



Release Note

Edgecore EAP111 Release v12.7.0

Document # EAP111-v12.7.0-3295-1ab8b4507-01f8941

Enhancement from v12.6.13-2955-a8e68518e-0c141b2

Table of Contents

1	Feature.....	4
1.1	Support Wi-Fi EasyMesh (Multi-AP)	4
1.2	Support RadSec client certificate installation	4
1.3	Ability to disable IPv6	4
1.4	Support LAN port upload and download rate limit	4
1.5	Support Web Filter	5
1.6	Support Vietnam regulatory domain	5
1.7	Support SHA authentication and AES privacy for SNMPv3	5
1.8	Uplink self-diagnostic panel on the Dashboard	5
1.9	Warning when Band Steering and Minimum signal allowed are both enabled	5
1.10	ARP table and Ethernet port error counters reported to ecCLOUD	6
2	Issue Fixed	7
2.1	5 GHz radio could stay down when RRM selected a weather-radar channel.....	7
2.2	Client count shows 200+ clients after a firmware upgrade or cloud configuration push ...	7
2.3	AP not reachable from WAN after enabling ARP Inspection, and crash reboot with ARP Inspection enabled.....	7
2.4	Force DHCP did not block clients with a static IP address	7
2.5	False 'Network diagnostics detected connectivity issues: FAIL' alert.....	7
2.6	Kernel panic when the WAN port is linked at 100 Mbps full duplex without auto-negotiation	7
2.7	Lower UDP throughput on 5 GHz SSIDs in router (NAT) mode.....	8
2.8	Clients unable to connect after several days of operation	8
2.9	Repeated critical 'txmon' log messages after reboot	8
2.10	Clients could not authenticate when a backup RADIUS authentication server was configured	8
2.11	Cloud agent could stop reconnecting after a network disconnection	8
2.12	Web UI accepted AIFS value 0 in WME Configure, taking both radios down.....	8
2.13	RRM threshold after upgrade did not follow the highest Interference Detection value	9
2.14	Applying settings from a CAPWAP controller failed and the AP lost the controller connection.....	9
2.15	DS-Lite tunnel not established when the configuration was pushed from ecCLOUD	9
2.16	NAS ID field not shown when first selecting Enterprise security on an SSID	9
2.17	802.11r fast roaming failed between this access point and other Edgecore models	9
2.18	LLDP packets were not sent at the configured transmit interval	10
2.19	Cloud agent could stay offline indefinitely when the TLS handshake with the cloud stalled	10
3	Known Issue.....	11
3.1	SSIDs tunnelled to a CAPWAP wireless controller may not work	11

3.2	802.11r Fast Roaming May Fail or Be Delayed on Some Client Devices	11
4	Compatible Version for AP Management	12

1 Feature

1.1 Support Wi-Fi EasyMesh (Multi-AP)

EAP111 now supports Wi-Fi EasyMesh (Wi-Fi Alliance Multi-AP). Several access points can form a self-organising mesh over a dedicated wireless backhaul: one unit acts as the root node (controller and agent, connected to the wired network) and the other units join as member nodes (agents) and extend the same SSIDs. EasyMesh is configured per radio from the local Web UI or from ecCLOUD with Enable, Root Node, Mesh ID, Security Method (Open or WPA3-Personal), Key and Network Behavior (Bridge to Internet or Route to Internet). The Dashboard shows the EasyMesh role and topology, and EasyMesh information is included in the troubleshooting file.

Limitations: exactly one root node is required per EasyMesh network; at most three regular SSIDs can be enabled on the radio used for EasyMesh; DFS channels are not supported for EasyMesh.

1.2 Support RadSec client certificate installation

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. RadSec settings of an open SSID with Radius MAC Auth are displayed correctly when the page is reloaded.

1.3 Ability to disable IPv6

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; the setting can also be pushed from ecCLOUD. When Disable is selected the AP no longer acquires or uses IPv6 addresses on its management interfaces. The option is hidden when the IPv4 address mode is DS-Lite, because DS-Lite requires IPv6. The default remains enabled, so existing deployments are not affected by the upgrade.

1.4 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 in kbps (256 to

10,000,000). Traffic of devices connected to that port is shaped to the configured rates.

1.5 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.

1.6 Support Vietnam regulatory domain

Vietnam (VN) is now supported as a country setting on EAP111. 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 at up to 19 dBm, and 5 GHz channels 36-64, 100-140 and 149-165 at up to 18 dBm (channel 144 excluded). The limits are also applied when the country is changed from ecCLOUD, and units upgraded with settings kept are migrated automatically.

1.7 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, from the local UI (System > Services) and from ecCLOUD. Existing SNMPv3 users configured with MD5/DES continue to work unchanged.

1.8 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.

1.9 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. The warning is updated immediately when SSIDs are added, removed, enabled or disabled on the page. It is informational and does not block saving.

1.10 ARP table and Ethernet port error counters reported to ecCLOUD

The AP now includes its ARP table (MAC address, interface and IP address of each neighbour) and per-Ethernet-port receive/transmit error and discard counters in the periodic status report sent to ecCLOUD, so they can be used for monitoring and integration with external OSS systems.

2 Issue Fixed

2.1 5 GHz radio could stay down when RRM selected a weather-radar channel

With RRM enabled, automatic channel selection could pick a 5 GHz weather-radar channel (120, 124 or 128, or a channel that bonds into them at 40/80 MHz) and the 5 GHz radio then failed to come up. Weather-radar channels are now excluded from the channel list while RRM is enabled, and units already running RRM are adjusted automatically on upgrade.

