



Release Note

Edgecore EAP105 Release v12.6.15

Document # EAP105-v12.6.15-3206-a7cea89f2-fa8e21a

Enhancement from v12.6.13-3130-81bc87a36-b8ff7ea

Table of Contents

1	Feature.....	3
1.1	Support RadSec.....	3
1.2	Support IPv6 Disabled	3
1.3	Support LAN port upload and download rate limit.....	3
1.4	Support Web Filter	3
1.5	Support Vietnam regulatory domain	3
1.6	Support SHA authentication and AES privacy for SNMPv3.....	4
1.7	Uplink Self-Diagnostic panel on the Dashboard	4
1.8	Warning when Band Steering and Minimum signal allowed are both enabled.....	4
2	Issue Fixed	5
2.1	Client count shows incorrect users after upgrading the firmware	5
2.2	Unstable communication when many wireless clients are connected under heavy multicast load.....	5
2.3	Web UI accepted AIFS value 0 in WME Configure, taking both radios down.....	5
2.4	False 'Network diagnostics detected connectivity issues: FAIL' alert.....	5
2.5	RRM threshold after upgrade did not follow the highest Interference Detection value	5
2.6	Client signal strength reported as -95 dBm, causing Minimum signal allowed to disconnect a nearby client.....	6
2.7	Cloud agent could stay offline indefinitely when the TLS handshake with the cloud stalled	6
3	Known Issue.....	7
3.1	The WDS link is not established if the wireless security is no security.	7
3.2	ARP resolution failure to GW when ARP Inspection is enabled.....	7
3.3	802.11r Fast Roaming May Fail or Be Delayed on Some Client Devices	7
4	Compatible Version for AP Management	8

1 Feature

1.1 Support RadSec

RADIUS over TLS (RadSec) can now be used with a CA certificate, a client certificate and a client private key installed on the access point, so the AP can authenticate to RADIUS servers that require mutual TLS, such as ISP authentication relay servers.

On a standalone AP the certificate set is uploaded from the Wireless Settings page (RadSec Certificate). The same certificate set is shared by all SSIDs. On a cloud-managed AP the certificates are downloaded from the URLs pushed by ecCLOUD. RadSec (Auth) and RadSec (Acct) are enabled per SSID with default port 2083; enabling RadSec without an installed certificate is blocked with a warning. The installed certificates survive a firmware upgrade.

1.2 Support IPv6 Disabled

IPv6 can now be disabled on the access point. In the local UI, Network > Internet > IPv6 Settings, the IP Address Mode selector offers a new Disable option in addition to DHCP and Static IP. When Disable is selected the AP no longer acquires or uses IPv6 addresses on its management interfaces.

1.3 Support LAN port upload and download rate limit

Per-port rate limiting is now available for the Ethernet LAN ports. In Network > Ethernet Settings each port tab offers Limit Upload and Limit Download switches with a rate. Traffic of devices connected to that port is shaped to the configured rates.

1.4 Support Web Filter

A Web Filter is now available under Network > Web Filter. Up to four filter profiles can be created, each holding a list of blocked domains or IP addresses. A profile can be applied to any SSID (Wireless > SSID edit > Network Settings > Web Filter Profile) or to an Ethernet LAN port, independently of the captive portal setting. Domains in a profile are resolved and blocked for the clients on that SSID or port.

1.5 Support Vietnam regulatory domain

Vietnam (VN) is now supported as a country setting on AP. When the country is set to Viet Nam the AP applies the Vietnamese channel plan and transmit power limits: 2.4 GHz channels 1-13, and 5 GHz channels 36-64, 100-140 and 149-165.

1.6 Support SHA authentication and AES privacy for SNMPv3

SNMPv3 users can now be configured with SHA as the authentication protocol and AES as the privacy (encryption) protocol, in addition to MD5 and DES. The options are available in the SNMP settings of the local UI. Existing SNMPv3 users configured with MD5/DES continue to work unchanged.

1.7 Uplink Self-Diagnostic panel on the Dashboard

The local UI Dashboard (General Status) now includes a Diagnostic Analysis panel. The AP diagnoses its own uplink, from the WAN configuration and link state, through DHCP/PPPoE, duplicate IP and subnet overlap checks, to gateway, Internet, DNS and cloud controller reachability, and shows in plain language where the uplink breaks and what to try first, without SSH access. A notice band above the Dashboard tabs highlights CRITICAL/WARNING results, and a diagnostic report can be downloaded for support. The diagnostic is read-only and does not change any configuration; nothing is uploaded to the cloud.

