Release Note

Important Notice:
This firmware upgrade is irreversible. Contact support if issues are encountered after the firmware upgrade.

Version Info:

1. **Firmware Version:** 1.3.6 Build 20260306 Rel. 14246
2. **Applied Model:** EAP673-Extender v1.20
3. **Minimum FW Version for Update**: 1.1.6 Build 20260306 Rel. 11532
4. **Fully Adapted Omada Controller version:** 6.0.
5. **Fully Adapted Omada App version:** 5.0.
6. For downloading any firmware version, please refer to Omada Download Center.

New Features:

1. Added support for Prohibit Wi-Fi Sharing.
2. Added support for GRE Tunnel.
3. Added support for PPSK By GRE Tunnel.
4. Added support for multiple RADIUS servers in PPSK deployments.
5. Added support for Bluetooth Location and iBeacon.
6. Added support for refined encryption suites to enable WPA3-only mode.
7. Added support for IP address renewal after gateway replacement.
8. Added support for HTTPS redirection of the Portal page.
9. Added support for LDAP authentication in MAC Authentication.
10. Added support for Hotspot 2.0.
11. Added support for PPSK over GRE Tunnel.
12. Added support for disabling the Reset button in Controller mode.
13. Added support for RADIUS Login/Log Off and CHAP authentication in Standalone mode.
14. Added support for VLAN Pool.
15. Added support for Non-Stick Roaming and Ping-Pong Roaming Suppression.
16. Added support for client identification.
17. Added support for configuring WPA3-Enterprise SSIDs in Standalone mode.
18. Added support for configuring the DNS adoption toggle on the Standalone web UI.

Enhancements:

1. Optimized overall system stability.
2. Optimized LLDP function by adding device power information.
3. Optimized SNMPv3 configuration support in Controller mode.
4. Optimized troubleshooting by enabling over-the-air packet capture.

Bug Fixed:

1. Fixed an issue where accounting packets could not be sent after 802.11r roaming when PPSK with RADIUS and MAC Binding was enabled.
2. Fixed an issue where the device could go offline in certain scenarios.
3. Fixed a security vulnerability in the RADIUS protocol.
4. Fixed a memory leak issue in certain scenarios.

Additional Information:

1. Adapted to the new Omada VI.
2. Adapted for RED Certification.