open feature and clients that do not. For clients that do not support the WiFi open enhanced feature, traffic is not encrypted.

If you clear the **Allow Devices to Connect with Open** check box, the WiFi network can only accept clients that support the WiFi enhanced open feature.

- **WPA2 Personal**: This option allows only WiFi clients that support WPA2 to connect to the SSID. Select this option if all WiFi clients are capable of supporting WPA2. This option uses AES encryption.
- **WPA2/WPA Personal**: This option allows both WPA and WPA2 WiFi clients to connect to the SSID. This option uses TKIP and AES encryption. Broadcast packets use TKIP. For unicast (that is, point-to-point) transmissions, WPA clients use TKIP and WPA2 clients use AES.
- **WPA3 Personal**: This option allows only WiFi clients that support WPA3 to connect to the SSID. Select this option if all WiFi clients are capable of supporting WPA3. This option uses SAE encryption. In the **Passphrase** field, enter a new passphrase for the WiFi network.
- **WPA3/WPA2 Personal**: This option allows both WPA2 and WPA3 WiFi clients to connect to the SSID. This option uses AES and SAE encryption. WPA2 clients use AES and WPA3 clients use SAE.

Note: After you complete the setup process, you can set up WPA2 Enterprise or WPA3 Enterprise security with RADIUS servers. For more information, see Change the authentication and encryption for a WiFi network on page 49.

7. In the **Passphrase** field, enter a new passphrase for the WiFi network.

   Note: By default, the **Complex passphrase** check box is enabled to enforce minimum password requirements that help improve wireless network security. To disable the complex passphrase feature:

   - Select the **Complex passphrase** check box.
   - A confirmation pop-up window displays.
   - Click the **OK** button.

8. Click the **Apply** button.

   Your settings are saved. A pop-up window displays the IP address and the new WiFi network and password (passphrase).

   If you specified a static IP address, save the IP address information because you must enter the IP address when you log in again.

   You are disconnected from the access point. If you changed the default country, the access point restarts.

9. Reconnect over WiFi to the access point's WiFi network using the new SSID and passphrase that you just defined on the Day Zero Easy Setup page.
10. Enter the access point IP address in the address bar of your browser.

    If you changed the IP address, enter the IP address that you specified in Step 5.

Your browser might display a security warning because of the self-signed certificate on the access point, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

A login window displays.

11. Enter the access point user name and password.

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

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

Connect over the LAN to the local browser UI for initial configuration

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

To connect over the LAN to the local browser UI for initial configuration:

1. To determine the IP address that the DHCP server assigned to the access point, access the DHCP server or use an IP network scanner.

   If you use a Windows-based computer, launch File Explorer (or Windows Explorer), select **Network** from the Navigation pane, right-click the access point device icon, and select **Properties** to display the IP address.

2. On the computer, launch a web browser and, in the address bar, enter the IP address that is assigned to the access point.

   Your browser might display a security warning because of the self-signed certificate on the access point, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and default password.

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

   The Day Zero Easy Setup page displays.

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

4. To let the access point check for the latest firmware, click the **Check for Upgrade** button.

   If new firmware is available for the access point, we recommend that you upgrade the firmware. After the firmware upgrade completes, the access point restarts. When the access point is ready, depending on your situation, go back to Step 2 or Step 3 of this procedure.

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

Setting	Description
Country/Region	From the menu, select the country and region in which the access point is operating. **Note**: In some countries, the access point 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 access point'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 access point 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.
Time Zone	From the menu, select the time zone for the country and region in which the access point is operating.
DHCP Client	By default, the DHCP client of the access point allows the access point to receive an IP address from a DHCP server (or router that functions as a DHCP server) in your network. To set up the access point with a static (fixed) IP address, do the following: a. Select the **Disable** radio button. Additional fields display. b. Specify the IP address, IP subnet mask, IP address of the default gateway, and IP address of the DNS server.
AP Name	As an option, enter a new name for the access point. The name must contain alphanumeric characters, must contain at least one alphabetical character, cannot be longer than 15 characters, and can contain hyphens but cannot start or end with a hyphen. By default, the access point name is Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address.
AP Login New Password	Enter a new admin password. This is the password that you must use to log in to the access point's local browser UI. (It is *not* the password that you use for WiFi access.) The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. Save the password for future use.
Confirm New Password	Enter exactly the same password that you entered in the **AP Login New Password** field.
SSID	You cannot use the setup SSID for regular operation. The setup SSID is for initial setup only. Enter a new name with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).

6. From the **Authentication** menu, select one of the following authentication types for the WiFi network, and, if applicable, set a new passphrase (network key or WiFi password) for the WiFi network:
   - **Open**: A legacy open WiFi network does not provide any security. Any WiFi device can join the network. We recommend that you do *not* use a legacy open WiFi network but configure WiFi security. However, a legacy open network might be appropriate for a WiFi hotspot.

     Note: You do not need to create a passphrase for an open network.

     If you select **Open** from the **Authentication** menu, the **Enhanced Open** check box displays.
     - **Enhanced Open check box cleared**: The WiFi network is a legacy open network without any security. This is the default option for an open network. Clients are not authenticated, traffic is not encrypted, and 802.11w (PMF) is automatically disabled.
     - **Enhanced Open check box selected**: The WiFi enhanced open feature is enabled. This feature is based on opportunistic wireless encryption (OWE). The encryption is set to CCM mode protocol (CCMP) and 802.11w (PMF) is automatically set to mandatory. If you select the **Enhanced Open** check box, the **Allow Devices to Connect with Open** check box displays.

       If you select the **Allow Devices to Connect with Open** check box, the WiFi network can accept both clients that support the WiFi enhanced open feature and clients that do not. For clients that do not support the WiFi open enhanced feature, traffic is not encrypted.

       If you clear the **Allow Devices to Connect with Open** check box, the WiFi network can only accept clients that support the WiFi enhanced open feature.
   - **WPA2 Personal**: This option allows only WiFi clients that support WPA2 to connect to the SSID. Select this option if all WiFi clients are capable of supporting WPA2. This option uses AES encryption.
   - **WPA2/WPA Personal**: This option allows both WPA and WPA2 WiFi clients to connect to the SSID. This option uses TKIP and AES encryption. Broadcast packets use TKIP. For unicast (that is, point-to-point) transmissions, WPA clients use TKIP and WPA2 clients use AES.
   - **WPA3 Personal**: This option allows only WiFi clients that support WPA3 to connect to the SSID. Select this option if all WiFi clients are capable of supporting WPA3. This option uses SAE encryption.
   - **WPA3/WPA2 Personal**: This option allows both WPA2 and WPA3 WiFi clients to connect to the SSID. This option uses AES and SAE encryption. WPA2 clients use AES and WPA3 clients use SAE.

Note: After you complete the setup process, you can set up WPA2 Enterprise or WPA3 Enterprise security with RADIUS servers. For more information, see Change the authentication and encryption for a WiFi network on page 49.

7. In the **Passphrase** field, enter a new passphrase for the WiFi network.

   Note: By default, the **Complex passphrase** check box is enabled to enforce minimum password requirements that help improve wireless network security. To disable the complex passphrase feature:

   - Select the **Complex passphrase** check box.
   - A confirmation pop-up window displays.
   - Click the **OK** button.

8. Click the **Apply** button.

   Your settings are saved. A pop-up window displays the IP address and the new WiFi network and password (passphrase).

   If you specified a static IP address, save the IP address information because you must enter the IP address when you log in again.

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

   Note: Do not close the page.

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

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

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

   a. Take one of the following actions:

      - If you assigned a static IP address to the access point, enter the IP address that you specified in Step 5 in the address bar of the web browser.
      - If you did not assign a static IP address, reenter the IP address that is displayed in the address bar of the web browser. If that does not work, write down the IP address, close the web browser, launch the web browser again, and then reenter the IP address in the address bar of the web browser.
      - If you did not assign a static IP address and you closed the page so that you cannot see the IP address of the access point, use an IP scanner tool, use a network discovery tool, or access the DHCP server to discover the IP address of the access point in your network.

        Then, launch a browser and enter the IP address in the address bar of the web browser.

      Your browser might display a security warning because of the self-signed certificate on the access point, which is expected behavior. You can proceed, or

add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

A login window displays.

b. Enter the access point user name and password.

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

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

Configure the offline using a directly connected computer

You can take the offline (that is, disconnect it from your network), connect a computer through an Ethernet cable to the LAN/PoE port of the access point, and connect to the over its default IP address so that you can configure it offline. After you complete the configuration, you can bring the access point online.

Note: Because the access point is not connected to a PoE switch, you can use this configuration method only if you have a power adapter for the access point.

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

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

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

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

   Your browser might display a security warning because of the self-signed certificate on the access point, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

5. Enter the access point user name and default password.

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

   The Day Zero Easy Setup page displays.

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

6. To let the access point check for the latest firmware, click the **Check for Upgrade** button.

   If new firmware is available for the access point, we recommend that you upgrade the firmware. After the firmware upgrade completes, the access point restarts. When the access point is ready, depending on your situation, go back to Step 4 or Step 5 of this procedure.

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

Setting	Description
Country/Region	From the menu, select the country and region in which the access point is operating. **Note**: In some countries, the access point 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 access point'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 access point 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.
Time Zone	From the menu, select the time zone for the country and region in which the access point is operating.
DHCP Client	By default, the DHCP client of the access point allows the access point to receive an IP address from a DHCP server (or router that functions as a DHCP server) in your network. To set up the access point with a static (fixed) IP address, do the following: a. Select the **Disable** radio button. Additional fields display. b. Specify the IP address, IP subnet mask, IP address of the default gateway, and IP address of the DNS server.
AP Name	As an option, enter a new name for the access point. The name must contain alphanumeric characters, must contain at least one alphabetical character, cannot be longer than 15 characters, and can contain hyphens but cannot start or end with a hyphen. By default, the access point name is Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address.

(Continued)

Setting	Description
AP Login New Password	Enter a new admin password. This is the password that you must use to log in to the access point's local browser UI. (It is *not* the password that you use for WiFi access.) The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. Save the password for future use.
Confirm New Password	Enter exactly the same password that you entered in the **AP Login New Password** field.
SSID	You cannot use the setup SSID for regular operation. The setup SSID is for initial setup only. Enter a new name with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).

8. From the **Authentication** menu, select one of the following authentication types for the WiFi network, and, if applicable, set a new passphrase (network key or WiFi password) for the WiFi network:
   - **Open**: A legacy open WiFi network does not provide any security. Any WiFi device can join the network. We recommend that you do *not* use a legacy open WiFi network but configure WiFi security. However, a legacy open network might be appropriate for a WiFi hotspot.

     Note: You do not need to create a passphrase for an open network.

     If you select **Open** from the **Authentication** menu, the **Enhanced Open** check box displays.
     - **Enhanced Open check box cleared**: The WiFi network is a legacy open network without any security. This is the default option for an open network. Clients are not authenticated, traffic is not encrypted, and 802.11w (PMF) is automatically disabled.
     - **Enhanced Open check box selected**: The WiFi enhanced open feature is enabled. This feature is based on opportunistic wireless encryption (OWE). The encryption is set to CCM mode protocol (CCMP) and 802.11w (PMF) is automatically set to mandatory. If you select the **Enhanced Open** check box, the **Allow Devices to Connect with Open** check box displays.

       If you select the **Allow Devices to Connect with Open** check box, the WiFi network can accept both clients that support the WiFi enhanced open feature and clients that do not. For clients that do not support the WiFi open enhanced feature, traffic is not encrypted.

If you clear the **Allow Devices to Connect with Open** check box, the WiFi network can only accept clients that support the WiFi enhanced open feature.

- **WPA2 Personal**: This option allows only WiFi clients that support WPA2 to connect to the SSID. Select this option if all WiFi clients are capable of supporting WPA2. This option uses AES encryption.
- **WPA2/WPA Personal**: This option allows both WPA and WPA2 WiFi clients to connect to the SSID. This option uses TKIP and AES encryption. Broadcast packets use TKIP. For unicast (that is, point-to-point) transmissions, WPA clients use TKIP and WPA2 clients use AES.
- **WPA3 Personal**: This option allows only WiFi clients that support WPA3 to connect to the SSID. Select this option if all WiFi clients are capable of supporting WPA3. This option uses SAE encryption.
- **WPA3/WPA2 Personal**: This option allows both WPA2 and WPA3 WiFi clients to connect to the SSID. This option uses AES and SAE encryption. WPA2 clients use AES and WPA3 clients use SAE.

Note: After you complete the setup process, you can set up WPA2 Enterprise or WPA3 Enterprise security with RADIUS servers. For more information, see Change the authentication and encryption for a WiFi network on page 49.

9. In the **Passphrase** field, enter a new passphrase for the WiFi network.

   Note: By default, the **Complex passphrase** check box is enabled to enforce minimum password requirements that help improve wireless network security. To disable the complex passphrase feature:

   - Select the **Complex passphrase** check box.
   - A confirmation pop-up window displays.
   - Click the **OK** button.

10. Click the **Apply** button.

    Your settings are saved. A pop-up window displays the IP address and the new WiFi network and password (passphrase).

    If you specified a static IP address, save the IP address information because you must enter the IP address when you log in again.

    You are disconnected from the access point. If you changed the default country, the access point restarts.

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

    If you changed the IP address, enter the IP address that you specified in Step 7.

    Your browser might display a security warning because of the self-signed certificate on the access point, which is expected behavior. You can proceed, or add an

exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

A login window displays.

12. Enter the access point user name and password.

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

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

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

Log in to the access point after initial setup

After initial setup, the access point is ready for use and you can change the settings and monitor the traffic.

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

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

The Dashboard page displays various panes that let you see the status of your access point at a glance. For more information about the Dashboard page and its various panes, see Monitor the Access Point and the Network on page 146.

What to do if you get a browser security warning

When you enter the IP address that is assigned to the access point in the address field of your browser, a security warning might display because of the self-signed certificate on the device. This is expected behavior. You can proceed, or add an exception for the security warning.

To proceed with a security warning or add an exception for a security warning:

- **Google Chrome**: Click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the domain name or IP address of the device.
- **Apple Safari**: Click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window displays, click the **Visit Website** button. If another pop-up window displays to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.
- **Mozilla Firefox**: Click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
- **Microsoft Edge**: Select **Details > Go on to the webpage**.
- **Microsoft Internet Explorer**: Click the **Continue to this website (not recommended)** link.

4

Manage the Basic WiFi Features for a WiFi network

The access point can support eight WiFi networks, each with its own unique WiFi settings, including WiFi security. This chapter describes how you can manage the basic WiFi features for a WiFi network.

For information about the advanced WiFi features for a WiFi network, see Manage the Advanced WiFi Features for a WiFi network on page 162.

The chapter includes the following sections:

- Set up an open or secure WiFi network
- View or change the settings of a WiFi network
- Remove a WiFi network
- Hide or broadcast the SSID for a WiFi network
- Change the VLAN ID for a WiFi network
- Change the authentication and encryption for a WiFi network
- Enable or disable PMF for a WiFi network
- Set up Multi PSK for a WiFi network
- Disable or enable a WiFi network or set up a WiFi activity schedule
- Enable or disable band steering with 802.11k RRM and 802.11v WiFi network management

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

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

Set up an open or secure WiFi network

The access point provides one setup SSID that is enabled by default and that broadcasts on the 2.4 GHz band and the 5 GHz band. This is the SSID that you renamed and for which you set a new passphrase when you initially connected to the access point. We also refer to this SSID as the default WiFi network, and it is displayed as SSID1 in the local browser UI. You can add more SSIDs: The access point can support a total of eight SSIDs.

The access point can simultaneously support the 2.4 GHz band for 802.11b/g/n/ax WiFi devices and the 5 GHz band for 802.11a/na/ac/ax WiFi devices. Each band supports two WiFi streams for a total of four WiFi streams.

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

If you plan to use WPA2 Enterprise security or WPA3 Enterprise security for your WiFi network, first set up RADIUS servers (see Set up RADIUS servers on page 88). Note that WPA2 Enterprise security and WPA3 Enterprise security are not compatible with a multicast DNS (mDNS) gateway (see Manage the multicast DNS gateway on page 113).

To set up a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The page that displays lets you select and add an SSID.
5. Click the **+** button to the left of Add SSID.

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

Setting	Description
Wireless Network Name (SSID)	The SSID is the WiFi network name of the VAP. Enter a name for the SSID with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\). For a WiFi device to be able to connect to the VAP, the SSID on the WiFi device must match the SSID of the VAP.
Broadcast SSID	By default, the VAP broadcasts its SSID so that WiFi clients can detect the SSID in their scanned network lists. To turn off the SSID broadcast, select the **No** radio button. Turning off the SSID broadcast provides additional WiFi security, but users must know the SSID to be able to join the VAP.
VLAN ID	You can enter the VLAN ID that must be associated with the VAP. By default, the VLAN ID is 1. The VLAN ID must be between 1 and 4094. This VLAN ID is not the same as the 802.1Q VLAN ID that is used for the wired network (see Set the 802.1Q VLAN and management VLAN on page 106).

7. Specify the WiFi security by selecting an option from the **Authentication** menu and, if applicable, by specifying a passphrase in the **Passphrase** field or selecting an option from the **Encryption** menu:
   - **Open**: A legacy open WiFi network does not provide any security. Any WiFi device can join the network. We recommend that you do *not* use a legacy open WiFi network but configure WiFi security. However, a legacy open network might be appropriate for a WiFi hotspot.

     If you select **Open** from the **Authentication** menu, the **Enhanced Open** check box displays.
     - **Enhanced Open check box cleared**: The WiFi network is a legacy open network without any security. This is the default option for an open network. Clients are not authenticated, traffic is not encrypted, and 802.11w (PMF) is automatically disabled (see Step 8).
     - **Enhanced Open check box selected**: The WiFi enhanced open feature is enabled. This feature is based on opportunistic wireless encryption (OWE). The encryption is set to CCM mode protocol (CCMP) and 802.11w (PMF) is automatically set to mandatory (see Step 8). If you select the **Enhanced Open** check box, the **Allow Devices to Connect with Open** check box displays.

       If you select the **Allow Devices to Connect with Open** check box, the WiFi network can accept both clients that support the WiFi enhanced open feature and clients that do not. For clients that do not support the WiFi open enhanced feature, traffic is not encrypted.

       In this case, the SSID name can have a maximum length of 28 characters. Also, you can configure a maximum of two WiFi networks with OWE security and the option to allow both clients that support the WiFi enhanced open feature and clients that do not.

       If you clear the **Allow Devices to Connect with Open** check box, the WiFi network can only accept clients that support the WiFi enhanced open feature.
   - **WPA2 Personal**: This option, which is the same as WPA2-PSK, uses AES encryption. This type of security enables only WiFi devices that support WPA2 to join the VAP.

     WPA2 provides a secure connection but some legacy WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select **WPA2/WPA Personal** authentication.

     In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To view the passphrase in clear text, click the eye icon.
   - **WPA2/WPA Personal**: This option, which is the same as WPA2-PSK/WPA-PSK, enables WiFi devices that support either WPA2 or WPA to join the VAP. This option uses AES and TKIP encryption.

WPA-PSK (which uses TKIP) is less secure than WPA2-PSK (which uses AES) and limits the speed of WiFi devices to 54 Mbps.

In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To view the passphrase in clear text, click the eye icon.

- **WPA2 Enterprise**: This enterprise-level security uses RADIUS for centralized Authentication, Authorization, and Accounting (AAA) management. For WPA2 Enterprise security to function, you must set up RADIUS servers (see Set up RADIUS servers on page 88).

  WPA2 Enterprise security and a captive portal are mutually exclusive.

  From the **Encryption** menu, select the data encryption mode:

  - **TKIP + AES**. This type of data encryption enables WiFi devices that support either WPA or WPA2 to join the access point's WiFi network. This is the default mode.
  - **AES**. This type of data encryption provides a secure connection but some older WiFi devices do not detect WPA2 and support only WPA. Therefore, if your network includes such older devices, select **TKIP + AES** encryption.

  When you select **WPA2 Enterprise** authentication, the **Dynamic VLAN** radio buttons display:

  - **Enable**: The RADIUS server can assign a VLAN ID to clients. If the RADIUS server does not do so, the clients are automatically assigned the VLAN ID that you configured for the SSID.
  - **Disable**: The clients are assigned the VLAN ID that you configured for the SSID. This is the default setting.

  A dynamic VLAN is mutually exclusive with a captive portal, NAT mode, wireless client isolation, and a multicast DNS (mDNS) gateway.

- **WPA3 Personal**: This option is the most secure personal authentication option. WPA3 uses SAE encryption and enables only WiFi devices that support WPA3 to join the VAP. If you select this option, 802.11w (PMF) is automatically set to mandatory (see Step 8).

  WPA3 provides a secure connection but some legacy WiFi devices do not detect WPA3 and support only WPA2. If your network also includes WPA2 devices, select **WPA3/WPA2 Personal** authentication.

  In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To view the passphrase in clear text, click the eye icon.

- **WPA3/WPA2 Personal**: This option, which is the same as WPA3/WPA2-PSK, is the default setting. It enables WiFi devices that support either WPA3 or WPA2 to join the VAP. This option uses SAE and AES encryption.

WPA2-PSK (which uses AES) is less secure than WPA3 (which uses SAE).

In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To view the passphrase in clear text, click the eye icon.

- **WPA3 Enterprise**: This enterprise-level security uses RADIUS for centralized Authentication, Authorization, and Accounting (AAA) management. For WPA3 Enterprise security to function, you must set up RADIUS servers (see Set up RADIUS servers on page 88). If you select this option, 802.11w (PMF) is automatically set to mandatory (see Step 8).

  WPA3 Enterprise security and a captive portal are mutually exclusive.

  When you select WPA3 Enterprise security, the encryption is automatically set to GCMP256, which is a 256-bit encryption protocol.

  When you select **WPA3 Enterprise** authentication, the **Dynamic VLAN** radio buttons display:

  - **Enable**: The RADIUS server can assign a VLAN ID to clients. If the RADIUS server does not do so, the clients are automatically assigned the VLAN ID that you configured for the SSID.
  - **Disable**: The clients are assigned the VLAN ID that you configured for the SSID. This is the default setting.

  A dynamic VLAN is mutually exclusive with a captive portal, NAT mode, wireless client isolation, and a multicast DNS (mDNS) gateway.

8. Optionally, enable 802.11w Protected Management Frames (PMF).

   Protected Management Frames (PMF), according to the 802.11w standard, is a security feature that protects unicast and multicast management frames from being intercepted and changed for malicious purposes. The type of authentication that you select determines if this feature is mandatory, optional, or disabled. You can also set it manually.

   - **Mandatory**: This option requires devices to use PMF. Devices that do not support PMF cannot connect to the WiFi network. If you select Enhanced Open authentication, WPA3 Personal authentication, or WPA3 Enterprise authentication, the radio button for PMF is set to **Mandatory**, and you cannot change it.
   - **Optional**: This option lets the access point automatically activate PMF based on whether devices can support PMF. If you select WPA3/WPA2 Personal authentication, the radio button for PMF is set to **Optional**, but you can change it.
   - **Disable**: This option disables PMF. If you select Open, WPA2 Personal, WPA2/WPA Personal, or WPA2 Enterprise authentication, the radio button for PMF is set to **Disabled**, but you can change it (except for Open authentication).

9. Optionally, enable Multi Pre-Shared Key (PSK), which lets you segregate the WiFi network into different VLANs, each accessible with a unique passphrase.

   Multi PSK is supported only if the WiFi security is WPA2 Personal or WPA2/WPA Personal.

   In a way, Multi PSK lets you create different sub WiFi networks on the WiFi network that you are setting up.

   Although you can also configure this feature while you set up a WiFi network, this feature is more complex and therefore described separately. For more information, see Set up Multi PSK for a WiFi network on page 54.

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

    - **Always ON**: When you set up an SSID, you are creating a new VAP. By default, the new VAP is enabled and the **Always ON** radio button is selected.
    - **Always OFF**: Select this radio button to set up the SSID but temporarily disable the VAP.
    - **Custom**: Select this radio button to set up a broadcast schedule. An icon displays to the right of the radio button. Do the following:

      a. Click the icon next to the radio button.

         A pop-up window displays.

      b. Either select a predefined time from the **Preset** menu or select custom time blocks by clicking the time blocks.

         A blue color for a time block indicates that the VAP will be enabled (on). A gray color for a time block indicates that the VAP will be disabled (off).

      c. Click the **Done** button.

         The pop-up window closes.

      For each SSID, you can create a single custom schedule. In that schedule, for each day from 12:00 a.m. to 11:59 p.m., you specify the time or times that the VAP is disabled.

11. Optionally, select a single radio band only.

    Select a radio button for a single band (**2.4 GHz** or **5 GHz**) or keep the default selection. By default, the **Both** radio button is selected, which lets the access point broadcast the SSID on both bands.

12. Optionally, enable band steering with 802.11k radio resource management (RRM) and 802.11v WiFi network management.

    By default, band steering with 802.11k RRM and 802.11v WiFi network management is disabled for the VAP.

    To enable band steering with 802.11k RRM and 802.11v WiFi network management, select the **Enable** radio button. Doing so allows the access point, under certain

channel conditions, to steer WiFi devices that are dual-band capable to the 2.4 GHz or 5 GHz band of the VAP. Compared to the 2.4 GHz band, generally more channels and bandwidth are available in the 5 GHz band, causing less interference and allowing for a better user experience.
802.11k RRM and 802.11v WiFi network management affect the network in the following ways:

- **802.11k RRM**: This feature lets the access point and 802.11k-aware clients dynamically measure the available radio resources. In an 802.11k-enabled network, access points and clients can send neighbor reports, beacon reports, and link measurement reports to each other, allowing 802.11k-aware clients to automatically select the best access point for initial connection or for roaming.
- **802.11v WiFi network management**: This feature lets the access point steer its WiFi clients to the 2.4 GHz or 5 GHz band, based on the access point's channel load.

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

13. To set the addressing and traffic mode, configure client isolation, configure URL tracking, configure if a DHCP Offer message is unicast or broadcast, or do all of this, scroll down and click the **> Advanced** tab.
14. Optionally, set the NAT mode or Bridge mode for addressing and traffic.

    By default, the addressing and traffic mode of the access point is Bridge mode, which means that WiFi clients receive IP addresses from a DHCP server (or a router that functions as a DHCP server) in your network. This is usually the same DHCP server that assigns an IP address to the access point itself.

    You can also set NAT mode, which enables the access point's DHCP server for WiFi clients. The access point's DHCP server assigns an IP address in a different range from the IP address of the access point itself. NAT mode and Multi PSK (see Step 9) are mutually incompatible.

    From the **Addressing and Traffic** menu, select the addressing and traffic mode:

    Note: This option is not supported in India.

