



Release Note

Edgecore EAP104 Release v12.5.97

Document # EAP104-v12.5.97-1616-e16697005-b2b20e4

Enhancement from v12.5.9-1457-f754fbff3-d427326

Table of Contents

1	Feature.....	4
1.1	Support LAN PoE Out (Only for EAP104)	4
1.2	Support Wedge IPv6	4
1.3	Support Offload FW Recovery Version	4
1.4	Support RadSec Client Certificate Management.....	4
1.5	Support WireGuard VPN	5
1.6	Support Ping Watchdog	5
1.7	Support RTTY Remote Console.....	5
1.8	Band Steering and Minimum Signal Conflict Warning	5
2	Issue Fixed	6
2.1	The client cannot connect to the Internet after connecting to the AuthPort SSID.	6
2.2	When upgrading the AP to a newer version, it shows that the uploaded firmware is older than the current version.	6
2.3	The client cannot be automatically removed after exceeding the idle timeout.	6
2.4	The logout event on the AuthPort activity page doesn't reflect the actual logout time.	6
2.5	The customize service schedule is not working properly.	6
2.6	The SNMP service doesn't have a response sometimes.....	6
2.7	Limit Upload for SSID is not working when the SSID network behavior is Hotspot controlled.....	6
2.8	Devices establish WDS, but AP mode did not display connection information in the wireless status dashboard.....	7
2.9	The network connection becomes unstable when a large number of ARP packets exist in the network environment.	7
2.10	The client cannot connect to the Internet after connecting to the AuthPort SSID.	7
2.11	When upgrading the AP to a newer version, it shows that the uploaded firmware is older than the current version.	7
2.12	The client cannot be automatically removed after exceeding the idle timeout.	7
2.13	The logout event on the AuthPort activity page doesn't reflect the actual logout time.	7
2.14	The customize service schedule is not working properly.	8
2.15	The SNMP service doesn't have a response sometimes.....	8
2.16	Limit Upload for SSID is not working when the SSID network behavior is Hotspot controlled.....	8
2.17	Devices establish WDS, but AP mode did not display connection information in the wireless status dashboard.....	8
2.18	The Force DHCP function is not operational.....	8
2.19	The network connection becomes unstable when a large number of ARP packets exist in the network environment.	8
2.20	The hotspot throughput of the LAN port is lower than expected.....	8

2.21	SNMP service monitor may reload the SNMP daemon periodically and cause memory leak.....	8
2.22	Hotspot captive portal does not pop up when client connects to the SSID.....	9
2.23	Force DHCP doesn't work properly.....	9
2.24	The UDP packet continues to be sent when band steering is enabled.	9
2.25	Force DHCP Bypassed by Static IP Clients	9
2.26	Connected SSID Shows "null" in Dashboard for Client Mode Device.....	9
2.27	Memory Usage Continues to Increase	9
2.28	Network Connectivity Lost After Firmware Upgrade	9
3	Known Issue.....	11
3.1	The connection of Microsoft surface laptop is unstable using WPA2-PSK SSID.....	11
3.2	The SSID compatible issue in Windows 10 devices with the specific ethernet card.	11
3.3	The dynamic VLAN is not supported in the mesh network.	11
3.4	There is a low probability that the mesh connection can't recover after MAP is re-configured.	11
3.5	Authport with VLAN tagged does not support on IOS device.....	11
3.6	When upgrading the FW from 12.0.0, Hotspot controlled SSID can only work after an additional reboot.	11
3.7	The captive portal cannot be popped up sometimes in the open roaming SSID.	11
3.8	Clients may fail to connect immediately after AP boot.....	11
4	Compatible Version for AP Management	12

1 Feature

1.1 Support LAN PoE Out (Only for EAP104)

The LAN PoE Out setting now provides an On option in addition to Auto and Off. Auto enables PoE Out only when the AP detects an 802.3at PoE power source, which is not always reliable with third-party PoE switches. With On, PoE Out is always enabled so the connected device stays powered.

Ethernet Settings

Ethernet Port #0	Ethernet Port #1	Ethernet Port #2	Ethernet Port #3	Ethernet Port #4
Network Behavior Route to Internet ▼				
Network Name Default local network ▼				
CAPWAP Tunnel Interface Disable ▼				
PoE Out On ▼				

1.2 Support Wedge IPv6

Support IPv6 ports for Wedge Security Service Add-on IPv6 traffic scanning.

1.3 Support Offload FW Recovery Version

Added support for offload firmware recovery version. When the AP encounters a firmware failure, the recovery mechanism can now restore the device using the offload recovery image. In this version, the feature has been implemented.

1.4 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.

1.5 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.

1.6 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.

1.7 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.

1.8 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 The client cannot connect to the Internet after connecting to the AuthPort SSID.

The client connects to the AuthPort SSID. After entering the correct username and password, the client cannot connect to the Internet. In this version, the client can connect to the Internet successfully.

