Release Note

Edgecore EAP101 Release v11.2.0

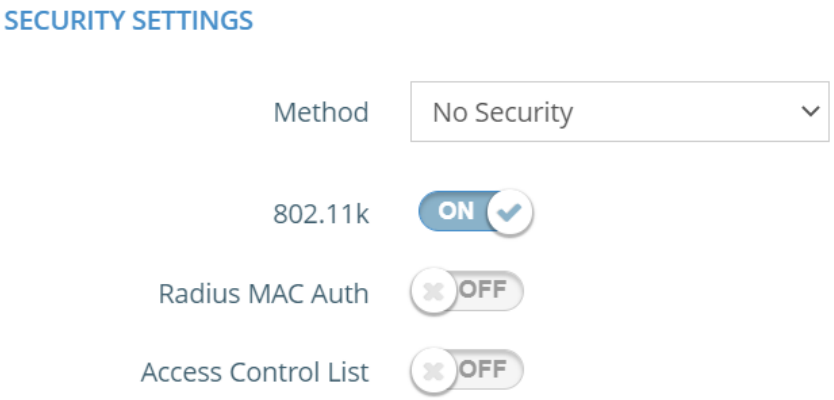
Document # EAP101-v11.2.0-795-824dd3ea

Enhancement from v11.1.1-549-a0b95da

Table of Contents

1 Feature

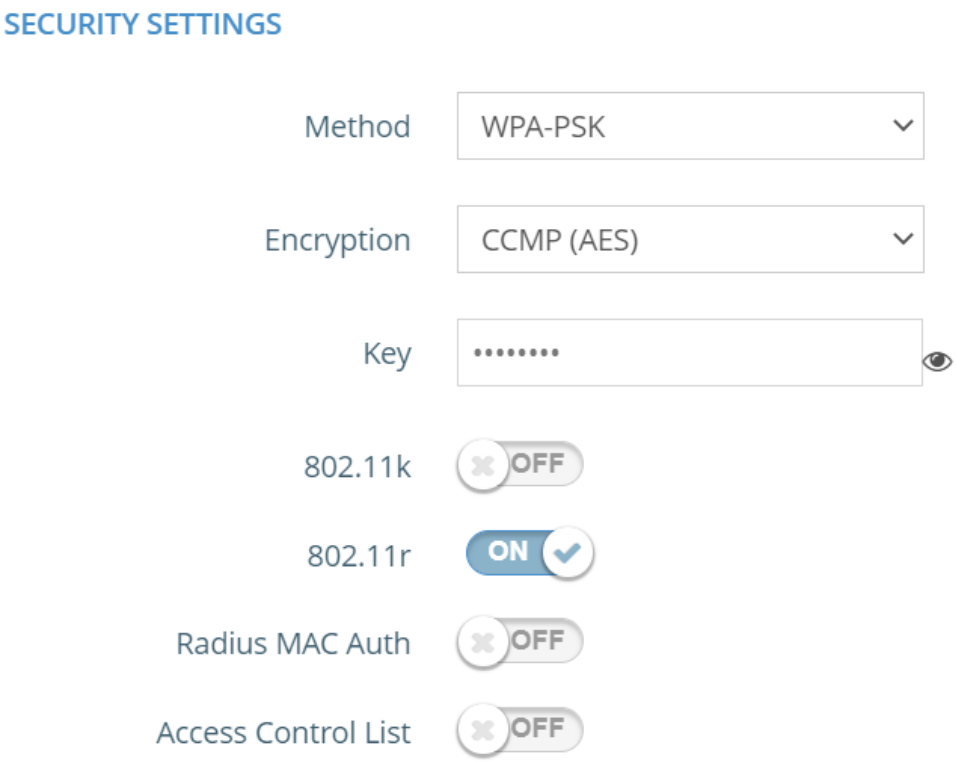
1.1 802.11k



Support 802.11k in the Radio 5/2.4 GHz of Wireless page.

1. 802.11k — Enable or disable 802.11k feature.