    - **Bridge**: The WiFi clients receive their IP addresses from the DHCP server in the same network as the access point. This is the default mode.
    - **NAT**: WiFi clients receive their IP addresses from a private DHCP address pool on the access point. If you select this mode, by default, the WLAN network address is 172.31.4.0 and the default subnet mask is 255.255.252.0. This means that WiFi clients are assigned an IP address in the range from 172.31.4.2 to 172.31.7.254. The IP address of the default DNS server for the WLAN is 8.8.8.8, and the default lease time is 1440 minutes (24 hours).

To change the default range for the DHCP address pool, the default DNS server, the lease time, or all NAT settings, do the following:

a. In the **Network Address** field, enter a network address that is different from the network address for the access point. For example, if the access point's IP address is in the range from 192.168.0.1 to 192.168.0.254 (a common IP address range), enter a network address that is different from 192.168.0.0.

b. From the **Subnet Mask** menu, select the subnet mask that is appropriate for your network address.

c. In the **DNS** field, enter the IP address for the DNS server that you want to use. This IP address must be different from the WLAN network address that you set in the previous step.

d. In the **Lease Time (in mins)** field, enter the lease time that is applied to WiFi clients.

   The range is from 5 minutes to 43200 minutes.

NAT mode is mutually exclusive with a dynamic VLAN (DVLAN), Multi PSK (see Step 9), a multicast DNS (mDNS) gateway, and a management VLAN other than VLAN 1.

15. Optionally, configure WiFi client isolation.

    By default, client isolation is disabled for the VAP, and the **Disable** radio button is selected. Client isolation and Multi PSK (see Step 9) are mutually incompatible.

    To block communication between WiFi clients that are associated with the same SSID or different SSIDs on the access point, select the **Enable** radio button.

    When you select the **Enable** radio button, the following check box displays:

    Allow access to devices listed below: You can specify static IP addresses or domains (that resolve to static IP addresses) of network devices that are exempt from isolation so that clients are allowed to reach them. For more information, see Enable or disable client isolation for a WiFi network on page 164.

16. Optionally, enable URL tracking.

    By default, URL tracking is disabled, and the **Disable** radio button is selected. To enable URL tracking for all URLs that are requested by WiFi clients that are connected to the SSID, select the **Enable** radio button.

    For information about how to view the tracked URLs per SSID or per WiFi client, see Display or download tracked URLs on page 157.

17. Optionally, change the DHCP Offer message settings.

    When a device tries to associate with the WiFi network and negotiates an IP address, the access point converts the broadcast DHCP offer message that it receives from the DHCP server to a unicast message, and forwards it to the device. This is the default option (that is, the **Enable** radio button is selected). To disable this option so that the access point does *not* convert the broadcast DHCP offer messages to unicast messages, select the **Disable** radio button.

18. To disallow broadcast and multicast traffic in the WiFi network, clear the **Allow Broadcast/Multicast Traffic** check box.

    By default, broadcast and multicast traffic is allowed.

19. To configure a captive portal, a MAC ACL for WiFi clients, and bandwidth rate limits, see the information in the following sections:

    - Set Up and Manage a Captive Portal on page 74

      Captive portals and Multi PSK (see Step 9) are mutually incompatible.
    - Manage MAC ACLs for WiFi clients on page 94 and Select a MAC ACL for WiFi clients in a WiFi network on page 168
    - Set bandwidth rate limits for a WiFi network on page 170

    Although you can also configure these features while you set up a WiFi network, these features are more complex and therefore described separately.

20. To configure advance rate selection, see Configure advanced rate selection for a WiFi network on page 171.

    Although you can also configure this feature while you set up a WiFi network, the feature is more complex and therefore described separately.

21. Click the **Apply** button.

    Your settings are saved.

22. Make sure that you can connect to the new WiFi network.

    If you cannot connect to the new WiFi network, check the following:

    - If your WiFi-enabled computer or mobile device is already connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the correct WiFi network. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
    - If your WiFi-enabled computer or mobile device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your WiFi-enabled computer or mobile device to match the current settings for your network.
    - Does your WiFi device display as a connected client? (See Display client distribution, connected clients, and client trends on page 152.) If it does, it is connected to the network.
    - Are you using the correct WiFi network name (SSID) and password?
    - If the WiFi authentication and encryption is set to WPA3 Personal, make sure that the WiFi adapter device driver is updated to the latest version on your WiFi-enabled computer or mobile device.

View or change the settings of a WiFi network

You can view or change the settings of the default WiFi network (SSID or VAP) or any custom WiFi network. The default WiFi network is the SSID that you renamed and for which you set a new passphrase when you initially connected to the access point. This SSID is displayed as SSID1 in the local browser UI.

To view or change the settings of a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

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

   For detailed descriptions of the settings, see Set up an open or secure WiFi network on page 36.
7. If you made changes, click the **Apply** button.

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

   If you cannot connect over WiFi, check the following:

   - If your WiFi-enabled computer or mobile device is already connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to

the correct WiFi network. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.

- If your WiFi-enabled computer or mobile device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your WiFi-enabled computer or mobile device to match the current settings for your network.
- Does your WiFi device display as a connected client? (See Display client distribution, connected clients, and client trends on page 152.) If it does, it is connected to the network.
- Are you using the correct WiFi network name (SSID) and password?

Remove a WiFi network

You can remove a custom WiFi network (SSID or VAP) that you no longer need. You cannot remove the default WiFi network. The default WiFi network is the SSID that you renamed and for which you set a new passphrase when you initially connected to the access point. This SSID is displayed as SSID1 in the local browser UI.

To remove a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The page that displays lets you select an SSID.
5. Click the **trash can** icon to the right of the SSID.

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

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

Hide or broadcast the SSID for a WiFi network

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

Note: If you set up a wireless distribution system (WDS; see Set up a WiFi Bridge on page 177), you must keep the SSID broadcast enabled.

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

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

   The settings for the selected SSID display.
6. Under Broadcast SSID, select one of the following radio buttons:
   - **No**: The SSID is hidden for the WiFi network.
   - **Yes**: The SSID is broadcast for the WiFi network.
7. Click the **Apply** button.

   Your settings are saved.

Change the VLAN ID for a WiFi network

The VLAN ID for a WiFi network is not the same as the 802.1Q VLAN ID that is used for the wired network (see Set the 802.1Q VLAN and management VLAN on page 106).

Caution: Before you change the VLAN ID, be sure that the VLAN is configured on the network switch and the DHCP server and that the access point and its clients can get IP addresses over the new VLAN.

To change the VLAN ID for a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

   The settings for the selected SSID display.
6. In the **VLAN ID** field, enter an ID (that is, a number).

   By default, the VLAN ID for a WiFi network is 1. The VLAN ID must be between 1 and 4094.
7. Click the **Apply** button.

   Your settings are saved.

Change the authentication and encryption for a WiFi network

You can change the authentication and encryption of the default WiFi network (SSID or VAP) or any custom WiFi network. The default WiFi network is the SSID that you renamed and for which you set a new passphrase when you initially connected to the access point. This SSID is displayed as SSID1 in the local browser UI.

Before you change the authentication and encryption, consider the types of clients that must be able to connect to the WiFi network. WPA3 provides a more secure connection than WPA2, but many WiFi devices might not yet detect WPA3 and support only WPA2. Similarly, WPA2 provides a more secure connection than WPA, but some legacy WiFi devices do not detect WPA2 and support only WPA.

If you plan to use WPA2 Enterprise security or WPA3 Enterprise security for your WiFi network, first set up RADIUS servers (see Set up RADIUS servers on page 88).

To change the authentication and encryption for a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The page that displays lets you select and add an SSID.
5. Click the **+** button to the left of Add SSID.

   The settings for the selected SSID display.
6. From the **Authentication** menu, select one of the following authentication types for the WiFi network, and, if applicable, set a new passphrase (network key or WiFi password) in the **Passphrase** field or select an option from the **Encryption** menu:
   - **Open**: A legacy open WiFi network does not provide any security. Any WiFi device can join the network. We recommend that you do *not* use a legacy open

WiFi network but configure WiFi security. However, a legacy open network might be appropriate for a WiFi hotspot.

If you select **Open** from the **Authentication** menu, the **Enhanced Open** check box displays:

- **Enhanced Open check box cleared**: The WiFi network is a legacy open network without any security. This is the default option for an open network. Clients are not authenticated, traffic is not encrypted, and 802.11w (PMF) is automatically disabled (see Enable or disable PMF for a WiFi network on page 53).
- **Enhanced Open check box selected**: The WiFi enhanced open feature is enabled. This feature is based on opportunistic wireless encryption (OWE). The encryption is set to CCM mode protocol (CCMP) and 802.11w (PMF) is automatically set to mandatory (see Enable or disable PMF for a WiFi network on page 53).

  If you select the **Enhanced Open** check box, the **Allow Devices to Connect with Open** check box displays.

  If you select the **Allow Devices to Connect with Open** check box, the WiFi network can accept both clients that support the WiFi enhanced open feature and clients that do not. For clients that do not support the WiFi open enhanced feature, traffic is not encrypted.

  In this case, the SSID name can have a maximum length of 28 characters. Also, you can configure a maximum of two WiFi networks with OWE security and the option to allow both clients that support the WiFi enhanced open feature and clients that do not.

  If you clear the **Allow Devices to Connect with Open** check box, the WiFi network can only accept clients that support the WiFi enhanced open feature.

- **WPA2 Personal**: This option, which is the same as WPA2-PSK, uses AES encryption. This type of security enables only WiFi devices that support WPA2 to join the VAP.

  WPA2 provides a more secure connection than WPA but some legacy WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select **WPA2/WPA Personal** authentication.

  In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To view the passphrase in clear text, click the eye icon.

- **WPA2/WPA Personal**: This option, which is the same as WPA2-PSK/WPA-PSK, enables WiFi devices that support either WPA2 or WPA to join the VAP. This option uses AES and TKIP encryption.

  WPA-PSK (which uses TKIP) is less secure than WPA2-PSK (which uses AES) and limits the speed of WiFi devices to 54 Mbps.

In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To view the passphrase in clear text, click the eye icon.

- **WPA2 Enterprise**: This enterprise-level security uses RADIUS for centralized Authentication, Authorization, and Accounting (AAA) management. For WPA2 Enterprise security to function, you must set up RADIUS servers (see Set up RADIUS servers on page 88).

  WPA2 Enterprise security and a captive portal are mutually exclusive.

  From the **Encryption** menu, select the data encryption mode:

  - **TKIP + AES**: This type of data encryption enables WiFi devices that support either WPA or WPA2 to join the access point's WiFi network. This is the default encryption.
  - **AES**: This type of data encryption provides a secure connection but some older WiFi devices do not detect WPA2 and support only WPA. Therefore, if your network includes such older devices, select **TKIP + AES** encryption.

  When you select **WPA2 Enterprise** authentication, the **Dynamic VLAN** radio buttons display:

  - **Enable**: The RADIUS server can assign a VLAN ID to clients. If the RADIUS server does not do so, the clients are automatically assigned the VLAN ID that you configured for the SSID.
  - **Disable**: The clients are assigned the VLAN ID that you configured for the SSID. This is the default setting.

  A dynamic VLAN is mutually exclusive with a captive portal, NAT mode, wireless client isolation, and a multicast DNS (mDNS) gateway.

- **WPA3 Personal**: This option is the most secure personal authentication option. WPA3 uses SAE encryption and enables only WiFi devices that support WPA3 to join the VAP. If you select this option, 802.11w (PMF) is automatically set to mandatory (see Enable or disable PMF for a WiFi network on page 53).

  WPA3 provides a more secure connection than WPA2 but many WiFi devices might not yet detect WPA3 and support only WPA2. If your network also includes WPA2 devices, select **WPA3/WPA2 Personal** authentication.

  In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To view the passphrase in clear text, click the eye icon.

- **WPA3/WPA2 Personal**: This option, which is the same as WPA3/WPA2-PSK, enables WiFi devices that support either WPA3 or WPA2 to join the VAP. This option uses SAE and AES encryption.

  WPA2-PSK (which uses AES) is less secure than WPA3 (which uses SAE).

In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To view the passphrase in clear text, click the eye icon.

- **WPA3 Enterprise**: This enterprise-level security uses RADIUS for centralized Authentication, Authorization, and Accounting (AAA) management. For WPA3 Enterprise security to function, you must set up RADIUS servers (see Set up RADIUS servers on page 88). If you select this option, 802.11w (PMF) is automatically set to mandatory (see Enable or disable PMF for a WiFi network on page 53).

  WPA3 Enterprise security and a captive portal are mutually exclusive.

  When you select WPA3 Enterprise security, the encryption is automatically set to GCMP256, which is a 256-bit encryption protocol.

  When you select **WPA3 Enterprise** authentication, the **Dynamic VLAN** radio buttons display:

  - **Enable**: The RADIUS server can assign a VLAN ID to clients. If the RADIUS server does not do so, the clients are automatically assigned the VLAN ID that you configured for the SSID.
  - **Disable**: The clients are assigned the VLAN ID that you configured for the SSID. This is the default setting.

  A dynamic VLAN is mutually exclusive with a captive portal, NAT mode, wireless client isolation, and a multicast DNS (mDNS) gateway.

7. Click the **Apply** button.

   Your settings are saved.

8. Make sure that you can connect to the new WiFi network.

   If you cannot connect to the new WiFi network, check the following:

   - If your WiFi-enabled computer or mobile device is already connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the correct WiFi network. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
   - If your WiFi-enabled computer or mobile device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your WiFi-enabled computer or mobile device to match the current settings for your network.
   - Does your WiFi device display as a connected client? (See Display client distribution, connected clients, and client trends on page 152.) If it does, it is connected to the network.

- Are you using the correct WiFi network name (SSID) and password?
- If you changed the WiFi authentication and encryption to WPA3 Personal, make sure that the WiFi adapter device driver is updated to the latest version on your WiFi-enabled computer or mobile device.

Enable or disable PMF for a WiFi network

Protected Management Frames (PMF), according to the 802.11w standard, is a security feature that protects unicast and multicast management frames from being intercepted and changed for malicious purposes. The type of authentication that you select determines if this feature is mandatory, optional, or disabled. You can also set it manually.

To enable or disable PMF for a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

   The settings for the selected SSID display.
6. Under 802.11w (PMF), select one of the following radio buttons:
   - **Mandatory**: Requires devices to use PMF. Devices that do not support PMF cannot connect to the WiFi network. If you select Enhanced Open authentication,

WPA3 Personal authentication, or WPA3 Enterprise authentication, the radio button for PMF is set to **Mandatory**, and you cannot change it.

- **Optional**: Lets the access point automatically activate PMF based on whether devices can support PMF. If you select WPA3/WPA2 Personal authentication, the radio button for PMF is set to **Optional**, but you can change it.
- **Disable**: PMF is disabled for the WiFi network. If you select Open, WPA2 Personal, WPA2/WPA Personal, or WPA2 Enterprise authentication, the radio button for PMF is set to **Disabled**, but you can change it (except for Open authentication).

7. Click the **Apply** button.

   Your settings are saved.

Set up Multi PSK for a WiFi network

Multi Pre-Shared Key (PSK) lets you segregate a single WiFi network into different VLANs, each accessible with a unique passphrase. In a way, Multi PSK lets you create different sub WiFi networks on a single WiFi network. When connecting to the WiFi network, the passphrase that a user enters determines the VLAN that the WiFi client is placed in.

In addition to a VLAN and passphrase, you can associate a key identifier with the VLAN-to-passphrase mapping. The key identifier lets you identify the VLANs in the WiFi network for network monitoring purposes. For example, when you display WiFi clients, the key identifier can also display (see Display client distribution, connected clients, and client trends on page 152).

As examples of key identifiers, you could use terms such as corporatenetwork_22, corporatenetwork_23, and corporatenetwork_24. These key identifiers (or the associated VLAN IDs) are not visible to a user trying to connect to the WiFi network: the user sees the SSID and enters the passphrase.

If you enable Multi PSK, the WiFi network's passphrase and VLAN are replaced by the passphrases and VLANs that are part of the Multi PSK configuration.

Note: Multi PSK is supported only if the WiFi security is WPA2 Personal or WPA2/WPA Personal. To configure Multi PSK on the default WiFi network (displayed as SSID1 in the local bowser UI), which is the WiFi network that you defined when you initially connected to the access point, you must first change the WiFi security to WPA2 Personal or WPA2/WPA Personal.

In addition, the following restrictions apply to Multi PSK:

- You can configure Multi PSK on a maximum of four WiFi networks.
- Each WiFi network on which you configure Multi PSK can support a maximum of eight VLAN-to-passphrase mappings. Within each WiFi network, each passphrase

and key identifier must be unique. The access point can support a maximum of 32 Multi PSK VLAN-to-passphrase mappings. For example, four WiFi networks each can support eight Multi PSK VLAN-to-passphrase mappings.

- Within a Multi PSK on a single WiFi network, you can map the same VLAN ID to different passphrases. You can also use the same VLAN ID for Multi PSK in different WiFi networks.
- If inter-VLAN routing is disabled in the network to which the access point is connected, the following applies:
  - WiFi clients that are connected to different VLANs on the same WiFi network (that is, the WiFi clients use different passphrases to connect to the same WiFi network) cannot communicate with each other and remain isolated.
  - WiFi clients that are connected to the *same* VLAN on different WiFi networks *can* communicate with each other.
- Multi PSK and the following features are mutually exclusive:
  - Captive portal (see Set Up and Manage a Captive Portal on page 74)
  - mDNS gateway (see Manage the multicast DNS gateway on page 113)
  - NAT mode (see Set NAT mode or Bridge mode for addressing and traffic on page 163)
  - Client isolation (see Enable or disable client isolation for a WiFi network on page 164)

To set up Multi PSK for a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

   The settings for the selected SSID display.

You cannot configure Multi PSK on the default WiFi network (displayed as SSID1 in the local bowser UI), which is the WiFi network that you defined when you initially connected to the access point.

6. Select the Multi PSK **Enable** radio button.
7. Click the **+** button to the left of Add New Passphrase.

   The page adjusts.
8. Configure the Multi PSK settings:
   a. To add a new Multi PSK entry, specify the following settings:
      - **VLAN ID**: The VLAN ID, which is the VLAN that a WiFi client becomes a member of.

        The VLAN ID must be between 1 and 4094.
      - **Passphrase**: The unique passphrase (WiFi password) that a user must enter to let the WiFi client connect to the associated VLAN of the WiFi network.

        The passphrase must be between 8 and 63 characters.
      - **Key Identifier**: The phrase or term that lets you identify the VLAN in the WiFi network for monitoring purposes. The maximum length is 30 alphanumeric characters, including the following special characters: hyphen (-) and underscore (_).

   b. To add another Multi PSK entry, click the **+** button to the left of Add New Passphrase and repeat the previous step a.
   c. To remove a Multi PSK entry, click the **trash can** icon to the right of the entry.
9. Click the **Apply** button.

   Your settings are saved.

Disable or enable a WiFi network or set up a WiFi activity schedule

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

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

For each WiFi network, you can create a single custom schedule. In that schedule, for each day from 12:00 a.m. to 11:59 p.m., you specify the time or times that the VAP is disabled.

To disable or enable a WiFi network or set up a WiFi activity schedule:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

   The settings for the selected SSID display.
6. Under Schedule, select one of the following radio buttons:
   - **Always ON**: The WiFi network is enabled.
   - **Always OFF**: The WiFi network is disabled.
   - **Custom**: The WiFi network is enabled or disabled according to a schedule that you must set up.

     An icon displays to the right of the radio button.
7. If you selected **Custom** in the previous step, do the following:
   a. Click the icon next to the radio button.

      A pop-up window displays.

   b. Either select a predefined time from the **Preset** menu or select custom time blocks by clicking the time blocks.

      A blue color for a time block indicates that the WiFi network will be enabled (on). A gray color for a time block indicates that the WiFi network will be disabled (off).

   c. Click the **Done** button.

      The pop-up window closes.
8. Click the **Apply** button.

   Your settings are saved.

Enable or disable band steering with 802.11k RRM and 802.11v WiFi network management

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

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

- **802.11k RRM**: This feature lets the access point and 802.11k-aware clients dynamically measure the available radio resources. In an 802.11k-enabled network, access points and clients can send neighbor reports, beacon reports, and link measurement reports to each other, allowing 802.11k-aware clients to automatically select the best access point for initial connection or for roaming.
- **802.11v WiFi network management**: This feature lets the access point steer its WiFi clients to the 2.4 GHz or 5 GHz band, based on the access point's channel load. In an environment with multiple access points, 802.11v WiFi network management helps WiFi clients that are roaming to select the best access point.

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

To enable or disable band steering with 802.11k RRM and 802.11v WiFi network management for a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

The Dashboard displays.

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

   The page that displays lets you select an SSID.

5. Click the **>** button to the left of the SSID.

   The settings for the selected SSID display.

6. Under Band Steering, select one of the following radio buttons:
   - **Disable**: Band steering is disabled for the VAP. This is the default setting.
   - **Enable**: Under certain channel conditions, the access point steers WiFi devices that are dual-band capable to the 2.4 GHz or 5 GHz band of the VAP.

7. Click the **Apply** button.

   Your settings are saved.

5

Manage the Basic Radio Features

This chapter describes how you can manage the basic radio features of the access point. For information about the advanced radio features, see Manage the Advanced Radio Features on page 182.

Caution: If you change a radio feature on the 2.4 GHz radio, the change affects all WiFi networks that broadcast on the 2.4 GHz radio. Similarly, if you change a radio feature on the 5 GHz radio, the change affects all WiFi networks that broadcast on the 5 GHz radio. If the change is not specific to one radio, the change affects *all* WiFi networks on the access point.

The chapter includes the following sections:

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

Note: If you want to change the radio settings, use a wired connection to avoid being disconnected when the new radio settings take effect.

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

Manage the basic WiFi settings for the radios

The basic WiFi settings for each radio apply to all WiFi networks (VAPs or SSIDs) that are configured on the radio. You can specify the radio settings for the 2.4 GHz and 5 GHz radios individually.

To manage the basic WiFi settings for the radios:

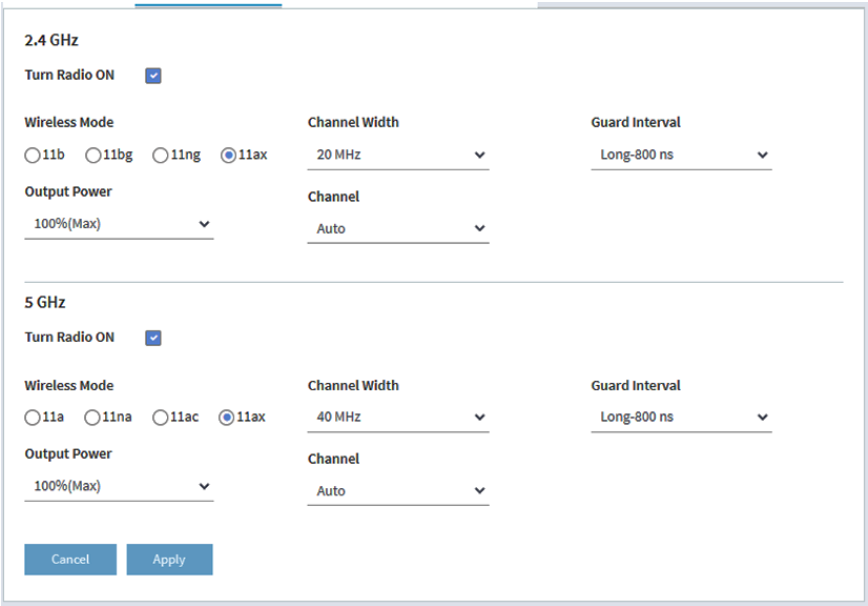
1. Launch a web browser from a computer that is connected to the same network as the access point or directly to the access point through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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



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

5. Configure the following settings:
   - **Turn Radio ON**: By default, the **Turn Radio ON** check box is selected and the radio broadcasts. Turning off a radio disables WiFi access for the band, which can be helpful during configuration, network tuning, or troubleshooting.
   - **Wireless Mode**:

     Select one of the following wireless modes (WiFi modes) for the 2.4 GHz radio:
     - **11ax**: 802.11ax, 802.11ng, 802.11bg, and 802.11b WiFi clients can connect to the access point. This is the default setting.
     - **11ng**: 802.11ax, 802.11ng, 802.11bg, and 802.11b WiFi clients can connect to the access point. However, the speed of 802.11ax clients is limited to the maximum speed that is supported by 802.11ng (about 450 Mbps).
     - **11bg**: 802.11ax, 802.11ng, 802.11bg, and 802.11b WiFi clients can connect to the access point. However, the speed of 802.11ax and 802.11ng clients is limited to the maximum speed that is supported by 802.11bg (about 54 Mbps).
     - **11b**: 802.11ax, 802.11ng, 802.11bg, and 802.11b WiFi clients can connect to the access point. However, the speed of 802.11ax, 802.11n, and 802.11bg clients is limited to the maximum speed that is supported by 802.11b (about 11 Mbps).

     Select one of the following wireless modes (WiFi modes) for the 5 GHz radio:
     - **11ax**: 802.11ax, 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. This is the default setting.
     - **11ac**: 802.11ax, 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. However, the speed of 802.11ax clients is limited to the maximum speed that is supported by 802.11ac (about 867 Mbps).
     - **11na**: 802.11ax, 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. However, the speed of 802.11ax and 802.11ac clients is limited to the maximum speed that is supported by 802.11na (about 450 Mbps).
     - **11a**: 802.11ax, 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. However, the speed of 802.11ax, 802.11ac, 802.11na clients is limited to the maximum speed that is supported by 802.11a (up to about 54 Mbps).
   - **Channel Width**: From the menu, select the channel width for the radio. Your selection from the **Wireless Mode** menu determines if you can set the channel width, and if so, which channel widths are available.

     Use the following guidelines:

- A wider channel improves the performance (no or minimal interference and better data rates).
- A narrower channel generally results in lower throughput but might provide a more stable connection in a demanding situation, such as an environment with a long distance between the access point and WiFi clients and more than normal interference.
- The 802.11n specification allows a 40 MHz–wide channel in addition to the legacy 20 MHz channel width that is available with other modes.
- The 802.11ac specification allows an 80 MHz–wide channel in addition to the 20 MHz and 40 MHz channel widths that are available with other modes.
- The 802.11ax specification for the 5 GHz radio allows a 160 MHz–wide channel in addition to the 20 MHz, 40 MHz, and 80 MHz channel widths that are available with other WiFi modes.
- The 40 MHz, 80 MHz, and 160 MHz channel widths enable higher data rates but leave fewer channels available for use on the 5 GHz radio.

For more information, see Change the channel width for a radio on page 67.

- **Guard Interval**: The guard interval protects radio transmissions from interference. Your selection from the **Wireless Mode** menu determines if you can set the guard interval, and if so, which guard intervals are available. For the 11a, 11b, and 11bg WiFi modes, you cannot set the guard interval at all.

