purple

MAC Randomization Checklist

Checklist for Adapting to iOS 18 and macOS 15 MAC Randomization

September 2024

❑ 1. Understand the Changes

- Review the changes in iOS 18 & macOS 15 regarding MAC address randomization:
  - Rotating MAC addresses every 14 days for open or less secure WiFi networks.
  - Fixed MAC addresses for secure WiFi networks (e.g., WPA2/WPA3).
- Identify how these changes impact your specific network operations and guest WiFi provision.

❑ 2. Assess Your Current Network Environment

- Identify all WiFi networks under your control including those for both your infrastructure, visitors and staff.
- Determine which WiFi networks rely on MAC addresses for authentication, access control, analytics, or monitoring.
- Evaluate if these WiFi networks use open or less secure protocols that will trigger frequent MAC rotations.
- Check your hardware types to see what functionality this supports.

❑ 3. Update Authentication methods

- Add Apple ID log in to your authentication methods - this allows Apple users to more easily re-authenticate using biometric information such as their face or fingerprint.
- To do this, ensure you have whitelisted the required domains on your controller/AP settings - you can find these here. Simply select your hardware type and scroll down to “Apple ID”. Once done, edit your splash page and add the Apple ID authentication method. Full instructions are available here.

❑ 4. Add a profile installation to your access journey or app

- Profiles are a settings file containing information on how to connect to a specific WiFi network, which includes the network type, credentials and connection preferences.
- Devices will recognize and connect to a WiFi network without the end user having to manually connect to it, even if they have never connected to it before. After the profile is installed, the device will securely and seamlessly connect to the network when it is within range - without any user interaction.
- To enable users to download a profile via your brand mobile app, fill in this form to speak to one of our experts about SecurePass.
- Purple will soon allow profile installation via web, and will send more information about this soon.

❑ 5. Consider changing your SSID to a secure SSID

- All customers can set up a secure WiFi network with a WPA2/WPA3 key for their guests, and modify the splash page on their their open network to advertise the secure network and key.
- We recommend broadcasting a secure SSID so that customers benefit from the network effect of only needing users to connect once.
- For this, the end user will connect to the SSID on their first visit to a supported venue, and thereafter be automatically connected. Because this is classed as a 'private' and secure network, the MAC address should not change as the default Private MAC address option will default to 'Fixed' on the SSID rather than 'Rotating'.
- However, Apple could change this in future versions to also rotate, so this is not seen as a long term solution.
- This is a controller/AP side configuration change.
- For Purple customers, please contact our support team here for help with changing your SSID.

❑ 6. Prepare for Future Updates

- Purple is a member of industry groups such as the WBA, and we'll keep you informed of any updates so please check back periodically for new information.

To view our latest webinar and other iOS or mac OS information click here.
To learn about Purple's SecurePass solution to the recent changes click here.

Mac Randomization Checklist

Want to find out more?
Speak to an expert **here**

purple