



Release Note

Edgecore EAP104 Release v12.4.0

Document # EAP104-v12.4.0-980-c4ad2d45

Enhancement from v12.1.0-760-6f3567ae

Table of Contents

1	Feature.....	4
1.1	Aprecomm Addon	4
1.2	Interference Detection Enhancement	4
1.3	Disconnect the Associated Client	4
1.4	Dynamic PSK	4
1.5	Beacon Enhancement.....	5
1.6	The Security Enhancement.....	5
1.7	Upgrade the version of OpenSSL	5
1.8	Hotspot 2.0 Enhancement.....	5
1.9	Service Schedule	6
1.10	802.11v	6
1.11	Airtime Fairness	7
1.12	BLE Scan	7
1.13	SNMP Trap.....	8
1.14	Remove the BSS coloring value 0 from UI	8
1.15	Support client OS on the controller's AP list.....	9
1.16	QR code onboarding Enhancement	9
1.17	Minimum Signal Allowed Modification	9
1.18	Support Cloud Daemon Log Level Adjustment.....	9
1.19	Support SNMPv3	10
1.20	Support Frame-IP-Address in Radius Accounting.....	10
1.21	Dynamic VLAN Enhancement	10
1.22	Support RF Isolation.....	11
1.23	Support SpeedTest	11
1.24	Support Thailand Regulation	12
2	Issue Fixed	13
2.1	The AP cannot connect to the ecCLOUD if 5222 port is blocked.	13
2.2	Clients can connect to the internet with authport SSID when the traffic quota exceeds the limitation.	13
2.3	It takes 30 seconds to pop up the captive portal page when using external captive portal of hotspot.	13
2.4	The name and IP address of mesh information are N/A in the open mesh page.....	13
2.5	There are a lot of cron messages in the syslog.	13
2.6	The wireless status is not correct if the first SSID is disabled.	13
2.7	The channel list cannot be displayed sometimes.....	13
2.8	Fail to communicate with EPSON TM-m30II-H under MPP in the mesh topology.....	14
2.9	The authport clients will be logout when the traffic usage of clients exceeds 2GB.....	14
2.10	The hostname cannot be displayed correctly when the windows client is connected to	

the SSID with static IP.....	14
2.11 The AP cannot get the IP address for the VLAN tag or mgmt VLAN of Internet setting.	14
2.12 There is no IP address displayed in the web UI when the associated client uses the static IP.....	14
2.13 Interference detection is not working after the user account is added or deleted.....	14
2.14 The UI is not correct when the security is set to WPA3 Enterprise 192-bit.....	14
2.15 The channel list of 40MHz is not correct.....	15
2.16 The 5GHz radio cannot work in the auto channel with DFS channel sometimes after applying the wireless configuration multiple times.	15
2.17 “MARK” and “NOTRACK” cannot work in firewall rule.	15
2.18 The CAPWAP broadcast and multicast discovery are not working.....	15
2.19 Firewall does not block ICMP packet when the source and destination are set to “Any”.	15
2.20 iPhone cannot connect to the hidden SSID with access control list allowed policy.	15
2.21 Authport captive portal is not working when the https port configuration of web server is not 443.....	16
2.22 The duplicate signal value on the wireless status page.	16
2.23 The radio driver cannot be recovered automatically from random crash and cause the device reboot in some harsh scenarios.....	16
2.24 Fail to upgrade the FW from 12.3.1 to other versions.	16
3 Known Issue.....	18
3.1 The connection of Microsoft surface laptop is unstable using WPA2-PSK SSID.....	18
3.2 The SSID compatible issue in Windows 10 devices with the specific ethernet card.	18
3.3 The Multiple Keys of WPA3 Personal Transition is not supported on iOS devices.....	18
3.4 The dynamic VLAN is not supported in the mesh network.	18
3.5 There is a low probability that the mesh connection can’t recover after MAP is re-configured.	18
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).	18
3.7 Authport with VLAN tagged does not support on IOS device.....	18
3.8 When upgrading the FW from 12.0.0, Hotspot controlled SSID can only work after an additional reboot.	18
3.9 The AP does not support split tunnel with WPA2 enterprise SSID.	18

1 Feature

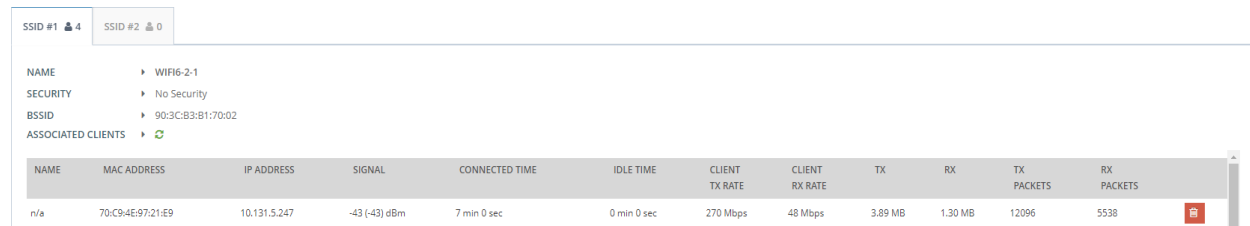
1.1 Aprecomm Addon

Support Aprecomm feature on ecCLOUD. When Aprecomm addon is enabled on ecCLOUD, the AIOps service will be integrated with their own Wi-Fi networks.