  From the menu, select one of the following settings:

  - **Auto**: The guard interval is set automatically by the access point. This option is not available in the 11ax WiFi mode.
  - **Long-800 ns**: This option is available in the 11ax, 11ac, 11na, and 11ng modes. In the 11ax WiFi mode, this option is the default setting.
  - **Double Long-1600 ns**: This option is available only in the 11ax WiFi mode.
  - **Quadruple Long-3200 ns**: This option is available only in the 11ax WiFi mode.
- **Output Power**: From the menu, select the transmission power of the radio. You can select **100%(Max)**, **50%**, **25%**, **12.5%**, or **4%(Min)**. The default is 100%(Max).

  Note: If two or more access points are operating in the same area and on the same channel, interference can occur. In this situation, you might want to decrease the output power for the access point. Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.
- **Channel**: From the menu, select the WiFi channel for the radio. The available WiFi channels and frequencies depend on the country that you selected for the

access point and on the radio. The default is Auto, which enables a radio to automatically select the most suitable channel.

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

Note: If you use multiple access points, 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, in the 2.4 GHz band, use channels 1 and 5, or 6 and 10).

6. Click the **Apply** button.

   A warning pop-up window displays.

7. Click the **OK** button.

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

Turn a radio on or off

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

To turn a radio on or off:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Wireless Settings page displays.

5. Take one of the following actions:
   - **Turn a radio on**: Select the **Turn Radio ON** check box for the radio.
   - **Turn a radio off**: Clear the **Turn Radio ON** check box for the radio.
6. Click the **Apply** button.

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

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

Change the WiFi mode for a radio

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

To change the WiFi mode for a radio:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Wireless Settings page displays.
5. Select the WiFi mode for the radio:
   - **2.4 GHz radio**: Select one of the following WiFi modes for the 2.4 GHz radio:

- **11ax**: 802.11ax, 802.11ng, 802.11bg, and 802.11b WiFi clients can connect to the access point. This is the default setting.
- **11ng**: 802.11ax, 802.11ng, 802.11bg, and 802.11b WiFi clients can connect to the access point. However, the speed of 802.11ax clients is limited to the maximum speed that is supported by 802.11ng (about 450 Mbps).
- **11bg**: 802.11ax, 802.11ng, 802.11bg, and 802.11b WiFi clients can connect to the access point. However, the speed of 802.11ax and 802.11ng clients is limited to the maximum speed that is supported by 802.11bg (about 54 Mbps).
- **11b**: 802.11ax, 802.11ng, 802.11bg, and 802.11b WiFi clients can connect to the access point. However, the speed of 802.11ax, 802.11n, and 802.11bg clients is limited to the maximum speed that is supported by 802.11b (about 11 Mbps).

- **5 GHz radio**: Select one of the following WiFi modes for the 5 GHz radio:
  - **11ax**: 802.11ax, 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. This is the default setting.
  - **11ac**: 802.11ax, 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. However, the speed of 802.11ax clients is limited to the maximum speed that is supported by 802.11ac (about 867 Mbps).
  - **11na**: 802.11ax, 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. However, the speed of 802.11ax and 802.11ac clients is limited to the maximum speed that is supported by 802.11na (about 450 Mbps).
  - **11a**: 802.11ax, 802.11ac, 802.11na, and 802.11a WiFi clients can connect to the access point. However, the speed of 802.11ax, 802.11ac, 802.11na clients is limited to the maximum speed that is supported by 802.11a (up to about 54 Mbps).

6. Click the **Apply** button.

   A warning pop-up window displays.

7. Click the **OK** button.

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

Change the channel width for a radio

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

- A wider channel generally improves the performance (no or minimal interference and better data rates).
- A narrower channel generally results in lower throughput but might provide a more stable connection in a demanding situation, such as an environment with a long distance between the access point and WiFi clients and more than normal interference.
- The 802.11n specification allows a 40 MHz–wide channel in addition to the legacy 20 MHz channel width that is available with other WiFi modes.
- The 802.11ac specification and the 802.11ax specification for the 5 GHz band allow an 80 MHz–wide channel in addition to the 20 MHz and 40 MHz channel widths that are available with other WiFi modes.
- The 802.11ax specification for the 5 GHz radio allows a 160 MHz–wide channel in addition to the 20 MHz, 40 MHz, and 80 MHz channel widths that are available with other WiFi modes.
- The 40 MHz, 80 MHz, and 160 MHz channel widths enable higher data rates but leave fewer channels available for use on the 5 GHz radio.

Note: We recommend that you leave the default options (20 MHz for the 2.4 GHz radio and 40 MHz for the 5 GHz radios).

The WiFi mode (see Change the WiFi mode for a radio on page 65) determines if you can set the channel width, and if so, which channel widths are available.

To change the channel width for a radio:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

The Dashboard displays.

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

   The Wireless Settings page displays.

5. From the **Channel Width** menu for the radio, select one of the following settings.
   - **20 MHz**: This is the default setting for the 2.4 GHz radio.
   - **40 MHz**: This is the default settings for the 5 GHz radio.
   - **80 MHz**: This selection is available only for the 5 GHz radio.
   - **160 MHz**: This selection is available only for the 5 GHz radio.
   - **Dynamic 20 / 40 MHz**. This selection is available only for the 2.4 GHz radio.
   - **Dynamic 20 / 40 / 80 / 160 MHz**. This selection is available only for the 5 GHz radio.
6. Click the **Apply** button.

   A warning pop-up window displays.

7. Click the **OK** button.

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

Change the guard interval for a radio

From the menu, select the guard interval, which protects radio transmissions from interference. The WiFi mode (see Change the WiFi mode for a radio on page 65) determines if you can set the guard interval, and if so, which guard intervals are available. For the 11a, 11b, and 11bg WiFi modes, you cannot set the guard interval at all.

Use the following guidelines:

- A shorter guard interval supports more throughput in an environment in which WiFi devices operate at a shorter distance from the access point.
- A longer guard interval works well in an environment with multiple SSIDs and WiFi devices that operate at a longer distance from the access point.
- Some legacy devices can operate with a long –800ns guard interval only.

To change the guard interval for a radio:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Wireless Settings page displays.
5. From the **Guard Interval** menu for the radio, select one of the following settings:
   - **Auto**: The guard interval is set automatically by the access point. This option is not available in the 11ax WiFi mode.
   - **Long-800 ns**: This option is available in the 11ax, 11ac, 11na, and 11ng modes. In the 11ax WiFi mode, this option is the default setting.
   - **Double Long-1600 ns**: This option is available only in the 11ax WiFi mode.
   - **Quadruple Long-3200 ns**: This option is available only in the 11ax WiFi mode.
6. Click the **Apply** button.

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

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

Change the output power for a radio

By default, the output power of the access point is set at the maximum. If two or more access points are operating in the same area and on the same channel, interference can occur. In such a situation, you might want to decrease the output power for the

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

To change the output power for a radio:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Wireless Settings page displays.
5. From the **Output Power** menu for the radio, select **100%(Max)**, **50%**, **25%**, **12.5%**, or **4%(Min)**.

   The default is 100%(Max).
6. Click the **Apply** button.

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

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

Change the channel for a radio

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

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

Note: If you use multiple access points, 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, in the 2.4 GHz band, use channels 1 and 5, or 6 and 10).

To change the channel for a radio:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

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

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

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

Manage Quality of Service for a WiFi radio

You can specify the Quality of Service (QoS) setting for the 2.4 GHz and 5 GHz radios separately. These settings are enabled by default for both radios. Disabling QoS for a radio might impact the throughput and speed of WiFi traffic on the access point.

To manage the QoS settings for a WiFi radio:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The QoS Settings page displays.
5. Enable or disable the following features for the radio by selecting the applicable **Enable** or **Disable** radio buttons:
   - **Wi-Fi Multimedia (WMM)**: WiFi Multimedia (WMM) is a subset of the 802.11e standard. Time-dependent information such as video or audio is given higher priority than normal traffic. For WMM to function correctly, WiFi clients must also support WMM. By enabling WMM, you allow WMM to control upstream traffic flowing from WiFi devices to the access point and downstream traffic flowing from the access point to WiFi devices. WMM defines the following four queues in decreasing order of priority:
     - **Voice**: The highest priority queue with minimum delay, which makes it very suitable for applications such as VoIP and streaming media.
     - **Video**: The second highest priority queue with low delay. Video applications are routed to this queue.
     - **Best effort**: The medium priority queue with medium delay. Most standard IP applications use this queue.
     - **Background**: The low priority queue with high throughput. Applications such as FTP that are not time-sensitive but require high throughput can use this queue.

     Note: Wi-Fi Multimedia (WWM) cannot be disabled for 802.11n, 802.11ac, and 802.11ax modes.
   - **WMM Powersave**: Enabling the WMM Powersave feature saves power for battery-powered devices and fine-tunes power consumption.
6. Click the **Apply** button.

A warning pop-up window displays.

7. Click the **OK** button.

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

6

Set Up and Manage a Captive Portal

This chapter describes how you can set up and manage a captive portal on the access point.

A captive portal is a web page that users see when they attempt to connect to a WiFi network. A captive portal includes a splash page and usually requires some form of authentication for the user. The access point supports two types of captive portals:

- **Click-through captive portal**: A basic portal for which the splash page is stored on the access point. For each WiFi network, you can set up a unique click-through captive portal.
- **External captive portal**: A portal that is hosted by an external captive portal vendor. You can apply an external captive portal to multiple WiFi networks or you can apply a unique external captive portal to each WiFi network.

The chapter includes the following sections:

- Set up a click-through captive portal for a WiFi network
- Set up an external captive portal for a WiFi network

Note: A captive portal is not compatible with Multi PSK. To enable a captive portal, first disable Multi PSK (see Set up Multi PSK for a WiFi network on page 54).

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

Set up a click-through captive portal for a WiFi network

A click-through captive portal is a basic portal for which the splash page is stored on the access point, that is, it is not an external captive portal. Use a click-through captive portal to welcome or instruct WiFi users and limit their sessions. You can require users to agree to an end user license agreement (EULA) and redirect them to a specific website. A click-through captive portal is specific to the WiFi network (SSID) on which you set it up.

To set up a click-through captive portal for a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

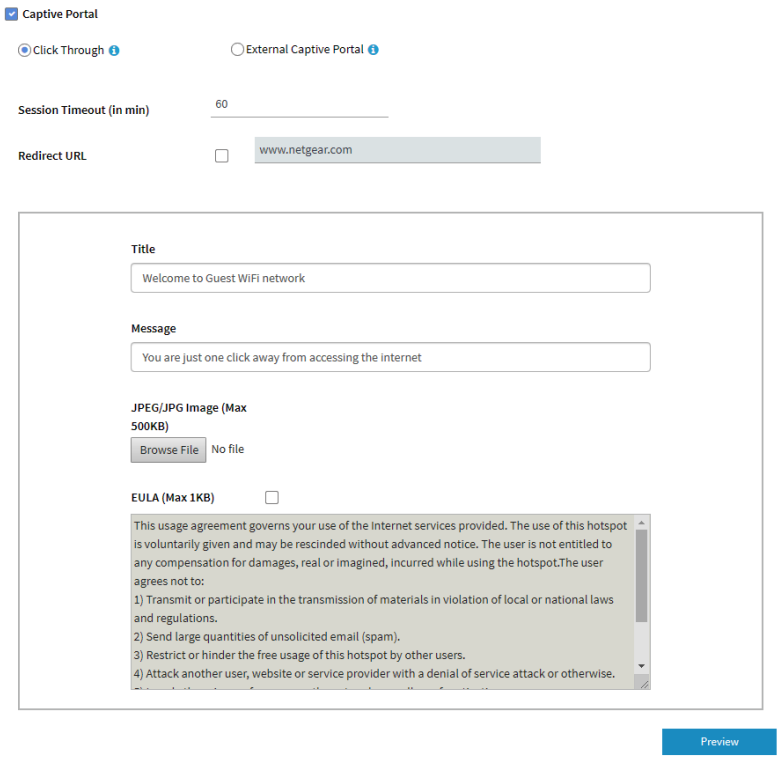
   The Dashboard displays.
4. Select **Management > Configuration > Wireless > Basic**.

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

   The settings for the selected SSID display.
6. Scroll down and click the **> Advanced** tab.

   The page expands.
7. Select the **Captive Portal** check box.

The page adjusts. By default, the **Click Through** radio button is selected.



8. Specify the click-through settings as described in the following table.

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

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

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

10. Click the **Apply** button.

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

    Note: An HTTPS session is blocked until after the captive portal authentication occurs.

Set up an external captive portal for a WiFi network

An external captive portal is a portal that is hosted by an external captive portal vendor. That is, this type of portal is not stored on the access point. For an external captive portal, you generally must register your devices with and purchase licenses from the vendor.

You can apply an external captive portal to multiple WiFi networks or you can apply a unique external captive portal to each WiFi network

To set up an external captive portal for a WiFi network:

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

   A login window displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The page that displays lets you select an SSID.

5. Click the **>** button to the left of the SSID.

   The settings for the selected SSID display.

6. Scroll down and click the **> Advanced** tab.

   The page expands.

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

   The page adjusts. By default, the **Click-Through** radio button is selected.

8. Click the **External Captive Portal** radio button.

   The page adjusts.

9. In the **Splash Page URL** field, enter the URL that is provided by the vendor.

   This URL redirects a user to the splash page on the website that hosts the captive portal.

10. Select one of the following **Captive Portal Authentication Type** radio buttons:

    - **Web/HTTP**: Authentication for access to the splash page occurs on the access point using the HTTPS protocol. Specify the following settings:
      - **Web Authentication URL**: Enter the web authentication URL that is provided by the vendor.

        The length of the web authentication URL can be up to 256 characters.
      - **Key**: Enter the key credential that is provided by the vendor. This field is optional and depends on the authentication requirements of the vendor.

        The length of the key can be up to 32 characters.
      - **Secret**: Enter the secret credential that is provided by the vendor. This field is optional and depends on the authentication requirements of the vendor.

        The length of the secret can be up to 64 characters.
    - **Radius**: Authentication for access to the splash page occurs on an external RADIUS authentication server. The vendor might also require an accounting RADIUS server. Specify the following settings for *each* RADIUS server, as directed by the vendor:

- **IPv4 Address**: Enter the IP address of the server. The IP address is provided by the vendor.
- **Port**: Enter the port number that is used by the server. The IP port number is provided by the vendor. By default, an authentication server uses port number 1812; an accounting server uses port number 1813.

  The port number range can be from 1 to 65535.
- **Password**: Enter the password (shared secret) for interaction with the server. The password is provided by the vendor.

  The password must be a minimum of 8 characters and can be a maximum of 64 characters.
- **Accounting Interval**: Enter the accounting interval, which indicates the number of seconds between each transmittal of an interim update or live packets for a specific session. In the **Accounting Interval** field, enter a value from 60 seconds (the minimum) to 600 seconds (the maximum).
- **NAS-Identifier**: Enter a network access server identifier (NAS-ID).

  A NAS-ID distinguishes the source of a RADIUS access or accounting request, which enables the RADIUS server to choose a policy for that request. The default NAS-Identifier setting is the Ethernet MAC address of the access point.

11. Select one of the following **FailSafe** buttons to specify if users are allowed to reach the splash page and access the Internet if authentication is not possible:
    - **Enable**: If authentication is not possible—for example, because captive portal servers do not respond—users are still allowed to access the Internet for a period of 30 minutes.
    - **Disable**: This is the default setting. If authentication is not possible, users cannot reach the splash page and cannot access the Internet. Instead, they get a message *Oops. Something went wrong. Please try after some time*.
12. Select one of the following **Allow HTTPS** buttons to specify when secure HTTP (HTTPS) traffic is allowed to pass through:
    - **Enable**: Before authentication occurs, HTTPS traffic is allowed to pass through.
    - **Disable**: This is the default setting. HTTPS traffic is allowed only *after* authentication occurs.
13. Configure the walled garden settings.

    The walled garden specifies the external applications and sites that a user can access from the captive portal. Generally, the vendor provides information about the applications and sites. The vendor splash page, domain name, and authentication servers must also be included in the walled garden. Follow the directions of the vendor.

    You can do the following to configure the walled garden:

- **Add a single URL**: In the right field, type the URL, press **Enter**, and click the **Move** button.
- **Add multiple URLs**: In the right field, paste a list of URLs, and click the **Move** button.
- **Remove one or more URLs**: Select the check boxes for URLs, and click the **Remove** button.
- **Remove all URLs**: Select the **Select All** check box, and click the **Remove** button.

14. Click the **Apply** button.

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

7

Manage Access and Security

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

The chapter includes the following sections:

- Manage user accounts
- Block specific URLs and keywords for Internet access
- Set up RADIUS servers
- Manage neighbor AP detection
- Manage MAC ACLs for WiFi clients
- Enable L2 security
- Manage the denial of service protection

Note: For information about essential WiFi security (network authentication and encryption), see Set up an open or secure WiFi network on page 36.

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

Manage user accounts

User accounts provide either read/write or read-only access to the local browser UI of the access point. You cannot delete the admin user account or change its user name, but you can change its password. You can add accounts for other users, and you can change or delete these accounts.

The following sections describe how you can manage user accounts:

- Add a user account
- Change the time-out period for a user session
- Change the settings for a user account
- Remove a user account

For information about changing the password for the default admin user account, see Change the admin user account password on page 120.

Add a user account

To add a user account:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The User Accounts page displays.
5. Click the add user account icon.

   Additional fields and a menu display.
6. Specify the settings for the new user account:

- **User Name**: Enter a user name.

  The user name must consist of up to 15 alphanumeric characters without any special characters. Do not use admin or Admin as the user name.
- **Password**: Enter a password between 8 and 64 characters in length. The password must contain at least one uppercase letter, one lowercase letter, and one number.
- **Privilege**: From the menu, select **Read-Write** or **Read-Only**.
- **Session Timeout**: Use the **Hours** and **Minutes** fields to specify the period after which a session automatically expires and the user must log in again.

  By default, a session expires after 45 minutes.

7. Click the **Apply** button.

   Your settings are saved.

Change the time-out period for a user session

When a user logs in to the local browser UI, the session times out automatically after 45 minutes. You can change the time-out period, which applies to all users, including the admin user.

To change the time-out period for a user session:

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

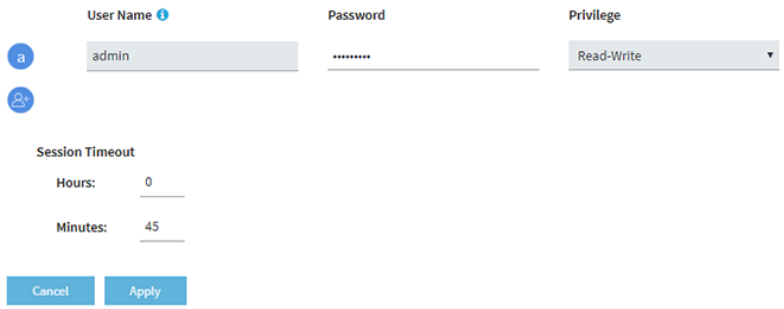
   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

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



5. Under Session Timeout, use the **Hours** and **Minutes** fields to specify the period after which a session automatically expires and the user must log in again.

   By default, a session expires after 45 minutes.

6. Click the **Apply** button.

   Your settings are saved. Your session is terminated and you must log in again.

Change the settings for a user account

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

To change the user name, password, or access privilege for a user account:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The existing user accounts display.

5. To the right of the user account, change the existing settings as needed:

- **User Name**: Enter another user name.
- **Password**: Enter another password between 8 and 64 characters in length. The password must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed:

  ! @ # $ % ^ & * ( )
- **Privilege**: From the menu, select **Read-Write** or **Read-Only**.

6. Click the **Apply** button.

   Your settings are saved.

Remove a user account

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

To remove a user account:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The existing user accounts display.
5. Click the **X** to the right of the user account.

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

   The pop-up windows closes and the user account is removed.

Block specific URLs and keywords for Internet access

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

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

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

   A login window displays.

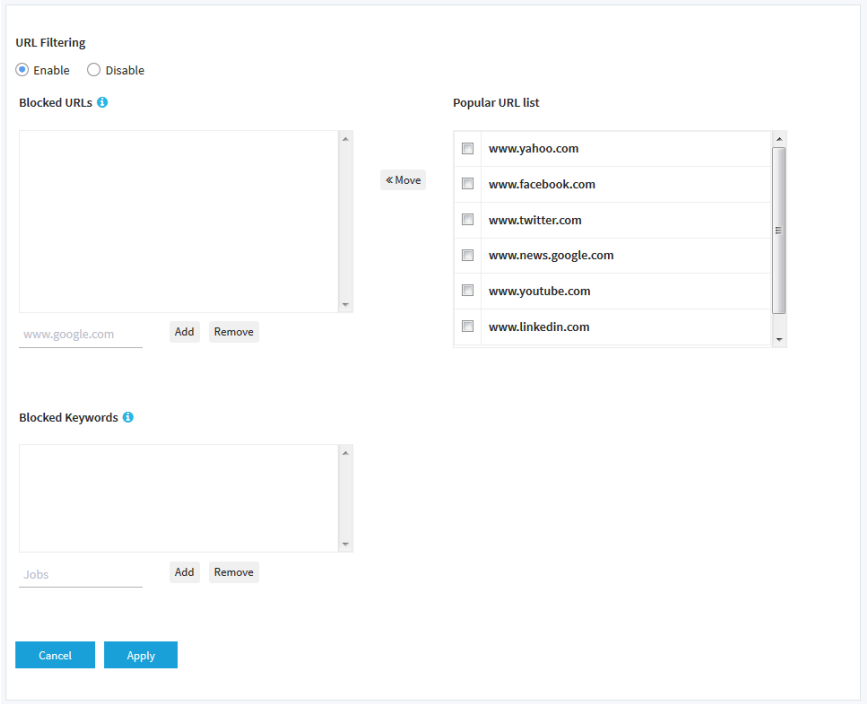
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The URL Filtering page displays.

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



6. Compose the blacklist in the following ways:
   - **Blocked URLs**: To add a URL to the blacklist, type or copy the URL in the upper field (to the left of the upper **Add** button) and click the upper **Add** button. You can also select one or more URLs from the Popular URL list by selecting the check boxes for the URLS and clicking the **<< Move** button.

     To remove a URL from the blacklist, select the check box for the URL and click the upper left **Remove** button.

     When you block a URL, the domain and all URLs in the domain are blocked. For example, if you add www.google.com, all web pages in the www.google.com domain are blocked, including, for example, www.google.com/finance.
   - **Blocked Keywords**: To add a keyword entry to the blacklist, enter the keyword in the lower field (to the left of the lower **Add** button) and click the lower **Add** button.

     To remove a keyword entry from the blacklist, select the check box for the entry and click the lower **Remove** button.

     All URLs that contain the keyword are blocked. For example, if you add Jobs, all URLs that contains Jobs (or jobs) are blocked.
7. Click the **Apply** button.

   Your settings are saved.

Set up RADIUS servers

If you use WPA2 Enterprise security, WPA3 Enterprise security, or a RADIUS MAC ACL, you must set up RADIUS servers for authentication or both authentication and accounting using RADIUS. You must set up a primary IPv4 server and you can set up a secondary IPv4 server. These RADIUS server settings apply either to all WiFi networks that use WPA2 Enterprise security or WPA3 Enterprise security (see Set up an open or secure WiFi network on page 36) or to all WiFi networks that use a RADIUS MAC ACL.

Note: Either WPA2 Enterprise security or WPA3 Enterprise security and a RADIUS MAC ACL are mutually exclusive. If you want to use a RADIUS MAC ACL for a WiFi network, select a different type of WiFi security (see Set up an open or secure WiFi network on page 36). If you want to use WPA2 Enterprise security or WPA3 Enterprise security for a WiFi network, use a local MAC ACL (see Manage MAC ACLs for WiFi clients on page 94).

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

To set up RADIUS servers:

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

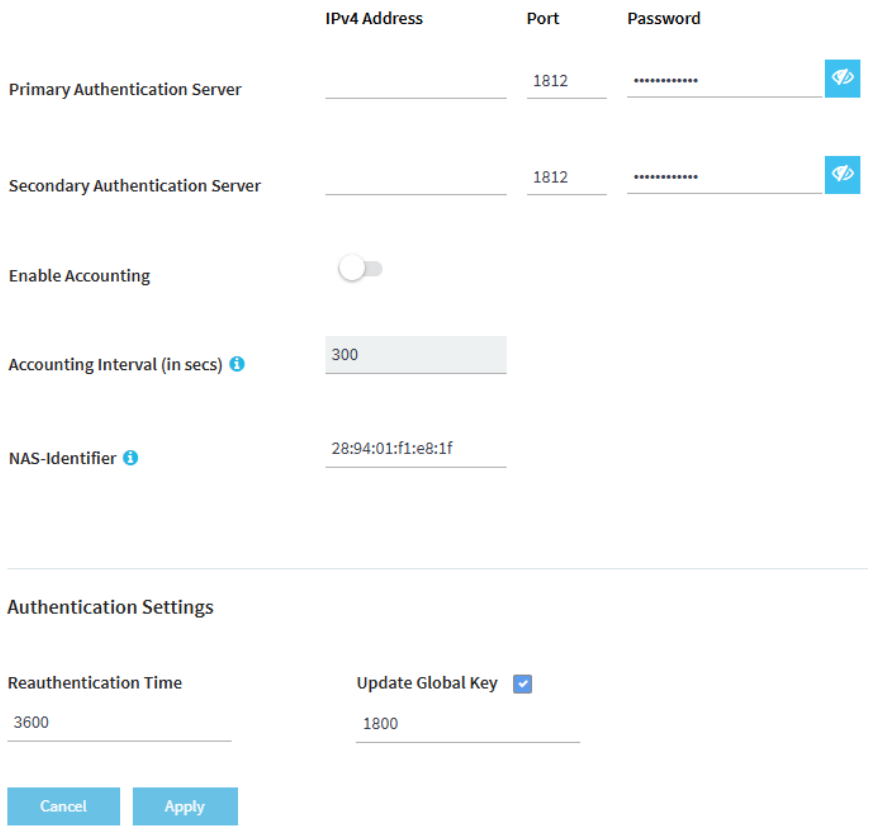
   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

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



5. For each RADIUS server that you want to set up, configure the following settings:
   - **IPv4 Address**: Enter the IPv4 address of the RADIUS server. The access point must be able to reach this IP address.
   - **Port**: Enter the number of the UDP port on the access point that is used to access the RADIUS server. The default port number is 1812.
   - **Password**: Enter the password (shared key) that is used between the access point and the RADIUS server during the authentication or accounting process. By default, the password is sharedsecret.
6. To enable accounting on the authentication servers, click the **Enable Accounting** button so that the button displays blue.
7. In the **Accounting Interval** field, enter an accounting interval.

   An accounting interval indicates the number of seconds between each transmittal of an interim update or live packets for a specific session. In the **Accounting Interval** field, enter a value from 60 seconds (the minimum) to 600 seconds (the maximum).
8. In the **NAS-Identifier** field, enter a network access server identifier (NAS-ID).

