

[Store](#)[Mac](#)[iPad](#)[iPhone](#)[Watch](#)[AirPods](#)[TV & Home](#)[Only on Apple](#)[Accessories](#)[Support](#)

Recommended settings for Wi-Fi routers and access points

For the best security, performance, and reliability, we recommend these settings for Wi-Fi routers, base stations, or access points used with Apple products.

This article is primarily for network administrators and others who manage their own network. If you're trying to join a Wi-Fi network, one of these articles should help:

[Connect to Wi-Fi with your Mac >](#)

[Connect to Wi-Fi with your iPhone or iPad >](#)

About privacy and security warnings on your device

If your Apple device shows a privacy warning or weak-security warning about a Wi-Fi network, that network could expose information about your device.

- If you administer the Wi-Fi network, we recommend that you update the settings of your Wi-Fi router to meet or exceed the security standards in this article.
- If you don't administer the Wi-Fi network, you can bring the recommended settings in this article to the attention of the network administrator.

Router settings

To ensure that your devices can connect securely and reliably to your network, apply these settings consistently to each Wi-Fi router and access point, and to each band of a dual-band, tri-band, or other multiband router. Before changing the settings, you should take these steps:

- Back up your existing settings, in case you need to restore them.
- Install the latest firmware updates for your router. This is generally done from the app or webpage that you use to administer the router.
- Update the software on your other devices, such as [on your Mac](#) and [on your iPhone or iPad](#), to ensure that they have the latest security updates and work best with each other.

After changing the settings, you might need to [forget the network](#) on each device that previously joined the network. This ensures that the device uses the router's new settings when rejoining the network.

Security



Set to **WPA3 Personal** for better security

Set to **WPA2/WPA3 Transitional** for compatibility with older devices

The security setting defines the type of authentication and encryption used by your router, and the level of privacy protection for data transmitted over its network. Whichever setting you choose, always set a strong password for joining the network.

- **WPA3 Personal** is the newest, most secure protocol currently available for Wi-Fi devices. It works with all devices that support Wi-Fi 6 (802.11ax), and some older devices.
- **WPA2/WPA3 Transitional** is a mixed mode that uses WPA3 Personal with devices that support that protocol, while allowing older devices to use WPA2 Personal (AES) instead.
- **WPA2 Personal (AES)** is appropriate when you can't use one of the more secure modes. In that case, also choose AES as the encryption or cipher type, if available.

Weak security settings to avoid on your router

Don't create or join networks that use older, deprecated security protocols. These are no longer secure, they reduce network reliability and performance, and they cause your device to show a security warning:

- WPA/WPA2 mixed modes
- WPA Personal
- WEP, including WEP Open, WEP Shared, WEP Transitional Security Network, or Dynamic WEP (WEP with 802.1X)
- TKIP, including any security setting with TKIP in the name

Settings that turn off security, such as None, Open, or Unsecured, are also strongly discouraged. Turning off security disables authentication and encryption and allows anyone to join your network, access its shared resources (including printers, computers, and smart devices), use your internet connection, and monitor the websites you visit and other data transmitted over your network or internet connection. This is a risk even if security is turned off temporarily or for a guest network.

Network name (SSID)



Set to a **single, unique name** (case-sensitive) for all bands

The Wi-Fi network name, or SSID (service set identifier), is the name your network uses to advertise its presence to other devices. It's also the name that nearby users see on their device's list of available networks.

Use a name that's unique to your network, and make sure that all routers on your network use the same name for every band they support.

- Don't use common names or default names such as *linksys*, *netgear*, *dlink*, *wireless*, or *2wire*.
- Don't give your 2.4GHz, 5GHz, or 6GHz bands different names. All bands should have the same name.

If you don't follow this guidance, devices might not connect reliably to your network, to all routers on your

network, or to all available bands of your routers. And devices that join your network are more likely to encounter other networks that have the same name, and then automatically try to connect to them.

Hidden network

Set to Disabled

A router can be configured to hide its network name (SSID). Your router might incorrectly use “closed” to mean hidden, and “broadcast” to mean not hidden.

Hiding the network name doesn't conceal the network from detection or secure it against unauthorized access. And because of the way that devices search for and connect to Wi-Fi networks, using a hidden network might expose information that can be used to identify you and the hidden networks you use, such as your home network. When connected to a hidden network, your device might show a privacy warning because of this privacy risk.

To secure access to your network, use the appropriate [security setting](#) instead.

MAC address filtering, authentication, access control

Set to Disabled

When this feature is enabled, your router can be set up to allow only devices that have specified MAC (media access control) addresses to join the network. You shouldn't rely on this feature to prevent unauthorized access to your network, for these reasons:

- It doesn't prevent network observers from monitoring or intercepting traffic on the network.
- MAC addresses can easily be copied, spoofed (impersonated), or changed.
- To help protect user privacy, [some Apple devices use a different MAC address for each Wi-Fi network](#).

To secure access to your network, use the appropriate [security setting](#) instead.

Automatic firmware updates

Set to Enabled

If possible, set your router to automatically install software and firmware updates as they become available. These updates can affect the [security settings](#) available to you, and they deliver other important improvements to the stability, performance, and security of your router.

Radio mode


Set to All (preferred), or Wi-Fi 2 through Wi-Fi 6 or later

Radio mode settings, available separately for 2.4GHz, 5GHz, and 6GHz bands, control which versions of

the Wi-Fi standard the router uses for wireless communication. Newer versions offer better performance and support more devices concurrently.

It's usually best to enable every mode offered by your router, rather than a subset of those modes. All devices, including older devices, can then connect using the fastest radio mode they support. This also helps reduce interference from nearby legacy networks and devices.

Bands

 **Enable all bands supported by your router**

A Wi-Fi band is like a street over which data can flow. More bands provide more data capacity and performance for your network.