2.2 Client count shows 200+ clients after a firmware upgrade or cloud configuration push

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 more than 200 and stay there, although far fewer clients were connected. The periodic maintenance tasks of the AP could be lost during the configuration apply, so clients that had left were never removed.

2.3 AP not reachable from WAN after enabling ARP Inspection, and crash reboot with ARP Inspection enabled

After enabling ARP Inspection the AP could stop answering pings from the WAN side until the bridge firewall rules were flushed or the AP rebooted. In addition, heavy broadcast or multicast traffic hitting the broadcast and multicast rate limiting applied with ARP Inspection could trigger a kernel alignment fault and an unexpected reboot. Both problems are fixed.

2.4 Force DHCP did not block clients with a static IP address

With ARP Inspection and Force DHCP enabled, a wireless client configured with a static IP address could still communicate through the AP, and on tagged-VLAN SSIDs Force DHCP could break communication for legitimate clients. Clients that did not obtain their address through DHCP are now blocked unless their MAC/IP is in the static trust list, on bridged, routed and VLAN SSIDs.

2.5 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 DHCP probe is now evaluated only when the uplink uses DHCP and has no valid lease.

2.6 Kernel panic when the WAN port is linked at 100 Mbps full duplex without

auto-negotiation

When the WAN port was connected to a switch port forced to 100 Mbps full duplex without auto-negotiation and NAT traffic was run through the AP, the AP could hit a kernel panic and reboot. This no longer occurs with the new kernel and Ethernet driver.

2.7 Lower UDP throughput on 5 GHz SSIDs in router (NAT) mode

On 5 GHz SSIDs set to Route to Internet, UDP download and upload throughput was less than half of the throughput of a bridged SSID. Router-mode throughput is now in line with bridge mode.

2.8 Clients unable to connect after several days of operation

After running for several days, an AP could stop accepting client connections until it was rebooted; the log pointed to the wireless receive path of the Wi-Fi driver. The Wi-Fi driver has been replaced in this release to address this condition.

2.9 Repeated critical 'txmon' log messages after reboot

After a reboot (for example after a configuration template was applied from a wireless controller) the system log showed a burst of critical 'txmon' messages every few seconds. The obsolete monitor producing these messages has been removed.

2.10 Clients could not authenticate when a backup RADIUS authentication server was configured

When a backup RADIUS authentication server was configured on an SSID, the access point switched between the primary and the backup server on every retransmission of an authentication request, instead of failing over only after the primary server stopped responding. With RadSec, as used for OpenRoaming, this re-opened the TLS connection each time so that it never completed: clients could not authenticate and CPU load stayed high, even when both servers were reachable. The access point now stays on the primary server while it responds and moves to the backup server only after repeated failed attempts.

2.11 Cloud agent could stop reconnecting after a network disconnection

If the network was unreachable when the cloud agent tried to reconnect over TLS 1.3, the agent could enter a loop without recovering, so the AP stayed offline in ecCLOUD until it was restarted.

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

The WME Configure dialog accepted an AIFS value of 0. After Save & Apply the wireless service

rejected the configuration and failed to start on both radios, and no client could connect until the value was corrected. The Web UI now rejects AIFS values below 1, and the AP additionally clamps AIFS to a minimum of 1. CWmin greater than CWmax is also rejected.

2.13 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 depended on the order of the radios in the configuration. The migration now uses the highest Interference Detection value across all radios (radios with 0 are ignored; if all are 0, RRM stays disabled with the default threshold 70).

2.14 Applying settings from a CAPWAP controller failed and the AP lost the controller connection

When the AP was managed by a CAPWAP wireless controller, applying a configuration template that contained a WPA3-Enterprise SSID failed, all SSIDs on that radio stayed down and the AP lost its connection to the controller.

2.15 DS-Lite tunnel not established when the configuration was pushed from ecCLOUD

When the DS-Lite IPv4 address mode was configured from ecCLOUD (it worked in standalone mode), the DS-Lite tunnel was not established if bridged SSIDs were attached to the WAN, so the AP had no IPv4 connectivity and the configuration was rolled back.

2.16 NAS ID field not shown when first selecting Enterprise security on an SSID

When WPA2/WPA3 Enterprise, WPA2-PSK with DPSK or RADIUS MAC Authentication was first selected on an SSID in the Wireless Settings page, the NAS ID selector was not shown until the settings were saved and the page was reloaded. The NAS ID field is now shown immediately, with BSSID MAC as the default.

2.17 802.11r fast roaming failed between this access point and other Edgecore models

With 802.11r (Fast Transition) enabled on a WPA2-Personal or WPA3-Personal SSID and no fast-transition keys provisioned, clients could not fast-roam between this access point and other Edgecore models (for example EAP102) in the same mobility domain, because the models derived their fast-transition key in different ways. The key is now derived from the mobility domain and the SSID passphrase, in the same way as on other Edgecore models that include

this change. 802.1X (Enterprise) SSIDs are not affected.

Note: fast-transition roaming works only between access points that all run firmware including this change. Upgrade all access points that share a mobility domain; until then, clients moving between an upgraded and a non-upgraded access point fall back to a full connection.

2.18LLDP packets were not sent at the configured transmit interval

With LLDP enabled (for example Tx Interval 60 s, Tx Hold 10), LLDP frames were not transmitted every Tx Interval on the LAN/WAN ports. They are now sent at the configured interval.

2.19Cloud 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 SSIDs tunnelled to a CAPWAP wireless controller may not work

When the AP is managed by a CAPWAP wireless controller, clients on SSIDs using split tunnel or complete tunnel may fail to join the SSID, or may obtain an address but not see the captive portal. Under investigation.

3.2 802.11r 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