Release Note

Edgecore EAP102 Release v12.5.99

Document # EAP102-v12.5.99-1663-f77b5efcd-7da97dd

Enhancement from v12.5.97-1616-e16697005-b2b20e4

Table of Contents

1 Feature 3

1.1 Support Radio Resource Management 3

1.2 Support IPv6 Disabled 3

1.3 Support LAN port upload and download rate limit 3

1.4 Support Web Filter 4

1.5 Support SHA authentication and AES privacy for SNMPv3 4

1.6 Uplink Self-Diagnostic panel on the Dashboard 4

2 Issue Fixed 5

2.1 Web UI accepted AIFS value 0 in WME Configure, taking both radios down 5

2.2 5 GHz radio stayed silent after a radar event on a single DFS channel 5

2.3 OS Blacklist misidentified Nintendo Switch as Android 5

2.4 False 'Network diagnostics detected connectivity issues' alert 5

2.5 LAN clients received non-routable IPv6 (ULA) addresses from the AP 5

2.6 Band steering warning did not update for SSIDs added or removed on the same page 5

2.7 802.11r Fast Transition roaming failed between this AP and newer Edgecore models 6

2.8 Setup Wizard settings could be lost if the browser was closed before the configuration was applied 6

2.9 Aprecomm add-on logged routine messages at error level 6

3 Known Issue 7

3.1 The connection of Microsoft surface laptop is unstable using WPA2-PSK SSID. 7

3.2 The SSID compatible issue in Windows 10 devices with the specific ethernet card. 7

3.3 The dynamic VLAN is not supported in the mesh network. 7

3.4 There is a low probability that the mesh connection can’t recover after MAP is re-configured. 7

3.5 Authport with VLAN tagged does not support on IOS device. 7

3.6 When upgrading the FW from 12.0.0, Hotspot controlled SSID can only work after an additional reboot. 7

3.7 The captive portal cannot be popped up sometimes in the open roaming SSID. 7

3.8 Clients may fail to connect immediately after AP boot. 7

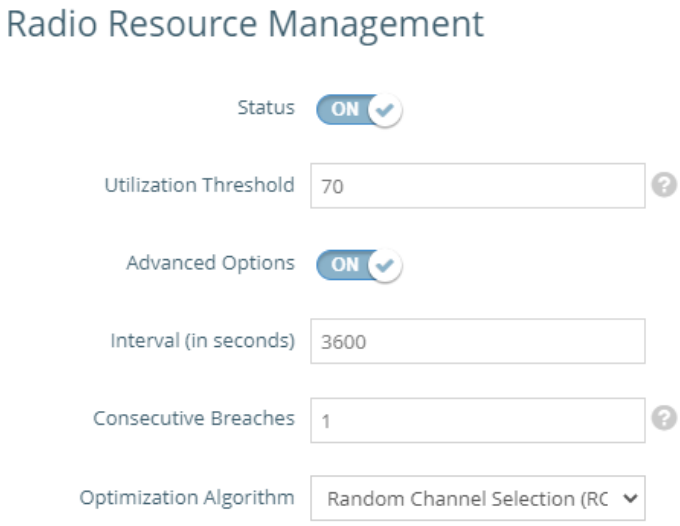
3.9 ARP resolution failure to GW when ARP Inspection is enabled 8

3.10 802.11r Fast Roaming May Fail or Be Delayed on Some Client Devices 8

4 Compatible Version for AP Management 9

1 Feature

1.1 Support Radio Resource Management



Support Radio Resource management on the Radio Resource management page.

1. Radio Resource management: Enable or disable the Radio Resource Management feature.
2. Utilization Threshold: The percentage of airtime utilization threshold. If set to 70, channel optimization considers triggering when utilization exceeds 70%.
3. Advanced Options: Enable or disabled the advance options.
4. Interval (Sec): It defines the interval (in seconds) to check channel utilization.
5. Consecutive Breaches: It specifies the number of consecutive times for the channel utilization to be higher than the threshold before triggering channel optimization.
6. Optimization Algorithm: "Auto Channel Selection (ACS)" or "Random Channel Selection (RCS)" for selection.

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 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.

1.6 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.

2 Issue Fixed

2.1 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.

2.2 5 GHz radio stayed silent after a radar event on a single DFS channel

When the 5 GHz radio was fixed to a single DFS channel and a radar event occurred, the radio correctly stopped transmitting, but after the 30-minute non-occupancy period it never restarted the channel availability check and stayed off the air until the AP was restarted. The radio now resumes service after the non-occupancy period.

2.3 OS Blacklist misidentified Nintendo Switch as Android

With OS Blacklist enabled to block Android devices, a Nintendo Switch was identified as Android and blocked. The device identification database now recognizes Nintendo devices, so a Nintendo Switch is no longer blocked as Android.

2.4 False 'Network diagnostics detected connectivity issues' alert

After the AP briefly lost its cloud connection, ecCLOUD could receive the alert 'Network diagnostics detected connectivity issues: FAIL' although the network was working, because a DHCP server check was evaluated even when the uplink already had a valid address or did not use DHCP. The DHCP check now runs only when the uplink uses DHCP and has no address, so the false alert is no longer sent.

2.5 LAN clients received non-routable IPv6 (ULA) addresses from the AP

With an SSID set to route to the Internet, wireless clients received an IPv6 unique-local address (fd00::/8) from the AP although no IPv6 Internet access was available through it. The AP's local network no longer advertises IPv6 to clients; it serves IPv4 DHCP only.

2.6 Band steering warning did not update for SSIDs added or removed on the

same page

On the Wireless radio page, the warning shown when Band Steering is enabled together with a Minimum signal allowed value did not react to an SSID that was added with Add SSID on the same page: changing that SSID's Minimum signal allowed or enabling and disabling it left the warning out of date until the page was reloaded. Removing an SSID did not update the warning either. The warning now updates immediately for added and removed SSIDs.

2.7 802.11r Fast Transition roaming failed between this AP and newer Edgecore models

In a roaming domain that mixed this AP with Edgecore models on newer firmware lines (for example EAP112), 802.11r Fast Transition failed because each model derived a different default key, so clients performed a full re-authentication and roaming took 20-40 seconds. The AP now derives the default Fast Transition key the same way as these models, and on Personal (PSK / SAE) networks the key also depends on the network passphrase.

2.8 Setup Wizard settings could be lost if the browser was closed before the configuration was applied

After Done was pressed in the Setup Wizard, the wireless and network settings entered in the wizard were saved only when the following page applied them. If the browser page was closed or left before "Applying configuration changes" appeared, the requested SSID, password and Internet settings were lost while the wizard was already marked complete, and on a cloud-managed AP two blank, disabled SSIDs could appear in the local UI. The Setup Wizard now saves all of its settings before the page is left, and empty SSID slots are no longer shown.

2.9 Aprecomm add-on logged routine messages at error level

When the Aprecomm add-on was active, its routine 'Router Config' and 'Router Stats' messages were written to the system log at error level (user.err), which made the error log noisy. These messages are now logged at info level. The fix is delivered with Aprecomm add-on version, which is installed from ecCLOUD.

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.

3.9 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.

3.10 802.11r 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

Compatible with EWS-Series controller v3.91.0000 or later