Release Note

Edgecore EAP101 Release v12.3.0

Document # EAP101-v12.3.0-862-4973a8d6

Enhancement from v12.2.0-780-fa0042e7

Table of Contents

1 Feature 4
1.1 Interference Detection Enhancement 4
1.2 Disconnect the Associated Client 4
1.3 Dynamic PSK 4
1.4 Support the new SNMP OID 5
1.5 SNMP Trap Enhancement 5
1.6 Beacon Enhancement 5
1.7 The Security Enhancement 5
1.8 Upgrade the version of OpenSSL 5
1.9 QR Code Onboarding Enhancement 5
1.10 LAN CAPWAP Tunnel 6
1.11 Hotspot 2.0 Enhancement 7
1.12 The Coldstart and Warmstart Trap Enhancement 7
1.13 Service Schedule 7
2 Issue Fixed 8
2.1 Interference detection is not working when the first SSID is disabled on the radio. 8
2.2 The client can't get the IP address with the hotspot-controlled SSID on ecCLOUD. 8
2.3 Fail to get all MIB values with snmpwalk command. 8
2.4 The hostname can't display correctly when the windows client is connected to the SSID. 8
2.5 The external captive portal service can't support https URL. 8
2.6 The AP can't connect to the ecCLOUD if 5222 port is blocked. 8
2.7 The SNMP community value is not correct after upgrading the FW. 8
2.8 The cold start trap message is sent to the SNMP trap server after the radio is down or up. 9
2.9 There is not internet connection for the VLAN tag of Internet setting. 9
2.10 There is no IP address when the associated client uses the static IP. 9
2.11 There is no OS when the client is connected to the SSID of AP. 9
2.12 The radio 5 GHz can't work normally occasionally. 9
2.13 The authport login page pops up every five minutes after clients can connect to the internet with authport SSID. 9
2.14 The authport page can't be popped up after the clients click the logout button and reconnect to the authport SSID. 9
2.15 The 2.4GHz channel list can't be displayed when the channel bandwidth is set to 40MHz. 10
3 Known issue 11
3.1 The connection of specific Microsoft surface devices is unstable using WPA2-PSK SSID. 11

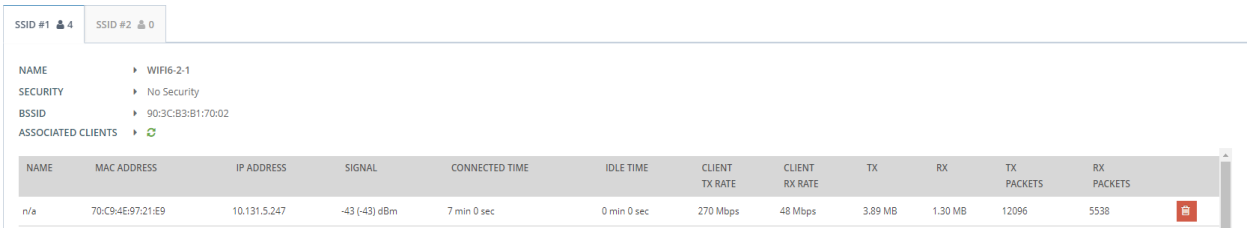
3.2 The SSID compatible issue in Windows 10 devices with the specific ethernet card. 11
3.3 The Multiple Keys of WPA3 Personal Transition can’t work on iOS devices. 11
3.4 The dynamic VLAN can’t work in the mesh network. 11
3.5 There is a low probability that the mesh connection can’t recover after MAP is re-configured. 11
3.6 Clients can’t get the IP when AP is set to client mode and connected to SP-W2-AC1200. 11
3.7 There is a low probability that when lots of clients are associated with the SSID and roam frequently between the APs, the AP will automatically reboot. 12
3.8 The successful page can’t be popped up occasionally after applying the template with complete and split tunnel. 12
3.9 The dynamic VLAN Id can’t be the same as the static VLAN Id. 12
3.10 The WPA2 enterprise and split tunnel can’t work at the same time. 12
3.11 IOS devices can’t connect to the internet when connecting to the authport SSID with VLAN tag traffic. 12
3.12 Clients can connect to the internet with authport SSID when the traffic quota exceeds the limitation. 12
3.13 Clients can’t connect to the Internet with Hotspot controlled SSID after upgrading the FW from the old version. 13
4 Compatible Version for AP Management 14

