Release Note

Edgecore OAP101 Release v12.5.7

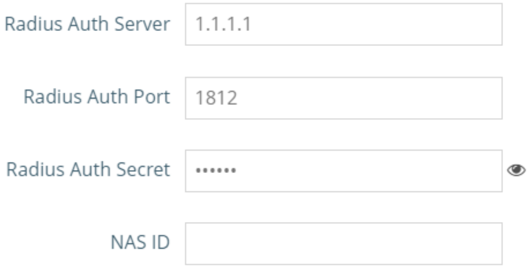
Document # OAP101-v12.5.7-1455-c379f8977

Enhancement from v12.4.3-1070-a14c95a37

Table of Contents

1 Feature

1.1 Support NAS ID



Radius Auth Server: 1.1.1.1

Radius Auth Port: 1812

Radius Auth Secret: ••••••

NAS ID:

Support NAS ID on the radio 5/2.4GHz of wireless page

1. NAS ID: The RADIUS NAS identifier for the SSID interface. This value must be between 1~48 characters long.

1.2 Modify the Default Value of Minimum Signal Allowed

The original default value of minimum signal allowed is -70. In this version, the default value is modified to -100.

1.3 Support Bandwidth Download and Upload per Client

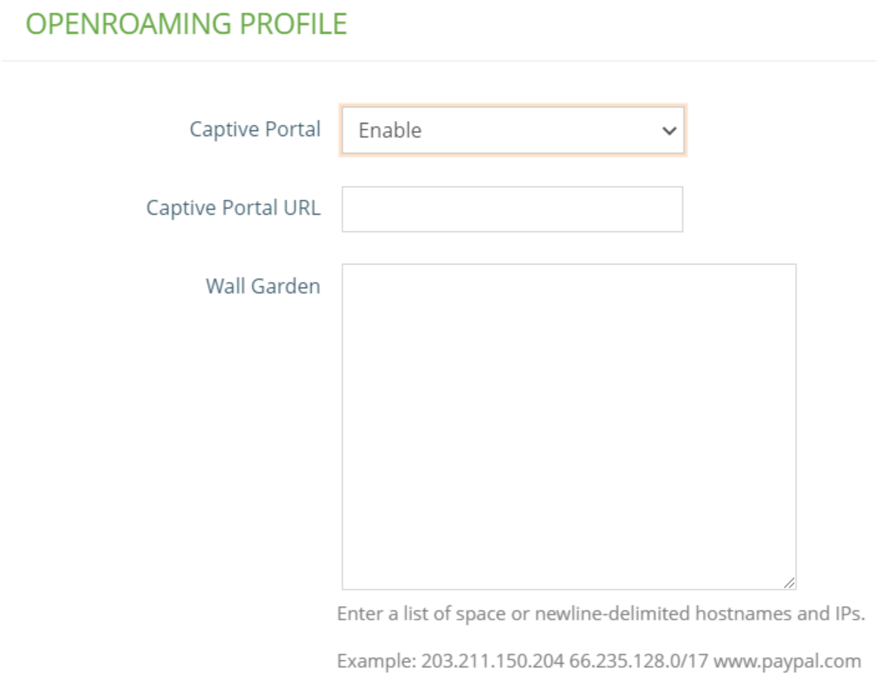
Set the WISPR VSA below in the radius server to configure bandwidth limits for both download and upload per client. When clients connect to the OpenRoaming SSID via the radius server, their bandwidth for download or upload will be restricted.

1. WISPr-Bandwidth-Max-Down: bandwidth download per client.
2. WISPr-Bandwidth-Max-Up: bandwidth upload per client.

1.4 Support Captive Portal in OpenRoaming

Support captive portal, walled garden on the OpenRoaming Profile page.

1. Captive Portal: Enabled or disabled captive portal.
2. Captive Portal URL: Enter the Valid captive portal URL, http or https.
3. Walled Garden: Enter a list of space or newline-delimited hostnames and IPs.