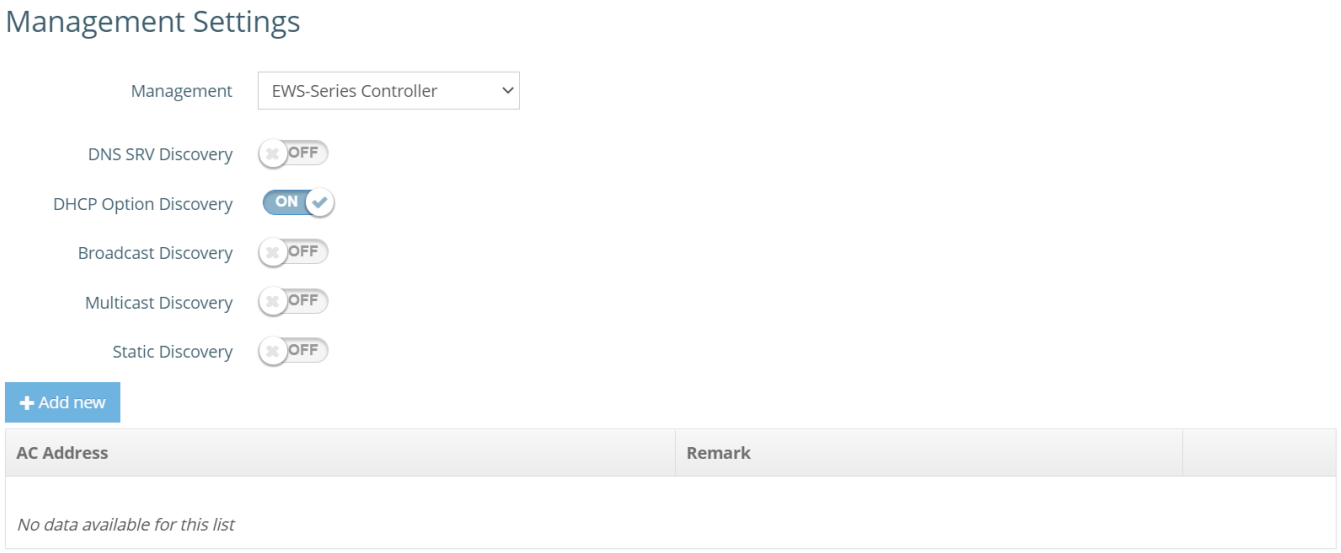
1.2 802.11r



Support 802.11r in the Radio 5/2.4 GHz of Wireless page.

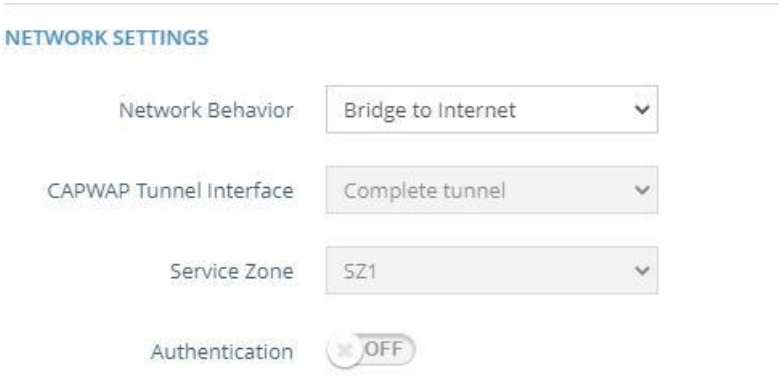
1 802.11r — Enable or disable 802.11r feature.

1.3 AP managed by EWS-Series Controller



Support AP managed by EWS-Series Controller in the System Settings of System page.

1 Management — Selecting EWS-Series Controller means AP is managed by EWS-Series Controller. This option enables the CAPWAP feature by default.
  1.1 DNS SRV Discovery — Using DNS SRV to discover access controller.
  1.2 Domain Name Suffix: Enter the suffix of the access controller, such as example.com.
  1.3 DHCP Option Discovery — Using DHCP option to discover access controller.
  1.4 Broadcast Discovery — Using Broadcast to discover access controller.
  1.5 Multicast Discovery — Using multicast to discover access controller.
  1.6 Static Discovery — Using Static approach to discover access controller.
    1.6.1 AC Address — The IP address of the access controller. If it cannot discover the first AC, it will try to discover the second AC.



