Release Note

Edgecore EAP101 Release v12.4.0

Document # EAP101-v12.4.0-971-24746b8b

Enhancement from v12.3.1-888-8ad4a0a8

Table of Contents

1 Feature

1.1 QR code onboarding Enhancement

Use the QR code onboarding SSID to configure set up the AP. In this version, the WAN port auto-detection feature has been added to the AP, which allows it to detect DHCP, PPPoE, and static IP configurations. In DHCP environments, the AP will automatically redirect to the management page without requiring any additional configuration. For PPPoE and static IP configurations, the AP will redirect to the relevant page for further configuration.

The management page can be used to manage the first AP either through ecCLOUD or in stand-alone mode. If the second AP needs to establish a mesh with the first AP, follow these steps:

1. Connect the LAN port of the first AP (MPP) to the LAN port of the second AP (MAP), which will allow the second AP to synchronize its configuration with the first AP.
2. After unplugging the LAN port, the mesh will be established automatically.

1.2 Minimum Signal Allowed Modification

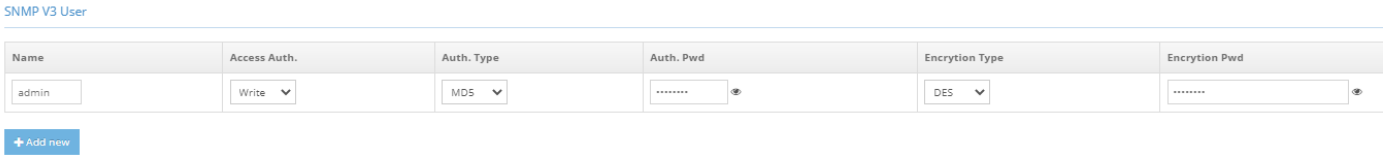
Modify the minimum singal allowed value from SNR to RSSI. In the previous version, the default value is 30 (SNR). In this version, the value will be changed to -70 (RSSI) automatically.
A client will only be allowed to associate to this Radio if their signal(RSSI) is greater than or equal to the value you specify the field. Set this field to -100 to disable this feature.

1.3 Support Cloud Daemon Log Level Adjustment

Support log level in the System settings of System page.

The following items are displayed on this page:
1. Log Level: The option to adjust the system log level for the ecCLOUD daemon (mgmtd). The default value is Info. The standard ranking of log level is as follows: Trace < Debug < Info < Warn < Error.

1.4 Support SNMPv3



Support SNMPv3 in the Services of System page.

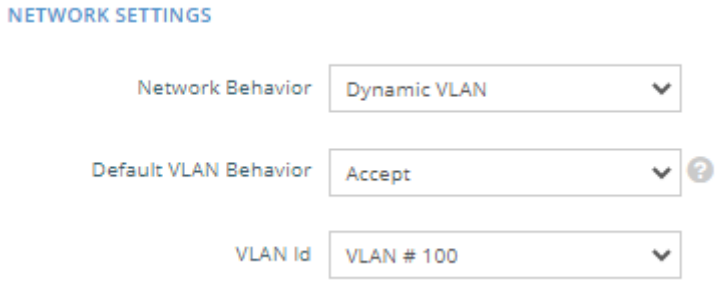
SNMP V3 User - The system allows SNMP Users with Read or Read & Write Access. Determine the Name, Access authority, Authentication Type, Authentication Password, Encryption Type, and Encryption Password on the SNMP Account List.

Note that the SNMPv3 will take effect after an addition reboot.

1.5 Support Frame-IP-Address in Radius Accounting

The Frame-IP-Address of the RADIUS account start packet now includes client IP address information. The accounting start packet output timing has to be delayed until the client has received the IP address from a DHCP server.

1.6 Dynamic VLAN Enhancement



Support dynamic VLAN enhancement on the radio 5/2.4GHz of wireless page.

1 Default VLAN Behavior: Accept or Reject. The default value is Reject.
  1.1 Reject: A client can't connect to this SSID when the client's VLAN Id is not designated in the RADIUS server.
  1.2 Accept: A client can connect to this SSID with the assigned or untagged VLAN Id when the client's VLAN Id is not designated in the RADIUS server.
2. Dynamic VLAN ID can be the same as Static VLAN ID.

Note that the following steps should be followed, when dynamic VLAN ID uses the same as the static VLAN ID.

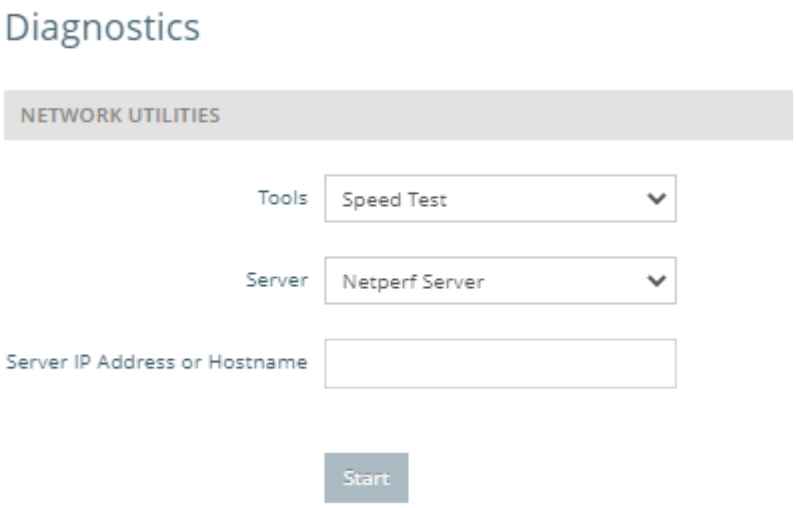
1. The static VLAN ID should be created at first
2. Set the dynamic VLAN SSID.
3. Save and apply the configuration to the AP.

