Adtran

Disabling Private MACs on Wi-Fi Devices

For optimal Intellifi™ operation and performance, Adtran recommends that where possible, Private or Randomized MAC features are disabled on all connected Wi-Fi devices. Disabling the private MAC feature on a device allows seamless connections to Intellifi without disrupting the effectiveness of network parental controls or creating inaccurate device usage and connection reports, incomplete activity logs, or misidentification of devices on the network.

Information and common questions about disabling these features, as well as the instructions for disabling the Private MAC or Randomized MAC setting on iOS or Android devices, are included in the following sections:

- *What is a Private or Randomized MAC, and Why Would I Use It?*
- *Is it Safe to Disable Private or Randomized MACs in my Home Network?*
- *How do I Disable Private MACs on my iOS Device?*
- *How do I Disable Randomized MACs on my Android Device?*

    NOTE: *The instructions describing how to disable the Private or Randomized MAC features on both iOS and Android devices are provided as examples for managing these features on typical Wi-Fi devices, and are not intended to represent every type of device, operating system, or feature management procedures available on Wi-Fi devices.*

What is a Private or Randomized MAC, and Why Would I Use It?

Private media access control (MAC) addresses are used as a security measure when Wi-Fi devices are accessing public networks. A MAC address is the unique identifier associated with the hardware of your Wi-Fi device, and is broadcast when your device is scanning for available Wi-Fi networks or connecting to a network. Because this unique identifier is broadcast across the network, if it is not hidden in some way, then the information broadcast can potentially allow tracking and profiling of a Wi-Fi user's movements and behavior, based on the MAC address.

Many operating systems and Wi-Fi device manufacturers have implemented the use of randomized MACs (or MAC randomization) functionality to mitigate privacy concerns when using public networks. In most cases, this feature is enabled by default. When enabled, the feature allows devices to generate a random MAC address that changes periodically (typically with each Wi-Fi connection attempt or network scan). This randomized address provides a MAC address that is private, in that it masks the permanent MAC address associated with the Wi-Fi device and keeps it safe during these network-related activities.

Adtran highly recommends that randomized MACs (or private MACs) are used when connecting to public Wi-Fi networks, although these private MACs should be disabled for use with your in-home Intellifi network. When private MACs are disabled for use with your in-home Intellifi network, they are done so on a per-network (SSID) basis, so access settings for public Wi-Fi networks will not be affected by the change to your home network MAC address settings.

# Is it Safe to Disable Private or Randomized MACs in my Home Network?

Yes, it is safe to disable the Private or Randomized MAC features on your Wi-Fi device when connecting to your home network. Disabling Private or Randomized MAC addresses is performed on a per-Wi-Fi network basis (SSID), so when you are connecting to your local home Wi-Fi network, there is no inherent risk associated with disabling these features.

In fact, randomized MAC addresses can interfere with parental controls that rely on MAC address filtering or monitoring by disrupting the effectiveness of the controls that track user devices locally, leading to inaccurate reporting, incomplete activity logs, or misidentification of devices. When using parental controls, on the Intellifi home network, disabling Private and Randomized MAC features provides a better and more reliable connection and management experience for your home network.

How do I Disable Private MACs on my iOS Device?

By default, iOS devices always use the Private MAC feature. To disable this feature when using your iOS device with Intellifi, follow these steps:

1. On your device, open the **Settings** app and select **Wi-Fi**.

2. Then, for iPhones, iPads, or iPods, select the **More Info** button next to your home network. For Apple watches, select the name of your home network from the list.

3. Toggle the **Private Wi-Fi Address** switch from right to left to disable the Private MAC address feature.
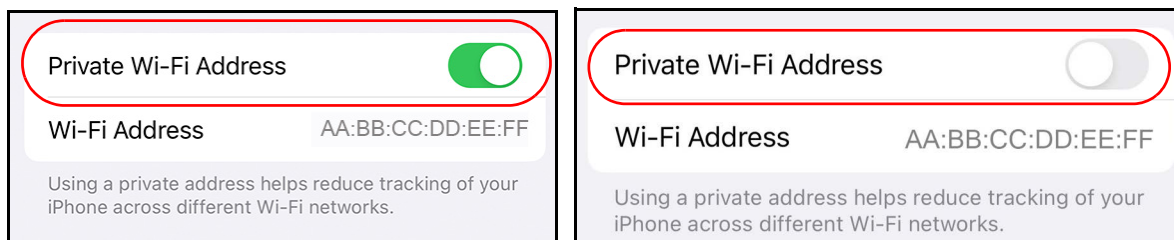
4. To re-enable this feature, toggle the **Private Wi-Fi Address** switch from left to right.

   *NOTE: When the **Private Wi-Fi Address** feature is enabled or disabled, your device will disconnect from the network briefly, and then reconnect as normal.*

How do I Disable Randomized MACs on my Android Device?

By default, most Android devices always use the Randomized MAC feature. To disable this feature when using your Android device with Intellifi, follow these steps:

1. On your device, open the **Settings** app.

2. Next, select **Connections** and then **Wi-Fi**.

3. Then, select the gear icon next to the name of your home network.

4. In the settings for this network, find the **MAC address type** menu item.

   *NOTE: You may have to select **View More** at the bottom of the menu to see this setting.*

5. Tap the **MAC address type** option and then tap the **Phone MAC** option to disable the Randomized MAC feature and use the device's native MAC address.
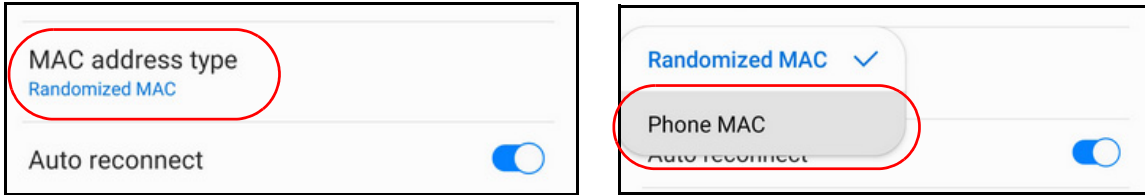
6. To re-enable this feature, tap the **MAC address type** option again and select **Randomized MAC**.