



Release Note

Edgecore EWS5203 Release v3.52.0100

Document # Edgecore_EWS5203_ERN_v3.52.0100

Enhancement from v3.52.0001

Copyright Notification

Edgecore Networks Corporation

© Copyright 2021 Edgecore Networks Corporation.

The information contained herein is subject to change without notice. This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered by Edgecore Networks Corporation. Edgecore Networks Corporation shall not be liable for technical or editorial errors or omissions contained herein.

Revision History

Date	Version	Author	Remark
2022/ 1 / 25	V1.0	Bill Chen	Release Note for v3.52.0100
2022/ 3 / 9	V1.1	Bill Chen	Release Note for v3.52.0100
2022/ 3 / 15	V1.2	Bill Chen	Release Note for v3.52.0100
2022/ 4 / 13	V1.3	Bill Chen	Release Note for v3.52.0100
2022/ 5 / 17	V1.4	Bill Chen	Release Note for v3.52.0100

Table of Contents

1	AP Management Compatibility.....	4
1.1	Compatible Versions for AP Management.....	4
2	Feature Enhancement.....	5
2.1	Support OAP100e and SP-W2M in WAPM and OAP100e in LAPM	5
2.2	Support WiFi6 QoS.....	5
2.3	Support NMS management	6
2.4	Add Download Button in Management Event Download	6
2.5	Modify Method to Security Method in New Generation WAPM template	7
2.6	Modify the Name of WAPM Template.....	7
2.7	Support USB syslog	8
2.8	Support Microsoft 365 Authentication.....	9
2.9	Support Import AP List.....	11
2.10	Support HA WAN Failover	11
2.11	Syslog and Remote Syslog Enhancement	12
2.12	Add the ARP Inspection Setting	13
2.13	Upgrade Firmware Procedure to Prevent Template Collapse in HA Mode	13
2.14	Add user event log when authentication method is 802.1x without CAPWAP tunnel	14
2.15	Support Midtrans Payment Gateway.....	14
2.16	Support Work from Home Mode for SP-W2M-AC1200.....	15
3	Issue Fixed.....	16
3.1	The OSM file format can't be uploaded to the floor plan of Wall in WiFi monitor	16
3.2	Radius MAC Auth and split tunnel can't be set at the same time in New Generation WAPM template.....	16
3.3	VLAN tag traffic of network behavior can be set to AP without VLAN ID in New Generation WAPM template.....	16
3.4	There is no input restriction on CCA Minimum power column in Legacy WAPM template ...	16
3.5	The information of service zone and VLAN data is not correct on online users after clients are associated to the WiFi6 AP SSID with enabling 802.1x, split tunnel and dynamic VLAN in New Generation WAPM template at the same time.	16
3.6	The service zone of split tunnel is incorrect in New Generation template	16
3.7	The wrong warning message of RSSI threshold in Legacy WAPM for Japanese version	16
3.8	There is no warning message if the VLAN tag traffic SSID with split tunnel is set to the same service zone as the bridge mode SSID with split tunnel in New Generation WAPM	16
3.9	The Radius MAC auth can't be enabled with Split tunnel and WPA2 PSK at the same time in New Generation WAPM.....	16
3.10	The Auto-Negotiation and Speed / Duplex of WAN information are not correct after HA is	

established	16
3.11 In HA mode, standby controller can't become active sometimes after upgrading the FW from the standby controller	16
3.12 Proxy ARP of Legacy WAPM template can't be configured by the controller	16
3.13 The OID (.1.3.6.1.4.1.259.3.4.3) can't be displayed correctly	16
3.14 Some descriptions are not correct in the MIB files	16
4 Known Issue	17
4.1 The Billing Plan Selection Page with Midtrans payment gateway can't display correctly when previewing the page. After clicking apply button, the page will display the correct page.	17