2 CAPWAP Tunnel Interface – When AP is managed by EWS-Series Controller, CAPWAP tunnel can be set by EWS5203 template.
  2.1 Disabled – Disable tunnel in EAP101.

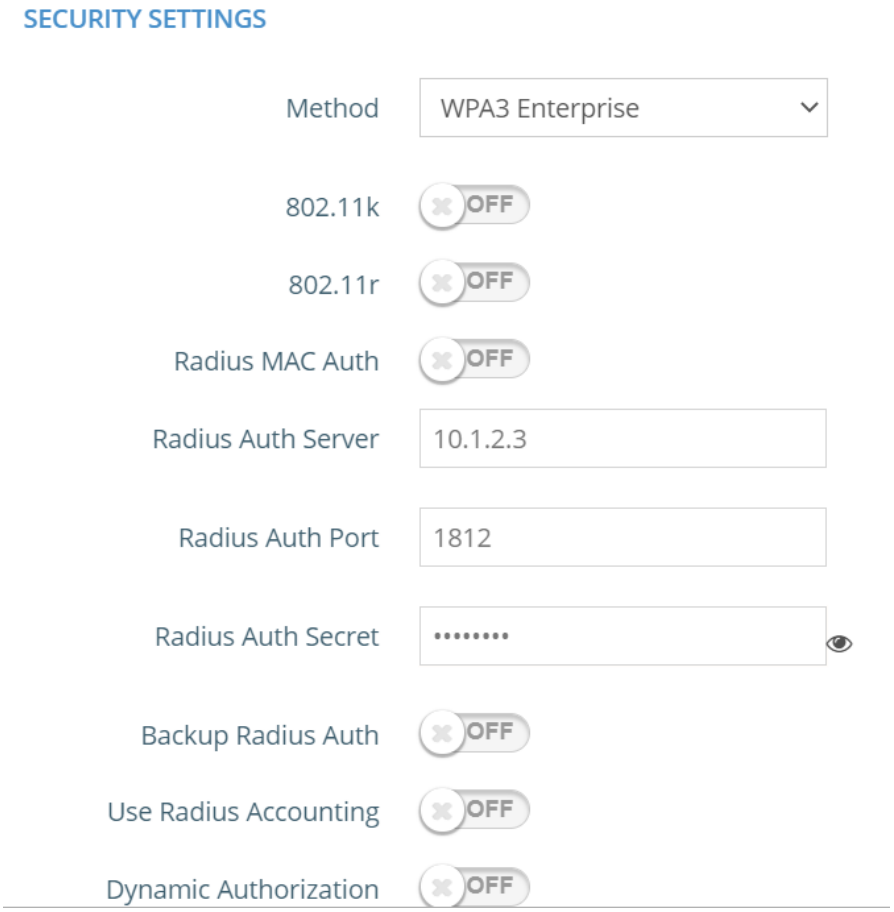
2.2 Complete tunnel – Enable complete tunnel feature.

Note that in this verion, if appying template and AP management are both used in EAP101, please enable CAPWAP and complete tunnel at the same time.

1.4 Japanese Language

Support Japanese Language when selecting the country to Japan in the setup wizard page.