1.7 Support RF Isolation

Support RF Isolation on the radio 5/2.4GHz of wireless page

1. RF Isolation: Enabled or disabled RF isolation. If enabled, clients are isolated between different radio cards.

1.8 Support SpeedTest



Support the netperf server in the Diagnostics of System page.

1. Server IP Address or Hostname: Enter the IP address or Hostname of netperf server to test the speed between AP and nerperf server.

1.9 Hotspot 2.0 UI Enhancement

1. The following field can be optional.
Roaming Consortium List, NAI Realm List, Cellular Network Information List (PLMN)

2. Cellular Network Information List(PLMN): Input the pair of MCC, MNC. E.g. 400, 00
MCC: Three decimal digits (000-999)

MNC: Two (00-99) or three decimal digits (000-999)

2 Issue Fixed

2.1 “MARK” and “NOTRACK” cannot work in firewall rule.

“MARK” and “NOTRACK” can’t work in firewall rule. In this version, “MARK” and “NOTRACK” are removed from UI.

2.2 The CAPWAP broadcast and multicast discovery are not working.

In the System settings of System page, if the management is selected to EWS-Series controller and the broadcast or multicast discovery is enabled, the AP can’t be managed by EWS-Series controller. In this version, the AP can be managed by EWS-Series controller through broadcast or multicast discovery.

2.3 Firewall does not block ICMP packet when the source and destination are set to “Any”.

Add the Reject rules with ICMP from any source to any destination. When the client is connected to the SSID with Route to Internet, the client can ping the domain or IP address of an external network. In this version, when the Firewall receives an ICMP packet from the client attempting to ping an external domain or IP address, the packet will be blocked successfully.

2.4 iPhone cannot connect to the hidden SSID with access control list allowed policy.

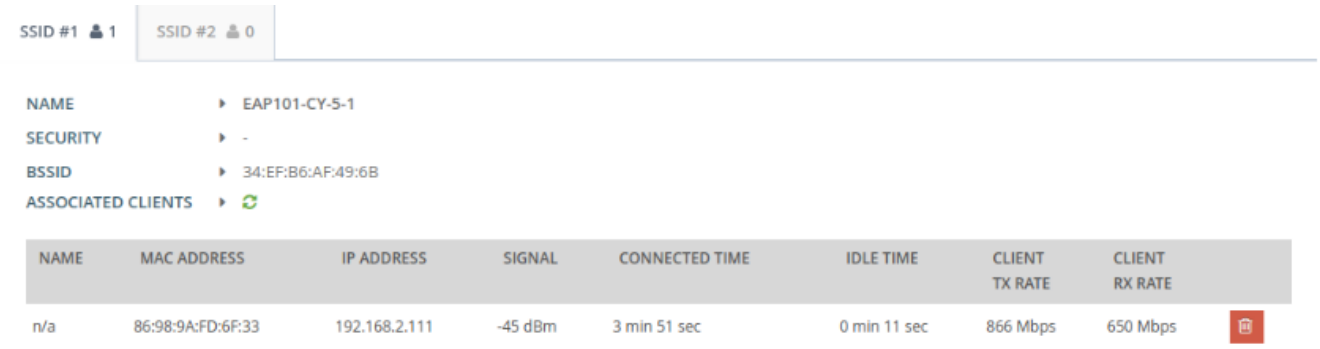
To create the hidden SSID, add the iPhone MAC address in the access control list with “allow all MACs on list” policy. The iPhone failed to connect to the hidden SSID if the private address of iPhone is disabled. In this version, the iPhone can connect to hidden SSID with ACL allowed policy.

2.5 Authport captive portal is not working when the https port configuration of web server is not 443.

Add the AP to ecCLOUD. Modify the https port to non-default port (e.g. 10443). When the client is associated to the authport SSID, the authport captive portal can’t be redirected to the correct page. In this version, the authport captive portal can work normally.

2.6 The duplicate signal value on the wireless status page.

There is the duplicate signal value of the associated clients on the wireless status page. In this version, remove the duplicate signal value on the wireless status page.



2.7 The radio driver cannot be recovered automatically from random crash and cause the device reboot in some harsh scenarios.

In this version, enhance the wireless stability to prevent the crashing issues.

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 Multiple Keys of WPA3 Personal Transition is not supported on iOS devices.

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

3.5 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.

3.6 When the EAP works as the client mode, the station of the AP can’t get the IP address from some DHCP servers (SP-W2-AC1200).

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

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

3.9 The AP does not support split tunnel with WPA2 enterprise SSID.