Release Note

Version Info:

1. **Firmware Version:** 1.5.6 Build 20260629 Rel. 20690.
2. **Applied Model:** EAP650 v3.0/v3.6.
3. **Minimum FW Version for Update**: 1.4.3 Build 20251128 Rel. 59259.
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 WPA3-Enterprise configuration in Standalone mode.
2. Added support for a Remote Adoption switch in DNS Adoption configuration in Standalone mode.
3. Added support for the Secure Firmware Download Policy.
4. Added support for the Platform Debug Tool.
5. Added support for RadSec (RADIUS over TLS) for RADIUS authentication.
6. Added support for RRM (Radio Resource Management) optimization.
7. Added support for 802.11r in WPA3-Enterprise deployments.
8. Added support for Expiration and Bandwidth Control settings for PPSK without RADIUS configurations.

Enhancements:

1. Optimized the validation rules for static IP configuration in the Standalone web interface.
2. Optimized the ACS mechanism.
3. Optimized the configuration synchronization mechanism.
4. Optimized the handling of automatic adoption failures.
5. Optimized the automatic bandwidth selection mechanism.
6. Optimized the background scanning mechanism.
7. Optimized the VLAN implementation mechanism.
8. Optimized the log reporting mechanism and added logs related to DFS events, CPU utilization, and memory utilization.
9. Optimized DFS channel switching and radar event conflict handling.
10. Optimized FDB table management by clearing wireless client connection information when FDB entries change.
11. Optimized the cache mechanism for CoA-ACK/NAK messages.
12. Optimized the Radius Profile implementation mechanism.
13. Optimized the deployment configuration application process.

Bug Fixed:

1. Fixed an issue where device adoption through redirection could fail in NAT environments while the device was under management.
2. Fixed an issue where the device was vulnerable to the BlastRADIUS attack, and added a Message-Authenticator attribute validation option.
3. Fixed an issue where Mesh APs could frequently enter the isolated state.

4. Fixed an issue where the last 48 bits of the UUID were incorrectly set to zero when sending UUID information during DHCPv6 dialing.
5. Fixed an issue where ACL configurations could be lost in certain scenarios.
6. Fixed an issue where unauthenticated Portal clients could not receive PMTUD (Path MTU Discovery) packets, potentially causing Portal authentication failures due to MTU mismatches.
7. Fixed an issue where configurations could be lost under certain special conditions in Cluster Mode.
8. Fixed an issue where Site URL validation rules prevented CBC Site URLs from being successfully applied on the device.