Release Note

Important Notice:

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

Version Info:

1. Firmware Version: 1.5.0 Build 20260629 Rel. 13902.

2. Applied Model: EAP603-Outdoor 1.0/1.6

3. Minimum FW Version for Update: 1.0.1 Build 20250320 Rel. 41321.

4. Recommended Omada Controller version: 6.1.

5. Recommended Omada App version: 5.1.

6. For downloading any firmware version, please refer to Omada Download Center .

New Features:

1. Added Support for configuration of WPA3 Enterprise on the Standalone page.
2. Added Support for configuration of DNS adoption switch (Remote Adoption) on the Standalone page.
3. Added Support for RadSec in RADIUS authentication.
4. Added support for the Platform Debug Tool.
5. Added Support for RRM (Radio Resource Management) Optimization.
6. Added Support for secure firmware download strategy.
7. Added Support for WPA3-Enterprise with 802.11r.
8. Added Support for expiration and bandwidth configuration for PPSK without RADIUS mode.
9. Added Support for verifying the "message-authenticator" attribute of the RADIUS server.

Enhancements:

1. Enhanced device security.
2. Optimized ACS Mechanism.
3. Optimized synchronization mechanism.
4. Optimized automatic adoption mechanism.
5. Optimized automatic bandwidth selection mechanism.
6. Optimized background scanning mechanism.
7. Optimized VLAN implementation mechanism.
8. Optimized Log reporting mechanism, adding related logs such as DFS, CPU and memory utilization.
9. Optimized DFS switching mechanism and radar wave conflict handling.
10. Optimized FDB table management mechanism.

11. Optimized CoA-ACK/NAK message cache mechanism.
12. Optimized verification rules for the static IP configuration items on the standalone page.
13. Optimized site URL validation rules.

Bug Fixed:

1. Fixed an issue where NAT scenario adoption failed during device management state redirection.
2. Fixed an issue where the mesh APs frequently became the isolated state.
3. Fixed an issue where the ACL configuration might be lost in some scenarios.
4. Fixed an issue where unauthenticated clients might fail the portal authentication.
5. Fixed an issue where configuration might be lost in cluster mode under specific scenarios.

Additional Information:

1. Adapted to the RED certification requirement.