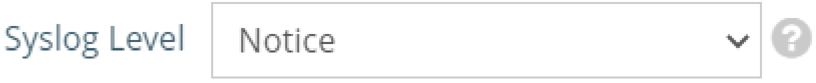
OPENROAMING PROFILE

Captive Portal	Enable
Captive Portal URL	
Wall Garden	

Enter a list of space or newline-delimited hostnames and IPs.

Example: 203.211.150.204 66.235.128.0/17 www.paypal.com

1.5 Support Syslog Level

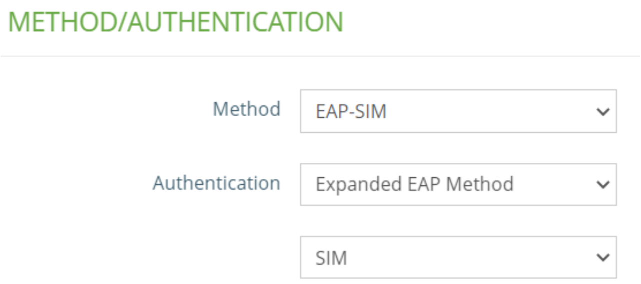


Syslog Level: Notice

Support syslog level on the System Settings page.

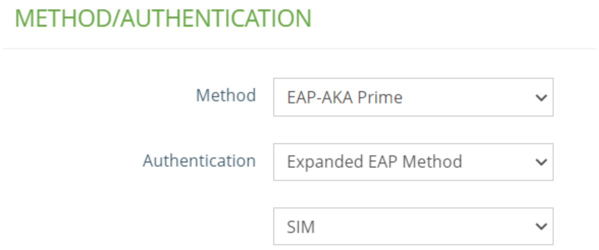
1. Syslog Level: Add the option to adjust the system log level. Info is the default value. The standard ranking of log level is as follows: Debug < Info < Notice < Warning < Error < Critical < Alert < Emergency.

1.6 OpenRoaming Enhancement



METHOD/AUTHENTICATION

Method	EAP-SIM
Authentication	Expanded EAP Method
	SIM



METHOD/AUTHENTICATION

Method: EAP-AKA Prime

Authentication: Expanded EAP Method

SIM

Method modification in the OpenRoaming page.

1. Support EAP-SIM in NAI Realm List.
2. Modify EAP-AKA to EAP-AKA Prime

1.7 Open Mesh Enhancement

In this version, the mesh version has been upgraded to address the issue of ping loss in the mesh.

Please refer to the following method to upgrade the firmware with mesh topology.

It's important to note that the mesh cannot be established with different mesh versions. If the APs are already in a mesh, upgrade the firmware starting from the farthest MAP and concluding with the MPP. If no mesh exists among the APs, upgrade all APs to the provided firmware and then proceed to establish the mesh network.

1.8 Upgrade the version of OpenSSL

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

1. CVE-2023-0286
2. CVE-2022-4304
3. CVE-2023-0215
4. CVE-2022-4450
5. CVE-2023-0464
6. CVE-2023-0465
7. CVE-2023-0466

1.9 TX Power Enhancement

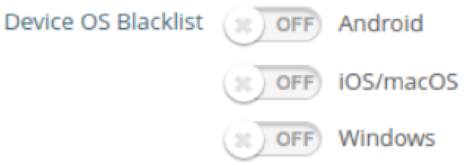
When selecting multiple 5GHz channels, the new version can select the higher TX power.

1.10 Minimum Signal Allowed Enhancement

In the original version, only one value can be set for the minimum allowed signal on the radio card. In this version, the minimum allowed signal can be set to different values for different

SSIDs.

1.11 Support Device OS Blacklist



Device OS Blacklist OFF Android
OFF iOS/macOS
OFF Windows

Support device platform accessibility on the Wireless page.

