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:** EAP650 v2.0
3. **Minimum FW Version for Update**: 1.0.0 Build 20230113 Rel. 32625
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 encrypted configuration file import and export.
2. Added support for configuring WPA3-Enterprise on the Standalone Mode.
3. Added support for configuring the DNS Adoption switch on the Standalone Mode.
4. Added support for the EAP CLI command.
5. Added support for a secure firmware download policy.
6. Added support for new debugging tool.
7. Added support Radsec for Radius Authentication.
8. Added support 802.1x.
9. Added support configuring expiration and bandwidth for PPSK without Radius.
10. Added support 802.11r for wpa3-enterprise mode.
11. Added support RRM optimization feature.

Enhancements:

1. Optimized the Auto Channel Selection mechanism.
2. Optimized the configuration synchronization mechanism.
3. Optimized the auto-adoption failure handling.
4. Optimized the automatic bandwidth selection mechanism.
5. Optimized the background scanning mechanism.
6. Optimized the VLAN implementation mechanism.
7. Optimized log reporting and added logs related to DFS, CPU usage, and memory utilization.
8. Optimized the DFS switching mechanism and radar interference handling.
9. Optimized the FDB table management mechanism to clear wireless association information when FDB changes.
10. Optimized the CoA-ACK/NAK message caching mechanism.
11. Enhanced overall security.
12. Enhanced validation rules for static IP configuration on the Standalone Mode.
13. Enhanced default security policies for SSID in factory settings. .

Bug Fixed:

1. Fixed an issue where device adoption failed under NAT scenarios when redirection occurred in managed mode.
2. Fixed an issue where the Blast RADIUS security vulnerability could be exploited.
3. Fixed an issue where mesh APs might frequently enter the isolated state.
4. Fixed an issue where the last 48 bits of the UUID sent during DHCPv6 dialing were set to 0.
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 packets, potentially causing portal authentication failure due to MTU mismatch.
7. Fixed an issue where configuration loss occurred in some special scenarios in cluster mode.
8. Fixed an issue where siteUrl validation rules prevented the CBC siteUrl from being successfully applied on the device.

Additional Information:

1. Adapted to meet RED certification requirements..