1 Feature

1.1 Interference Detection Enhancement

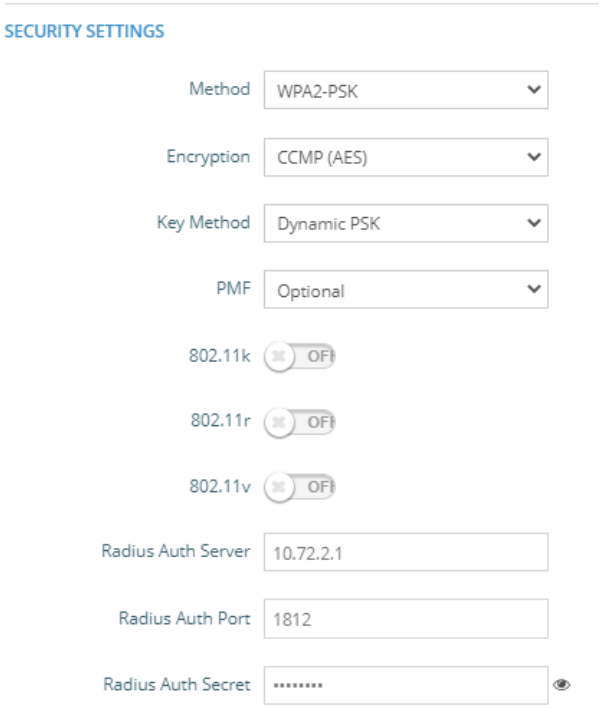
When utilization of the current or adjacent channel reaches the configured threshold (in %), enhance the channel selection mechanism to select the better channel with the lower utilization.

1.2 Disconnect the Associated Client



On the Dashboard > Wireless Status page, the associated clients can be disconnected when the red button is clicked.

1.3 Dynamic PSK



Support Dynamic PSK on the Radio 5/2.4 GHz page of Wireless. Set the configuration of radius auth server. The clients can connect to the dynamic PSK SSID using different passwords.

The following items are displayed on this page:

1. Key Method — Select the Dynamic PSK when the security method is WPA2-PSK.
2. Radius Auth Server — Specifies the IP address or host name of the RADIUS Authentication server.
3. Radius Auth port — Specifies the port of the RADIUS Authentication server.

4. Radius Auth Secret — Specifies the shared text string used between the access point and RADIUS server.

1.4 Support the new SNMP OID

The following new OID is added in the MIB files.

1. edgecoreAPRFClientDownloadRate: Combined clients download rate.
2. edgecoreAPRFClientUploadRate: Combined clients upload rate.
3. edgecoreAPRFChannelUtilization: The channel Utilization.
4. edgecoreAPRFRadioUtilization: The radio Utilization.
5. edgecoreAPRFNumberOfClients: Number of clients associated to radio.
6. edgecoreAPStaName: The name of associated client.
7. edgecoreAPStaIPAddress: The IP of associated client.
8. edgecoreAPRFInterferenceDetection: The configuration for interference detection.
9. edgecoreAPRFAirtimeFairness: The configuration for airtime fairness.
10. edgecoreAPSSID80211v: The configuration for 802.11v.

1.5 SNMP Trap Enhancement

In linkup and linkdown of SNMP trap, the name and value of ifIndex are added into the SNMP Trap for the affected interface.

1.6 Beacon Enhancement

Add the hostname of AP to the beacon management frame and probe request frame.

1.7 The Security Enhancement

The following CVE vulnerabilities are fixed in this version.

1. CVE-2022-41674
2. CVE-2022-42719
3. CVE-2022-42720
4. CVE-2022-42721
5. CVE-2022-42722

1.8 Upgrade the version of OpenSSL

Upgrade the version of OpenSSL. The following vulnerability is fixed in this version.