1. Device OS Blacklist: Check box for three options. Android, iOS / macOS, Windows. Check the box to deny the client OS to connect to the SSID. Uncheck the box to allow the client OS to connect to the SSID.

1.12 Interference Detection Log Enhancement

Add the related log in the syslog when the interference detection is enabled and syslog level is in debug level.

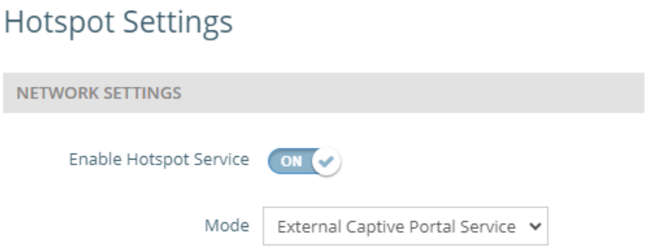
1.13 Support U-APSD

U-APSD ON

Support U-APSD on the Wireless page.

1. U-APSD: Enable or Disable U-ASPD feature that is an 802.11 power save mechanism that works with WMM.

1.14 Support Hotspot Enhancement

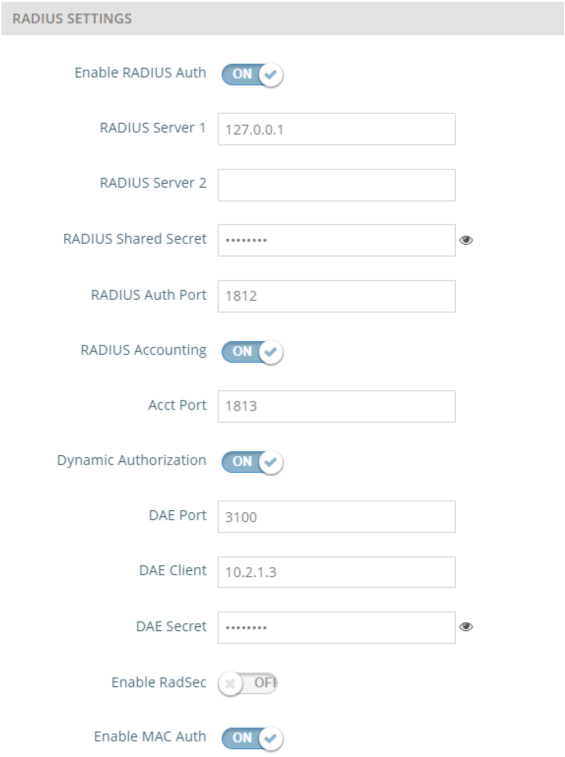


Hotspot Settings

NETWORK SETTINGS

Enable Hotspot Service ON

Mode External Captive Portal Service



RADIUS SETTINGS

Enable RADIUS Auth	ON ✓
RADIUS Server 1	127.0.0.1
RADIUS Server 2	
RADIUS Shared Secret	••••••••
RADIUS Auth Port	1812
RADIUS Accounting	ON ✓
Acct Port	1813
Dynamic Authorization	ON ✓
DAE Port	3100
DAE Client	10.2.1.3
DAE Secret	••••••••
Enable RadSec	✕ OFF
Enable MAC Auth	ON ✓

Hotspot Enhancement

1. Support RADIUS MAC auth. When Radius MAC authentication is enabled, if the associated client is in the RADIUS MAC list, the client can connect to the Internet directly; otherwise, the hotspot captive portal will be displayed.
2. Support Dynamic Authorization. When Dynamic Authorization is enabled, the AP can support dynamic authorization feature by DAE port, DAE client and DAE secret.
3. Support for RADIUS accounting disabled. When Radius accounting is disabled, the AP turns off the RADIUS accounting feature.

2 Issue Fixed

2.1 The value of SNMP sysObjectID is not correct.

In this version, the value of SNMP sysObjectID (1.3.6.1.2.1.1.2) is modified to 1.3.6.1.4.1.259.10.3.41.