1.5 WPA3-Enterprise / WPA3-Enterprise Transition



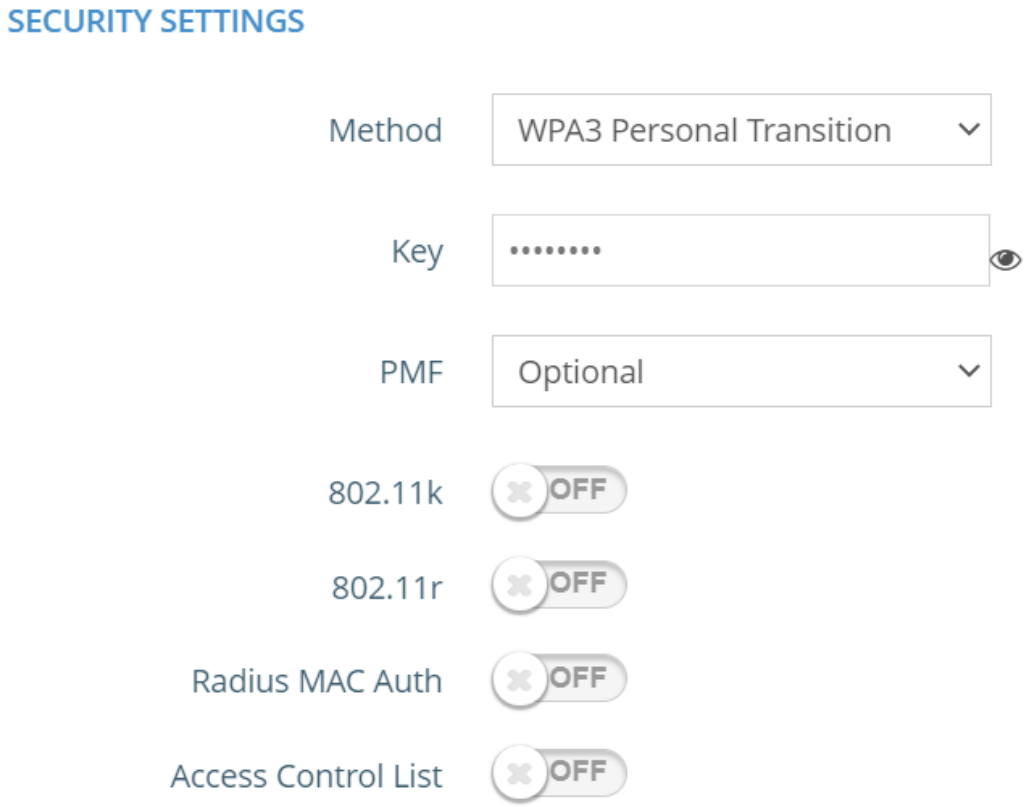
Support WPA3 Enterprise (Transition) in the Radio 5/2.4 GHz of Wireless page.

1 Radius Auth Server — Specifies the IP address or host name of the RADIUS authentication server.
2 Radius Auth Port — The UDP port number used by the RADIUS server for authentication messages.
3 Radius Auth Secret — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on

the RADIUS authentication server. Do not use blank spaces in the string.

4 Backup Radius Auth — Specifies the IP address or host name of the backup RADIUS authentication server.
   4.1 Radius Auth Server — Specifies the IP address or host name of the RADIUS authentication server.
   4.2 Radius Auth Port — The UDP port number used by the backup RADIUS server for authentication messages.
   4.3 Radius Auth Secret — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the backup RADIUS authentication server. Do not use blank spaces in the string.
5 Use Radius Accounting — Enables or disables the feature that the RADIUS server can be used to monitor login and logout times for accounting.
   5.1 Acct Server — Specifies the IP address or host name of the RADIUS accounting server.
   5.2 Acct Port — The UDP port number used by the RADIUS server for accounting messages.
   5.3 Acct Secret — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS accounting server. Do not use blank spaces in the string.
   5.4 Acct Interim Interval — The number of seconds that an accounting session is transmitted.

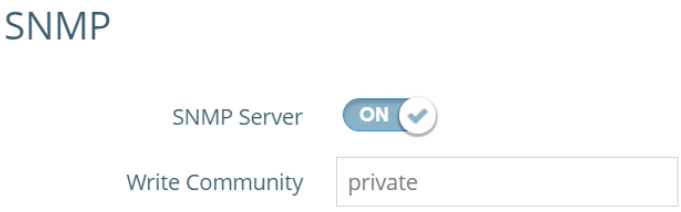
1.6 WPA3-Personal Transition



Support WPA3 Personal Transition in the Radio 5/2.4 GHz of Wireless page.