1 AP Management Compatibility

1.1 Compatible Versions for AP Management

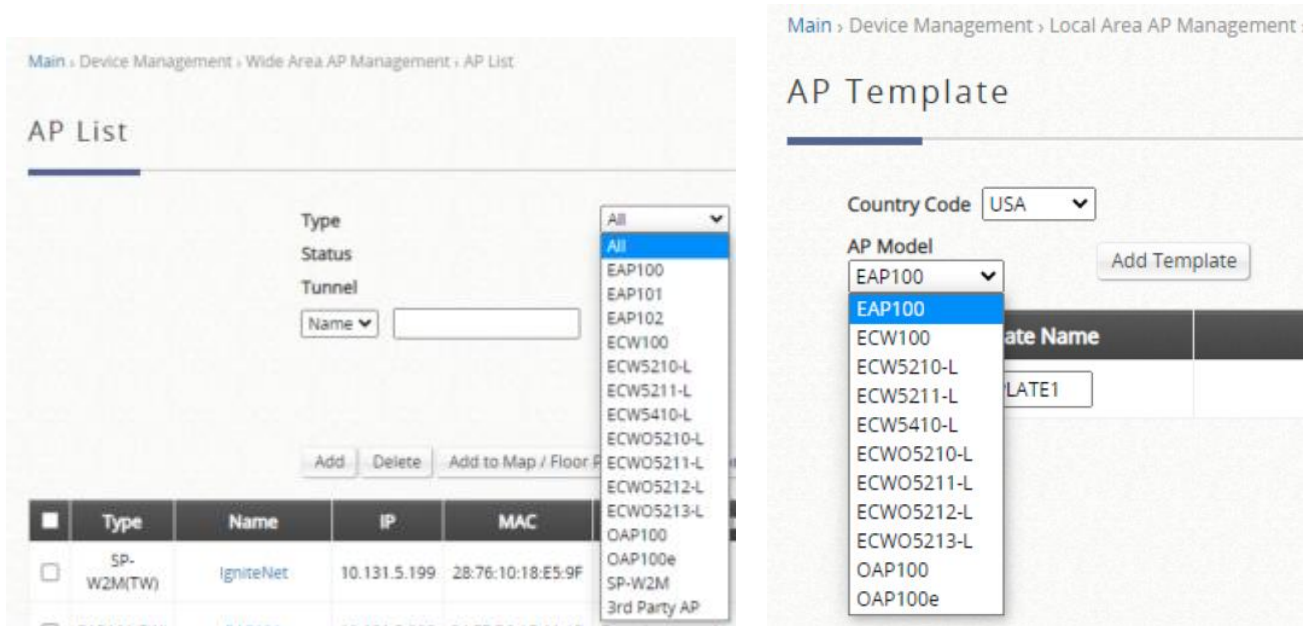
AP type	LAPM	WAPM	Compatible version
OAP100	V	V	3.45.0000 or newer
OAP100e	V	V	3.45.0000 or newer
EAP100	V	V	3.45.0000 or newer
ECW100	V	V	3.45.0000 or newer
ECW5210-L	V	V	3.45.0000 or newer
ECW5211-L	V	V	3.45.0000 or newer
ECW5410-L	V	V	3.45.0000 or newer
ECWO5210-L	V	V	3.45.0000 or newer
ECWO5211-L	V	V	3.45.0000 or newer
ECWO5213-L	V	V	3.45.0000 or newer
EAP101		V	11.2.0-795 or newer
EAP102		V	11.2.0-796 or newer
SP-W2M-AC1200		V	7.0.0-2987 or newer
3rd Party		V	

2 Feature Enhancement

2.1 Support OAP100e and SP-W2M in WAPM and OAP100e in LAPM

In Devices > WAPM, OAP100e and SP-W2M can be supported.

In Devices > LAPM, OAP100e can be supported.



2.2 Support WiFi6 QoS

The QoS feature can be supported in WiFi6 AP like EAP101 and EAP102.

With split tunnel SSID, only Individual maximum downlink/uplink are supported.

With complete tunnel SSID, Group total downlink/uplink, Individual maximum downlink/uplink, and individual request downlink/uplink are supported.