   A NAS-ID distinguishes the source of a RADIUS access or accounting request, which enables the RADIUS server to choose a policy for that request. The default NAS-Identifier setting is the Ethernet MAC address of the access point.

9. Configure the following authentication settings, which apply to all RADIUS server that you set up:
   - **Reauthentication time**: Enter the interval in seconds after which the supplicant (the WiFi client) must be reauthenticated with the RADIUS server. You can enter an interval in the range from 0 to 99999. The default interval is 3600 seconds (1 hour). Enter **0** to disable reauthentication.
   - **Update Global Key**: Select the check box to allow the global key update, and enter the interval in seconds. You can enter an interval in the range from 1 to 99999. The check box is selected by default, and the default interval is 1800 seconds (30 minutes). Clear the check box to prevent the global key update.
10. Click the **Apply** button.

    Your settings are saved.
11. To test if the configured RADIUS servers can be reached by the access point, do the following:
    a. Click the **Test RADIUS Settings** tab.

       The page expands.
    b. In the **Username** field, type a user name that must already be defined on the RADIUS server, and in the **Passphrase** field, type the associated passphrase to access the RADIUS server.

       The user name must be between 1 and 128 characters. All special characters are allowed except for space.

       The passphrase must be between 1 and 128 characters. All special characters are allowed.
    c. Click the **Begin Test** button.

       The access point attempts to reach the configured RADIUS servers using the user name and passphrase.

       The results of the test display in the Test RADIUS Result field.

Manage neighbor AP detection

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

If you enable neighbor AP detection for a radio band, the access point regularly scans the WiFi network, collects information about all access points on the channels, and maintains a list of access points it detects in the area. Initially all detected access points are displayed in the Unknown AP List. You can add access points that you are familiar

with to the Known AP List. You can also import a list of known access points in the Known AP List.

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

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

- Enable neighbor access point detection and move access points to the Known AP List
- Import an existing neighbor ACL in the Known AP List

Note: If you enable Energy Efficiency Mode, the access point cannot detect neighbor APs in the 5 GHz radio band. To use neighbor AP detection in the 5 GHz radio band, first disable Energy Efficiency Mode. For more information, see Manage the Energy Efficiency Mode on page 144.

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

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

By default neighbor access point detection is disabled.

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

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **Management > Configuration > Security > Neighbor AP**.

   The page that displays lets you select the radio band (2.4 GHz or 5 GHz).

5. Click the **>** button to the left of the radio band.

   The Neighbor AP page displays for the selected radio band.

6. Select the **Enable Neighbor AP** check box.
7. Click the **Apply** button.

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

8. To view detected neighbor access points and move them from the Unknown AP List to the Known AP List, do the following:
   a. Click the **Unknown AP List** tab.

      The page adjusts to display the unknown access points.

   b. If no access points display, click the **Refresh** button.
   c. Select the check boxes for the access points that you are familiar with and that you trust.
   d. Click the **<< Move to Known AP List** button.
   e. Click the **Known AP List** tab.

      The selected access points display in the Known AP List.

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

9. Click the **Apply** button.

   Your settings are saved.

Import an existing neighbor ACL in the Known AP List

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

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

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

For information about enabling neighbor AP detection, see Enable neighbor access point detection and move access points to the Known AP List on page 91.

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

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

   The Neighbor AP page displays for the selected radio band.
6. To download a sample of an AP list in the format that is required for importing in the Known AP List, click the **Download Sample** link.
7. Import and compose the Known AP List in the following way:
   a. Replace or merge the MAC addresses in the import list with the MAC addresses in the Known AP List by selecting one of the following radio buttons:
      - **Replace**: MAC addresses in the Known AP List are replaced with the ones in the import list.
      - **Merge**: MAC addresses in the Known AP List are merged with the ones in the import list.
   b. Click the **Browse** button and navigate to and select the import file.

The MAC addresses on the import list are placed in the Known AP List.

c. To remove a MAC address from the Known AP List, select the MAC address and click the **Delete** button.

   When you remove a device from the Known AP List, after the access point redetects the device, the device is once again placed in the Known AP List.

8. Click the **Apply** button.

   Your settings are saved.

Manage MAC ACLs for WiFi clients

The access point supports eight local access control lists (ACLs) that let you control which WiFi clients are allowed access and which WiFi clients are denied access. These ACLs are based on MAC addresses, and each local MAC ACL can contain a total number of 512 MAC addresses.

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

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

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

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

An ACL takes effect only after you apply it to a WiFi network. For information about applying an ACL for WiFi clients to a WiFi network, see Select a MAC ACL for WiFi clients in a WiFi network on page 168. You can apply a MAC ACL for WiFi clients to more than one WiFi network.

The following sections describe how you can manage MAC ACLs for WiFi clients:

- Manually set up a MAC ACL for WiFi clients
- Import an existing MAC ACL for WiFi clients

Manually set up a MAC ACL for WiFi clients

You can compose up to eight access control lists (ACLs) that are each based on up to 512 MAC addresses. The access point includes MAC ACLs with the following default group names and settings, which you can change:

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

By default, these MAC ACLs are disabled and do not include any stations. You can manually add devices, import devices (see Import an existing MAC ACL for WiFi clients on page 97), or do both.

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

To manually set up a MAC ACL for WiFi clients:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > Security > MAC ACL**.
5. Click the group name for the MAC ACL that you want to set up.

   The MAC ACL page displays, showing the settings for the selected MAC ACL.

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

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

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

   A group name can have a maximum of 32 characters. You cannot use special characters except for a hyphen (-), underscore (_), and space ( ). The group name must start and end with alphanumeric characters.

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

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

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

8. Compose the ACL in the following way:
   - For an ACL for which you selected the **Allow** radio button in Step 7, do the following:
     - To manually add a device to the Trusted Stations table, enter the MAC address in the format 00-00-00-00-00-00 in the field below the Trusted Stations table, and click the **Add** button.

       The device is added to the Trusted Stations table.
     - To move a device from the Available Stations table to the Trusted Stations table, select the check box for the device and click the **<< Move** button.

       You can search the Available Stations table. You can also filter devices in the Available Stations table by clicking the **filter** icon.
     - To remove a device from the Trusted Stations table, select the check box for the device and click the **Remove** button.

       You can search the Trusted Stations table.

       When you remove a device from the Trusted Stations table, after the access point redetects the device, the device is once again placed in the Available Stations table.
   - For an ACL for which you selected the **Deny** radio button in Step 7, do the following:

- To manually add a device to the Untrusted Stations table, enter the MAC address in the format 00-00-00-00-00-00 in the field below the Untrusted Stations table, and click the **Add** button.

  The device is added to the Untrusted Stations table.
- To move a device from the Available Stations table to the Untrusted Stations table, select the check box for the device and click the **<< Move** button.

  You can search the Available Stations table. You can also filter devices in the Available Stations table by clicking the **filter** icon.
- To remove a device from the Untrusted Stations table, select the check box for the device and click the **Remove** button.

  You can search the Untrusted Stations table.

  When you remove a device from the Untrusted Stations table, after the access point redetects the device, the device is once again placed in the Available Stations table.

9. Click the **Apply** button.

   Your settings are saved.

   For more information about applying an ACL to a WiFi network, see Select a MAC ACL for WiFi clients in a WiFi network on page 168.

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

Import an existing MAC ACL for WiFi clients

You can import an existing access control list (ACL) that is based on up to 512 MAC addresses. You can import the list into any MAC ACL, but the MAC addresses on the list are available only for the MAC ACL into which you import the list. That is, if you want to use the same list in another MAC ACL, you must also import the list into that MAC ACL.

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

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

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

To import an existing MAC ACL for WiFi clients:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > Security > MAC ACL**.
5. Click the group name for the MAC ACL that you want to set up.

   The MAC ACL page displays, showing the settings for the selected MAC ACL.

   Devices in the Available Stations table are automatically detected by the access point and are common to all MAC ACLs, which allows you to add a device to more than one MAC ACL. A neighboring station displays as Neighbor and a connected station displays as connected.
6. To change the group name, enter a new name in the **Group Name** field.

   The default group names for the eight MAC ACLs are Management, Guest, Guest 1, Custom, Custom 1, Custom 2, Custom 3, and Custom 4.
7. Select the ACL Policy **Allow** or **Deny** radio button.

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

   If you select the **Deny** radio button, a WiFi device for which you import the MAC address into the ACL is denied access to the WiFi network, but all other WiFi devices are allowed access to the WiFi network.
8. To download a sample of a MAC ACL in the format that is required for importing, click the **Download Sample** link.
9. Import and compose the ACL in the following way:
   - For an ACL for which you selected the **Allow** radio button in Step 7, do the following:

a. Replace or merge the MAC addresses in the import list with the MAC addresses in the Trusted Stations table (if any are already in the table) by selecting one of the following radio buttons:
   - **Replace**: MAC addresses in the Trusted Stations table are replaced with the ones in the import list.
   - **Merge**: MAC addresses in the Trusted Stations table are merged with the ones in the import list.

b. Click the **Browse** button and navigate to and select the import file.

   The MAC addresses on the import list are placed in the Trusted Stations table.

c. To remove a MAC address from the Trusted Stations table, select the MAC address and click the **Remove** button.

   You can search the Trusted Stations table.

   When you remove a device from the Trusted Stations table, after the access point redetects the device, the device is once again placed in the Available Stations table.

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

  a. Replace or merge the MAC addresses in the import list with the MAC addresses in the Untrusted Stations table (if any are already in the table) by selecting one of the following radio buttons:
     - **Replace**: MAC addresses in the Untrusted Stations table are replaced with the ones in the import list.
     - **Merge**: MAC addresses in the Untrusted Stations table are merged with the ones in the import list.

  b. Click the **Browse** button and navigate to and select the import file.

     The MAC addresses on the import list are placed in the Untrusted Stations table.

  c. To remove a MAC address from the Untrusted Stations table, select the MAC address and click the **Remove** button.

     You can search the Untrusted Stations table.

     When you remove a device from the Untrusted Stations table, after the access point redetects the device, the device is once again placed in the Available Stations table.

10. Click the **Apply** button.

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

For more information about applying an ACL to a WiFi network, see Select a MAC ACL for WiFi clients in a WiFi network on page 168.

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

Enable L2 security

L2 security can prevent attacks via VLAN stacking by blocking VLAN-tagged packets on the WiFi interface. If you enable L2 security, the access point allows only certain types of client traffic, such as ARP, IPv4, and IPv6 traffic, on any WiFi network. L2 security is disabled by default.

To enable L2 security:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > Security > L2 Security**.

   The L2 Security page displays.
5. Select the **Yes** radio button.

   By default the No radio button is selected, and L2 security is disabled.
6. Click the **Apply** button.

   Your settings are saved.

Manage the denial of service protection

A denial of service (DoS) attack is an attempt to make a computer or network resource unavailable to its intended users. DoS protection monitors and filters incoming traffic to prevent flood attacks that could overwhelm system resources. By default, DoS protection is disabled. When you enable DoS prevention, you can configure the following flood attack filtering options:

- **ICMP-Flood Attack Filtering**: Protects the access point network against ICMP flood attacks (ping floods).
- **TCP-SYN-Flood Attack Filtering**: Protects the access point network against TCP SYN flood attacks, which can exhaust connection resources.
- **UDP-Flood Attack Filtering**: Protects the access point network against UDP flood attacks, which can consume excessive bandwidth.

To manage the DoS prevention settings and configure flood attack filtering options:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > Security > DoS Prevention**.

   The DoS Prevention page displays.
5. Select a DoS Prevention radio button:
   - **Enable**: DoS prevention is enabled.
   - **Disable**: DoS prevention is disabled. This is the default setting.
6. Select a DoS Prevention ICMP-Flood Attack Filtering radio button:
   - **Enable**: ICMP-flood attack filtering is enabled.
   - **Disable**: ICMP-flood attack filtering is disabled. This is the default setting.

If you enable this option, in the field to the right, set the ICMP-flood attack packet threshold between 5 and 7200 to drop excess traffic exceeding that limit.

7. Select a DoS Prevention TCP-SYN-Flood Attack Filtering radio button:
   - **Enable**: TCP-SYN-flood attack filtering is enabled.
   - **Disable**: TCP-SYN-flood attack filtering is disabled. This is the default setting.

   If you enable this option, in the field to the right, set the TCP-SYN-flood attack packet threshold between 5 and 7200 to drop excess traffic exceeding that limit.
8. Select a DoS Prevention UDP-Flood Attack Filtering radio button:
   - **Enable**: UDP-flood attack filtering is enabled.
   - **Disable**: UDP-flood attack filtering is disabled. This is the default setting.

   If you enable this option, in the field to the right, set the UDP-flood attack packet threshold between 5 and 7200 to drop excess traffic exceeding that limit.
9. Click the **Apply** button.

   Your settings are saved.

8

Manage the Local Area Network and IP Settings

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

The chapter includes the following sections:

- Disable the DHCP client and specify a fixed IP address
- Enable the DHCP client
- Set the 802.1Q VLAN and management VLAN
- Set an existing domain name
- Enable or disable Spanning Tree Protocol
- Enable or disable the network integrity check function
- Enable or disable IGMP snooping
- Enable or disable Ethernet LLDP
- Enable or disable UPnP
- Manage the multicast DNS gateway

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

Disable the DHCP client and specify a fixed IP address

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

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

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The IPv4 Settings page displays. The fields are masked because the DHCP client is enabled.
5. Select the **Disable** radio button.

   The fields are unmasked.
6. Specify the settings that are described in the following table.

Setting	Description
IP Address	IP address in the range that is used by your LAN. By default, the IP address is 192.168.0.100.
Subnet Mask	The subnet mask must be compatible with your LAN. By default, the network mask is 255.255.255.0.
Gateway	IP address of the gateway on your LAN.

(Continued)

Setting	Description
Primary DNS	IP address of the primary Domain Name System (DNS) server on your LAN.
Secondary DNS	IP address of the secondary DNS server on your LAN, or leave this field blank.

7. Click the **Apply** button.

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

Enable the DHCP client

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

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

To enable the DHCP client:

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

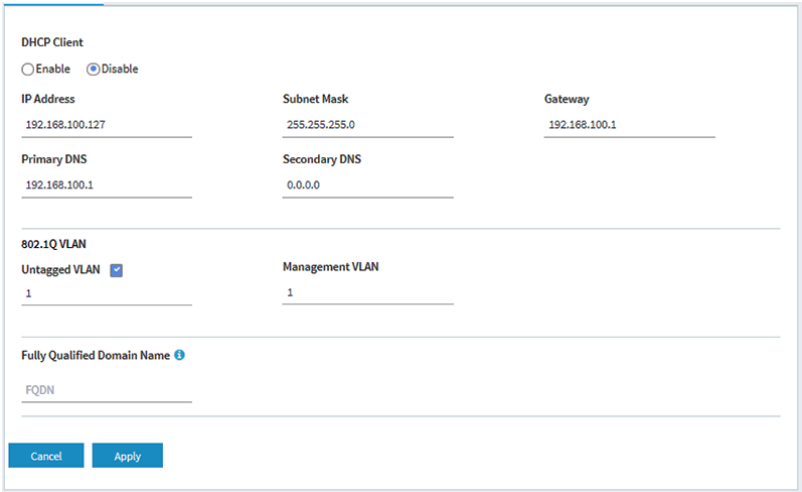
   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

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



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

   The fields are masked.

6. Click the **Apply** button.

   Your settings are saved. The access point restarts with the new IP settings. It might take a while before the access point receives its IP address setting from the DHCP server.

Set the 802.1Q VLAN and management VLAN

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

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

The management VLAN is used for managing traffic such as Telnet, SNMP, HTTP, and HTTPS traffic sent to and from the access point. Frames that belong to the management

VLAN and that are sent over the trunk do not receive an 802.1Q header. If a port is a member of a single VLAN, its traffic can be untagged.

A management VLAN and the following features are mutually exclusive:

- mDNS gateway (see Manage the multicast DNS gateway on page 113)
- NAT mode (see Set NAT mode or Bridge mode for addressing and traffic on page 163)

To set the 802.1Q VLAN and management VLAN:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The IPv4 Settings page displays.
5. To change the 802.1Q VLAN, either clear or select the **Untagged VLAN** check box:
   - **Untagged VLAN**: By default, the **Untagged VLAN** check box is selected. The access point sends untagged frames from its Ethernet interface. Incoming untagged frames are assigned to the untagged VLAN. By default, the untagged VLAN is VLAN 1 but you can enter another VLAN ID in the field if that VLAN ID is supported on your network.
   - **Tagged VLAN**: Clear the **Untagged VLAN** check box only if the hubs and switches on your LAN support the 802.1Q VLAN protocol. The access point tags all frames that it sends from its Ethernet interface. Only the incoming frames that are tagged with known VLAN IDs are accepted. Similarly, change the ID for the untagged VLAN only if the hubs and switches on your LAN support the 802.1Q VLAN protocol and the new VLAN ID is supported on your network.

   A VLAN ID must be in the range from 1 to 4094.
6. To change the VLAN ID for the management VLAN, enter another VLAN ID in the **Management VLAN** field.

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

7. Click the **Apply** button.

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

Set an existing domain name

You can specify an existing fully qualified domain name (FQDN) for the access point so that you can access the access point by using a domain name instead of an IP address.

The FQDN must be a domain name that is registered with a Domain Name System (DNS) provider.
The following are the requirements for the FQDN:

- The maximum length of the FQDN is 255 characters, with a maximum of 63 characters per label, separated by a dot (.) between each label.
- Alphanumeric characters are allowed (a–z and 1–9).
- A space is not allowed.
- A dot (.) and a hyphen (-) are allowed but the name cannot start with either.
- Numbers and special characters are not allowed in the last label of the FQDN.

An example is *myap01-firstfloor-myorganization.com*.

To set an existing FQDN:

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

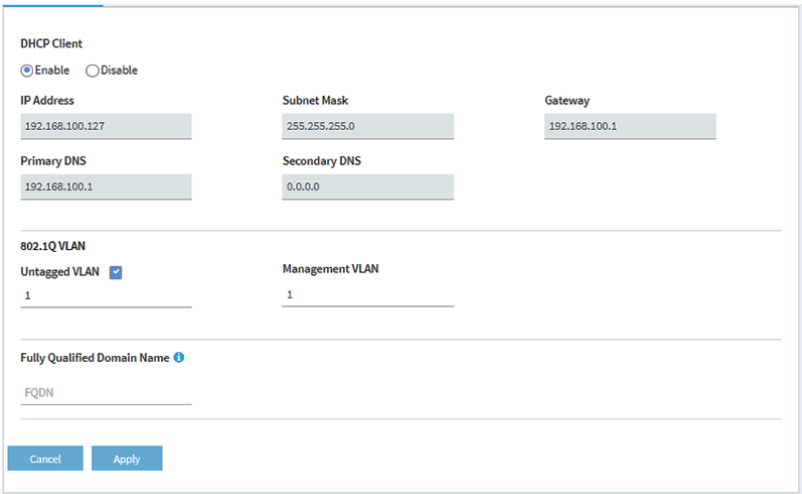
   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

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



5. In the **Fully Qualified Domain Name** field, specify the FQDN.
6. Click the **Apply** button.

   Your settings are saved. The access point attempts to resolve the FDQN to an IP address.

Enable or disable Spanning Tree Protocol

For locations where multiple access points are active and redundant network paths might be present, Spanning Tree Protocol (STP) can prevent network loops. If your location might include redundant network paths, we recommend that you enable STP.

To enable or disable Spanning Tree Protocol:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

The Dashboard displays.

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

   The General page displays.

5. Select a Spanning Tree Protocol radio button:
   - **Enable**: STP is enabled.
   - **Disable**: STP is disabled. This is the default setting.
6. Click the **Apply** button.

   Your settings are saved.

Enable or disable the network integrity check function

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

To enable or disable the network integrity check function:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The General page displays.
5. Select a Network Integrity Check radio button:

- **Enable**: The network integrity check function is enabled.
- **Disable**: The network integrity check function is disabled. This is the default setting.

6. Click the **Apply** button.

   Your settings are saved.

Enable or disable IGMP snooping

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

To enable or disable IGMP snooping:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The General page displays.
5. Select an IGMP Snooping radio button:
   - **Enable**: IGMP snooping is enabled.
   - **Disable**: IGMP snooping is disabled. This is the default setting.
6. Click the **Apply** button.

   Your settings are saved.

Enable or disable Ethernet LLDP

Link Layer Discovery Protocol (LLDP), as specified in IEEE 802.1AB, can provide link-layer messages to adjacent network devices. For example, LLDP lets network devices such as switches and management devices discover the access point in a network.

LLDP can also detect if the access point receives power through PoE. By default, LLDP is enabled.

To enable or disable the LLDP:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > System > Advanced > Ethernet LLDP**.

   The Ethernet LLDP page displays.
5. Select a radio button:
   - **Enable**: LLDP is enabled. This is the default setting.
   - **Disable**: LLDP is disabled.

   Caution: If the access point receives power from a PoE switch and you disable LLDP, power to the access point might be turned off after you click the **Apply** button. In that case, restart the access point.
6. Click the **Apply** button.

   Your settings are saved.

Enable or disable UPnP

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

To enable or disable UPnP:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The UPnP page displays.
5. Select a radio button:
   - **Enable**: UPnP is enabled. This is the default setting.
   - **Disable**: UPnP is disabled.
6. Click the **Apply** button.

   Your settings are saved.

Manage the multicast DNS gateway

The access point can function as a multicast DNS (mDNS) gateway to allow devices and services to be shared across different VLANs and WiFi networks. mDNS works even if inter-VLAN routing is disabled in the network to which the access point is connected.

Shared devices include printers, scanners, storage devices, and other hardware devices. Services include multiple predefined telephone, music, and video streaming services, file sharing services, and other services and applications.

For example, if a group of WiFi clients are on VLAN 20 and a printer is on VLAN 1, an mDNS gateway policy can make the printer available to the WiFi clients. Or, if a meeting

participant wants to use a phone connected to a WiFi network on VLAN 20 to cast a presentation to a large-screen device connected to a WiFi network on VLAN 30, another mDNS gateway policy can make this possible.

A service can run either on a wired or WiFi device, but for a WiFi client to be able to access the service, the WiFi client must be connected to a WiFi network on an access point that has the mDNS gateway feature enabled.

In a network with multiple access points that support the mDNS gateway feature, you can set one access point as the mDNS reflector access point, which re-advertises shared devices and services throughout the network.

An mDNS gateway and the following features are mutually exclusive:

- WPA2 Enterprise security and WPA3 Enterprise security that use a dynamic VLAN (see Set up an open or secure WiFi network on page 36)
- Multi PSK (see Set up Multi PSK for a WiFi network on page 54)
- Management VLAN (see Set the 802.1Q VLAN and management VLAN on page 106)
- NAT mode (see Set NAT mode or Bridge mode for addressing and traffic on page 163)
- Client isolation (see Enable or disable client isolation for a WiFi network on page 164)

Enable the multicast DNS gateway and add a policy

After you enable the multicast DNS (mDNS) gateway and add a policy, the access point can automatically discover devices and services that can be shared. The policy forms a bridge between the following two VLANs:

- **Service VLAN**: The VLAN that includes shared devices or services as members. For example, the type of shared device can be *printer*, in which case the service VLAN is the VLAN of which the printer is a member. Or, the type of shared service can be *Googlecast*, in which case the service VLAN is the VLAN of which the Googlecast device is a member.
- **VLANs on allowed WiFi networks**: The VLAN that includes as members the WiFi devices that must be able to use the shared devices or service on the service VLAN.

You can add up to eight policies. A policy enables access to a shared device or service. A WiFi client can access a shared device or service if the access point to which the client is connected has a policy configured for the shared device of service.

To enable the multicast DNS gateway and add a policy:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > mDNS Gateway**.

   The mDNS Gateway page displays.
5. Select the mDNS Gateway **Enable** radio button.

   By default, the mDNS gateway is disabled and the Disable radio button is selected.
6. If your network includes multiple access points that support the mDNS gateway feature and this access point must function as the mDNS reflector access point in your network, select the **Yes** radio button.

   By default, the No radio button is selected.
7. Click the **Apply** button.

   Your settings are saved. A section with policy information displays.
8. Click the Add Policy **+** button.

   A row is added to the table the with mDNS gateway policies. (You can add multiple rows for multiple policies.)
9. Define the mDNS gateway policy by specifying the following:
   - **Policy Name**: A name that lets you identify the policy. You can use up to 32 alphanumeric and special characters, except for the double quote (“”) and backslash (\) characters.
   - **Shared Services**: From the **Shared Services** menu, select the type of device (for example, printer) or service (for example, Googlecast) that must be shared.
   - **Service VLAN**: In the **Service VLAN** field, enter the VLAN ID that includes as members the type of shared device or service that you select from the **Shared Services** menu.

     The VLAN ID can be in the range from 1 to 4094.

- **Service IP**: Enter the IP address of the shared device or service that you select from the **Shared Services** menu.
- **Allowed Wireless Network**: From the **Allowed Wireless Network** menu, select the WiFi networks with their associated VLANs, which include as members the WiFi devices that must be able to use the type of shared devices or service that you select from the **Shared Services** menu.

10. To add another mDNS policy, click the Add Policy **+** button, and repeat the previous step.
11. Click the **Apply** button.

    Your settings are saved.

Change or remove a multicast DNS policy

You can change or remove a multicast DNS (mDNS) policy.

To change or remove an mDNS policy:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > mDNS Gateway**.

   The mDNS Gateway page displays.
5. To change a policy:
   a. Click the **pencil and notebook** icon to the right of the policy.
   b. Change the settings.

      For more information about the settings, see Enable the multicast DNS gateway and add a policy on page 114.
   c. Click the **Apply** button.

Your settings are saved.

6. To remove a policy:
   a. Click the **trash can** icon to the right of the policy.
   b. Confirm the deletion.

9

Manage and Maintain the Access Point

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

The chapter includes the following sections:

- Change the country or region of operation
- Change the admin user account password
- Change the system name
- Specify a custom NTP server
- Set the time zone
- Manage the syslog settings
- Manage the firmware of the access point
- Manage the configuration file of the access point
- Reboot the access point from the local browser UI
- Schedule the access point to reboot
- Return the access point to its factory default settings
- Enable SNMP and manage the SNMP settings
- Manage the LED
- Manage the Energy Efficiency Mode

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

Change the country or region of operation

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

- In some countries, the access point 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 access point'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 access point 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 or region of operation:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The General page displays the basic system settings.
5. Select a country or region from the **Country / Region** menu.
6. Click the **Apply** button.

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

The pop-up window closes and your settings are saved. The access point restarts with the default WiFi and radio settings that are specific to the selected country or region.

Change the admin user account password

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

The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number.

To change the password for the user name admin:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

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

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

point to factory default settings. Doing so restores the password to the default password.