1. Key — is used to encrypt data transmitted between wireless clients and the VAP.
2. PMF — Protected Management Frames, there are two options, Optional and Mandatory

1.7 SNMP v2

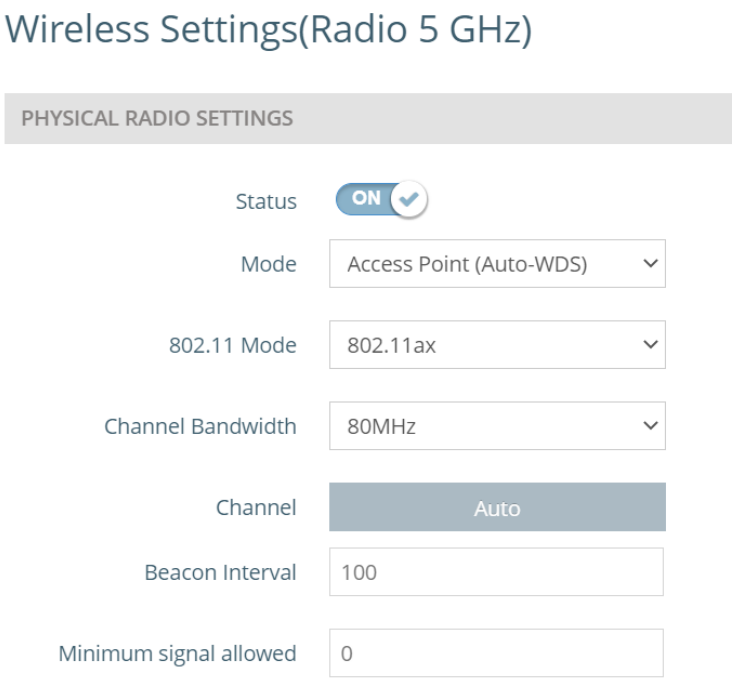


Support SNMP v2 feature in the Services of System page.

The following items are displayed on this page:

1. SNMP Server — Enables or disables SNMP on the access point.
2. Community String — A community string that acts like a password and permits access to the SNMP protocol.

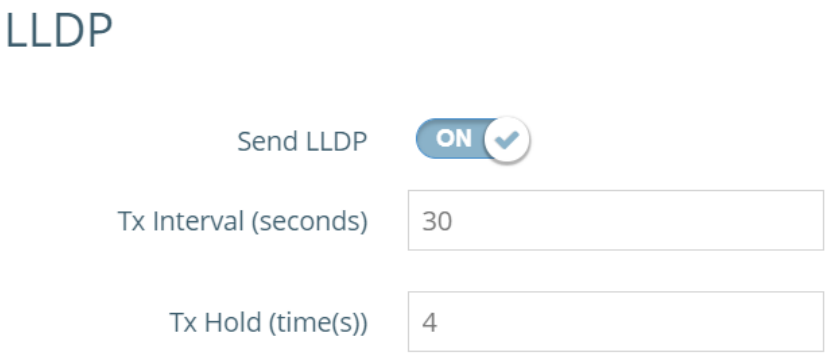
1.8 Minimum signal allowed



Support minimum signal allowed feature in the Radio 5/2.4 GHz of Wireless page.

Only allows clients to associate to this SSID if their signal strength (SNR) is equal or greater than the specified value. Setting the value to zero disables this feature.

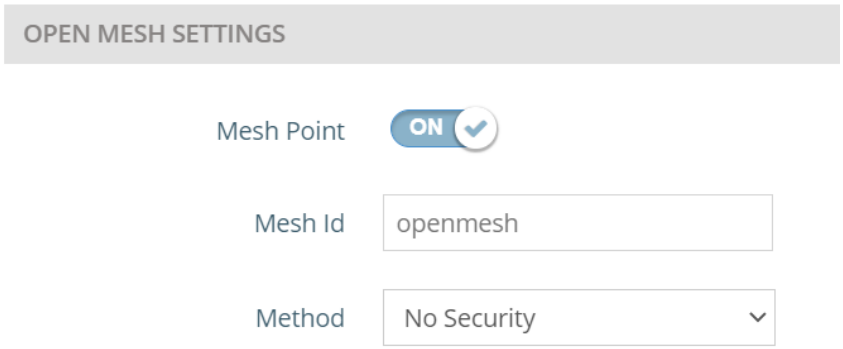
1.9 LLDP



Support LLDP feature in the Services of System page.

1. Send LLDP — Enables or disables LLDP service.
2. Tx Interval (seconds) — Set the number of seconds sending the packets.
3. Tx Hold (time(s)) — Set the times of interval for sending the packets.