Main > Users > Policies > QoS

Select QoS Profile QoS 1

QoS Configuration

QoS Profile Name QoS 1

Traffic Class IPv4 IPv6

Bandwidth Control Enable Disable

Group Total Downlink 0 Mbps

Group Total Uplink 0 Mbps

Individual Maximum Downlink 5 Mbps

Individual Maximum Uplink 5 Mbps

Individual Request Downlink 3 Mbps

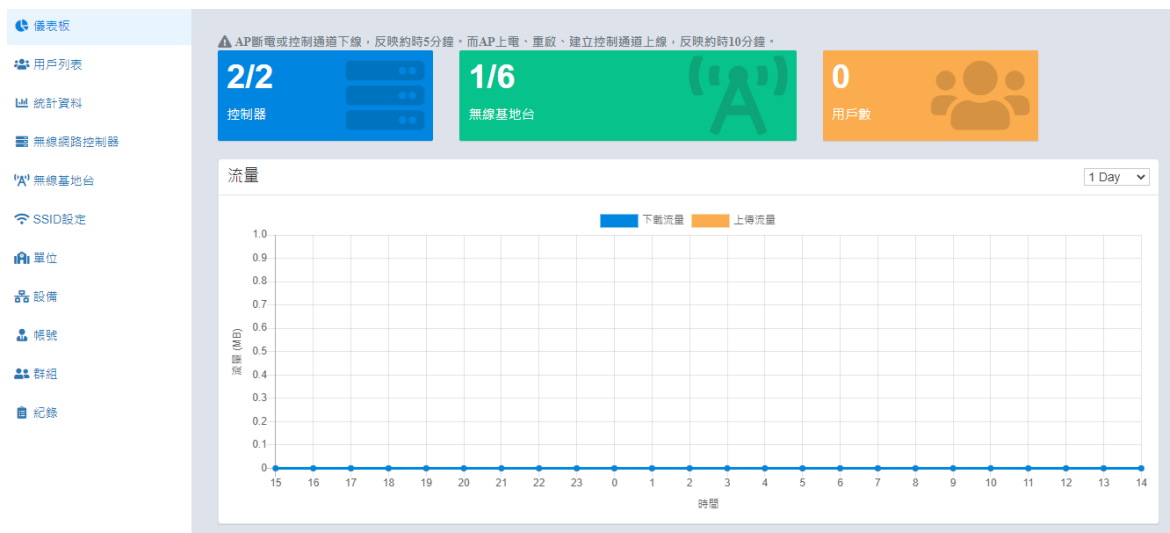
Individual Request Uplink 3 Mbps

*(Unlimit: 0, Range: 1-999)

Apply Cancel

2.3 Support NMS management

NMS can manage EWS5203. The AP, controller and user status can be displayed on NMS.



2.4 Add Download Button in Management Event Download

In Status > Logs & Reports > Management Events page, the download button is added. After clicking the button, the management event report will be written in the txt file and be downloaded into the device.

System Summary
Interfaces
Monitor Users
WiFi Monitor
Process Monitor
Logs & Reports
CAPWAP Log
Configuration Change Log
Local Monthly Usage
Local Web Log
Micros Opera Log
On-Demand Billing Report
RADIUS Server Log
SIP Call Usage
SMS API Log
System Log
UAMM Log
User Events
Alarm
Management Events
Reporting
Sessions
DHCP Leases
Routing Tables

Main > Status > Logs and Reports > Management Events
Management Events

Download

Show 10 entries

ID	Source	Item	Reason	Timestamp
1	EAP101	AP Online	AP Online.	Thu, 30 Dec 2021 11:20:28
2	EAP101	AP Online	AP Online.	Thu, 30 Dec 2021 11:20:58
3	EAP101	AP Offline	AP Offline.	Thu, 30 Dec 2021 11:37:10
4	EAP101	AP Offline	AP Offline.	Thu, 30 Dec 2021 11:46:10
5	EAP101	AP Offline	AP Offline.	Thu, 30 Dec 2021 13:44:23
6	EAP101	AP Online	AP Online.	Thu, 30 Dec 2021 13:47:59
7	EAP101	AP Offline	AP Offline.	Thu, 30 Dec 2021 14:18:11
8	EAP101	AP Offline	AP Offline.	Thu, 30 Dec 2021 18:00:15
9	EAP101	AP Online	AP Online.	Thu, 30 Dec 2021 18:02:08

Showing 1 to 9 of 9 entries

Previous 1 Next

2.5 Modify Method to Security Method in New Generation WAPM template

In Device > WAPM > Template page, modify the name from Method to Security Method in the Wireless Network.