Channel

 **Set to Auto**

Each band of your router is divided into multiple, independent communication channels, like lanes in a street. When channel selection is set to automatic, your router selects the best Wi-Fi channel for you.

If your router doesn't support automatic channel selection, choose whichever channel performs best in your network environment. That varies depending on the [Wi-Fi interference](#) in your network environment, which can include interference from any other routers and devices that are using the same channel. If you have multiple routers, configure each to use a different channel, especially if they are close to each other.


Channel width

 **Set to 20MHz for the 2.4GHz band**
Set to Auto or all widths for 5GHz and 6GHz bands

Channel width specifies how large of a “pipe” is available to transfer data. Wider channels are faster but more susceptible to interference and more likely to interfere with other devices.

- 20MHz for the 2.4GHz band helps to avoid performance and reliability issues, especially near other Wi-Fi networks and 2.4GHz devices, including Bluetooth devices.
- Auto or all channel widths for 5GHz and 6GHz bands ensures the best performance and compatibility with all devices. Wireless interference is less of a concern in these bands.

DHCP

 **Set to Enabled**, if your router is the only DHCP server on the network

DHCP (dynamic host configuration protocol) assigns IP addresses to devices on your network. Each IP

address identifies a device on the network and enables it to communicate with other devices on the network and internet. A network device needs an IP address much like a phone needs a phone number.

Your network should have only one DHCP server. If DHCP is enabled on more than one device, such as on both your cable modem and router, address conflicts might prevent some devices from connecting to the internet or using network resources.


DHCP lease time

 Set to 8 hours for home or office networks; 1 hour for hotspots or guest networks

DHCP lease time is the length of time that an IP address assigned to a device is reserved for that device.

Wi-Fi routers usually have a limited number of IP addresses that they can assign to devices on the network. If that number is depleted, the router can't assign IP addresses to new devices, preventing those devices from communicating with other devices on the network and internet. Reducing DHCP lease time allows the router to more quickly reclaim and reassign old IP addresses that are no longer being used.

NAT

 Set to Enabled, if your router is the only device providing NAT on the network

NAT (network address translation) translates between addresses on the internet and addresses on your network. NAT can be understood by imagining a company's mail department, where deliveries to employees at the company's street address are routed to employee offices within the building.

Generally, enable NAT only on your router. If NAT is enabled on more than one device, such as on both your cable modem and router, the resulting "double NAT" might cause devices to lose access to certain resources on the network or internet.

WMM

 Set to Enabled

WMM (Wi-Fi multimedia) prioritizes network traffic to improve the performance of a variety of network applications, such as video and voice. All routers that support Wi-Fi 4 (802.11n) or later should have WMM enabled by default. Disabling WMM can affect the performance and reliability of devices on the network.

Device features that can affect Wi-Fi connections

These features might affect how you set up your router or the devices that connect to it.


Private Wi-Fi Address

If you're connecting to a Wi-Fi network from an iPhone, iPad, or Apple Watch, [learn about using private Wi-Fi addresses](#) on those devices.



Location Services

Make sure that your device has Location Services turned on for Wi-Fi networking, because regulations in each country or region define the Wi-Fi channels and wireless signal strength allowed there. Location Services helps to ensure that your device can reliably see and connect to nearby devices, and that it performs well when using Wi-Fi or features that rely on Wi-Fi, such as AirPlay or AirDrop.

On your Mac with macOS Ventura or later

1. Choose Apple menu  > System Settings, then click Privacy & Security in the sidebar.
2. Click Location Services on the right.
3. Scroll to the bottom of the list of apps and services, then click the Details button next to System Services.
4. Turn on "Networking and wireless", then click Done.

On your Mac with macOS Monterey or earlier

1. Choose Apple menu  > System Preferences, then click Security & Privacy.
2. Click the lock  in the corner of the window, then enter your administrator password.
3. In the Privacy tab, select Location Services, then select Enable Location Services.
4. Scroll to the bottom of the list of apps and services, then click the Details button next to System Services.
5. Select Networking & Wireless (or Wi-Fi Networking), then click Done.


On your iPhone or iPad

1. Go to Settings > Privacy & Security (or Privacy) > Location Services.
2. Turn on Location Services.
3. Scroll to the bottom of the list, then tap System Services.
4. Turn on Networking & Wireless (or Wi-Fi Networking).

Auto-Join when used with wireless carrier Wi-Fi networks

Wireless carrier Wi-Fi networks are public networks set up by your wireless carrier and their partners. Your iPhone or other Apple cellular device treats them as known networks and automatically connects to them.

If you see "Privacy Warning" under the name of your carrier's network in Wi-Fi settings, your cellular identity could be exposed if your device were to join a malicious hotspot impersonating your carrier's Wi-Fi network. To avoid this possibility, you can prevent your iPhone or iPad from automatically rejoining your carrier's Wi-Fi network:

1. Go to Settings > Wi-Fi.
2. Tap  next to the wireless carrier's network.
3. Turn off Auto-Join.

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. [Contact the vendor](#) for additional information.

Published Date: October 24, 2022

Helpful?

Yes

No



Related topics

[Erase your Mac and reset it to factory settings >](#)

[Update macOS on Mac >](#)

[Create a bootable installer for macOS >](#)



Start a discussion in Apple Support Communities

Ask other users about this article

[Submit my question](#)

[See all questions on this article >](#)



Contact Apple Support

Need more help? Save time by starting your support request online and we'll connect you to an expert.

[Get started >](#)



> Support > Recommended settings for Wi-Fi routers and access points

Copyright © 2022 Apple Inc. All rights reserved.

[Privacy Policy](#)

[Terms of Use](#)

[Sales and Refunds](#)

[Site Map](#)

United States