2.2 When upgrading the AP to a newer version, it shows that the uploaded firmware is older than the current version.

On the System > Maintenance page, when upgrading the firmware to a new version, an error message shows that the uploaded firmware is older than the current version. The keep current settings after upgrade button will be disabled forcibly. In this version, the firmware can be uploaded to the AP successfully without an error message.

2.3 The client cannot be automatically removed after exceeding the idle timeout.

The clients remain connected to the SSID even past the idle timeout. In this version, the client can be removed automatically.

2.4 The logout event on the AuthPort activity page doesn't reflect the actual logout time.

The client connects to the AuthPort SSID. When the client logs out, the logout event on the AuthPort activity page is incorrect. In this version, the logout event displays normally.

2.5 The customize service schedule is not working properly.

Create the service schedule on the controller and assigned it to the AP, but it's not working properly. In this version, the issue has been resolved.

2.6 The SNMP service doesn't have a response sometimes.

The SNMP service sometimes fails to respond. In this version, the issue has been resolved.

2.7 Limit Upload for SSID is not working when the SSID network behavior is Hotspot controlled.

The 'Limit Upload' setting for the SSID is not working when the network behavior is set to

'Hotspot controlled'. In this version, the issue has been resolved.

2.8 Devices establish WDS, but AP mode did not display connection information in the wireless status dashboard.

In prior versions, despite devices establishing WDS, the AP mode did not show connection information within the wireless status. This issue has been rectified in the current version, and the wireless status dashboard now accurately displays client information.

2.9 The network connection becomes unstable when a large number of ARP packets exist in the network environment.

A large number of ARP packets in the network cause an unstable connection and high CPU load. In this version, the issue has been resolved.

2.10 The client cannot connect to the Internet after connecting to the AuthPort SSID.

The client connects to the AuthPort SSID. After entering the correct username and password, the client cannot connect to the Internet. In this version, the client can connect to the Internet successfully.

2.11 When upgrading the AP to a newer version, it shows that the uploaded firmware is older than the current version.

On the System > Maintenance page, when upgrading the firmware to a new version, an error message shows that the uploaded firmware is older than the current version. The keep current settings after upgrade button will be disabled forcibly. In this version, the firmware can be uploaded to the AP successfully without an error message.

2.12 The client cannot be automatically removed after exceeding the idle timeout.

The clients remain connected to the SSID even past the idle timeout. In this version, the client can be removed automatically.

2.13 The logout event on the AuthPort activity page doesn't reflect the actual logout time.

The client connects to the AuthPort SSID. When the client logs out, the logout event on the AuthPort activity page is incorrect. In this version, the logout event displays normally.

2.14 The customize service schedule is not working properly.

Create the service schedule on the controller and assigned it to the AP, but it's not working properly. In this version, the issue has been resolved.

2.15 The SNMP service doesn't have a response sometimes.

The SNMP service sometimes fails to respond. In this version, the issue has been resolved.

2.16 Limit Upload for SSID is not working when the SSID network behavior is Hotspot controlled.

The 'Limit Upload' setting for the SSID is not working when the network behavior is set to 'Hotspot controlled'. In this version, the issue has been resolved.

2.17 Devices establish WDS, but AP mode did not display connection information in the wireless status dashboard.

In prior versions, despite devices establishing WDS, the AP mode did not show connection information within the wireless status. This issue has been rectified in the current version, and the wireless status dashboard now accurately displays client information.

2.18 The Force DHCP function is not operational.

When the SSID was created and ARP inspection and Force DHCP were enabled, the static client can connect to the SSID successfully. This issue has been resolved in this firmware version.

2.19 The network connection becomes unstable when a large number of ARP packets exist in the network environment.

A large number of ARP packets in the network cause an unstable connection and high CPU load. In this version, the issue has been resolved.

2.20 The hotspot throughput of the LAN port is lower than expected.

While throughput was previously lower than expected when the LAN port was configured as a 'hotspot-controller,' this issue has been resolved in the current version.

2.21 SNMP service monitor may reload the SNMP daemon periodically and cause memory leak.

A memory leak has been identified in the SNMP process when using a non-public read community string with SNMP traps enabled. The issue has been resolved in this version.

2.22 Hotspot captive portal does not pop up when client connects to the SSID.

When a client connects to an SSID configured with Hotspot captive portal, the captive portal page does not automatically pop up on the client device. The client connects to the SSID successfully but is not redirected to the login or splash page, preventing guest authentication from completing. In this version, the issue has been resolved.

2.23 Force DHCP doesn't work properly.

When ARP inspection and Force DHCP are enabled on the AP, both wireless clients and devices connected to the LAN port lose Internet access. The issue occurs when the AP is configured to carry VLAN tagged traffic. Prior to enabling Force DHCP, all clients can obtain IP addresses and access the Internet normally. In this version, the issue has been resolved.

2.24 The UDP packet continues to be sent when band steering is enabled.

When band steering is enabled, the UDP packets will be sent continuously from the AP. In this version, no UDP packets will be sent.

2.25 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.

2.26 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.

2.27 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.

2.28 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