2.2 The UDP packet continues to be sent when bandsteering is enabled.

When bandsteering is enabled, the UDP packets will be sent continuously from the AP. In this version, no UDP packets will be sent.

2.3 The captive portal can’t be popped up after changing the hotspot mode.

Create the hotspot controlled SSID and change mode in hotspot settings. When clients are connected to the hotspot controlled SSID, the captive portal can’t be popped up. In this version, clients can connect to the Internet successfully after associated to the hotspot controlled SSID.

2.4 The AP shows the ‘Error parsing configuration’ message after re-adding the AP to ecCLOUD.

2.5 Fail to add the thirty-second OpenRoaming profile.

There is an error message when adding the thirty-second OpenRoaming profile. In this version, the thirty-second profile can be added successfully.

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

IOS devices cannot connect to the SSID with the multiple keys of WPA3 personal transition. In this version, the multiple keys of WPA3 personal transition has been removed.

2.7 The iPhone and laptop couldn't associate with the SSID using the backup RADIUS server.

The iPhone and laptop were unable to establish a connection with the SSID when utilizing the backup RADIUS server. In this version, the issue has been resolved.

2.8 Web display fields invalid when setting multiple keys without optional MAC address.

When configuring the wireless page with WPA2-PSK and multiple keys, an issue has been observed in the web interface. Specifically, when setting multiple keys without including the optional MAC address, the web display fields become invalid. In this version the issue has been resolved.

2.9 RF isolation is not working after restarting the AP.

After enabling the RF isolation feature, the observation was that after restarting the AP, clients could not be isolated by different radio cards. However, in this version, RF isolation now works correctly after restarting the AP.

2.10 With mesh enabled, the device MAC address changes after rebooting the AP multiple times.

When mesh is enabled, the device MAC address changes after multiple reboots of the AP. This issue has been resolved in the current version.

2.11 There is a syntax error during the compilation of the MIB file.

There is a syntax error when importing the MIB file in the MIB browser. In this version, this issue has been resolved.

2.12 ARP inspection is not working.

ARP inspection is not working in the SSID with bridge to Internet. In this version, ARP inspection can work normally.

2.13 There is a possibility that the AP may crash after adding the MAC ACL list on ecCLOUD.

After the addition of the MAC ACL list on ecCLOUD, there is a potential scenario where the AP may experience a crash. In this version, add the mechanism to avoid a crash on the AP.

2.14 ARP Inspection does not function properly when the Windows Netcut is in use.

Enable ARP inspection. The Windows Netcut can successfully disconnect other devices when the clients connect to the SSID bridged to the Internet. However, in this version, the Windows

Netcut cannot disconnect other devices when ARP inspection is enabled

2.15 Clients cannot obtain an IP address under the hotspot with a simple password-only splash page setting.

iPhone and Android clients are unable to obtain IP addresses when using the hotspot with a simple password-only splash page. In this version, the issue has been resolved.

2.16 Clients experience intermittent connectivity issues when connecting to the SSID routed to the Internet.

When clients connect to the SSID routed to the Internet, they experience a brief period where they cannot connect to the Internet, but can establish a connection after a while. In this version, the issue has been resolved.

2.17 The bandwidth control of Openroaming can’t work normally when only setting one bandwidth rule in the radius server.

If only WISPr-Bandwidth-Max-Down or WISPr-Bandwidth-Max-Up is set in the RADIUS server, the bandwidth control for openroaming doesn't function correctly. In this version, the issue has been resolved.

2.18 Some syslog messages are changed to the 'Notice' syslog level.

Some syslog messages were generated at the 'Notice' syslog level. Even the warning message has been changed to 'Notice'.

2.19 The hostname can’t display correctly when certain windows clients are connected to the SSID.

When certain windows clients are 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.

