



Release Note

Edgecore EAP101 Release v12.5.97

Document # EAP101-v12.5.97-1616-e16697005-b2b20e4

Enhancement from v12.5.96-1562-37fd8aa7b-bbdbfbc

Table of Contents

1	Feature.....	3
1.1	Support RadSec Client Certificate Management.....	3
1.2	Support WireGuard VPN	3
1.3	Support Ping Watchdog	3
1.4	Support RTTY Remote Console.....	3
1.5	Band Steering and Minimum Signal Conflict Warning	3
2	Issue Fixed	4
2.1	AP Self-Rebooted Due to Offload Firmware Crash.....	4
2.2	Force DHCP Bypassed by Static IP Clients	4
2.3	Connected SSID Shows "null" in Dashboard for Client Mode Device.....	4
2.4	Memory Usage Continues to Increase	4
2.5	Network Connectivity Lost After Firmware Upgrade	4
3	Known Issue.....	5
3.1	The connection of Microsoft surface laptop is unstable using WPA2-PSK SSID.....	5
3.2	The SSID compatible issue in Windows 10 devices with the specific ethernet card.	5
3.3	The dynamic VLAN is not supported in the mesh network.	5
3.4	There is a low probability that the mesh connection can't recover after MAP is re-configured.	5
3.5	Authport with VLAN tagged does not support on IOS device.....	5
3.6	When upgrading the FW from 12.0.0, Hotspot controlled SSID can only work after an additional reboot.	5
3.7	The captive portal cannot be popped up sometimes in the open roaming SSID.	5
3.8	Clients may fail to connect immediately after AP boot.....	5
4	Compatible Version for AP Management	6

1 Feature

1.1 Support RadSec Client Certificate Management

Added RadSec (RADIUS over TLS) client certificate management to the wireless configuration interface. Administrators can now upload CA certificates, client certificates, and private keys through either the local web UI or ecCLOUD. The feature supports per-SSID RadSec enable/disable for both authentication and accounting servers, with certificates shared across all SSIDs.

1.2 Support WireGuard VPN

Added WireGuard VPN tunnel support. Administrators can configure WireGuard interfaces with custom allowed IPs to selectively route traffic through the VPN tunnel while keeping other traffic on the default path. The feature includes a local web UI for standalone configuration and ecCLOUD integration for cloud-managed deployments.

1.3 Support Ping Watchdog

Added a Ping Watchdog feature that monitors network connectivity by periodically pinging a configured IP address. If consecutive ping failures exceed the configured threshold, the AP automatically reboots to recover connectivity. A failover IP address can be configured to prevent unnecessary reboots when the primary target is temporarily unreachable. The feature is configurable via the local web UI and ecCLOUD.

1.4 Support RTTY Remote Console

Added RTTY (Real-Time Terminal) support enabling administrators to access a remote console session to the AP directly from the ecCLOUD dashboard. The feature uses a secure TLS connection with certificate-based authentication to the RTTY server. Multiple session management, idle timeout, and device disconnect handling are supported.

1.5 Band Steering and Minimum Signal Conflict Warning

Added a non-blocking inline warning in the Wireless Settings UI when both Band Steering and Minimum Signal Allowed are enabled simultaneously. This combination may cause repeated client disconnections and increased AP CPU load. The warning is displayed in real-time as settings change, without preventing the administrator from saving the configuration.

2 Issue Fixed

2.1 AP Self-Rebooted Due to Offload Firmware Crash

Fixed an issue where the access point could unexpectedly reboot due to a Qualcomm wireless offload firmware crash. The firmware recovery mechanism now properly handles the crash and restores wireless service without requiring a full system reboot.

2.2 Force DHCP Bypassed by Static IP Clients

Fixed an issue where clients could bypass the Force DHCP security feature by first obtaining a DHCP address and then switching to a static IP. The DAI (Dynamic ARP Inspection) entry update algorithm has been corrected to prevent IP record overwriting, ensuring static IP clients are properly blocked when Force DHCP is enabled.

2.3 Connected SSID Shows "null" in Dashboard for Client Mode Device

Fixed an issue where the ecCLOUD dashboard displayed "Radio #0: null" for devices connected via client mode. The system now correctly resolves and displays the SSID name for client mode connections.

2.4 Memory Usage Continues to Increase

Fixed a memory leak issue where memory usage would gradually increase over time during normal operation. The issue has been resolved in this release.

2.5 Network Connectivity Lost After Firmware Upgrade

Fixed an issue where the AP could lose network connectivity after a firmware upgrade, particularly when upgrading across major versions.

3 Known Issue

3.1 The connection of Microsoft surface laptop is unstable using WPA2-PSK SSID.

3.2 The SSID compatible issue in Windows 10 devices with the specific ethernet card.

Using Intel AX200 (old version) or Realtek RTL8822BE with Windows 10 devices, the ping connection is randomly disconnected if the devices are connected to the SSID.

Note that there is no connection issue if the driver of Intel AX200 is updated to 22.60.0.6 or later version.

3.3 The dynamic VLAN is not supported in the mesh network.

3.4 There is a low probability that the mesh connection can't recover after MAP is re-configured.

In mesh topology, after MAP reboots or reconfigures the network configuration, there is a low probability that it takes a long time (~30mins) to rebuild the mesh connection. After rebooting all the AP, the mesh connection recovers.

3.5 Authport with VLAN tagged does not support on IOS device.

3.6 When upgrading the FW from 12.0.0, Hotspot controlled SSID can only work after an additional reboot.

3.7 The captive portal cannot be popped up sometimes in the open roaming SSID.

3.8 Clients may fail to connect immediately after AP boot.

After an AP reboot and Force DHCP enabled, the wireless SSID may become visible to clients before internal services and configuration are fully initialized. Clients that attempt to connect during this window may experience authentication failures or fail to obtain an IP address.

Workaround: Wait approximately 5 minutes after the AP boots before connecting WiFi clients.

4 Compatible Version for AP Management

Compatible with ecCLOUD

Compatible with EWS-Series controller v3.91.0000 or later