1.2 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.

1.3 Disconnect the Associated Client



NAME	MAC ADDRESS	IP ADDRESS	SIGNAL	CONNECTED TIME	IDLE TIME	CLIENT TX RATE	CLIENT RX RATE	TX	RX	TX PACKETS	RX PACKETS
n/a	70:C9:4E:97:21:E9	10.131.5.247	-43 (-43) dBm	7 min 0 sec	0 min 0 sec	270 Mbps	48 Mbps	3.89 MB	1.30 MB	12096	5538

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

1.4 Dynamic PSK

SECURITY SETTINGS

Method

Encryption

Key Method

PMF

802.11k

802.11r

802.11v

Radius Auth Server

Radius Auth Port

Radius Auth Secret

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.

1.5 Beacon Enhancement

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

1.6 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

1.7 Upgrade the version of OpenSSL

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

1. JVNDB-2022-001804

1.8 Hotspot 2.0 Enhancement

HOTSPOT 2.0

Hotspot2.0 ON

Internet Access OFF

Access Network Type

HESSID ?

Venue Group

Venue Type

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.
6. The following field can be optional.
Roaming Consortium List, NAI Realm List, Cellular Network Information List (PLMN)
7. 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)

1.9 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.

1.10802.11v

SECURITY SETTINGS

Method

Encryption

Key

Multiple Keys

Enter one Key and optional MAC per line.
Example: 12345678 00:12:34:56:78:9a

PMF

802.11k OFF

802.11r OFF

802.11v OFF

Support 802.11v on the Radio 5/2.4 GHz page of Wireless.

The following item is displayed on this page:

1. 802.11v — Enables or disables the 802.11v feature.

1.11 Airtime Fairness

PHYSICAL RADIO SETTINGS

Status ON

Mode

802.11 Mode

Channel Bandwidth

Channel

WME Configure

Beacon Interval

Bandsteering OFF

Airtime Fairness OFF

Support Airtime Fairness on the Radio 5/2.4 GHz page of Wireless.

The following item is displayed on this page:

1. Airtime Fairness — Enables or disables the Airtime Fairness feature. Enabling this feature improves the overall performance of wireless network.

1.12 BLE Scan

BLE

Send iBeacon ON

UUID - - - -

Major

Minor

Tx Power

BLE Scan

Support BLE Scan on the Services page of System.

The following item is displayed on this page:

1. BLE Scan — Click the button to get the BLE scan result. The MAC address, signal, and type of BLE are displayed on the page.

Only four types of BLE are displayed on the BLE scan page.

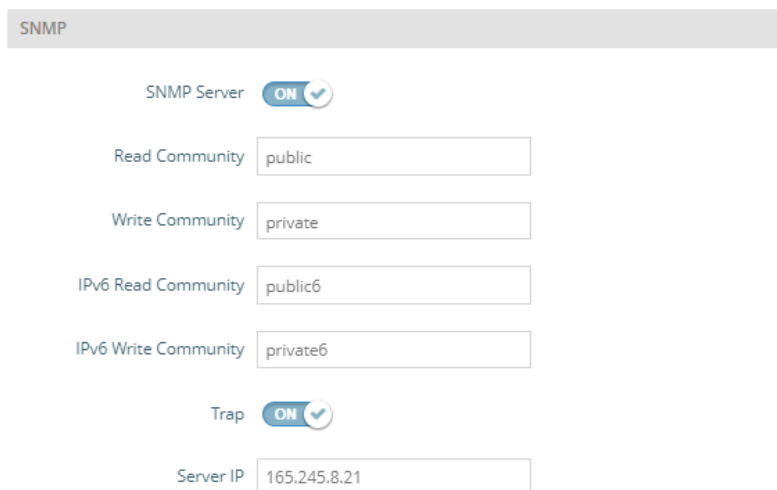
- a. EddyStone-UID
- b. EddyStone-URL
- c. EddyStone-TLM
- d. ibeacon



The screenshot shows a 'BLE SCAN' window with a 'BLE Scan Now' button and a close icon. Below is a table with three columns: MAC Address, Signal, and Type. The table lists six discovered BLE devices.