Change the system name

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

To change the system name:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The General page displays the basic system settings.
5. Enter a new name in the **System Name** field.

   Use the following guidelines:

   - The name must contain alphanumeric characters, can contain hyphens, and cannot be longer than 64 characters.
   - The name cannot start or end with a hyphen.
   - The name must contain at least one alphabetical character.
6. Click the **Apply** button.

   Your settings are saved.

Specify a custom NTP server

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

To specify a custom NTP server:

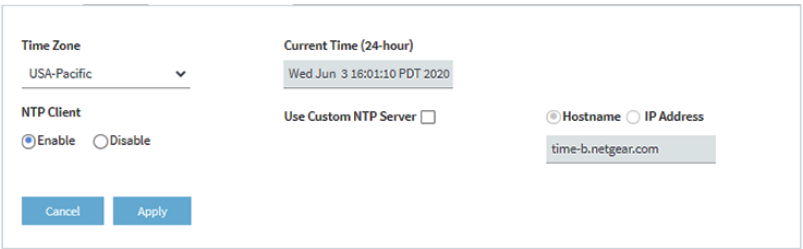
1. Launch a web browser from a computer that is connected to the same network as the access point or directly to the access point through an Ethernet cable or WiFi connection.
2. Enter the IP address that is assigned to the access point.

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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



   By default, the Enable radio button is selected and the access point receives its time from a default NETGEAR NTP server.
5. Select the **Use Custom NTP Server** check box.
6. Take one of the following actions:
   - Enter the host name of the NTP server.

     By default, the Hostname radio button is selected.
   - Select the **IP address** radio button and enter the IP address of the NTP server.
7. Click the **Apply** button.

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

For information about setting the time zone, see Set the time zone on page 123.

Set the time zone

When the access point synchronizes its clock with a Network Time Protocol (NTP) server, the page shows the date and time. If the page does not show the correct date and time, you might need to set the time zone.

To set the time zone:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The page that displays lets you change the time settings.
5. From the **Time Zone** menu, select the time zone for the area in which the access point operates.
6. Click the **Apply** button.

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

   For information about other time settings, see Specify a custom NTP server on page 122.

Manage the syslog settings

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

To manage the syslog settings and enable the syslog function:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Syslog page displays.
5. To enable the syslog server function, select the **Enable Syslog** check box.
6. Specify the IP address and port number for the syslog server:
   - **Syslog Server IP Address**: Enter the IP address of the syslog server on your network.
   - **Port Number**: Enter the port number at which the syslog can be reached. The port number can be in the range from 1 to 65535. By default, the port number is 514.
7. Configure the syslog server severity level by moving the Syslog Level slider.

   This feature enhances log management by filtering messages based on the importance of log data.

   Move the slider to one of the following positions:
   - **Emergency**
   - **Error**
   - **Warning**
   - **Info**
   - **Debug**

   Note: If you select a syslog level, all syslog levels below that level are also included. For example, if you select Warning, Info and Debug log messages are also included.

8. To log information that is collected from devices that are actively seeking network connections on the configured syslog server, select the **Log Probing Clients** check box.

   The log message uses the following format:

   ```
   Probe request-Client:<aa:bb:cc:dd:ee:ff>, SSID: <Name>, BSSID:
   <aa:bb:cc:dd:ff:ee>, RSSI: <-xx dbM>, Radio: <x>, Channel: <y>
   ```

   The fields in a log message mean the following:

   - Probe request-Client: MAC address
   - SSID: Name
   - BSSID: MAC address
   - RSSI: Negative value in dBm
   - Radio: Value in GHz
   - Channel: Value in GHz
9. Click the **Apply** button.

   Your settings are saved.

Manage the firmware of the access point

The access point firmware is stored in flash memory.

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

Depending on how you are connected to the access point, we recommend the following firmware update methods:

- **WiFi connection**: If you are connected over WiFi to the access point, let the access point check the Internet to see if new firmware is available. See Check for new firmware and update the firmware on the access point on page 126.

With this method, if new firmware is available, it is downloaded directly to the access point.

- **LAN connection**: If you are connected over the LAN to the access point, manually update the firmware from a computer or SFTP server. See Manually download firmware and update the access point on page 127 or Use an SFTP server to update the access point on page 130.

  With this mode, if new firmware is available, you must either download it to your computer and then upload it to the access point or upload it from an SFTP server to the access point.

The following sections describe the firmware management methods:

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

Check for new firmware and update the firmware on the access point

Connect the access point to the internet to check for new firmware.

To check for new firmware and update the access point:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The access point detects new firmware if any is available and displays the latest version available.

5. To read the release notes if any are available, click the **Release Notes** link.

   A web page displays the release notes.
6. To download and install the new firmware, click the **Upgrade Now** button, and follow the prompts and dialog boxes.

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

   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 access point. Wait until the access point finishes restarting and the LED remains solid green or solid blue.

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

   The firmware version is displayed on the Dashboard page.
8. Read the new firmware release notes to determine whether you must reconfigure the access point after updating.

Manually download firmware and update the access point

Downloading firmware to a local computer and updating the access point are two separate tasks that are combined in the following procedure. After you update the access point to new firmware, the old firmware is saved as backup firmware so that you can revert to it (see Revert to the backup firmware on page 129).

Caution: When you install an older firmware version (or the backup firmware version), that is, you downgrade rather than update the firmware, the configuration of the access point is reset (cleared) with the exception of the IP address, access point name, and password for the local browser UI. The access point restarts and broadcasts SSID Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address. The MAC address is listed on the product label. The default WiFi passphrase is **sharedsecret**.

To download firmware manually and update the access point:

1. Visit netgear.com/support/download/, locate the support page for your product, and download the new firmware.
2. Read the new firmware release notes to determine whether you must reconfigure the access point after upgrading.

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
5. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

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

   a. Click the **Browse** button.

   b. Navigate to the firmware file.

      The file name ends in `.tar`.

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

   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 access point. Wait until the access point finishes restarting and the LED remains solid green or solid blue.

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

    The firmware version is displayed on the Dashboard page.

Revert to the backup firmware

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

Caution: When you revert to the backup firmware and the backup firmware is an earlier version than the firmware version that is running on the access point, the configuration of the access point is reset (cleared) with the exception of the IP address, access point name, and password for the local browser UI. The access point restarts and broadcasts SSID Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address. The MAC address is listed on the product label. The default WiFi passphrase is **sharedsecret**.

To revert to the backup firmware on the access point:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Firmware Upgrade page displays. The page shows both the current firmware version and the backup firmware version.
5. Click the **Boot up Backup Firmware** button.

   A warning pop-up window displays.

   Caution: When you revert to the backup firmware, the configuration of the access point is reset (cleared) with the exception of the IP address, access point name, and password for the local browser UI. The access point restarts and broadcasts SSID Netgearxxxxxx, in which xxxxxx represents the last six hexadecimal digits of the access point's MAC address. The MAC address is listed on the product label. The default WiFi passphrase is **sharedsecret**.
6. Click the **Swap** button.

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

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

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

   The firmware version is displayed on the Dashboard page.

Use an SFTP server to update the access point

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

To update the firmware of the access point from an SFTP server:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Firmware Upgrade page displays.
5. From the **Upgrade Options** menu, select **SFTP**.
6. Specify the following server settings:
   - **Firmware File**: The name of the access point firmware file on the SFTP server.
   - **SFTP Server IP**: The IP address of the SFTP server on your network.

- **User Name**: The user name that is required to access the SFTP server.
- **Password**: The password that is required to access the SFTP server.

7. Click the **Upgrade** button.

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

   The firmware update process takes several minutes. When the update is complete, the access point restarts.

8. Verify that the access point runs the new firmware version by logging back in to the access point.

   The firmware version is displayed on the Dashboard page.

Manage the configuration file of the access point

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

Back up the access point configuration

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

Note: The backup file is saved in a binary format so that it is protected and cannot be opened by a regular application.

To back up the access point's configuration settings:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Backup Settings page displays.
5. Click the **Backup** button.

   A pop-up window displays.
6. Enter a password to protect the backup file, and click the **Continue** button.

   You can either use your existing password (the one that you use to log in to the access point) or enter a unique password.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number.

   Note: We recommend that you save the password because you must enter it again if you restore the configuration from the backup file.
7. Choose a location to store the file on your computer.

   The name of the backup file can be `WAX6XX-NETGEARYYYYYY-dd-mm-yy_hh-mm-ss-config.tar` or `WAX6XX-WAX6XX-YYYYYY-dd-mm-yy_hh-mm-ss-config.tar`.

   6XX represents the model number, YYYYYY represents the last six hexadecimal digits of the access point's MAC address (or the system name), dd is the date, mm is the month, yy is the year, hh is the hour (in 24-hour format), mm is the minutes, and ss is the seconds.

   Examples of the name of a backup file are `WAX6XX-NETGEAR1A2B3C-06-18-21_16-44-12-config.tar` and `WAX6XX-WAX6XX-1A2B3C-06-18-21_16-44-12-config.tar`.
8. Follow the directions of your browser to save the file.

Restore the access point configuration

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

To restore configuration settings that you backed up:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Restore Settings page displays.
5. Click the **Browse** button and navigate to and select the saved configuration file.

   The name of the backup file can be `WAX6XX-NETGEARYYYYYY-dd-mm-yy_hh-mm-ss-config.tar` or `WAX6XX-WAX6XX-YYYYYY-dd-mm-yy_hh-mm-ss-config.tar`.

   6XX represents the model number, YYYYYY represents the last six hexadecimal digits of the access point's MAC address (or the system name), dd is the date, mm is the month, yy is the year, hh is the hour (in 24-hour format), mm is the minutes, and ss is the seconds.

   Examples of the name of a backup file are `WAX6XX-NETGEAR1A2B3C-06-18-21_16-44-12-config.tar` and `WAX6XX-WAX6XX-1A2B3C-06-18-21_16-44-12-config.tar`.
6. Click the **Restore** button.

   A pop-up window displays.
7. Enter the password that you specified when you saved the backup file, and click the **Continue** button.
8. Click the **Restore** button.

   The pop-up window closes and the configuration is uploaded to the access point. When the restoration is complete, the access point reboots. This process takes about two minutes.

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

Reboot the access point from the local browser UI

If you cannot physically access the access point to reboot it (that is, disconnect the power and reconnect the power), you can use the local browser UI to reboot the access point.

To reboot the access point:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Maintenance > Reset > Reboot AP**.

   The Reboot AP page displays.
5. Click the **Reboot AP** button.

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

   The pop-up window closes and the access point reboots, which takes about one minute.

Schedule the access point to reboot

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

To schedule the access point to reboot:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Maintenance > Reset > Reboot AP**.

   The Reboot AP page displays.
5. Click the **Enable Scheduled Reboot** button so that the button displays blue.

   The scheduling controls display.
6. Select the check box for the day on which you want the access point to reboot.

   You can select multiple days.
7. Using the **Start Time** menus, specify the hour and minutes for the time at which the access point must reboot.

   Specify the hour in 24-hour format.
8. Click the **Apply** button.

   Your settings are saved.

Return the access point to its factory default settings

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

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

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

After you reset the access point to factory default settings, the password for the admin user name is **password**, the access point's DHCP client is enabled, the setup SSID is shown in the format NETGEARxxxxxx-SETUP, and the default password for WiFi access is **sharedsecret**. If the access point does not receive an IP address from a DHCP server, the LAN IP address is set to 192.168.0.100.

For an extensive list of factory default settings, see Factory default settings on page 206.

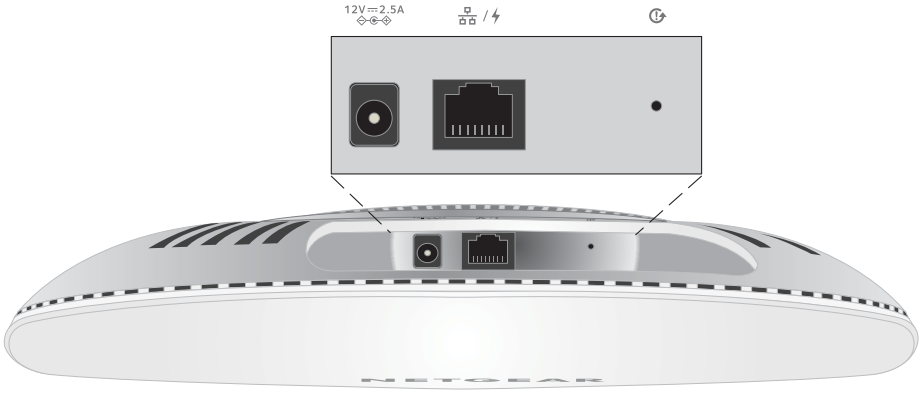
Use the Reset button to reset the access point

You can use the **Reset** button to return the access point to its factory default settings.

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

To reset the access point to factory default settings:

1. On the bottom panel of the access point, locate the recessed **Reset** button.



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

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

3. Release the **Reset** button.

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

   Warning: To avoid the risk of corrupting the firmware, do not interrupt the reset. Do not turn off the access point. Wait until the access point finishes restarting and the LED turns solid green or solid blue.

Use the local browser UI to reset the access point

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

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

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

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

   A login window displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Management > Maintenance > Reset > Restore Defaults**.

   The Restore Defaults page displays.

5. Click the **Restore Defaults** button.

   A warning pop-up window displays.

6. Click the **Restore** button.

   The pop-up windows closes and the configuration is reset to factory default settings. When the reset is complete, the access point reboots. This process takes about two minutes.

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

Enable SNMP and manage the SNMP settings

You can access the access point over a Simple Network Management Protocol (SNMP) connection, which allows SNMP network management software such as HP OpenView to manage the access point by using the SNMP v1/v2c or SNMPv3 protocol. By default, SNMP is disabled.

To enable SNMP and manage the SNMP settings:

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

   A login window displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Management > Maintenance > Remote Management**.

   The Remote Management page displays.

5. Select the SNMP **Enable** toggle.

   By default, SNMP is disabled.

   You can now configure the SNMPv1/v2c and SNMPv3 settings.

Configure the SNMPv1/v2c settings

You can configure the Simple Network Management Protocol (SNMP) v1/v2c setting after you enable SNMP on the access point. By default, SNMP is disabled.

To enable SNMP and manage the SNMPv1/v2c settings:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Maintenance > Remote Management**.

   The Remote Management page displays.
5. Select the SNMP **Enable** toggle.

   By default, SNMP is disabled.
6. Select the SNMP v1/v2c **Enable** toggle.
7. In the SNMP v1/v2c section, specify the following settings:
   - **Read-Only Community Name**: The community string that allows the SNMP manager to read the access point's MIB objects. The default name is snmpv1v2cuser.
   - **Trap Community Name**: The community name that is associated with the IP address that must receive traps. By default, the toggle to use the community name as the trap is selected. To create a different trap name, deselect the **Use the same name as Trap** toggle. The default trap name adjusts to trapuser.

   Note: For the read-only community name and the trap community name each, the name can be a maximum of 30 alphanumeric and special characters, except for the double quote (") and backslash (\) characters.
8. In the SNMP Trap section, specify the following settings:

- **IP Address (to receive traps)**: The IP address of the SNMP manager that must receive traps.
- **Trap Port**: The port number at which the SNMP manager must receive traps. The default is 162. The only other option is port number 161.

9. Click the **Apply** button.

   Your settings are saved.

Configure the SNMPv3 settings

You can configure the Simple Network Management Protocol (SNMP) v3 setting after you enable SNMP on the access point. By default, SNMP is disabled.

To enable SNMP and manage the SNMPv3 settings:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Maintenance > Remote Management**.

   The Remote Management page displays.
5. Select the SNMP **Enable** toggle.

   By default, SNMP is disabled.
6. Select the SNMP v3 **Enable** toggle.
7. In the SNMP v3 section, specify the following settings:
   a. In the **User Name** field, enter a user name for SNMPv3. The default is snmpv3user.
   b. In the **Auth Passphrase** field, enter a passphrase. The password must be 8 to 63 characters in length and must be a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\). The default passphrase is snmp1234.

c. In the **Priv Passphrase** field, enter a passphrase. The password must be 8 to 63 characters in length and must be a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\). The default passphrase is snmp1234.

d. Select a security level from the **Security Level** menu:

- **noAuthNoPriv**: No authentication, no privacy security level. You cannot edit the Auth Protocol, Auth Passphrase, Priv Protocol, or Priv Passphrase fields in this mode.
- **authNoPriv**: Authentication only security level. You can edit the Auth Protocol, Auth Passphrase, fields but you cannot edit Priv Protocol, or Priv Passphrase fields in this mode.
- **authPriv**: Authentication and privacy security level. You can edit all fields.

e. Select the authentication protocol from the **Auth Protocol** menu:

- **MD5**: Message Digest 5 (MD5) is the authentication protocol.
- **SHA**: Secure Hash Algorithm (SHA) is the authentication protocol. SHA provides stronger security than MD5.

f. Select the priviledge protocol from the **Priv Protocol** menu:

- **DES**: SNMPv3 are encrypted using the DES encryption protocol.
- **AES**: SNMPv3 packets are encrypted using the AES protocol, which provides stronger security than DES.

8. Optional: By default, the toggle to use the SNMPv3 name as the trap is selected. To create a different trap name, deselect the **Use the same name as Trap** toggle. The default trap name adjusts to snmptrap. Specify the following settings:

a. In the **User Name** field, enter a user name for SNMPv3. The default is snmptrap.

b. In the **Auth Passphrase** field, enter a passphrase. The password must be 8 to 63 characters in length and must be a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\). The default passphrase is snmp1234.

c. In the **Priv Passphrase** field, enter a passphrase. The password must be 8 to 63 characters in length and must be a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\). The default passphrase is snmp1234.

d. Select a security level from the **Security Level** menu:

- **noAuthNoPriv**: No authentication, no privacy security level. You cannot edit the Auth Protocol, Auth Passphrase, Priv Protocol, or Priv Passphrase fields in this mode.
- **authNoPriv**: Authentication only security level. You can edit the Auth Protocol, Auth Passphrase, fields but you cannot edit Priv Protocol, or Priv Passphrase fields in this mode.
- **authPriv**: Authentication and privacy security level. You can edit all fields.

e. Select the authentication protocol from the **Auth Protocol** menu:
   - **MD5**: Message Digest 5 (MD5) is the authentication protocol.
   - **SHA**: Secure Hash Algorithm (SHA) is the authentication protocol. SHA provides stronger security than MD5.

f. Select the priviledge protocol from the **Priv Protocol** menu:
   - **DES**: SNMPv3 are encrypted using the DES encryption protocol.
   - **AES**: SNMPv3 packets are encrypted using the AES protocol, which provides stronger security than DES.

9. In the SNMP Trap section, specify the following settings:
   - **IP Address (to receive traps)**: The IP address of the SNMP manager that must receive traps.
   - **Trap Port**: The port number at which the SNMP manager must receive traps. The default is 162. The only other option is port number 161.
10. Click the **Apply** button.

    Your settings are saved.

Manage the LED

By default, the single LED is enabled and functions as described in Top panel LED on page 12. You can manage whether the LED lights at all. This function is useful if you want the access point to function in a dark environment.

To enable or disable the LED:

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

   A login window displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Management > Configuration > System > Advanced > LED Control**.

   The LED Control page displays.

5. Select or clear one of the following radio buttons:
   - **Enable the LED**: The LED is enabled. This is the default setting.
   - **Disable the LED**: The LED is disabled.
   - **Enable the LED for power and cloud functions**: The LED is enabled for power and cloud functions only.
6. Click the **Apply** button.

   Your settings are saved.

Manage the Energy Efficiency Mode

If no WiFi clients are connected to the access point, the access point can automatically enter Energy Efficiency Mode (EEM) to reduce power consumption and save energy. When one or more WiFi clients connect, the access point automatically leaves the EEM to resume normal operation.

If EEM is enabled and no WiFi clients are connected to the access point, antenna stream operation is limited to 1x1. (Under normal circumstances, the access point can support multiple antenna streams.) If a WiFi client initiates a connection to the access point, the antenna streams resume normal operation.

Note the following restrictions:

- **Wireless distribution system**: EEM is mutually exclusive with a wireless distribution system (WDS, see Set up a WiFi Bridge on page 177).
- **Neighbor AP detection**: EEM does not let the 5 GHz radio detect neighbor APs (see Manage neighbor AP detection on page 90).
- **DFS channels**: When WiFi clients connect to the access point and the access point resumes normal operation, 5 GHz radio transmissions can be temporarily suspended if the access point operates in a DFS channel (about 1 minute suspension for a DFS channel; about 10 minutes suspension for a weather DFS channel).

Note: If use you EEM, we recommend that you enable band steering in your WiFi networks. Band steering lets 5-GHz-capable WiFi clients that are connected to the 2.4 GHz band to be steered to the 5 GHz band for improved performance. For more information, see Enable or disable band steering with 802.11k RRM and 802.11v WiFi network management on page 58.

To enable or disable the Energy Efficiency Mode:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > System > Advanced > Energy Efficiency Mode**.

   The Energy Efficiency Mode page displays.
5. Select a radio button:
   - **Enable**: Energy Efficiency Mode is enabled.
   - **Disable**: Energy Efficiency Mode is disabled. This is the default setting.
6. Click the **Apply** button.

   Your settings are saved.

10

Monitor the Access Point and the Network

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

The chapter includes the following sections:

- Display the access point Internet, IP, and system settings
- Display the WiFi radio settings
- Display unknown and known neighbor access points
- Display client distribution, connected clients, and client trends
- Display traffic volume, statistics, and channel utilization
- Display or download tracked URLs
- Display, save, download, or clear the logs
- Display a WiFi bridge connection
- Display alarms and notifications

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

Display the access point Internet, IP, and system settings

To display the access point, Internet, IP, and system settings:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Locate the Connection Status Information pane, System Information pane, and IP Settings Information pane, which are shown, respectively, on the left, upper center, and lower center of the Dashboard.

   If the page width on your device is narrow, these panes might be located elsewhere on the Dashboard.

   For information about the radio settings, see Display the WiFi radio settings on page 149.

   - **Connection Status Information pane**: This pane is in the top, left corner of the Dashboard (if the page width on your device is sufficient; otherwise, it might be elsewhere) and displays the following:
     - Status of the Internet connection.
     - Functioning mode of the access point, which is always Access Point.
     - Number of clients connected to the access point.
   - **System Information pane**: This pane is in the center at the top of the Dashboard (if the page width on your device is sufficient; otherwise, it might be elsewhere) and displays the following:
     - System name of the access point and country or region of operation.
     - Ethernet MAC address.
     - The serial number.

- Device uptime.
- Firmware version.
- The date and time that the access point itself or someone manually last checked if new firmware was available.

This pane also contains a button that you can click to check for firmware updates for the access point. If an update is available, the **Update Available** button displays. (For more information about firmware updates, see Check for new firmware and update the firmware on the access point on page 126).

- **IP Settings Information pane**: This pane is in the center of the Dashboard page (if the page width on your device is sufficient; otherwise, it might be elsewhere) and displays the following:
  - IP address of the access point and its DHCP status.
  - Gateway IP address.
  - Gateway status.
  - Wired traffic volume.

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

   The page shows four sections:

   - **System Information section**: The following settings are displayed:
     - **System Name**: The access point NetBIOS name.
     - **System Mode**: The access point system mode (AP).
     - **LAN MAC Address**: The MAC address of the LAN Ethernet port of the access point.
     - **Wireless MAC Address for 2.4 GHz**: The MAC address of 2.4 GHz WiFi interface (radio) of the access point.
     - **Wireless MAC Address for 5 GHz**: The MAC address of 5 GHz WiFi interface (radio) of the access point.
     - **Ethernet LLDP**: The status of Ethernet LLDP feature (Enabled or Disabled).
     - **LLDP Neighbor**: The neighbor that LLDP detected.
     - **Country / Region**: The country or region in which the access point operates or for which the access point is licensed.
     - **Current Firmware Version**: The version of the firmware that is running on the access point.
     - **Backup Firmware Version**: The version of the backup firmware on the access point.
     - **Bootloader Version**: The primary bootloader (U-Boot) version that is installed on the access point.

  - **Serial Number**: The serial number of the access point.
  - **Current Time**: The current system time of the access point.
  - **Uptime**: The time since the access point was last restarted.
- **AP Interface Status**: A green icon indicates that the interface is in use. A gray icon indicates that the interface is not in use.
- **IPv4 Settings section**: The following settings are displayed:
  - **IPv4 Address**: The IPv4 address of the access point.
  - **Subnet Mask**: The subnet mask of the access point.
  - **Default Gateway**: The default gateway for the access point.
  - **DHCP Client**: The status of DHCP client (Enabled or Disabled).
- **Wireless Settings section**: The following settings are displayed, with separate columns for the radios:
  - **Antenna**: The type of antenna (by default, 2x2).
  - **Wireless Mode**: The operating WiFi mode of the radio.
  - **Channel / Frequency**: The channel and frequency that are used by the radio.
  - **Tx Power (in dBm)**: The transmit power in dBm.

Display the WiFi radio settings

To display the WiFi radio settings of the access point:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Locate the Radio Information pane on the Dashboard page.

If the page width on your device is sufficient, it is at the top, right corner of the Dashboard page; otherwise, it might be elsewhere.

The following settings are displayed:

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

5. To view information about the other radio, click either the **2.4 GHz** or **5 GHz** tab.

   The pane adjusts.

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

   The page shows four sections:

   - **System Information section**: The following settings are displayed:
     - **System Name**: The access point NetBIOS name.
     - **System Mode**: The access point system mode (AP).
     - **LAN MAC Address**: The MAC address of the LAN Ethernet port of the access point.
     - **Wireless MAC Address for 2.4 GHz**: The MAC address of 2.4 GHz WiFi interface (radio) of the access point.
     - **Wireless MAC Address for 5 GHz**: The MAC address of 5 GHz WiFi interface (radio) of the access point.
     - **Ethernet LLDP**: The status of Ethernet LLDP feature (Enabled or Disabled).
     - **LLDP Neighbor**: The neighbor that LLDP detected.
     - **Country / Region**: The country or region in which the access point operates or for which the access point is licensed.
     - **Current Firmware Version**: The version of the firmware that is running on the access point.
     - **Backup Firmware Version**: The version of the backup firmware on the access point.
     - **Bootloader Version**: The primary bootloader (U-Boot) version that is installed on the access point.

  - **Serial Number**: The serial number of the access point.
  - **Current Time**: The current system time of the access point.
  - **Uptime**: The time since the access point was last restarted.
- **AP Interface Status**: A green icon indicates that the interface is in use. A gray icon indicates that the interface is not in use.
- **IPv4 Settings section**: The following settings are displayed:
  - **IPv4 Address**: The IPv4 address of the access point.
  - **Subnet Mask**: The subnet mask of the access point.
  - **Default Gateway**: The default gateway for the access point.
  - **DHCP Client**: The status of DHCP client (Enabled or Disabled).
- **Wireless Settings section**: The following settings are displayed, with separate columns for the 2.4 GHz and 5 GHz radios:
  - **Antenna**: The type of antenna (by default, 2x2).
  - **Wireless Mode**: The operating WiFi mode of the radio.
  - **Channel / Frequency**: The channel and frequency that are used by the radio.
  - **Tx Power (in dBm)**: The transmit power in dBm.