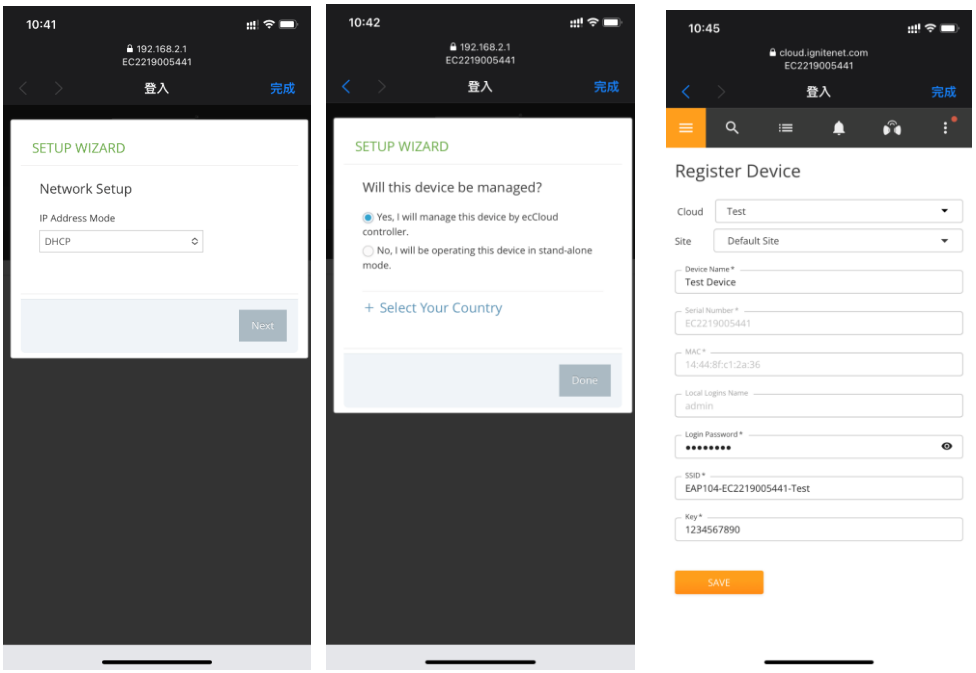
1. JVNDB-2022-001804

1.9 QR Code Onboarding Enhancement

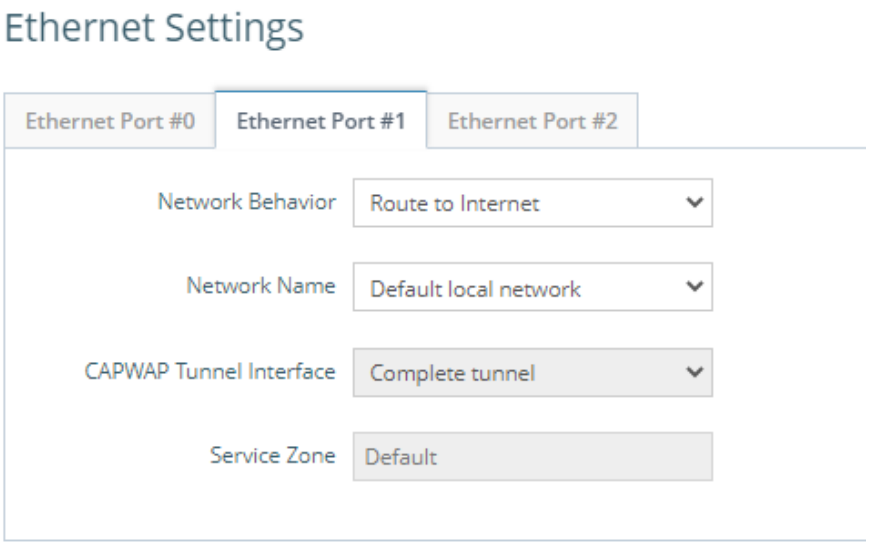
When the AP is reset to default, use the phone to scan the QR code under the device. The

browser will redirect to setup wizard page. In network setup page, DHCP, static IP, PPPoE can be configured depending on the network environment.

If selecting “stand-alone mode”, the SSID, user name and password can be configured in the setup wizard page.
If selecting “managed by Cloud”, the page will guide to ecCLOUD for registering the AP information including MAC and Serial Number. The SSID, user name and password can be configured in the register device page. QR code onboarding can help speed up the register process of the AP on ecCLOUD without typing the AP information.