2.20 Hotspot upload bandwidth limitation per client does not function.

The client connects to the SSID with hotspot controlled. If the bandwidth upload limitation VSA (WISPr-Bandwidth-Max-Up) is set in the radius server, the client's bandwidth can be exceeded beyond the limitation. In this version, the issue has been resolved, and the client's upload bandwidth will now be restricted to the specified limitation.

2.21 Some of the syslog times are not correct in the troubleshooting file.

Some timestamps in the troubleshooting file's syslog entries were incorrect. In this version, the issue has been resolved.

2.22 There is no syslog facility and level when the syslog is sent to remote syslog server.

When sending syslog to a remote syslog server, the syslog facility and level are not included. In this version, the syslog facility and level are included.

2.23 Radius failover does not function when the radius serv.er is not running

Fill in the primary and secondary RADIUS server details for the enterprise SSID. If the AP is connected to the enterprise SSID, the RADIUS server will not switch to a backup server when the original RADIUS server is not running but can be pinged.

2.24 The 802.11a mode is not correct.

Set the 802.11a mode on the Radio 5GHz page. The 802.11a configuration is incorrect; it is using the 802.11a+n mode. In this version, the 802.11a configuration is correct.

2.25 Sometimes, the Web UI cannot be accessed due to an out-of-memory issue.

If there are a lot of clients connected to the AP, the Web UI may sometimes become inaccessible due to an out-of-memory issue. In this version, the Web UI can be accessed normally.

2.26 All user accounts can be disabled if an invalid item is set and then the save button is clicked.

If an invalid item is configured and the save button is clicked, all user accounts can be disabled on the UI. In this version, the issue has been resolved.

2.27 High CPU load when there are a lot of multicast packets.

The device experiences a significant increase in CPU load when there is a high volume of multicast packets being processed. The issue has been resolved in this version.

2.28 Client cannot connect to the Internet when CAPWAP tunnel is not ready or disconnected.

Clients are unable to connect to the Internet if the CAPWAP tunnel is not ready or is disconnected. In this version, if the CAPWAP tunnel is not ready or is disconnected, the AP will reject the client association.

2.29 The AP does not support split tunnel with enterprise SSID.

When the AP is managed by the controller, clients can’t connect to the Internet if they connect to the enterprise SSID with a split tunnel. In this version, clients can connect to the SSID successfully.

2.30 Clients cannot connect to the Internet sometimes if switching between 2.4GHz and 5GHz SSID repeatedly.

Clients are unable to connect to the Internet sometimes if they repeatedly switch between the 2.4GHz and 5GHz SSIDs. In this version, the issue has been resolved. The cache mechanism has been enabled to make the client switching between the SSIDs smoothly.

2.31 The memory usage gradually increases when interference detection is running.

2.32 Client information will not be updated in cloud when connecting to Dynamic VLAN SSID.

When a client connects to an SSID with Dynamic VLAN, the ecCLOUD webUI displays correct details but shows incorrect or missing IP information, and marks the client as offline. In this version, the issue has been resolved.

2.33 The wireless client information on the dashboard is incorrect when the client is connected to the Dynamic VLAN SSID.

The dashboard displays incorrect wireless client information when a client is connected to the Dynamic VLAN SSID. In this version, the issue has been resolved.

2.34 SSID and VLAN interface status on the dashboard will occasionally be missing.

After creating multiple SSIDs and multiple VLANs, some SSIDs and interface statuses on the dashboard intermittently disappear after a certain period of time. In this version, the issue has been resolved.

2.35 The security field is not correct after deleting the SSID.

Add multiple SSIDs with WPA2-Personal. After deleting one of the SSIDs, if the security of the other SSIDs change to 'No Security', the WPA2-Personal-related field still remains. In this version, the issue has been resolved.

2.36 The wireless client IP on the dashboard is N/A when some clients are connected to the SSID.

The wireless client IP on the dashboard displays as N/A for certain clients connected to the SSID. This issue has been resolved in this version.

3 Compatible Version for AP Management

Compatible with ecCLOUD

Compatible with EWS-Series controller v3.91.0000 or later