Display unknown and known neighbor access points

If you enabled neighbor access point (AP) detection (see Manage neighbor AP detection on page 90), you can display the unknown access points in the Unknown AP list and the known access points in the Known AP list.

To display the detected neighbor access points:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

The Dashboard displays.

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

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

   For information about moving unknown access points to the Known AP list, see Enable neighbor access point detection and move access points to the Known AP List on page 91.

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

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

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

Display client distribution, connected clients, and client trends

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

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

4. Locate the Client Distribution pane and the Recent Clients pane.

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

The Recent Clients pane shows the top 5 recently connected clients list.

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

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

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

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

7. To display information about a connected client, click its device name.

   The page displays the MAC address, device type, IP address, and SSID for the client. You can also view more information, including very detailed information (see Step 11 and Step 12).

8. To display trends about clients, scroll down to the Hours Trend pane (usually at the bottom of the page).

   The Hours Trend pane shows a graph with the number of clients, the traffic in MBps, or the channel utilization over a period that you can select. By default, the client information is selected (that is, the **Client** button is selected) and the graph shows the total number of clients for both radios and the number of clients for each radio (2.4 GHz and 5 GHz).

   You can also click the **Traffic** button or the **Channel Utilization** button. For more information, see Display traffic volume, statistics, and channel utilization on page 155.

9. To display more information, point to a node on one of the lines on the graph.

10. To change the period over which information is filtered and displayed, select the number of recent hours from the menu to the right of the buttons.

11. To display more information about currently connected clients, select **Management > Monitoring > Connected Clients**.

    The Connected Clients page displays.

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

    For each radio and each WiFi client, the page displays the SSID, MAC address, IP address, host name, operating system (OS), WiFi mode, VLAN ID, and user name or key identifier (for a Multi PSK configuration).

12. To display very detailed information about a WiFi client, click the information (I) icon to the left of the client.

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

    - **MAC Address**: The MAC address of the client.
    - **IP Address**: The IP address associated with the client.
    - **Host Name**: The host name of the client.
    - **OS**: The operating system that runs on the client.
    - **BSSID**: The BSSID that the client connects to.
    - **SSID**: The SSID of the radio that the client connects to.
    - **Channel**: The channel that the client connects to.
    - **Channel Width**: The width of the channel that the client connects to.
    - **Tx Rate**: The rate of traffic transmission of the client.
    - **Rx Rate**: The rate of traffic reception of the client.
    - **RSSI**: The RSSI threshold value of the client.
    - **Tx Bytes**: The number of bytes that the client transmitted.
    - **Rx Bytes**: The number of bytes that the client received.
    - **Tx Unicast Packets/Bytes**: The number of unicast packets and bytes transmitted by the client.
    - **Rx Unicast Packets/Bytes**: The number of unicast packets and bytes received by the client.
    - **Tx Broadcast Packets/Bytes**: The number of broadcast packets and bytes transmitted by the client.
    - **Tx Multicast Packets/Bytes**: The number of multicast packets and bytes transmitted.
    - **Tx Errors/Retries**: The number of transmission errors or retry attempts made due to failed transmissions.
    - **Rx Errors/Retries**: The number of reception errors or retries due to packet loss or corruption.
    - **State**: The QoS state of the connection.
    - **Type**: The type of WiFi security that is used for the connection.
    - **Device Type**: The type of device that the client is.
    - **Mode**: The WiFi mode of the connection.
    - **Status**: The security status of the connection.
    - **Idle Time**: The time that the client remained idle.

- **Assoc Time Stamp**: The time that is associated with the information on the Detailed Client Information page.
- **VLAN ID**: The VLAN in which the client is placed.
- **User Name / Key Identifier**: The user name or key identifier (for a Multi PSK configuration) of the client.
- **PMF Support**: If PMF is enabled on the access point, indicates if the client supports PMF.

13. If you opened the Detailed Client Information page, click the **Close** button.

    The Detailed Client Information page closes.
14. To view the Connected Clients statistics in graphical format, click the graph icon on the right of the client.
    The Client Statistics page displays with the following two tabs:
    - **Tx/Rx Statistics**: You can view the Unicast, Broadcast and Multicast statistics separately. You can choose different time periods to view historical data.
      - Click the **All** button to view Tx and Rx traffic for Unicast, Broadcast and Multicast statistics all together.
      - Click the **Cumulative Tx/Rx** button to view total Tx and Rx packets (the sum of the Unicast, Broadcast and Multicast packets).
    - **Channel Utilization**: You can view the channel utilization percentage for each client. You can choose different time periods to view historical data.
15. To refresh the information on the Tx/Rx Statistics or Channel Utilization graph, click the **Refresh** button.
16. To reset the Client Statistics data, click the **Reset Stats** button.

Display traffic volume, statistics, and channel utilization

To display traffic volume, fan information, statistics, and channel utilization:

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

   A login window displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

4. Scroll down to the Hours Trend pane at the bottom of the Dashboard page.

   By default, the **Clients** button is selected. For more information, see Display client distribution, connected clients, and client trends on page 152.

5. To display traffic information, do the following:

   a. Click the **Traffic** button.

      The graph shows the information for Ethernet (wired LAN) traffic, total WiFi traffic, WiFi traffic for the 2.4 GHz radio, and WiFi traffic for the 5 GHz radio.

   b. To view more information, point to a node on one of the lines on the graph.

6. To display channel utilization, do the following:

   a. Click the **Channel Utilization** button.

      The graph shows the channel utilization for the 2.4 GHz radio.

      The graph displays the utilization percentages for three categories:

      - Total Channel Utilization: The overall utilization of the channel.
      - Self Channel Utilization: The utilization percentage of the current access point.
      - OBSS (Overlapping Basic Service Set) Channel Utilization: The utilization percentage of overlapping networks in the same operating channel.

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

7. To change the period over which information is filtered and displayed, select the number of recent hours from the menu to the right of the buttons.

8. To display traffic statistics, select **Management > Monitoring > Statistics**.

   The Statistics page displays.

   The Statistics page provides detailed insights into the traffic data of the access point since the access point started or rebooted:

   - **AP Statistics**: This tab displays the overall access point traffic
   - **Radio Statistics**: This tab displays the traffic for each WiFi radio. Select **2.4 GHz** or **5 GHz** from the menu to show the traffic statistics of that WiFi radio.
   - **SSID Statistics**: This tab displays the traffic statistics of a SSID. Select the SSID name from the menu to display the traffic statistics of that SSID.

- **WDS Statistics**: This tab displays the Wireless Distribution System (WDS) related traffic. Select the WDS interface name from the menu to show the traffic statistics of that WDS interface.
- **ARP Statistics**: This tab displays the Address Resolution Protocol (ARP) traffic statistics, including the number of proxied and dropped packets, if the ARP proxy is enabled. For more information, see Manage the ARP proxy on page 191.
- **Ethernet Statistics**: This tab displays the Ethernet interface traffic.

The traffic statistics display in the following formats:

- **Tabular representation**: You can view various traffic statistics in table format.
- **Graphical Representation**: You can view the access point, radio, and SSID statistics in graphical format.
  - You can view the unicast, broadcast and multicast statistics separately.
  - Click the **All Traffic** button to view Tx and Rx traffic for Unicast, Broadcast and Multicast statistics all together.
  - Click the **Cumulative Tx/Rx** button to view total Tx and Rx packets (the sum of the unicast, broadcast and multicast packets).
  - You can choose different time periods to view historical data.

9. To refresh the information on the Statistics page, click the **Refresh** button.
10. To reset the information on the Statistic page, click the **Reset Stats** button.

Display or download tracked URLs

If you enabled URL tracking for a WiFi network (see Enable or disable URL tracking for a WiFi network on page 166), you can display the tracked URLs by URL, WiFi client, and SSID. You can also download a URL tracking report as a `.csv` file.

To view or download tracked URLs:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **Management > Monitoring > URL Tracking**.

   The URL Tracking page displays.

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

5. To display additional information, click the **...** link to the right of a MAC address or SSID.
6. To display URL tracking information by WiFi client, do the following:
   a. From the **List by** menu, select **Client**.

      The table shows the MAC addresses of the WiFi clients, each with the client host name, and the first URL of the list of URLs that the client accessed.

   b. To display all URLs that a WiFi client accessed, click the **...** link to the right of the first URL.

      A pop-up window displays all URLs that the WiFi client accessed.

   c. Click the **Close** button.

      The pop-up window closes.

7. To display URL tracking information by SSID, do the following:
   a. From the **List by** menu, select **SSID**.

      The table shows the SSIDs and the first URL of the list of URLs that were accessed on the SSID.

   b. To display all URLs that were accessed on the SSID, click the **...** link to the right of the first URL.

      A pop-up window displays all URLs that the were accessed on the SSID.

   c. Click the **Close** button.

      The pop-up window closes.

8. To download a URL tracking report as a `.csv` file, click the **Download** button, and follow the directions of your browser.
9. To display the most recent information, click the **Refresh** button.
10. To clear all URL tracking information, do the following:
    a. Click the **Clear** button.

       A warning pop-up window displays.

    b. Click the **OK** button.

The pop-up window closes and the information is cleared.

Display, save, download, or clear the logs

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

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

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Monitoring > Logs**.

   The Logs page displays, showing all recent events with a date and time stamp.
5. To save the logs, do the following:
   a. Click the **Save** button.
   b. Follow the directions of your browser to save the file to your computer.
6. To download the detailed log entries, do the following:
   a. Click the **Download Detailed Logs** button.

      Depending on the size of the file, downloading the detailed log entries might take several minutes.
   b. Follow the directions of your browser to save the file to your computer.
7. To refresh the log entries onscreen, click the **Refresh** button.

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

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

Display a WiFi bridge connection

You can configure a wireless distribution system (WDS) that consists of point-to-point WiFi bridge connections between two access points (see Set up a WiFi Bridge on page 177).

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

To display a WiFi bridge connection:

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

   A login window displays.

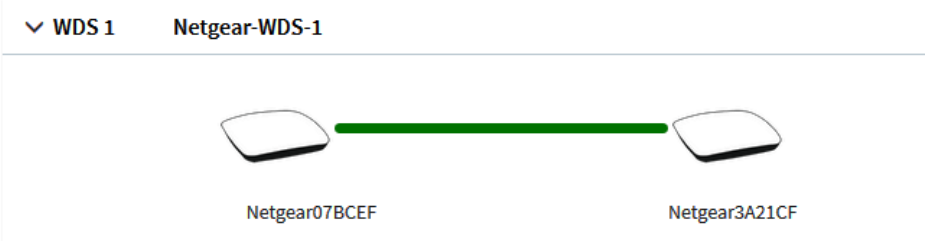
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Monitoring > Wireless Bridge**.

   The page that displays lets you select a WDS profile (WDS 1, WDS 2, WDS 3, or WDS 4).

5. Click the **>** button to the left of a WDS profile.



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

Display alarms and notifications

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

To display the alarms and notifications:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Locate the alarm bell icon at the top-right of the page.

   The icon shows a number, indicating the total number of new alarms and notifications since the last time that you viewed alarms and notifications.
5. Click the alarm bell icon.

   The pop-up window shows the alarms (indicated by a red bell) and notifications (indicated by a blue bell) with a description and time.
6. To view more alarms and notification, scroll down in the pop-up window.

11

Manage the Advanced WiFi Features for a WiFi network

This chapter describes how you can manage the advanced WiFi features for a WiFi network.

For information about the basic WiFi features for a WiFi network, see Manage the Basic WiFi Features for a WiFi network on page 35.

The chapter includes the following sections:

- Set NAT mode or Bridge mode for addressing and traffic
- Enable or disable client isolation for a WiFi network
- Enable or disable URL tracking for a WiFi network
- Change the format of the DHCP offer messages in a WiFi network
- Select a MAC ACL for WiFi clients in a WiFi network
- Set bandwidth rate limits for a WiFi network
- Configure advanced rate selection for a WiFi network
- Assign host names to WiFi clients and manage the host name list

Note: If you want to change the settings of a WiFi network on the access point, then use a wired connection to avoid being disconnected when the new WiFi settings take effect.

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

Set NAT mode or Bridge mode for addressing and traffic

By default, the addressing and traffic mode of the access point is Bridge mode, which means that WiFi clients receive IP addresses from a DHCP server (or a router that functions as a DHCP server) in your network. This is usually the same DHCP server that assigns an IP address to the access point itself.

You can also set NAT mode, which enables the access point's DHCP server for WiFi clients. The access point's DHCP server assigns an IP address in a different range from the IP address of the access point itself.

NAT mode and the following features are mutually exclusive:

- Dynamic VLAN (see Set up an open or secure WiFi network on page 36)
- Multi PSK (see Set up Multi PSK for a WiFi network on page 54)
- Management VLAN other than the default VLAN 1 (see Set the 802.1Q VLAN and management VLAN on page 106)
- mDNS gateway (see Manage the multicast DNS gateway on page 113)

To set NAT mode or Bridge mode for addressing and traffic:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

   The settings for the selected SSID display.
6. Scroll down and click the **> Advanced** tab.

The page expands.

7. From the **Addressing and Traffic** menu, select the addressing and traffic mode:

   Note: This option is not supported in India.

   - **Bridge**: The WiFi clients receive their IP addresses from the DHCP server in the same network as the access point. This is the default mode.
   - **NAT**: WiFi clients receive their IP addresses from a private DHCP address pool on the access point. If you select this mode, by default, the WLAN network address is 172.31.4.0 and the default subnet mask is 255.255.252.0. This means that WiFi clients are assigned an IP address in the range from 172.31.4.2 to 172.31.7.254. The IP address of the default DNS server for the WLAN is 8.8.8.8, and the default lease time is 1440 minutes (24 hours).

     To change the default range for the DHCP address pool, the default DNS server, the lease time, or all NAT settings, do the following:

     a. In the **Network Address** field, enter a network address that is different from the network address for the access point. For example, if the access point's IP address is in the range from 192.168.0.1 to 192.168.0.254 (a common IP address range), enter a network address that is different from 192.168.0.0.
     b. From the **Subnet Mask** menu, select the subnet mask that is appropriate for your network address.
     c. In the **DNS** field, enter the IP address for the DNS server that you want to use. This IP address must be different from the WLAN network address that you set in the previous step.
     d. In the **Lease Time (in mins)** field, enter the lease time that is applied to WiFi clients.

8. Click the **Apply** button.

   Your settings are saved.

Enable or disable client isolation for a WiFi network

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

Client isolation is not compatible with Multi PSK. To enable client isolation, first disable Multi PSK (see Set up Multi PSK for a WiFi network on page 54).

To enable or disable client isolation for a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

   The settings for the selected SSID display.
6. Scroll down and click the **> Advanced** tab.

   The page expands.
7. Under Wireless Client Isolation, select one of the following radio buttons:
   - **Disable**: Client isolation is disabled for the WiFi network. This is the default setting.
   - **Enable**: Client isolation is enabled for the WiFi network. The following check boxes display:

   If you select the **Enable** radio button, a check box displays (see the following step).
8. If the **Allow access to devices listed below** check box displays: To add network devices that are exempt from isolation so that clients are allowed to reach them, do the following:
   a. Select the **Allow access to devices listed below** check box.

      By default, the check box is cleared.

      The Allowlist displays.

   b. In the field to the right, enter up to 16 static IP addresses and domain names of devices that clients are allowed to reach over the WiFi network.

For example, you could enter the static IP address or domain name of a network printer that you want to make available to WiFi clients. A domain name on the Allowlist must resolve to a static IP address. A domain name can be up to 255 characters.

c. Click the **Move** button.

The addresses and domain names are added to the Allowlist.

d. To remove one, several, or all addresses and domain names, select individual check boxes or the **Select All** check box, and click the **Remove** button.

9. Click the **Apply** button.

Your settings are saved.

Enable or disable URL tracking for a WiFi network

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

For information about how to view the tracked URLs per SSID or per WiFi client, see Display or download tracked URLs on page 157.

To enable or disable URL tracking for a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

The settings for the selected SSID display.

6. Scroll down and click the **> Advanced** tab.

   The page expands.

7. Under URL Tracking, select one of the following radio buttons:
   - **Enable**: URL Tracking is enabled for the WiFi network.
   - **Disable**: URL Tracking is disabled for the WiFi network.
8. Click the **Apply** button.

   Your settings are saved.

Change the format of the DHCP offer messages in a WiFi network

When a device tries to associate with the WiFi network and negotiates an IP address, the access point converts the broadcast DHCP offer message that it receives from the DHCP server to a unicast message, and forwards it to the device. This is the default configuration. For the DHCP message exchange, unicast packets are more reliable and minimize the traffic in the network.

If your situation requires that DHCP offer messages must be distributed as broadcast packets in a specific WiFi network, you can change the message format for that WiFi network so that the access point does *not* convert the broadcast DHCP offer messages to unicast messages.

To change the format of the DHCP offer messages in a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

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

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

   The settings for the selected SSID display.
6. Scroll down and click the **> Advanced** tab.

   The page expands.
7. Under DHCP Offer Broadcast to Unicast, select one of the following radio buttons:
   - **Enable**. The access point forwards DHCP offer messages as unicast packets in the WiFi network. This is the default selection.
   - **Disable**. The access point forwards DHCP offer messages as broadcast packets in the WiFi network.
8. Click the **Apply** button.

   Your settings are saved

Select a MAC ACL for WiFi clients in a WiFi network

After you set up one or more local MAC access control lists (ACLs, also referred to as access lists) for WiFi clients, you can select an ACL for use with an SSID. For more information about setting up ACLs for WiFi clients, see Manage MAC ACLs for WiFi clients on page 94.

Depending on the policy that you defined for an ACL, WiFi devices for which the MAC address is on the MAC ACL are either allowed access to the access point through this SSID or denied access to the SSID. If denied access to the SSID, these devices might be able to connect to the access point through another SSID if you did not set up MAC ACL security for that SSID.

You can also set up a RADIUS server (see Set up RADIUS servers on page 88) and select the RADIUS MAC ACL. You must define the ACL on the RADIUS server, using the following format for client MAC addresses in the RADIUS server: If the client MAC address is 00:0a:95:9d:68:16, specify it as 000a959d6816 in the RADIUS server.

Note: A RADIUS MAC ACL cannot function if the WiFi security is WPA2 Enterprise or WPA3 Enterprise. If you want to use a RADIUS MAC ACL, select a different type of WiFi security for the WiFi network (see Change the authentication and encryption for a WiFi network on page 49).

Before you select a MAC ACL for a WiFi network, review the policy of the ACL:

- **ACL policy that allows access**: A WiFi device on the ACL is allowed access to the SSID while all other WiFi devices are denied access to the SSID.
- **ACL policy that denies access**: A WiFi device on the ACL is denied access to the SSID while all other WiFi devices are allowed access to the SSID.

To select a MAC ACL for WiFi clients in a WiFi network:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

   The settings for the selected SSID display.
6. Scroll down and click the **> Advanced** tab.

   The page expands.
7. Select the **MAC ACL** check box.
8. Do one of the following:
   - Select the **Local MAC ACL** radio button, and from the **Select Group** menu, select a MAC ACL that you defined earlier.

     To change the MAC ACL policy, MAC addresses in the ACL, or both, click the link next to the group. For more information, see Manage MAC ACLs for WiFi clients on page 94.
   - Select the **Radius MAC ACL** radio button.

     This option functions only if you set up a RADIUS server (see Set up RADIUS servers on page 88).

Caution: If you are accessing the local browser UI of the access point over a WiFi connection, make sure that your device is allowed access to the SSID. Otherwise, your device is denied access to the local browser UI after you click the **Apply** button.

9. Click the **Apply** button.

   Your settings are saved.

Set bandwidth rate limits for a WiFi network

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

Note: You can set bandwidth rate limits for a maximum of two WiFi networks on the access point.

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

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

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

   The settings for the selected SSID display.
6. Scroll down and click the **> Advanced** tab.

The page expands.

7. Select the **Rate Limit** check box.
8. Specify the values:
   - **Upload**: For the upload bandwidth limitation, enter a value from 64 to 1024 and select **Kbps** or **Mbps** from the menu.
   - **Download**: For the download bandwidth limitation, enter a value from 64 to 1024 and select **Kbps** or **Mbps** from the menu.
9. Click the **Apply** button.

   Your settings are saved.

Configure advanced rate selection for a WiFi network

Advanced rate selection lets you improve the capacity of an *individual* WiFi network (as opposed to a radio, which affects *all* WiFi network on the radio) so that you can reach the optimal balance between the following components in the WiFi network:

- Types of traffic (multicast, management, control, and data traffic)
- Number and proximity of clients (the client density)
- Types of clients (the WiFi modes that clients can support, including legacy WiFi modes)
- Throughput speed for clients
- Area that the WiFi network must cover

To successfully configure advanced rate selection, we recommend that you determine what the clients in your network can require (the types of traffic, the supported WiFi modes, and the expected throughput speed), how many clients potentially can connect simultaneously to the WiFi network, and where the clients can be located.

Note: By default, advanced rate selection is disabled. If you enable advanced rate selection, the access point applies rate control settings to WiFi connections in a regular WiFi network but not to connections in a wireless distribution system (WDS).

Advanced rate selection lets you configure the following settings for the 2.4 GHz and 5 GHz radio bands in a WiFi network:

- **Fixed multicast rate**: The multicast traffic transmission rate that you select is automatically applied. The rates that you can select are the basic multicast rates that the radio band supports.
- **Rate control**: The rate that you select is automatically applied to beacon and other management frames and to control and data frames. If you enable rate control, you can set the density level, which consists of four components that are described below. That is, the density level includes much more than the client density (the number and proximity of clients in the WiFi network).

  The available settings for the density level in the WiFi network depend on the WiFi mode in which the radio operates. (For more information about WiFi modes, see Change the WiFi mode for a radio on page 65.)

  You can set a density level of 0 (actually spanning 0–––4, the default setting), 1 (spanning 1–––4), 2 (spanning 2–––4), 3 (spanning 3–––4), or 4. The setting is then applied to the following *interdependent* components, which you cannot set individually precisely because they are interdependent:

  - **Density**: The density (the number and proximity) of clients in the WiFi network. (The density is one of the four components of the density *level*.) A setting of 0 means a very low client density. A setting of 4 means a very high client density.
  - **Compatibility**: The compatibility with WiFi modes for legacy clients in the WiFi network. A setting of 0 means compatibility with 802.11b/g/n/ax clients. A setting of 4 means compatibility with 802.11g/n/ax clients but not with 802.11b legacy clients.
  - **Overall performance**: The throughput speed for the clients in the WiFi network. A setting of 0 means a reduced performance. A setting of 4 means an optimal performance. As an example, you can deliberately select a reduced performance if you require a very wide coverage area.
  - **Coverage**: The area that the WiFi network must cover. A setting of 0 means a very wide coverage area. A setting of 4 means a very narrow coverage area. As an example, you can deliberately select a very narrow area if you require an optimal performance.

Another way to describe the density level is that a selected level is mapped to a corresponding client density level, WiFi mode, minimum legacy rate, beacon rate, and minimum Modulation Coding Scheme (MCS) rate.

To configure advanced rate selection for a WiFi network:

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

   A login window displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.

3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

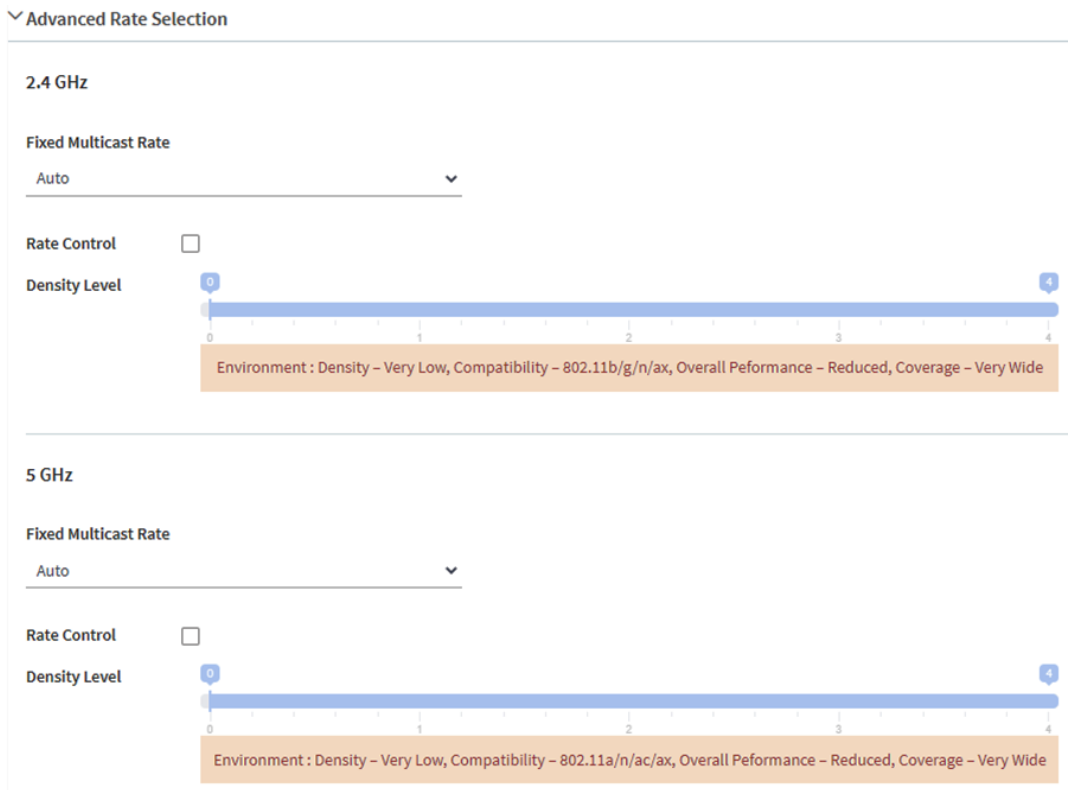
4. Select **Management > Configuration > Wireless > Basic**.

   The page that displays lets you select and add an SSID.

5. Click the **>** button to the left of the SSID.

   The settings for the selected SSID display.

6. Scroll down and click the **Advanced Rate Selection** tab.



Note: For the selected SSID, you can specify the radio settings for the 2.4 GHz and 5 GHz radio bands individually. The descriptions in the following steps apply to both radios.

7. To apply basic fixed multicast rates, from the **Fixed Multicast Rate** menu, select one of the following rates, depending on the radio band:

- **2.4 GHz**: **1**, **2**, **5.5**, or **11** Mbps or **Auto**. (By default, Auto is 11 Mbps.)
- **5 GHz**: **6**, **12**, or **24** Mbps or **Auto**. (By default, Auto is 24 Mbps.)

