Release Note

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

Version Info:

1. **Firmware Version:** 1.5.6 Build 20260629 Rel. 20690
2. **Applied Model:** EAP653 UR v1.0/v1.20/v1.26/v1.6
3. **Minimum FW Version for Update**: 1.4.2 Build 20251208 Rel. 43830
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 the 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 updated validation rules for static IP configuration in Standalone mode.
6. Added support for RadSec (RADIUS over TLS) for RADIUS authentication.
7. Added support for RRM (Radio Resource Management) optimization.
8. Added support for 802.11r in WPA3-Enterprise deployments.
9. Added support for Expiration and Bandwidth Control settings for PPSK without RADIUS configurations.

Enhancements:

1. Optimized the ACS mechanism.
2. Optimized the configuration synchronization mechanism.
3. Optimized the auto-adoption failure handling mechanism.
4. Optimized the automatic bandwidth selection mechanism.
5. Optimized the background scanning mechanism.
6. Optimized the VLAN implementation mechanism.
7. Optimized the log reporting mechanism and added logs related to DFS, CPU utilization, and memory utilization.
8. Optimized the DFS channel switching mechanism and radar event handling.
9. Optimized the FDB table management mechanism by clearing wireless connection information when FDB entries change.
10. Optimized the CoA-ACK/NAK packet caching mechanism.
11. Optimized the Radius Profile implementation mechanism.
12. 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.