1.8 Warning when Band Steering and Minimum signal allowed are both enabled

Enabling Band Steering together with a per-SSID Minimum signal allowed threshold can make the two mechanisms work against each other, causing repeated client disconnections, extra AP CPU load and degraded roaming. The Wireless Settings page now shows an advisory warning directly below the Band Steering toggle when Band Steering is on and at least one enabled SSID on the same radio has a Minimum signal allowed threshold configured: 'Please configure this with caution. Band steering may conflict with Minimum Allowed Signal threshold, and it can also increase AP CPU loading and affect client connectivity and roaming behavior.' The warning is informational and does not block saving.

2 Issue Fixed

2.1 Client count shows incorrect users after upgrading the firmware

After a firmware upgrade or a configuration push from ecCLOUD, the 2.4 GHz and 5 GHz client counts reported to the cloud could suddenly rise to a lot of clients, although far fewer clients were actually connected. Clients that had left were never removed from the list. The periodic maintenance tasks of the AP could be lost during the configuration apply, so the client list was no longer refreshed.

2.2 Unstable communication when many wireless clients are connected under heavy multicast load

In a corporate network carrying a high rate of ARP, mDNS and IGMP traffic, communication with the AP became unstable once about ten wireless clients were connected: the first clients to connect could no longer be pinged while later clients saw ping times of 2-3 seconds. The same clients worked normally in an isolated network. The multicast rate limiting toward wireless clients, which had been removed from earlier AP builds due to kernel panic issue, is restored so multicast storms on the wired side no longer saturate the wireless transmit queue.

2.3 Web UI accepted AIFS value 0 in WME Configure, taking both radios down

The WME Configure dialog (Wireless > Radio > WME Configure) accepted an AIFS value of 0 and advertised a range of 0-15. After Save & Apply hostapd rejected the configuration ('Invalid AIFS value 0') and failed to start on both radios: the radios appeared up but with Tx-Power 0 dBm and channel unknown, and no client could connect until the value was corrected. The Web UI now rejects AIFS values below 1 for all four access categories, and the AP additionally clamps AIFS to a minimum of 1 before writing the hostapd configuration.

2.4 False 'Network diagnostics detected connectivity issues: FAIL' alert

APs with a static or PPPoE uplink could repeatedly raise the ecCLOUD alert 'Network diagnostics detected connectivity issues: FAIL. Cloud connection: PASS.' although the gateway was reachable and the AP was online. The diagnostic probed for a DHCP server on the uplink regardless of the uplink mode and reported a failure when none answered. The DHCP probe is now only evaluated when the uplink uses DHCP and has no valid lease.

2.5 RRM threshold after upgrade did not follow the highest Interference Detection value

When an AP is upgraded from a release with per-radio Interference Detection to a release with RRM, and the radios had different Interference Detection values, the RRM threshold kept after

the upgrade was the value of whichever radio happened to appear first in the configuration, so the result was not predictable across units. The migration now uses the highest Interference Detection value across all radios.

2.6 Client signal strength reported as -95 dBm, causing Minimum signal allowed to disconnect a nearby client

With some client adapters, the AP may report the client's signal strength as -95 dBm or 0 although the client is close to the AP. When a Minimum signal allowed threshold is configured on the SSID, such a client is repeatedly disconnected for low signal and reconnects in a loop.

2.7 Cloud agent could stay offline indefinitely when the TLS handshake with the cloud stalled

If the TLS handshake to the cloud stopped making progress (for example a DS-Lite uplink with MTU 1280 where a full-size server segment cannot reach the AP), the cloud agent waited forever without logging or reconnecting, and the AP stayed offline in ecCLOUD until the cloud agent was restarted manually or the AP was rebooted. The handshakes now time out and the agent reconnects by itself.

3 Known Issue

3.1 The WDS link is not established if the wireless security is no security.

3.2 ARP resolution failure to GW when ARP Inspection is enabled

Environment limitation: when the same MAC address is used with different IP addresses in the environment, ARP inspection cannot be used in this scenario.

3.3 802.11r Fast Roaming May Fail or Be Delayed on Some Client Devices

On some client devices (e.g., iOS), 802.11r fast roaming may fail or take several seconds. If this occurs, forget the network on the device and rejoin it. Turning Wi-Fi off and on does not resolve the issue.

4 Compatible Version for AP Management

Compatible with ecCLOUD