8. To enable automatic minimum rate control for beacon and other management frames and for control and data frames, select the **Rate Control** check box.

   If you select the **Rate Control** check box, the **Density Level** slider becomes available.

9. To set the density level for your environment, move the **Density Level** slider to **0**, **1**, **2**, **3**, or **4**.

   As you move the slider, the selected density level is mapped to a corresponding WiFi mode, beacon rate, minimum legacy rate, and minimum MCS rate. The available settings depend on the WiFi mode that you select for the radio (see Change the WiFi mode for a radio on page 65). By default, the WiFi mode for each radio is 11ax.

   The density level for the WiFi network is based on the following interdependent components, for which a setting is assigned by the position of the slider but *which you cannot set individually*:

   - **Density of the WiFi clients**: In the default 11ax WiFi mode for the radios, the setting can be very low, low, medium, high, or very high, depending on the position of the slider.
   - **Compatibility with WiFi modes for legacy clients**: In the default 11ax WiFi mode for the radios, this setting can be as follows:
     - **2.4 GHz**: 802.11b/g/n/ax, which supports 802.11b clients, or 802.11g/n/ax, which does not.
     - **5 GHz**: 802.11a/n/ac/ax, which supports all types of clients in the 5 GHz radio band in any position of the slider.
   - **Overall performance for the WiFi clients**: In the default 11ax WiFi mode for the radios, the setting can be reduced, moderate, good, very good, or optimal, depending on the position of the slider.
   - **WiFi coverage**: In the default 11ax WiFi mode for the radios, the setting can be very narrow, narrow, average, wide, or very wide, depending on the position of the slider.

   Note: The help text in the local browser UI provides a table with detailed information about how the WiFi mode of a radio affects these components and how these components depend on each other.

10. Click the **Apply** button.

    Your settings are saved.

Assign host names to WiFi clients and manage the host name list

You can manually assign host names to WiFi clients for easier identification. The access point can support a maximum of 600 host name entries.

You must know the MAC address of the WiFi client for which you want to add a host name. The MAC address might be displayed on the Connected Clients page (see Display client distribution, connected clients, and client trends on page 152).

Note: You cannot assign a host name for a randomized MAC address.

To assign host names to WiFi clients and manage the host name list:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > Wireless > HostName Override**.

   The Hostname Override page displays.
5. To manually add a host name for a WiFi client, do the following in the fields below the Client Hostnames List:
   a. In the left field, type or copy the MAC address of the client in the format 00-00-00-00-00-00.
   b. In the **Enter a host name** field, type a name for the client.

      The host name must contain alphanumeric characters, can contain hyphens, and cannot be longer than 32 characters. The host name cannot start or end with a hyphen.
   c. To add another host name, repeat the previous two substeps.

You can add a maximum of 10 host names at a time.

d. Click the **Add** button.

   Your settings are saved.

6. To change a host name, do the following in the Client Hostnames List:
   a. Select the check box for the name.
   b. Click the **Edit** button.
   c. Change the host name.
   d. To change another host name, repeat the previous three substeps.

      You can change a maximum of 10 host names at a time.
   e. Click the **Apply** button.

      Your settings are saved.
7. To delete one or more host names, do the following in the Client Hostnames List:
   a. Select the check boxes for the names.

      You can delete a maximum of 10 host names at a time.
   b. Click the **Delete** button.

      The host names are removed.

12

Set up a WiFi Bridge

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

The chapter includes the following sections:

- WiFi base station, WiFi repeater, and WiFi bridge requirements
- Set up a WiFi bridge between access points

Note: If you enable Energy Efficiency Mode, you cannot use a WDS. To use a WDS, first disable Energy Efficiency Mode. For more information, see Manage the Energy Efficiency Mode on page 144.

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

WiFi base station, WiFi repeater, and WiFi bridge requirements

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

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

The following figure shows two access points in a WiFi repeating setup with a WiFi base station on the left side and a single WiFi repeater on the right side.

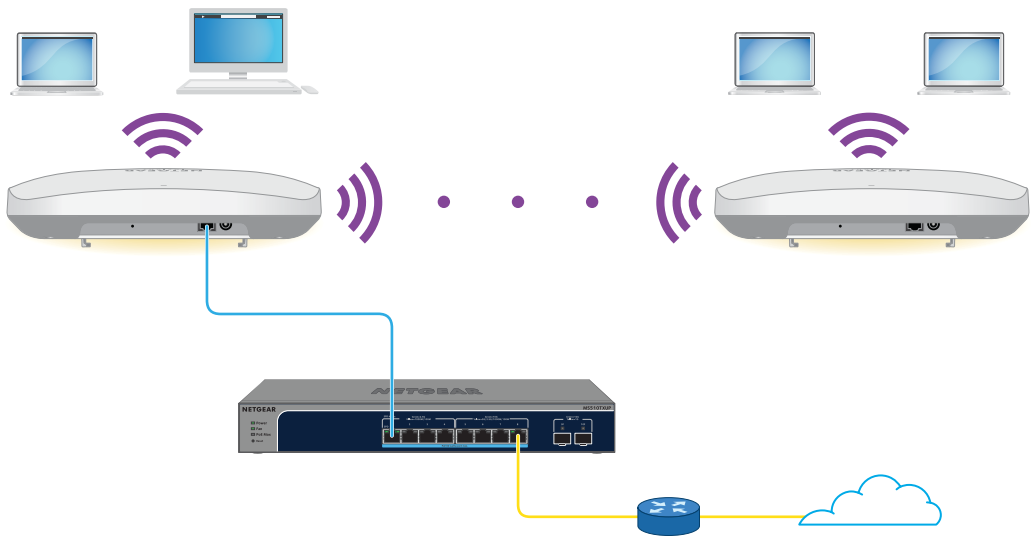


Figure 6. WiFi bridge configuration between two access points in the 5 GHz radio band

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

For a WiFi bridge, you must set up one access point as a WiFi base station and another access point as a WiFi repeater:

- **WiFi base station**: The base station is connected over Ethernet to a network switch (usually with an Internet connection) and bridges traffic to and from the repeater.

The base station also handles local WiFi and wired traffic. To configure this mode, you must know the MAC address of the 2.4 GHz or 5 GHz radio on the repeater.

- **WiFi repeater**: The repeater sends all traffic from its local WiFi or wired devices to the WiFi base station. Similarly, the repeater receives all traffic for its local WiFi or wired computers from the base station. The repeater is connected to the network (and Internet) over the WiFi connection to the base station. To configure this mode, you must know the MAC address of the 2.4 GHz or 5 GHz radio on the base station.

By default, the access point functions in dual-band concurrent mode. If you enable the WiFi repeater in either radio band, the WiFi base station or WiFi repeater cannot be enabled in the other radio band. However, if you enable the WiFi base station in either radio band and use the other radio band for either client access or as a WiFi base station, dual-band concurrent mode is not affected.
Before you can set up a WiFi network with WDS, your configuration must meet the following conditions:

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

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

Caution: Before you set up a WiFi bridge between two access points, enable STP on the access points (see Enable or disable Spanning Tree Protocol on page 109) and on the switches to which the access points are connected. If your switches do not support STP, after the WiFi bridge is established, disconnect one of the access points from its switch to prevent a network loop and connectivity problems. If you used a PoE switch for that access point, you now must use a power adapter.

Set up a WiFi bridge between access points

The following procedure describes how you can configure the WiFi bridge settings on one access point and then do the same on another access point, allowing the WiFi bridge to be established.

To set up a WiFi bridge between two access points:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

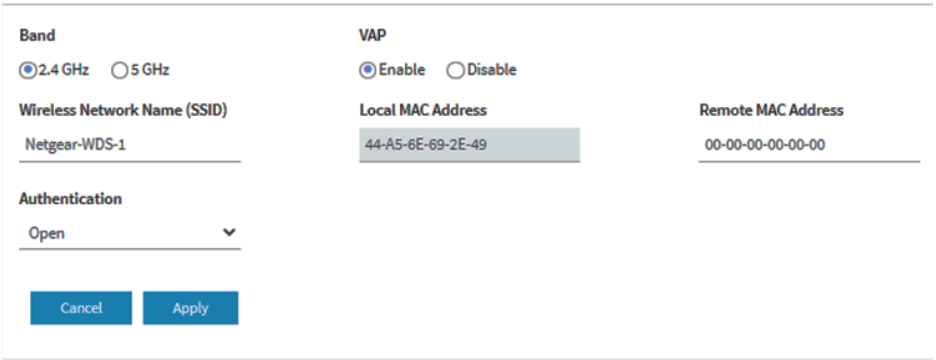
   The Dashboard displays.
4. Select **Management > Configuration > Wireless Bridge**.

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

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

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

   By default, a WDS profile is disabled.



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

Setting	Description
Wireless Network Name (SSID)	The WiFi network name of the network on which the WDS is established. The default name is Netgear-WDS-x, in which x is the number of the WDS (1, 2, 3, or 4). The WiFi network name can be up to 32 characters in length and cannot include backslash or double quote characters. **Note**: The WiFi network name must be identical on the WiFi base station and the WiFi repeater.
Local MAC Address	The MAC address of the local WDS radio interface, that is, the MAC address of the local radio on which the WDS is established. You cannot change this MAC address on this page. The MAC address is displayed for your information. Enter this MAC address on the remote access point of the WDS connection. **Note:** The local MAC address must be different from the remote MAC address.
Remote MAC Address	The MAC address of the remote WDS radio interface, that is, the MAC address of the remote radio on which the WDS is established. **Note:** The remote MAC address must be different from the local MAC address.
Network Authentication, Data Encryption, and Passphrase	By default, the selection from the menu is Open, in which case authentication and data encryption are not applicable. To secure the WDS connection, select **WPA2 Personal** and specify the following settings: • **Encryption**: The data encryption is AES and you cannot change this setting. • **Passphrase**: The passphrase for the WDS connection. The passphrase can be between 8 and 63 characters in length. For you to enable the WDS connection, the passphrase on the remote access point must match the passphrase that you define in this field.

9. Click the **Apply** button.

   Your settings are saved.

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

    Note: If the device at the other end of the WiFi bridge is a NETGEAR access point, you might not need to restart it.

    The WiFi bridge is established.

11. Verify connectivity across the LANs of both access points.

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

Note: After the WiFi bridge is established, you cannot change the WiFi channel for the radio on which the WiFi bridge is established.

13

Manage the Advanced Radio Features

This chapter describes how you can manage the advanced radio features of the access point. For information about the basic radio features, see Manage the Basic Radio Features on page 60.

Caution: If you change a radio feature on the 2.4 GHz radio, the change affects all WiFi networks that broadcast on the 2.4 GHz radio. Similarly, if you change a radio feature on the 5 GHz radio, the change affects all WiFi networks that broadcast on the 5 GHz radio. If the change is not specific to one radio, the change affects *all* WiFi networks on the access point.

The chapter includes the following sections:

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

Note: If you want to change the radio settings, use a wired connection to avoid being disconnected when the new radio settings take effect.

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

Manage the advanced WiFi settings for the radios

The advanced WiFi settings for the radios apply to all WiFi networks (VAPs or SSIDs). Although these settings work fine for most network environments and it is unlikely that you need to change them, you *can* change the radio settings, and you can do so for the 2.4 GHz and 5 GHz radios individually.

Caution: We recommend that you change these advanced WiFi settings only if you fully understand the consequences. Incorrect configuration might cause connectivity problems for devices trying to connect to the access point.

A radio must be turned on for you to change the settings. For more information about turning on a radio, see Turn a radio on or off on page 64.

To manage the advanced WiFi settings for the radios:

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

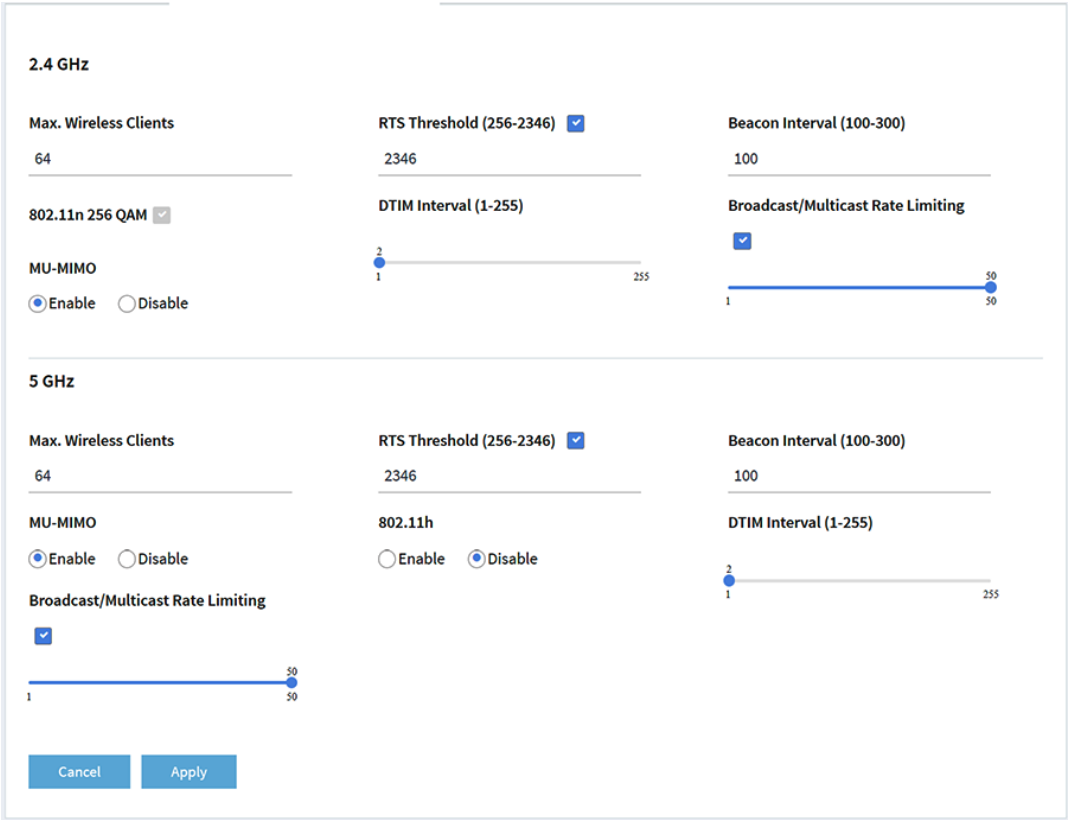
   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.

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



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

   The descriptions in the table apply to both radios. You can specify the radio settings for the 2.4 GHz and 5 GHz radios individually, but the check box for the 802.11n 256 QAM feature applies to the 2.4 GHz radio only (the feature is always enabled for the 5 GHz radio).

Setting	Description
Max. Wireless Clients	Enter the maximum number of WiFi clients that can simultaneously associate with the radio. For each radio, the range is from 1 to 64 WiFi clients, and the default is 64.
RTS Threshold (256-2346)	Enter the Request to Send (RTS) threshold. The range is from 256 to 2346. The default is 2346. If the packet size is equal to or less than the RTS threshold, the radio uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism and the data frame is transmitted immediately after the silence period. If the packet size is larger than the RTS threshold, the system uses the CSMA with Collision Avoidance (CSMA/CA) mechanism. In this situation, the transmitting device sends the RTS packet to the receiving device and waits for the receiving device to return a Clear to Send (CTS) packet before sending the actual packet data.

(Continued)

Setting	Description
Beacon Interval (100-300)	Enter an interval between 100 ms and 300 ms for each beacon transmission, which allows the radio to synchronize the WiFi network. The default is 100 ms. **Note**: If you set up more than four WiFi networks, the beacon interval is automatically changed to 300.
802.11n 256 QAM	When the WiFi mode is 802.11n, you can select the **802.11n 256 QAM** check box to enable the 2.4 GHz radio to function over 256-quadrature amplitude modulation (QAM), which can increase the 2.4 GHz radio throughput for 802.11n clients that are capable of supporting 256 QAM. By default, 256 QAM is disabled for the 2.4 GHz radio, that is, the check box is cleared. By default, 256-QAM is enabled for the 5 GHz radio and you cannot disable it (the page does not provide a check box for the 5 GHz radio).
DTIM Interval (1-255)	Move the slider to specify the delivery traffic indication message (DTIM) interval or the data beacon rate, which indicates the beacon delivery traffic indication message period in multiples of beacon intervals. This value must be between 1 and 255. The default is 3.
Broadcast/Multicast Rate Limiting	Multicast and broadcast rate limiting is enabled by default to improve the overall network performance by limiting the number of packets that are transmitted across the network. By default, the setting is 64, which specifies a maximum rate limit of 64 packets per second. The limit ranges from 1 to 512 packets per second. To change the setting, move the slider. To disable multicast and broadcast rate limiting, clear the small check box.
MU-MIMO	By default, the MU-MIMO **Enable** radio button is selected and multiuser MIMO (MU-MIMO) is enabled. To disable MU-MIMO, select the MU-MIMO **Disable** radio button. MU-MIMO enables multiple users to receive data from the access point simultaneously using the same channel. With MU-MIMO, the access point can transmit to multiple clients simultaneously using the same channel. MU-MIMO is used in the downstream direction and requires both the access point and the WiFi clients to be capable of 802.11ac Wave 2 or 802.11ax.

6. Click the **Apply** button.

   A warning pop-up window displays.

7. Click the **OK** button.

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

Manage the maximum number of clients for a radio

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

By default, one radio allows up to 64 client associations. You can specify a lower number of clients. If the number of associated clients exceeds the maximum number that you specify, the radio rejects new client associations until the number drops below that maximum number.

To manage the maximum number of clients for a radio:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Wireless Settings page displays.
5. In the **Max.Wireless Clients** field for the radio, enter the maximum number of WiFi clients that can simultaneously associate with the radio.

   The range is from 1 to 64 WiFi clients, and the default is 64.
6. Click the **Apply** button.

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

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

Manage the broadcast and multicast settings for a radio

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

By default, multicast and broadcast rate limiting is enabled to improve the overall network performance by limiting the number of packets that are transmitted across the network.

To manage the broadcast and multicast settings for a radio:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Wireless Settings page displays.
5. To change the multicast and broadcast rate limiting setting for a radio, move the **Broadcast/Multicast Rate Limiting** slider.

   By default, the setting is 64, which specifies a maximum rate limit of 64 packets per second. The limit ranges from 1 to 512 packets per second.
6. To disable or enable multicast and broadcast rate limiting for a radio, clear or select the **Broadcast/Multicast Rate Limiting** check box.
7. Click the **Apply** button.

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

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

Manage load balancing for the radios

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

If you enable load balancing, client associations depend on the maximum number of clients per radio, the channel load per radio, and each client's Received Signal Strength Indicator (RSSI). New client associations are allowed if a radio's utilization remains within the defined load balancing settings. If a radio's utilization exceeds the defined load balancing settings, new client associations are temporary halted until the radio's utilization falls within the defined load balancing settings.

Note: The Dashboard page can show information about the client and traffic distribution per radio as well as the client, traffic, and channel utilization for each radio (see Display client distribution, connected clients, and client trends on page 152 and Display traffic volume, statistics, and channel utilization on page 155).

By default, all of the following types of load balancing are enabled with their default settings:

- **Load balancing based on the maximum number of clients**: The access point allows client associations up to the specified maximum number of clients. After the maximum number is exceeded, new clients are rejected. Even though this is a global setting, it is implemented per radio.
- **Load balancing based on the channel load**: The access point allows client associations up to the defined maximum channel utilization. After the maximum channel utilization is exceeded, new clients are rejected. Even though this is a global setting, it is implemented per radio.

  Note: If a client is rejected but persistently tries to associate with the access point, the access point grants access to that client.
- **Load balancing based on the RSSI of the client**: Clients with an RSSI that is equal to or higher than the defined minimum are allowed to associate with the access point. Clients with an RSSI below the defined minimum are rejected. Even though this is a global setting, it is implemented per radio.

  Note: If a client is rejected but persistently tries to associate with the access point, the access point grants access to that client.

You can change the default settings for each type of load balancing, or completely disable one or more types of load balancing.

To manage load balancing for the radios:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > Wireless > Advanced > Load Balancing**.
5. To globally enable load balancing for the radios, select the Load Balancing Mode **Enable** radio button.

   The page adjusts and displays a slider for each type of load balancing and each radio.

   By default, load balancing is disabled. When you enable load balancing, all three types of load balancing are enabled. You can individually disable one or more types of load balancing.

6. To individually enable or disable one or more types of load balancing, do the following:
   - To disable a particular type of load balancing, clear the small blue check box to the left of the *Based On* text.
   - To enable a particular type of load balancing, select the small blue check box to the left of the *Based On* text.

7. To change the load balancing settings, do the following:
   - **Based On Maximum Number Of Clients**: For each radio, move the associated slider to specify the maximum number of clients allowed, before the radio stops accepting new client associations.

     For each radio, the minimum number of clients is 5 and the maximum number is 64, and the default number is 64.
   - **Based On Channel Load**: For each radio, move the associated slider to specify the maximum percentage of channel load that is allowed on the radio, before it stops accepting new client associations.

     For each radio, the minimum percentage of channel load is 50, the maximum percentage is 90, and the default percentage is 70.
   - **Based on Channel Receive Signal Strength**: For each radio, move the associated slider to specify the minimum required RSSI value for an individual client, below which the radio does not accept the client association.

     For each radio, the minimum RSSI value is 1, the maximum value is 50, and the default value is 23.
8. Click the **Apply** button.

   Your settings are saved.

Manage sticky clients

During roaming, sticky clients do not change to an access point with a better signal but remain associated with (that is, *stick to*) their initial access point, even though the quality of the connection to that access point is degraded. Such a situation causes delay for other clients that are associated with that access point.

Note: For a home WiFi network with a single access point, a sticky client is useful because no other access point is available to associate with during roaming. For a business or enterprise network with multiple access points, a sticky client can cause a drain on WiFi resources.

You can force sticky clients to disassociate from the radios of the access point.

If load balancing based on the RSSI of the client is enabled (see Manage load balancing for the radios on page 188), after a client is forced to disassociate, the client can join again in the following situations:

- The client can associate again if its RSSI is equal to or higher than the minimum required RSSI.
- If the client persistently tries to associate with the access point, the access point grants access to that client, even if its RSSI is below minimum required RSSI.

To manage sticky clients:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

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

   The Load Balancing page displays.
5. Either select or clear the **Force Sticky Clients To Disassociate** check box:
   - **Sticky clients are forced to disassociate**: Select the check box. If a client's RSSI value falls below the minimum required RSSI value that you set for a radio, the client is forcibly disassociated.

     For each radio, you can move the **Based on Channel Receive Signal Strength** slider to specify the minimum required RSSI value for an individual client, below which the radio does not accept the client association.

     For each radio, the minimum RSSI value is 1, the maximum value is 50, and the default value is 23.
   - **Sticky clients are allowed to remain associated**: Clear the check box. This is the default setting.
6. Click the **Apply** button.

   Your settings are saved.

Manage the ARP proxy

By default, the ARP proxy is enabled on the access point, allowing it to inspect all ARP broadcast packets for its clients. In this way, the access point responds to ARP requests for its clients, preventing unnecessary broadcast traffic on the radios.

For information about the ARP statistics, including the number of proxied and dropped packets, see Display traffic volume, statistics, and channel utilization on page 155.

To manage the ARP proxy:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Configuration > Wireless > Advanced > ARP Proxy**.

   The ARP Proxy page displays.
5. Select one of the following radio buttons
   - **Enable**: The ARP proxy is enabled. This is the default setting.
   - **Disable**: The ARP proxy is disabled. Broadcast traffic on the radios might increase.
6. Click the **Apply** button.

   Your settings are saved.

14

Diagnostics and Troubleshooting

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

The chapter includes the following sections:

- Perform a ping test
- Capture WiFi and Ethernet packets
- Quick tips for WiFi troubleshooting
- Troubleshoot with the LED
- Troubleshoot WiFi connectivity for a WiFi client device
- Troubleshoot Internet browsing
- You cannot log in to the access point over a LAN connection
- Changes are not saved
- You enter the wrong password and can no longer log in to the access point
- Troubleshoot your network using the ping utility

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

Perform a ping test

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

To perform a ping test:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Diagnostics > Ping Test**.

   The Ping Test page displays.
5. Specify the settings that are described in the following table.

Setting	Description
Ping Count	The number of pings that the access point must send. The number can be between 1 and 1024. The default number is 16.
Packet Size (in Bytes)	The size of each ping packet. The size can be between 4 and 1024 bytes. The default size is 64 bytes.
Ping Interval (in sec)	The interval between pings. The interval can be between 0.5 and 10 seconds. The default interval is 1 second.
Ping Timeout (in sec)	The period after which a ping times out. The period can be between 1 and 300 seconds. The default period is 60 seconds.
Remote Host	The IP address that the access point must ping. This field can contain a maximum of 100 characters. The default address is 8.8.8.8.

6. To start the ping test, click the **Start** button.

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

Capture WiFi and Ethernet packets

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

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

You can select to capture all packets or selected packets only. You can select a bridge interface, Ethernet interface, or WLAN interfaces (radio 0 - 2.4 GHz / radio 1 - 5 GHz) to capture packets.

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

To capture packets:

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

   A login window displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 34.
3. Enter the access point user name and password.

   The user name is **admin**. The password is the one that you specified. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Management > Diagnostics > Packet Capture**.

   The Packet Capture page displays.
5. Specify the settings that are described in the following table.

Setting	Description
Capture Interface	From the **Capture Interface** menu, select one of the following interfaces on which packets must be captured: • **br-lan**: All packets are captured, that is, packets on the Ethernet interfaces, 2.4 GHz radio, and 5 GHz radio. • **eth0**: Packets on the Ethernet interface are captured. • **eth1**: Packets on the Ethernet interface 2 are captured (if available). • **radio0**. Packets passing through the 2.4 GHz radio are captured. • **radio1**: Packets passing through the 5 GHz radio are captured.
Capture File Size (64-12288 KB)	Enter the maximum size that the file with captured packets is limited to. The range is from 64 to 12288 KB. The default is 1024 KB. **Note:** When multiple interfaces are selected, the total capture file size of all selected interfaces must be within the range of 64 to 12288 KB.
Capture Duration (10-3600 secs)	Enter the maximum duration of the capture process (that is, if you do not click the **Stop** button). The range is from 10 to 3600 seconds. By default, the maximum duration is 300 seconds.
Filter	Specify a tcpdump filter expression to capture only the desired network traffic. By default, the filter is set to **NONE**.
Promiscuous Capture (Ethernet interfaces only)	To allow the access point to capture packets in Promiscuous Capture mode, select the **Enable** check box. By default, Promiscuous Capture mode is disabled. In Promiscuous Capture mode, the radio or radios receive all traffic on the channel, including traffic that is not destined for the access point. Promiscuous Capture mode, the Ethernet interface captures all network traffic on the segment, even packets not addressed to the access point. While operating in Promiscuous Capture mode, the interface continues to function normally. Packets that are not addressed to the access point are not forwarded. When the capture process stops, the interface reverts to non-promiscuous mode.
Channel (radio interfaces only)	From the Channel menu, select a specific channel to capture packets. The wireless clients disconnect and reconnect if you change the channel.