MAC Address	Signal	Type
51:F2:DE:6F:5F:5A	-74dBm	ibeacon
52:3A:8D:30:CF:64	-75dBm	EddyStone-UID
56:62:39:B2:7B:DB	-73dBm	EddyStone-URL
6E:A3:1A:DA:CA:DF	-81dBm	EddyStone-TLM
79:2C:9F:37:EC:8A	-84dBm	EddyStone-UID
7E:67:D5:E9:78:C7	-74dBm	ibeacon

1.13 SNMP Trap



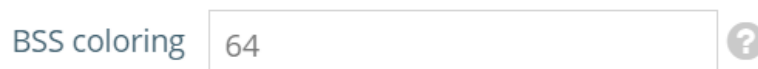
The screenshot shows the 'SNMP' configuration page. It includes a toggle for 'SNMP Server' (ON), four text input fields for community strings (Read, Write, IPv6 Read, IPv6 Write), a 'Trap' toggle (ON), and a 'Server IP' text input field.

Support SNMP trap on the Services page of System.

The following items are displayed on this page:

1. Trap — Enables or disables the SNMP trap feature.
2. Server IP — Specifies the IP address of a SNMP trap server that will be sent trap messages including cold start, warm start, link up and link down.

1.14 Remove the BSS coloring value 0 from UI



The screenshot shows a configuration field for 'BSS coloring' with the value '64' entered. A help icon (?) is visible to the right of the field.

In this version, remove the BSS coloring value 0 from UI. The valid range of the BSS coloring is 1-64.

1.15 Support client OS on the controller's AP list

When AP is managed by the controller and the client is connected to the SSID of AP, the client OS can be displayed correctly on the AP online users of controller's AP list.

1.16 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.

1.17 Minimum Signal Allowed Modification

Minimum signal allowed ?

Modify the minimum signal 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.

1.18 Support Cloud Daemon Log Level Adjustment

Log Level ?

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.

1.19 Support SNMPv3

SNMP V3 User

Name	Access Auth.	Auth. Type	Auth. Pwd	Encryption Type	Encryption Pwd
admin	Write	MDS	DES

+ Add new

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.

1.20 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.

1.21 Dynamic VLAN Enhancement

NETWORK SETTINGS

Network Behavior

Default VLAN Behavior ?

VLAN Id

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.

1.22 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.

1.23 Support SpeedTest

Diagnostics

NETWORK UTILITIES

Tools

Server

Server IP Address or Hostname

Start

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.

1.24Support Thailand Regulation

Support Indonesia Regulation. The supported channels are listed below.

1. 2.4GHz: channel 1-13
2. 5GHz: channel 36-48, channel 52-140, channel 149-165

2 Issue Fixed

2.1 The AP cannot connect to the ecCLOUD if 5222 port is blocked.

If 5222 port is blocked, the AP will use 5222 port to connect to the ecCLOUD sometimes. It causes the AP cannot work normally on ecCLOUD. In this version, the issue has been fixed.

2.2 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. This issue has been resolved in this version.

2.3 It takes 30 seconds to pop up the captive portal page when using external captive portal of hotspot.

Enable external captive portal of hotspot on ecCLOUD, create the hotspot-controlled SSID. It takes 30 seconds to pop up the captive portal page. This issue has been resolved in this version.

2.4 The name and IP address of mesh information are N/A in the open mesh page.

Establish the mesh topology. The open mesh link is displayed on wireless status of dashboard page. There is no name and IP address information of the mesh link. In this version, the name and IP address column have been removed in the open mesh page.

2.5 There are a lot of cron messages in the syslog.

Register the AP on ecCLOUD. There are a lot of cron messages printed in the syslog. In this version, these messages have been removed.

2.6 The wireless status is not correct if the first SSID is disabled.

On the radio 5/2.4GHz page, create two or more SSID and disable the first SSID. It cannot display other SSID information on the wireless status of Dashboard. The SSID information can only be displayed if the SSID tab is clicked. This issue has been resolved in this version.

2.7 The channel list cannot be displayed sometimes.

On the radio 5/2.4GHz page, click the channel list. It cannot display the channel list sometimes.

This issue has been resolved in this version.

2.8 Fail to communicate with EPSON TM-m30II-H under MPP in the mesh topology.

Establish the mesh for two APs. The clients are connected to the 2.4 or 5 GHz SSID of MPP. The ping connection with EPSON TM-m30II-H under MPP is periodically disconnected if MAP is connected to MPP through the mesh. This issue has been resolved in this version.

2.9 The authport clients will be logout when the traffic usage of clients exceeds 2GB.

Enable authport on ecCLOUD, create the authport SSID. When the traffic usage of clients exceeds 2GB, clients will be logout forcibly. This issue has been resolved in this version.

2.10 The hostname cannot be displayed correctly when the windows client is connected to the SSID with static IP.

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

2.11 The AP cannot get the IP address for the VLAN tag or mgmt VLAN of Internet setting.

Set the VLAN tag or mgmt VLAN on the Internet settings page of network. The AP cannot get IP through the VLAN tag or mgmt VLAN.