1.10 Open Mesh



Support Open Mesh feature in the Radio 5/2.4 GHz of Wireless page.

1. Mesh Point — Enable or disable Open Mesh feature.
2. Mesh Id — Create the mesh id for the purpose of mesh connection.
3. Method — Choose the method for Mesh Id to enhance the security of mesh connection. If selecting the security, the password is needed for all the devices which join the same mesh connection.

2 Issue Fixed

2.1 MTU size is not working

On the Network > Internet Settings page, package can be fragmented to the corresponding MTU size after enter the correct value in the MTU size column.

2.2 Clients can’t connect SSID smoothly when switching to the different EAP101

On the Wireless > Radio 5/2.4 GHz page, set the same SSID name and Bridge to Internet to the SSID in two EAP101. When users connect to the SSID in one EAP101, and switch to another EAP101. Users can connect smoothly without waiting for a long time.

2.3 Auto reboot

In some condition, the AP will experience self-reboot when there is client connecting to the WiFi. This behaviour is resolved in this version.

2.4 Time format is inconsistent

In previous version, the “Local Time” in the System settings display format is different from the NTP display. In this version, both time display will have the same standard.

2.5 Unstable connection issue

Under some condition, there will be some connection issue, where some pings will be lost. In this version we have resolved this behaviour.

2.6 Diagnostics log unable to download

It was reported in the previous version, sometimes cannot download the Diagnostics log.

```
Failed to stat requested path: No such file or directory
```

In this version, this behavior is resolved.

2.7 Dynamic VLAN issue

In the previous version, client cannot connect to the secondary Radius Sever via Dynamic VLAN, after client disconnected from the primary Radius server, and this behaviour is resolved.

2.8 Unable to delete SSID

In some condition, users cannot successfully delete the SSID, and can only delete the SSID which is last created, and this is resolved in this version.

2.9 Unable to connect

This version has resolved the behaviour when the Minimum Signal allowed is configured as 0, users might not be able to connect.

2.10 Duplicate VLAN warning message

When setting the same VLAN-tagged SSID at the same time, UI will show multiple duplicate warning message, in this version, the warning message will be displayed once.

2.11 Unable to check incorrect MAC address format in ACL

This version has resolved the issue that UI doesn’t have the MAC address data check rule in filtered MACs of Access Control List (ACL), this may cause radio unstable.

2.12 Unable to use 802.11r in WPA3 Personal

In this version, 802.11r can work normally in WPA3 Personal SSID.

2.13 Unstable 2.4G radio

When changing 2.4G & 5G mode & bandwidth repeatedly, 2.4G radio can’t work normally, in this version, this is resolved.

2.14 The missing IP and name of associated clients

The version has resolved the behavior when clients are associated to the SSID setting to Bridge or VLAN-tagged traffic mode, the IP and name can’t be displayed in the associated clients list of wireless status page.

2.15 LAN2 port link-down

When changing network behavior of LAN2 port for several times, LAN2 can’t work normally. This issue is resolved in this version.

2.16 SSID reduction during open mesh operation

This version has resolved the behavior that when repeatedly enable and disable the open mesh

button in Radio 5 GHz page, the number of SSID will decrease.

2.17 Unstable open mesh

In this version, the connection of WAN port can work normally when using open mesh.

2.18 Incorrect total associated client using dynamic VLAN

In this version, the total associated client can be displayed normally when clients are associated to the SSID using dynamic VLAN.

2.19 EAP102 config data can restore to EAP101

This version has resolved that EAP102 config data can’t restore to EAP101 successfully.

2.20 Auto beacon interval adjustment

This version has added the beacon interval adjustment rule that in the same radio card, if using more than 7 SSIDs, the beacon interval will be adjust to 500ms automatically. If using more than 4 SSIDs, the beacon interval will be adjust to 250ms automatically.

2.21 Save & apply button can’t work

This version has resolved that “save&apply” button can’t work normally in wireless page.

2.22 Backup radius authentication UI can’t work properly using WPA2-EAP

When enabling WPA2-EAP and backup radius authentication, the UI can’t display correctly. In this version, this issue has been resolved.

3 Compatible Version for AP Management

Compatible with ecCLOUD
Compatible with EWS5203 v3.50.0000