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

   If any captured packets are already stored on the access point, you are prompted to allow the packet capture process to overwrite the old information.
7. To stop the packet capture process, click the **Stop** button.

   If you do not stop the process manually, the process is automatically stopped when the capture duration period is exceeded.
8. To download the file with captured packets, do the following:
   a. Click the **Download** button.
   b. Follow the directions of your browser to save the file to your computer.
9. To display the latest information on the page, click the **Refresh** button.

Quick tips for WiFi troubleshooting

Problems with a WiFi network

If one or more WiFi networks do not function normally, consider to repower the access point:

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

Problems with a WiFi client

If a WiFi client device cannot connect to the access point, check the following:

- Make sure that the WiFi radios are not off. For more information about the WiFi radios, see Turn a radio on or off on page 64.
- Make sure that the WiFi settings in the WiFi client device and access point match exactly.

  The WiFi network name (SSID) and WiFi security settings of the access point and WiFi client device must match exactly.

  For information about accessing the access point for initial configuration over a WiFi connection, see Connect to the access point for initial configuration on page ?.
- Make sure that the WiFi client device supports the authentication and encryption that you are using for the WiFi network. For more information, see Change the authentication and encryption for a WiFi network on page 49.

  Note: If the access point's WiFi authentication and encryption is set to WPA3 Personal and the WiFi client device does support WPA3, make sure that the WiFi adapter device driver is updated to the latest version on the WiFi client device.
- Make sure that the WiFi client device is not too far from the access point or too close. To see if the signal strength improves, move the WiFi client device near the access point but at least 6 feet (1.8 meters) away.
- Make sure that the WiFi signal is not blocked by objects between the access point and the WiFi client device.
- Make sure that the access point's SSID broadcast is not disabled.

  If the access point's SSID broadcast is disabled, the WiFi network name is hidden and does not display in the WiFi client device's scanning list. To connect to a hidden network, the user must enter the network name and the WiFi password. For more

information about the SSID broadcast, see Hide or broadcast the SSID for a WiFi network on page 47.

- Make sure that the WiFi client device does not use a static IP address but is configured to receive an IP address automatically with DHCP. (For most devices, DHCP is the default setting.)

Troubleshoot with the LED

For general information about the LED, see Top panel LED on page 12.

When you connect the access point to a power source and you did not disable the LED (see Manage the LED on page 143), the LED lights as described here:

1. The LED lights solid amber initially and then blinks amber slowly. After about two minutes, the LED turns solid green, indicating that the startup procedure is complete and the access point is ready.
2. When the startup procedure is complete, if clients are connected to a radio, the LED is blinking green.

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

- LED remains off
- LED remains solid amber
- LED is blinking amber slowly, continuously

LED remains off

If you use a PoE connection and the LED is off when the Ethernet cable is connected to a PoE switch, do the following:

- Make sure that the LED is not disabled (see Manage the LED on page 143).
- Make sure that the Ethernet cable between the access point and the PoE switch is correctly connected at both ends.
- Make sure that the other end of the Ethernet cable is plugged into a PoE port on a PoE switch that is receiving power.
- Make sure that the PoE power budget of the PoE switch is not oversubscribed so that the PoE switch is capable of delivering PoE (802.3af) power to the access point.

If you use an optional power adapter and the LED remains off when the access point is turned on, do the following:

- Make sure that the LED is not disabled (see Manage the LED on page 143).
- Make sure that the power adapter is correctly connected to the access point, and that the power adapter is correctly connected to a functioning power outlet. If it is plugged into a power strip, make sure that the power strip is turned on. If it is plugged directly into the wall, verify that the outlet is not switched off.
- Make sure that you are using the NETGEAR power adapter for this product. That is, do not use the NETGEAR 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

When you connect the access point to a power source, the LED lights solid amber initially, then blinks amber slowly, and finally turns solid green or solid blue, indicating that the startup procedure is complete and the access point is ready.

If the LED remains solid amber after five minutes, either a boot error occurred or the access point is malfunctioning.

Do the following:

1. Disconnect the access point from its power source, reconnect it, and wait several minutes to see if the startup procedure completes successfully.
2. If the startup procedure still does not complete successfully and the LED remains solid amber after five minutes, use the **Reset** button to return the access point to its factory default settings.

   For more information, see Use the Reset button to reset the access point on page 136.

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 is blinking amber slowly, continuously

When you connect the access point to a power source, the LED lights solid amber temporarily and then turns solid green or solid blue, indicating that the startup procedure is complete and the access point is ready. 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 blinks amber slowly and continuously, the access point did not receive an IP address from a DHCP server.

Check to make sure that the DHCP client of the access point is enabled (see Enable the DHCP client on page 105), that your network includes a DHCP server (or a router that functions as a DHCP server), and that the DHCP server can reach the access point (both must be on the same network).

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 access point (see Disable the DHCP client and specify a fixed IP address on page 104).

Troubleshoot WiFi connectivity for a WiFi client device

If a WiFi client device cannot connect to the access point or the WiFi connectivity is not normal, try to isolate the problem:

- Make sure that the WiFi settings in the WiFi client device and access point match exactly.

  The WiFi network name (SSID) and WiFi security settings of the access point and WiFi device must match exactly. Make sure that the WiFi client device uses the correct passphrase for the WiFi network.

  For information about accessing the access point for initial configuration over a WiFi connection, see Connect to the access point for initial configuration on page ?.

- Does the WiFi client device support the authentication and encryption that you configured for the WiFi network?

  For more information, see Change the authentication and encryption for a WiFi network on page 49.

  Note: If the access point's WiFi authentication and encryption is set to WPA3 Personal and the WiFi client device does support WPA3, make sure that the WiFi adapter device driver is updated to the latest version on the WiFi client device.

- Make sure that the WiFi radios ar not off. For more information about the WiFi radios, see Turn a radio on or off on page 64.
- If you disabled the access point's SSID broadcast for the WiFi network, the WiFi network is hidden and does not display in the WiFi device's network scanning list. (By default, SSID broadcast is enabled.) For more information about the SSID broadcast, see Hide or broadcast the SSID for a WiFi network on page 47.

Note: If you want to change the settings of a WiFi network on the access point, use a wired LAN connection to avoid being disconnected when the new WiFi settings take effect.

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

- Is the WiFi client device too far from the access point, or too close?

  Place the WiFi client device near the access point, but at least 6 feet (1.8 meters) away, and see whether the signal strength improves.
- Are objects between the WiFi client device and the access point blocking the WiFi signal?

Troubleshoot Internet browsing

If a WiFi device is connected to the access point but unable to load any web pages from the Internet, it might be for one of the following reasons:

- The WiFi device might not recognize any DNS server addresses.

  If you manually entered a DNS address when you set up the access point (that is, the access point uses static IP address settings), restart the WiFi device and verify the DNS address.
- The WiFi device might not use the correct TCP/IP settings.

  If the WiFi device obtains its information by DHCP, reboot the WiFi device and verify the address of the switch or Internet modem to which the access point is connected.

  For information about TCP/IP problems, see Troubleshoot your network using the ping utility on page 203.

You cannot log in to the access point over a LAN connection

If you are unable to log in to the access point from a computer on your LAN and use the access point's local browser UI, check the following:

- 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 user name and password are case-sensitive.
- Make sure that the IP address of your computer is in the same subnet as the access point.

  If you disabled the access point's DHCP client and configured a fixed (static) IP address when you connected the access point to your network (see Disable the DHCP client and specify a fixed IP address on page 104), change the IP address and subnet mask on your computer to so that the IP addresses of your computer and the access point are in the same IP subnet.
- Try quitting the browser and launching it again.
- If you are using on older type of browser, make sure that Java, JavaScript, or ActiveX is enabled in your browser. For example, if you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.
- If your access point's IP address was changed (for example, the DHCP server in your network issued an IP address to the access point) and you do not know the current IP address, use an IP scanner application to detect the IP address.

  If you still cannot find the IP address, reset the access point's configuration to factory defaults. This sets the access point's IP address to 192.168.0.100 and enables the DHCP client. For more information, see Use the Reset button to reset the access point on page 136.

Changes are not saved

If you are logged in to the access point's local browser UI and the access point does not save the changes that you make on a page, do the following:

- When entering configuration settings, always click the **Apply** button before moving to another page or tab or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. It is possible that the changes occurred but that the old settings remain in the web browser's cache.

You enter the wrong password and can no longer log in to the access point

If you enter the wrong admin password five times, access to the access point's local browser UI is blocked for five minutes.

After five minutes, the counter for failed login attempts is reset, and you can attempt to log in again.

In addition, the following rules apply to the number of failed login attempts:

- The last access attempt determines whether the counter for failed login attempts is increased.
- If you restart the access point, the counter for failed login attempts is reset.

Troubleshoot your network using the ping utility

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a network using the ping utility in your computer or workstation.

Test the LAN path to your access point

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

To ping the access point from a Windows-based computer:

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

   ping 192.168.0.100
3. Click the **OK** button.

   A message such as the following one displays:

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

If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections

  Check that the appropriate LEDs are on for your network devices. If your access point and computer are connected to a separate Ethernet switch, make sure that the link LEDs are lit for the switch ports that are connected to your computer and access point.

- Wrong network configuration

  Verify that the IP addresses for your computer and the access point are correct and that the addresses are in the same subnet.

Test the path from your computer to a remote device

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

To test the path from your computer to a remote device:

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

   IP address is the IP address of a remote device such as a remote DNS server.

If the path is functioning correctly, replies as described in Test the LAN path to your access point on page 203 display. If you do not receive replies, do the following:

- Check to see that your computer lists the IP address of the router to which the access point is connected as the default router. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel.
- Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

A

Factory Default Settings and Technical Specifications

This appendix includes the following sections:

- Factory default settings
- Technical specifications

Factory default settings

You can reset the access point to the factory default settings, which are shown in the following table.

For more information about resetting the access point to its factory settings, see Return the access point to its factory default settings on page 136.

Table 2. Factory default settings

Feature	Default Setting
Management and login settings	
User login URL	192.168.0.100, if not connected to a network. **Note**: If connected to a network, the access point receives an IP address from a DHCP server or router in the network.
User name	**admin**, nonconfigurable
AP login password	**password**, case-sensitive, configurable **Note**: The first time that you log in to the local browser UI, you must change the AP login password.
WiFi network settings for initial setup and WiFi login	
Initial SSID name	The SSID for initial setup is NETGEARxxxxxx-SETUP, where xxxxxx is the last six hexadecimal digits of the access point's MAC address. **Note**: The first time that you log in to the local browser UI, you must change the SSID.
Initial WiFi security	WPA3/WPA2 Personal (which is WPA3-PSK/WPA2-PSK) WiFi password (network key): **sharedsecret** **Note**: The first time that you log in to the local browser UI, you must change the WiFi password.
RF channels	Automatically selected (Auto) for all radios. **Note**: The available and supported channels depend on the country and region that you select for the access point.
General system settings	
Operating mode	AP mode
DHCP client	Enabled so that the access point receives an IP address from a DHCP server or router in the network.
NTP client	Enabled
Spanning Tree Protocol	Disabled
Network integrity check	Disabled
IGMP snooping	Disabled

Table 2. Factory default settings (Continued)

Feature	Default Setting
802.1Q VLAN	Untagged VLAN with VLAN ID 1
Management VLAN	VLAN ID 1
Syslog	Disabled
Ethernet LLDP	Enabled
UPnP	Enabled
LED	Enabled
Energy Efficiency Mode	Disabled
Multicast DNS gateway	Disabled
WLAN settings for an individual WiFi network (SSID or VAP)	
Broadcast SSID	Enabled
VLAN ID (for WiFi clients)	1
Network authentication	WPA3/WPA2 Personal (which is WPA3-PSK/WPA2-PSK) The nonconfigurable data encryption for WPA3 is SAE The nonconfigurable data encryption for WPA2 is AES
802.11w (PMF)	Optional
Multi PSK	Disabled
Broadcast schedule	Always on
Radio bands	All enabled
Band steering	Disabled
Addressing and Traffic	Bridge
WiFi client isolation	Disabled
URL tracking	Disabled
DHCP offer broadcast to unicast	Enabled
Captive portal	None
MAC ACL for WiFi client access	None assigned
Rate limit	None
Advanced rate selection	Fixed multicast rate: Auto Rate control: Disabled

Table 2. Factory default settings (Continued)

Feature	Default Setting
Basic radio settings that apply to all WiFi networks (SSIDs or VAPs)	
Radio broadcast	2.4 GHz radio: Enabled 5 GHz radio: Enabled
WiFi mode	2.4 GHz radio: 11ax mode, which also supports 11b, 11bg, and 11na 5 GHz radio: 11ax mode, which also support 11a, 11na, and 11ac
Channel width	2.4 GHz radio: 20 MHz 5 GHz radio: 40 MHz
Guard interval	2.4 GHz radio: Long-800 ns 5 GHz radio: Long-800 ns
Output power	2.4 GHz radio: Maximum (100%) 5 GHz radio: Maximum (100%)
Channel	2.4 GHz radio: Auto 5 GHz radio: Auto
Wi-Fi Multimedia (WMM)	2.4 GHz radio: Enabled 5 GHz radio: Enabled
WMM Powersave	2.4 GHz radio: Enabled 5 GHz radio: Enabled
Advanced radio settings that apply to all WiFi networks (SSIDs or VAPs)	
Number of WiFi clients	2.4 GHz radio: 64 default (also the maximum number) 5 GHz radio: 64 default (also the maximum number)
RTS threshold	2.4 GHz radio: Enabled at 2346 5 GHz radio: Enabled at 2346
Beacon interval	2.4 GHz radio: 100 millisec. 5 GHz radio: 100 millisec.
802.11n 256 QAM	2.4 GHz radio: Disabled (QAM applies in the 11ng WiFi mode only) 5 GHz radio: Nonconfigurable
MU-MIMO	2.4 GHz radio: Enabled 5 GHz radio: Enabled
DTIM interval	2.4 GHz radio: 3 5 GHz radio: 3
Broadcast and multicast rate limiting	2.4 GHz radio: Enabled with a limit of 64 pps 5 GHz radio: Enabled with a limit of 64 pps

Table 2. Factory default settings (Continued)

Feature	Default Setting
Load balancing between radios	Disabled
Force sticky clients to disassociate	Disabled
ARP proxy	Enabled
Wireless bridge	None configured
Security	
URL filtering	Disabled
RADIUS servers	None configured
Neighbor AP detection	2.4 GHz radio: Disabled 5 GHz radio: Disabled
MAC ACLs for WiFi client access	Eight default ACLs but none configured with MAC addresses
L2 security	Disabled
DoS Prevention	Disabled
Remote management	
SNMP	Disabled
Other	
Hostname override	None configured

Technical specifications

The following table shows the technical specifications.

Table 3. Technical specifications

Feature	Description
WiFi modes	2.4 GHz radio: 802.11ax, 802.11ng, 801.11bg, and 802.11b 5 GHz radio: 802.11ax, 802.11ac, 802.11na, and 802.11a The access point supports 2.4 GHz and 5 GHz band concurrent operation.
Maximum theoretical throughput	About 3000 Mbps simultaneous throughput (600 Mbps in the 2.4 GHz band and 2400 Mbps in the 5 GHz band). **Note**: Throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, affect the data throughput rate.
Maximum number of supported clients	2.4 GHz radio: 64 5 GHz radio: 64
802.11 security	WPA3 Personal, WPA3 Enterprise, WPA3/WPA2 Personal, WPA2 Personal, WPA2 Enterprise, WPA2/WPA Personal, Open Enhanced, and Open
WiFi standards	WiFi Multimedia Prioritization (WMM) Wireless distribution system (WDS)
WiFi streams	4 (2+2) streams: 2.4 GHz radio: 2 streams 5 GHz radio: 2 streams
Operating frequency range 2.4 GHz band	2.402–2.482 GHz
Operating frequency ranges 5 GHz band	5.150~5.250 GHz 5.250~5.350 GHz 5.470~5.725 GHz 5.725~5.850 GHz
Power over Ethernet	If you do not use a power adapter, the LAN/PoE port requires 802.3af (PoE) power. **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).
Power consumption	12.8W maximum
Power adapter	12 VDC, 1.5A The plug is localized to the country of sale. **Note**: For model WAX605PA, a power adapter is included. For model WAX605, a power adapter is not included but can be ordered as an option.

Table 3. Technical specifications (Continued)

Feature	Description
Hardware interfaces	One RJ-45 LAN/PoE Ethernet port that supports 1 Gbps, 100 Mbps, and 10 Mbps. The port also supports Auto Uplink (Auto MDI-X). **Note:** Without a power adapter, the LAN/PoE port requires 802.3af (PoE).
Dimensions (W x D x H)	6.3 x 6.3 x 1.2 in (160 x 160 x 30 mm)
Weight	0.82 lb (371 g)
Operating temperature	32° to 104°F (0° to 40°C)
Operating humidity	up to 90% maximum relative humidity, noncondensing
Storage temperature	–40° to 176°F (–40° to 80°C)
Storage humidity	up to 90% maximum relative humidity, noncondensing
Regulatory compliance US	EMI, FCC part 15 subpart B, Class B RF, FCC ID approved
Regulatory compliance Europe	CE EMC, EN 55032, EN 55035, EN 301489-1/-17, Class B CE RED, EN 300 328, EN 301 893, DFS, EN 50566
Safety and energy compliance	IEC 62368-1 Certificate and Test Report CE LVD Report, EN 62368-1 Report EC 2019/1782, External Power Supply Ecodesign Directive 2009/125/EC and the implementation (EC)1275/2008 and amendment (EC) No 801/2013, and (EU) No 278/2009.

B

Mount the Access Point to a Wall or Ceiling

The access point package includes wall-mounting and ceiling-mounting components.

You can mount the access point to a solid surface (a wall or a ceiling) or to a ceiling with a 9/16 in. (14.3 mm) or 15/16 in. (23.8 mm) T-bar, or you can install the access point freestanding on a flat surface.

We recommend that you use a flat Ethernet cable so that the cable fits in the narrow space between the access point and the surface on which it is mounted or placed.

This appendix includes the following sections:

- Mount the access point to a solid wall or ceiling
- Mount the access point to a T-bar
- Unmount the access point

Mount the access point to a solid wall or ceiling

Caution: Make sure that the wall or ceiling is not damaged. For example, water damage can destroy a drywall or ceiling.

For mounting to a solid wall or ceiling, use the 15/16 in. (23.8 mm) bracket.

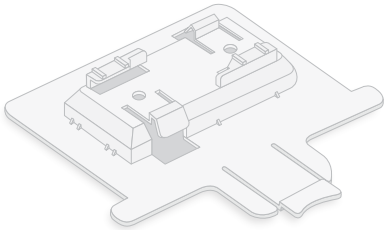
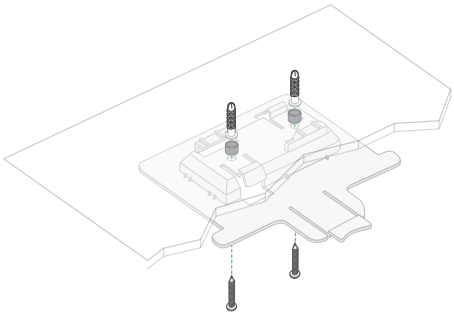


Figure 7. 15/16 in. (23.8 mm) bracket

To mount the access point to a solid wall or ceiling:

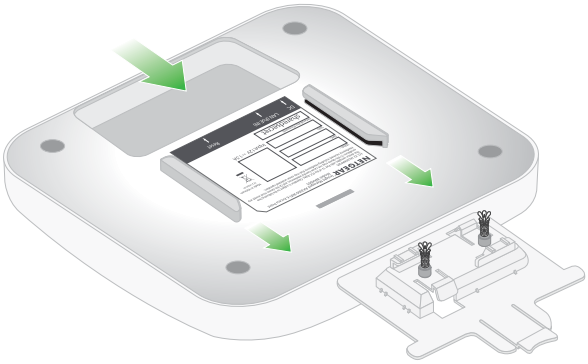
1. Using the anchors, screws, and spacers provided, attach the 15/16 in. (23.8 mm) bracket with the screw holes to the wall or ceiling.

   The rectangular protruding part of the bracket must be facing the ceiling.

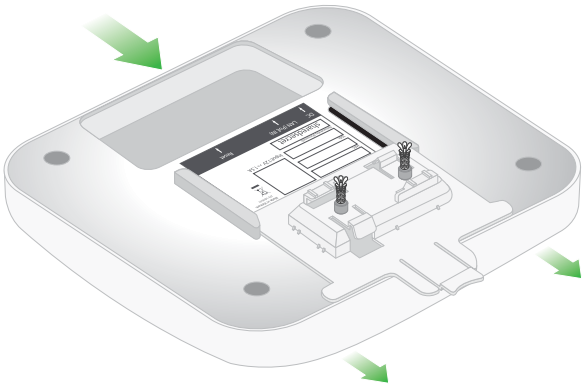


2. Hold the access point upside down with the back of the access point (the side with the LED) facing the bracket.

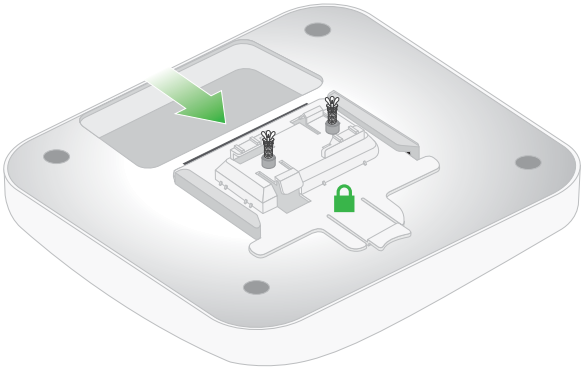
3. Line up the guides on the bottom of the access point with the bracket.



4. Slide the access point into the bracket until it locks in place.



The locking tab must be at the back of the access point.



Mount the access point to a T-bar

Depending on the size of the T-bar, use the 9/16 in. (14.3 mm) or 15/16 in. (23.8 mm) bracket.

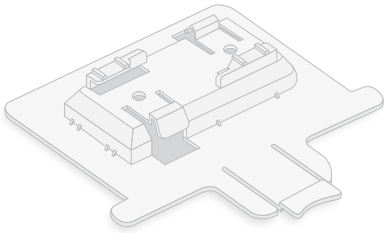


Figure 8. 9/16 in. (14.3 mm) bracket

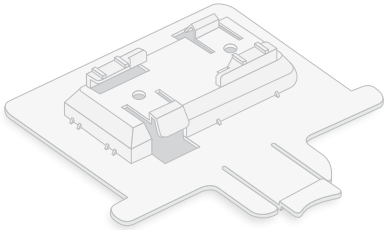
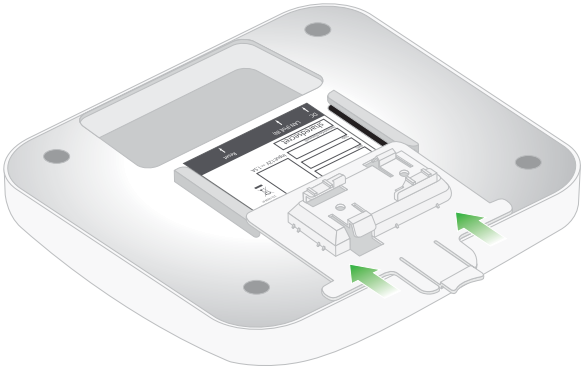


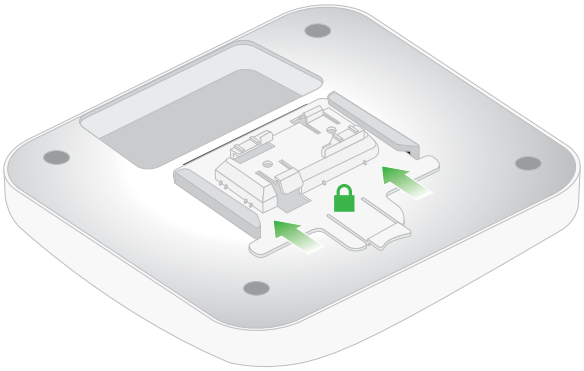
Figure 9. 15/16 in. (23.8 mm) bracket

To mount the access point to a T-bar:

1. Slide the bracket between the guides on the bottom the access point until it locks in place.

   The locking tab must be at the back of the access point (the side with the LED).

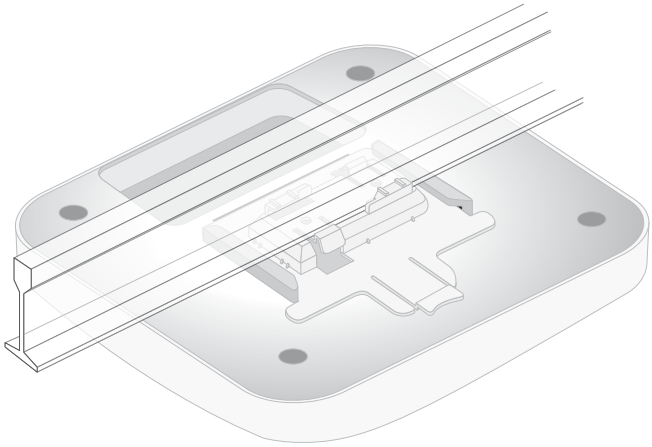




2. Hold the access point upside down.

   Note: If you can reach behind the T-bar, hold the T-bar with one hand and the access point with your other hand.

3. Align the rectangular protruding part of the bracket with the T-bar.
4. Hook the bracket onto one side of the T-bar.
5. Hook the bracket onto the other side of the T-bar until the bracket locks onto the T-bar.



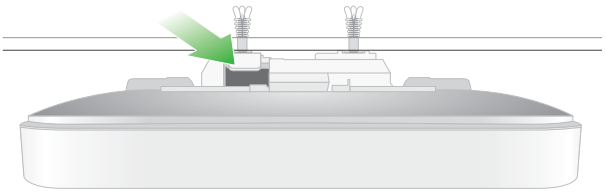
Unmount the access point

Caution: Make sure you hold the access point so that it does not drop when you release it from the mounting bracket.

To unmount the access point:

1. Find the locking latch by placing your thumb on the LED, and your finger on the other side of the access point, directly opposite the thumb.

The following figure shows a side view of the access point, with the bracket attached to a solid ceiling. The green arrow indicates the locking tab.



2. Press and hold the latch down to release the lock and keep the lock open.
3. Slide the access point out of the bracket.

   The bracket remains attached to the solid wall or ceiling or to the T-bar.