Main > Device Management > Wide Area AP Management > Template > Wireless Network Settings

Wireless Network Settings - 13: Template 13

Radio	5G
VAP	Guest Network <input type="button" value="Add"/> <input type="button" value="Remove"/>
Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
SSID	Guest Network
Broadcast	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Client Isolation	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
WMM	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Max Clients	127
Idle Timeout	300
Security Method	None

2.6 Modify the Name of WAPM Template

In Device > WAPM > Template page, modify from WiFi5 to Legacy and WiFi6 to New Generation in the Select Product Type.

Legacy devices supported: OAP100, OAP100e, EAP100, ECW100, ECW5210-L, ECW5211-L, ECW5410-L, ECWO5210-L, ECWO5211-L, ECWO5213-L

New Generation devices supported: EAP101, EAP102, SP-W2M-AC1200

Main > Device Management > Wide Area AP Management > Template

Template AP Setting

Select Product Type	New Generation ▾	
Select Template	1: Template 1 ▾	
Template Name	Template 1	Apply
Country	Taiwan ▾	
Radio	Configure	
Wireless Network	Configure	
VLAN Settings	Configure	
Copy Settings to	None ▾	Apply

2.7 Support USB syslog

1. HA Mode – standby controller

In System > High Availability page, SYSLOG Settings page can be supported in standby controller when HA is established. Syslog can be stored into the USB storage when plugging into the USB port of standby controller.

Main > System > High Availability Configuration

Current Status

Dedicated Port	LAN1	
Status	Peer is detected	
Link to Peer's UI	SYSLOG Settings ▾	Goto
Version	10000	

2. HA Mode – active controller

Syslog can be stored into the USB storage when plugging into the USB port of active controller.

SYSLOG Settings

SYSLOG Enabled Disabled

SYSLOG Server

Server 1

IP Address:

Port:

Server 2

IP Address:

Port:

USB Storage No Device

Severity Level

3. Non-HA Mode

Syslog can be stored into the USB storage when plugging into the USB port of controller.

SYSLOG Settings

SYSLOG Enabled Disabled

SYSLOG Server

Server 1

IP Address:

Port:

Server 2

IP Address:

Port:

USB Storage No Device

Severity Level

2.8 Support Microsoft 365 Authentication

In the Users > External Authentication > Microsoft 365, the Microsoft 365 can be configured. When using Service zones, Microsoft 365 can be selected to be the authentication that users can be authenticated by.

Microsoft 365 Settings

Group: Group 1

LDAP Server Settings

Server: (Domain Name/IP Address)

Port: (e.g. 389 for LDAP, 636 for LDAPS)

Service Protocol: LDAP LDAPS LDAP+StartTLS

Base DN:

Binding Type: Anonymous

Account Attribute: UID CN

Attribute-Group Mapping: Configure

Authorization Endpoint: *

Token Endpoint: *

Client Id: *

Permissions: *

Client Secret: *

Redirect URI:

Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>
Guest	FREE	N/A	<input type="radio"/>	<input type="checkbox"/>
Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>
One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>
Microsoft 365	MICROSOFT365	N/A	<input type="radio"/>	<input type="checkbox"/>

2.9 Support Import AP List

In the Device > Wide Area AP Management > AP list, add import button to import the csv file. After importing the list including default template, AP can apply the default template when adding the AP into the WAPM.

Main > Device Management > Wide Area AP Management > AP List

AP List

Type: All
 Status: All
 Tunnel: None
 Name: Search

Refresh Interval: 10 seconds Refresh

Add Delete Add to Map / Floor Plan Backup Config Restore Config Upgrade Apply Settings Reboot Export Import

■	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number	Repair Method	From Template/Config
<input type="checkbox"/>	SP-W2M(TW)	IgniteNet	10.131.5.199	28:76:10:18:E5:9F	Overview	1	Offline	0	N/A	Go	N/A	7.0.0-2978	AI29022089	Disabled	
<input type="checkbox"/>	EAP101(TW)	EAP101	10.131.5.208	34:EF:B6:AF:4A:1B	Overview	1	Online	0	N/A	Go	RUN	11.4.0-1076	EC2038000743	Disabled	
<input type="checkbox"/>	OAP100e	Edgecore-OAP100e	10.131.5.88	1C:EA:0B:C7:34:E4	Overview	1	Online	0	Edit	System Overview Go	RUN	3.45.0000	EC1939001533	Disabled	

Main > Device Management > Wide Area AP Management > Import AP List

Import AP List

Option: Insert Update

File Name: 選擇檔案 未選擇任何檔案

2.10 Support HA WAN Failover

In System > WAN page, enter IP address or domain name in the "Target for detecting Internet connection" of WAN traffic settings. Set up the HA peer. WAN HA failover mechanism will be enabled to switch HA when WAN1 fails to ping IP address or domain name.