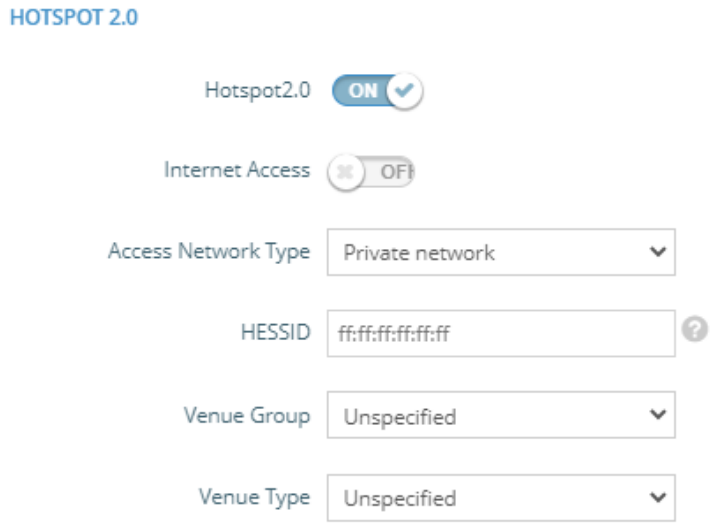


1.10 LAN CAPWAP Tunnel



The LAN port supports CAPWAP tunnel, complete tunnel and disabled tunnel, when the AP is managed by the controller. The configuration of CAPWAP tunnel on LAN port can be applied from the controller template.

1.11 Hotspot 2.0 Enhancement



Add the following option to provide the advanced setting for hotspot 2.0. The hotspot 2.0 only supports when the security method is set to WPA2-EAP.

1. HESSID: Specifies an MAC address for all APs belonging to the same network.
2. Venue URL: Specifies the URL to provide additional venue information to the user.
3. Network Auth Type: List of authentication types.
4. Operator Friendly Name: The operator friendly name.
5. Operating Class: An index into a set of values for AP supported channel.

1.12 The Coldstart and Warmstart Trap Enhancement

The following snmpTrapEnterprise is added into the coldstart and warmstart trap.

1. OID: snmpTrapEnterprise (1.3.6.1.6.3.1.1.4.3). Value: 1.3.6.1.4.1.259 (edgecore)

1.13 Service Schedule

When the AP is managed by EWS-Series controller, service schedule can be configured in the template. After applying the template to the AP, the service hour of the SSID can be customized.

2 Issue Fixed

2.1 Interference detection is not working when the first SSID is disabled on the radio.

Interference detection is not working when the first SSID is disabled on the radio. This issue has been resolved in this version.

2.2 The client can’t get the IP address with the hotspot-controlled SSID on ecCLOUD.

Configure the hotspot-controlled SSID on ecCLOUD. Upgrade the FW from the older version. The clients can’t get the IP address when connecting to the hotspot-controlled SSID. This issue has been fixed in this version.

2.3 Fail to get all MIB values with snmpwalk command.

If the WAN port of AP is not connected or the AP can’t get the IP address, the snmpwalk command can’t get all MIB values. This issue has been resolved in this version.

2.4 The hostname can’t display correctly when the windows client is connected to the SSID.

When the windows client is connected to the SSID, the hostname shows N/A on the wireless status of dashboard. After the issued is fixed, the hostname can be displayed correctly.

2.5 The external captive portal service can’t support https URL.

In the Network > Hotspot Settings page, select the mode to External Captive Portal Service. Enter https URL in the captive portal URL field. The captive portal page can’t be popped up when the client is connected to the hotspot-controlled SSID. This issue has been resolved in this version.

2.6 The AP can’t connect to the ecCLOUD if 5222 port is blocked.

If 5222 port is blocked, the AP can’t connect to the ecCLOUD successfully. In this version, the issue has been fixed.

2.7 The SNMP community value is not correct after upgrading the FW.

After upgrading the FW from 11.6, the SNMP community value is not correct. In this version, this issue has been fixed.

2.8 The cold start trap message is sent to the SNMP trap server after the radio is down or up.

Set the SNMP trap server. After the radio is down or up, the cold start trap message is sent to the trap server along with link down or up. In this version, this issue has been fixed.

2.9 There is not internet connection for the VLAN tag of Internet setting.

Set the VLAN tag and VLAN Tag Id on the Internet settings page of network. The AP can’t connect to the Internet through the VLAN tag IP.

2.10 There is no IP address when the associated client uses the static IP.

When the client uses the static IP to connect to the SSID of AP, the IP address of the client can’t display correctly.

2.11 There is no OS when the client is connected to the SSID of AP.

When the client is connected to the SSID of AP, the client OS can’t display correctly on the wireless status of dashboard.