2.12 There is no IP address displayed in the web UI 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 cannot display correctly.

2.13 Interference detection is not working after the user account is added or deleted.

Interference detection is not working after the user account is added or deleted. The function can work after the device is rebooted. This issue has been resolved in this version.

2.14 The UI is not correct when the security is set to WPA3 Enterprise 192-bit

Create the SSID with WPA3 Enterprise 192-bit. After clicking the "Save and Apply" button, the

security of this SSID displays no security on the radio setting page. In this version, the security of the SSID is shown as WPA3 Enterprise 192-bit.

2.15The channel list of 40MHz is not correct.

Go to the Radio 2.4 GHz page of Wireless using the Firefox browser. Select the 40MHz in the channel bandwidth. The channel list of 40MHz is not correct. In the previous version, if the channel list of 20MHz is channel 1-13. The channel list of 40MHz is channel 1-13. This issue has been resolved. In this version, the channel list of 40Mhz is channel 1-9.

2.16The 5GHz radio cannot work in the auto channel with DFS channel sometimes after applying the wireless configuration multiple times.

Select the 5GHz auto channel with DFS channel. Apply the configuration multiple times. Sometimes, the 5GHz radio cannot work. AP should apply configuration again or have the additional reboot. In this version, the 5GHz radio can work normally without any reconfiguration or reboot.

2.17“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.

2.18The 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.

2.19Firewall 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.

2.20iPhone 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

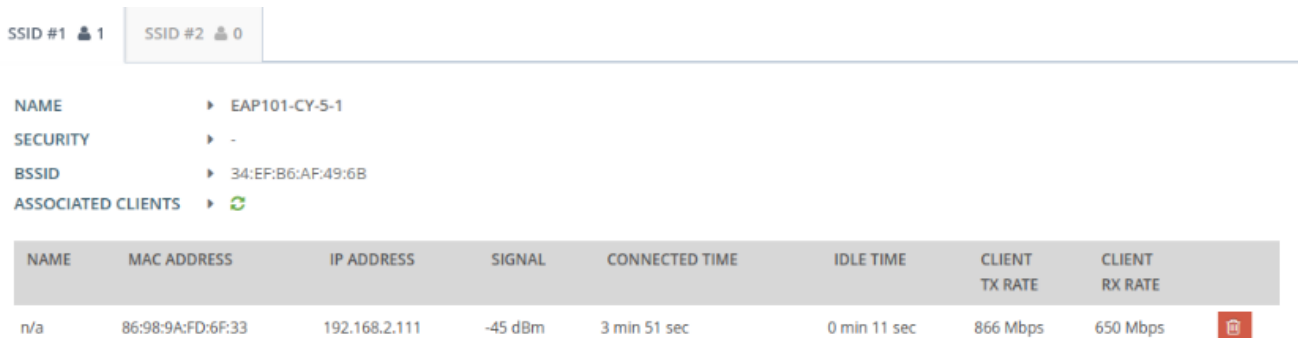
MACs on list” policy. The iPhone failed to connect to the hidden SSID if the private address of iPhone is disabled. In this version, the iPhone can connect to hidden SSID with ACL allowed policy.

2.21 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.

2.22 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.



The screenshot shows the wireless status page for SSID #1 (EAP101-CY-5-1). It displays configuration details like NAME, SECURITY, BSSID, and ASSOCIATED CLIENTS. Below this is a table of associated clients with columns for NAME, MAC ADDRESS, IP ADDRESS, SIGNAL, CONNECTED TIME, IDLE TIME, CLIENT TX RATE, and CLIENT RX RATE. The table shows one client with a signal value of -45 dBm.

NAME	MAC ADDRESS	IP ADDRESS	SIGNAL	CONNECTED TIME	IDLE TIME	CLIENT TX RATE	CLIENT RX RATE
n/a	86:98:9A:FD:6F:33	192.168.2.111	-45 dBm	3 min 51 sec	0 min 11 sec	866 Mbps	650 Mbps

2.23 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.

2.24 Fail to upgrade the FW from 12.3.1 to other versions.

If the current FW version is 12.3.1, the AP can't upgrade the FW to another version in the specific hardware. In this version, this issue has been fixed, and the AP can upgrade to other versions normally.

Affected hardware:

Model	EAP104
HW version	R01 or later version

If firmware v12.3.1 has been installed into the AP, please refer to the following steps on how to

upgrade to v12.4.0 or later version.

- 1 Login to the AP through SSH.
- 2 Type the command below.
 - 2.1 `com-wr.sh /dev/ttyMSM1 1 "\x01\x8B\xFE\x01\x00"`
- 3 Follow the normal procedure to upgrade the firmware.

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.