Note: Only WAN1 is connecting to the Internet. If WAN1 fails to ping each IP address or domain name in the above list, HA will be triggered.

Target for Detecting Internet Connection

8.8.8.8

Enter IP Address/Domain Name Here

Enter IP Address/Domain Name Here

Warning of Internet Disconnection

When the addresses for detecting Internet connection are unreachable, this message will be shown on the browser.

Sorry! The service is temporarily unavailable.

2.11 Syslog and Remote Syslog Enhancement

There are four types of the log to be recorded into the system log and remote syslog server.

1. In HA mode, when the active controller becomes standby, remote syslog and local system log will receive the message below:

Active gateway, IP address, mode changed to DOWN.

Standby gateway mode is going to change to ACTIVE.

```
2022-03-07T16:33:38+08:00 10.131.5.166 logd@EWS5203 ciphahellod[2698]: HOTSWAP event is got, go to Disbaled Mode
2022-03-07T16:33:38+08:00 10.131.5.166 logd@EWS5203 root: Active gateway, 10.131.5.166, mode changed to DOWN.
2022-03-07T16:33:38+08:00 10.131.5.166 logd@EWS5203 root: Standby gateway mode is going to change to ACTIVE.
2022-03-07T16:33:43+08:00 10.131.5.166 logd@EWS5203 root: [Process Monitor] Last check time: 2022-03-07 16:33:43 +0800
2022-03-07T16:34:33+08:00 10.131.5.166 logd@EWS5203 root: [Process Monitor] Last check time: 2022-03-07 16:34:33 +0800
```

2. In HA mode, when the standby controller becomes active, remote syslog and local system log will receive the message below:

Standby gateway mode changed to DOWN.

```
2022-03-08T11:41:17+08:00 10.131.5.166 logd@EWS5203 root: NTP time.nist.gov synchronized successfully.
2022-03-08T11:41:25+08:00 10.131.5.166 logd@EWS5203 proxy: Proxy Server starts!
2022-03-08T11:41:25+08:00 10.131.5.166 logd@EWS5203 proxy: Proxy.Logout Server starts!
2022-03-08T11:41:25+08:00 10.131.5.166 logd@EWS5203 proxy: Proxy.Fake Server starts!
2022-03-08T11:41:25+08:00 10.131.5.166 logd@EWS5203 proxy: Proxy Server: Can't bind local address
2022-03-08T11:41:25+08:00 10.131.5.166 logd@EWS5203 root: Standby gateway mode changed to DOWN.
2022-03-08T11:41:25+08:00 10.131.5.166 logd@EWS5203 ciphahellod[2579]: Primary Mode is running
2022-03-08T11:41:26+08:00 10.131.5.166 logd@EWS5203 root: [Process Monitor] Last check time: 2022-03-08 11:41:26 +0800
```

3. In HA mode, the active controller detects down of standby controller because HA peer is disconnected, remote syslog and local system log will receive the message below:
Standby is not found.

```

2022-03-08T11:41:25+08:00 10.131.5.166 logd@EWS5203 proxy: Proxy Server: Can't bind local address
2022-03-08T11:41:25+08:00 10.131.5.166 logd@EWS5203 root: Standby gateway mode changed to DOWN.
2022-03-08T11:41:25+08:00 10.131.5.166 logd@EWS5203 ciphahellod[2579]: Primary Mode is running
2022-03-08T11:41:26+08:00 10.131.5.166 logd@EWS5203 root: [Process Monitor] Last check time: 2022-03-08 11:41:26 +0800
2022-03-08T11:41:28+08:00 10.131.5.166 logd@EWS5203 root: Error: Standby is not found.