2.12 The radio 5 GHz can’t work normally occasionally.

After rebooting the AP or configuring the wireless settings, the radio 5 GHz can’t work occasionally. In this version, this issue has been fixed.

2.13 The authport login page pops up every five minutes after clients can connect to the internet with authport SSID.

Enable Authport on ecCLOUD, create the authport SSID. After the clients can connect to the internet, the authport login pops up every five mintues. This issue has been resolved in this version.

2.14 The authport page can’t be popped up after the clients click the logout button and reconnect to the authport SSID.

Enable Authport on ecCLOUD, create the authport SSID. After the clients can connect to the internet, click the logout button. After reconnecting to the authport SSID, the clients can connect to the Internet without logging to the authport page. The authport page should be popped up for authentication. This issue has been resolved in this version.

2.15 The 2.4GHz channel list can’t be displayed when the channel bandwidth is set to 40MHz.

In the Radio 2.4GHz page, the 2.4GHz channel list can’t be displayed when the channel bandwidth is set to 40MHz.

3 Known issue

3.1 The connection of specific Microsoft surface devices is unstable using WPA2-PSK SSID.

If the 5Ghz SSID is set to WPA2-PSK SSID, the connection of some Microsoft surface devices is unstable.

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 connection of the devices is unstable connecting 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 can’t work on iOS devices.

Create the SSID with WPA3 personal transition. Enter the password in the multiple keys field. The iOS devices can’t connect to this SSID using multiple keys.

3.4 The dynamic VLAN can’t work in the mesh network.

In the mesh topology, create the SSID with dynamic VLAN. Clients can’t connect to the internet after associated to this SSID.

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 can’t establish the mesh connection. After rebooting all the AP, the mesh connection recovers.

3.6 Clients can’t get the IP when AP is set to client mode and connected to SP-W2-AC1200.

Set AP to client mode in the radio 5 GHz. AP is connected to the SSID in SP-W2-AC1200 with AP mode. When clients are connected to the 2.4G SSID of the client mode AP, clients can’t get the IP. This is the current limitation that the DHCP release protection should be disabled from the DHCP server. After the DHCP release protection is disabled, clients can get the IP normally.

3.7 There is a low probability that when lots of clients are associated with the SSID and roam frequently between the APs, the AP will automatically reboot.

Create the SSIDs. A lot of clients are connected to the SSID of the AP and roam frequently between the APs. There is a low probability that the AP reboots automatically because of the current recovery mechanism.

3.8 The successful page can’t be popped up occasionally after applying the template with complete and split tunnel.

AP is managed by EWS-Series controller. Apply the template with complete and split tunnel SSID to the AP. Clients can’t see the successful login page occasionally when they enter the correct username and password on the web page. Please update the controller to the latest version to fix the issue.

3.9 The dynamic VLAN Id can’t be the same as the static VLAN Id.

Add the static VLAN ID, 100. Create the SSID with dynamic VLAN. Configure the same VLAN Id, 100, in the radius server. When the clients with VLAN Id 100 are connected to the SSID, they can’t be connected to the Internet. If the dynamic VLAN Id is different from the static VLAN Id, the clients can be connected to the Internet normally.

3.10 The WPA2 enterprise and split tunnel can’t work at the same time.

Apply the New Generation template to the AP. WPA2 Enterprise and split tunnel can’t work at the same time. This is the current limitation in this version.

3.11 IOS devices can’t connect to the internet when connecting to the authport SSID with VLAN tag traffic.

Enable Authport on ecCLOUD, create the authport SSID. Clients can’t connect to the internet when connecting to the SSID with VLAN tag.

3.12 Clients can connect to the internet with authport SSID when the traffic quota exceeds the limitation.

Enable Authport on ecCLOUD, create the authport SSID. When the traffic quota exceeds the limitation, clients can use the authport SSID to connect to the internet.

3.13 Clients can’t connect to the Internet with Hotspot controlled SSID after upgrading the FW from the old version.

Enable Hotspot controlled SSID on ecCLOUD. Clients can’t connect to the Internet with the SSID after upgrading the FW from 12.0.0 version. If AP reboots or changes the wireless configure, this issue can be fixed.

4 Compatible Version for AP Management

Compatible with ecCLOUD
Compatible with EWS5203 v3.60.0100 or later