```

4. When WAN detection is enabled, all WANs are down. The local system log will receive the message below:

root: WAN FAIL

```

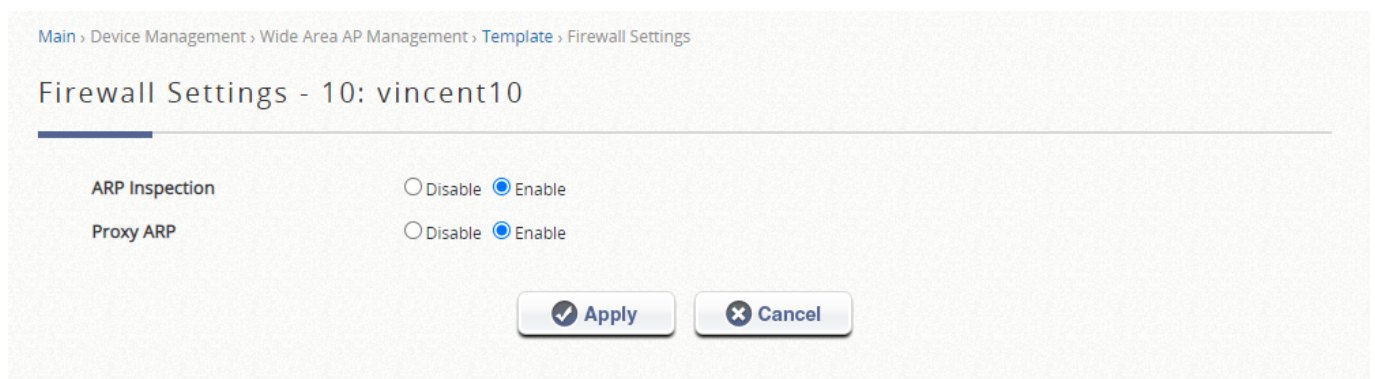
Mar  8 12:18:58 @EWS5203 <daemon.info> root: [Process Monitor] Last check time: 2022-03-08 12:18:58 +0800
Mar  8 12:19:48 @EWS5203 <daemon.info> root: [Process Monitor] Last check time: 2022-03-08 12:19:48 +0800
Mar  8 12:20:38 @EWS5203 <daemon.info> root: [Process Monitor] Last check time: 2022-03-08 12:20:38 +0800
Mar  8 12:21:28 @EWS5203 <daemon.info> root: [Process Monitor] Last check time: 2022-03-08 12:21:28 +0800
Mar  8 12:22:18 @EWS5203 <daemon.info> root: [Process Monitor] Last check time: 2022-03-08 12:22:18 +0800
Mar  8 12:22:50 @EWS5203 <user.notice> root: WAN FAIL
Mar  8 12:22:50 @EWS5203 <daemon.info> dnsmasq[20736]: reading /etc/resolv.conf
Mar  8 12:22:50 @EWS5203 <daemon.info> dnsmasq[20736]: using nameserver 8.8.4.4#53
Mar  8 12:22:50 @EWS5203 <daemon.info> dnsmasq[20736]: using nameserver 8.8.8.8#53
Mar  8 12:22:50 @EWS5203 <daemon.info> dnsmasq[20736]: exiting on receipt of SIGTERM
Mar  8 12:22:50 @EWS5203 <daemon.info> dnsmasq[21907]: started, version 2.51 cachesize 150

```

2.12 Add the ARP Inspection Setting

In Device > WAPM > Template page, add the ARP inspection setting in Legacy template to be compatible with the APs which use the Edgecore developed proxy ARP and original proxy ARP.

Note that if the AP uses Edgecore developed proxy ARP, ARP Inspection should be enabled when using Proxy ARP feature.



2.13 Upgrade Firmware Procedure to Prevent Template Collapse in HA Mode

In HA mode, if there is a major version change marked as red font (e.g., 3.50.0001 to 3.52.0100) and the FW should be updated to controller, HA should be disabled before upgrading the FW. Follow the below upgrade procedure to prevent template collapse after upgrading the FW.

1. Both units using firmware (e.g., 3.50.0001) have HA enabled and configured the desired templates.

2. Unplug both WAN and LAN1 port connections on the Standby unit and locally access unit to disable HA.
3. Upgrade Active unit to the latest FW (3.52.0100) first.
4. Upgrade Standby unit to the latest FW (3.52.0100) by connecting a computer to any LAN on the unit and perform the upgrade locally.
5. Once both units have been upgraded, connect to Standby unit and enable HA. While controller is rebooting, please connect both WAN and LAN port to the unit.

2.14 Add user event log when authentication method is 802.1x without CAPWAP tunnel

Create the SSID with 802.1x without CAPWAP tunnel in the AP. After users is connected to this SSID, there are four types of user event logs shown in the user events messages. (Status > Logs & Reports > User Events)

Radius events	User events
Accept	Login
Reject	Reject
Accounting start	Online
Accounting stop	Offline

2.15 Support Midtrans Payment Gateway

In Users > Internal Authentication > On-Demand > Payment Gateway, Midtrans option is added in the external payment gateway option. The On-demand account will be created after buying a new account online through Midtrans payment.

Main > Users > Internal Authentication > On-Demand Authentication > External Payment Gateway

External Payment Gateway

Selection

Disable
 Authorize.Net
 PayPal
 SecurePay
 WorldPay
 PeleCard
 Midtrans

Number of SMS quota *(1-10) [SMS gateway configure](#)

The function to send SMS after purchasing an account is not ready. This is the given SMS quota to the client when multiple messages are required, either for multiple devices or if the SMS needs to be re-sent.

Midtrans Payment Page Configuration

Transaction URL *

Server Key *

Client Key *

Currency *

2.16 Support Work from Home Mode for SP-W2M-AC1200

In Device > WAPM > New Generation Template > Wireless Network, add WFH (Work from home) mode in the CAPWAP Tunnel Interface. This feature is only compatible with SP-W2M-AC1200.

The screenshot shows the configuration interface for the CAPWAP Tunnel Interface. The settings are as follows:

- Network Behavior:** Bridge to Internet (dropdown)
- Vlan Id:** 1000 (dropdown) with a **Configure** button
- CAPWAP Tunnel Interface:** WFH Mode (dropdown)
- Service Zone:** Default (dropdown)
- WFH Subnet List:** An empty text area for entering subnets.
- Limit Upload:** Disable (dropdown)
- Limit Download:** Disable (dropdown)

At the bottom right, there are **Apply** and **Cancel** buttons.

3 Issue Fixed

- 3.1 The OSM file format can't be uploaded to the floor plan of Wall in WiFi monitor**
- 3.2 Radius MAC Auth and split tunnel can't be set at the same time in New Generation WAPM template**
- 3.3 VLAN tag traffic of network behavior can be set to AP without VLAN ID in New Generation WAPM template**
- 3.4 There is no input restriction on CCA Minimum power column in Legacy WAPM template**
- 3.5 The information of service zone and VLAN data is not correct on online users after clients are associated to the WiFi6 AP SSID with enabling 802.1x, split tunnel and dynamic VLAN in New Generation WAPM template at the same time.**
- 3.6 The service zone of split tunnel is incorrect in New Generation template**
- 3.7 The wrong warning message of RSSI threshold in Legacy WAPM for Japanese version**
- 3.8 There is no warning message if the VLAN tag traffic SSID with split tunnel is set to the same service zone as the bridge mode SSID with split tunnel in New Generation WAPM**
- 3.9 The Radius MAC auth can't be enabled with Split tunnel and WPA2 PSK at the same time in New Generation WAPM**
- 3.10 The Auto-Negotiation and Speed / Duplex of WAN information are not correct after HA is established**
- 3.11 In HA mode, standby controller can't become active sometimes after upgrading the FW from the standby controller**
- 3.12 Proxy ARP of Legacy WAPM template can't be configured by the controller**
- 3.13 The OID (.1.3.6.1.4.1.259.3.4.3) can't be displayed correctly**
- 3.14 Some descriptions are not correct in the MIB files**

4 Known Issue

4.1 The Billing Plan Selection Page with Midtrans payment gateway can't display correctly when previewing the page. After clicking apply button, the page will display the correct page.

Main > Users > Internal Authentication > On-Demand Authentication > External Payment Gateway > Payment Gateway Web Page Customization

Payment Gateway Message Pages

Service Disclaimer	Default	<input checked="" type="radio"/> Edgecore Default <input type="radio"/> Customize with Template <input type="radio"/> Upload You Own <input type="radio"/> Use External Page
Billing Plan Selection Page	Default	
Account Credentials Page	Default	

Preview