

GGM WCAP300 – CENTRALIZED WIFI CONTROLLER

4 Ports Lan 10/100/1000, 2 WAN

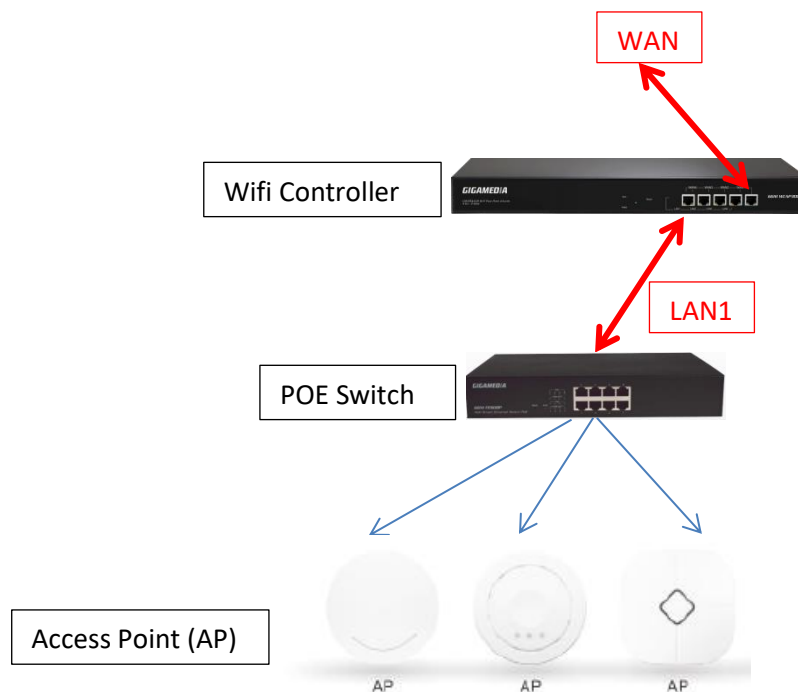
Quick Guide



1- Diagram / How to use WIFI Controller

The Wi-Fi controller allows the deployment and the easy and fast management of several Wifi access points (AP) in your network.

Wireless network management includes real-time control of Access Point (AP) status, quality of service, and enhanced security policy.



2- Quick Installation

Connect your PC with the LAN Port then login Web Management with Internet Explorer.
You must configure your PC with a fixed IP address 192.168.10.X (X between 2 and 253)

IP Address by default (LAN): **http://192.168.10.1**

Identification: **admin**

Password: **admin**



LAN Settings: Tab **Gateway** then LAN, to modify IP Parameters

LAN

LAN Settings Apply Static DHCP

■ LAN Settings

IP Address 192 . 168 . 10 . 1

Subnet Mask 255 . 255 . 252 . 0

Spanning Tree Enable

■ DHCP Server Setting

DHCP Server Setting Enable

Initial allocation base address 50

Maximum DHCP address allocation 500

DHCP Lease Time 24 H

DHCP allocation quantity 1 [DHCP List](#)

WAN Settings

Please choose your WAN Settings according to your connection Mode:

WAN Setting

WAN Setting Load Balance Policy Routing

■ WAN Setting

⚠ Modify the wan port number, please manually reboot the device!

WAN Name	Status	Connect Method	Config
WAN1	Not Configure		☒
WAN2	Not Configure		☒
WAN3	Not Configure		☒
WAN4	Not Configure		☒

WAN Setting

Connect Method Dynamic IP

MTU 1492 (1400-1500)

Band Type 100M Fiber

Downstream 100000 Kbps

Upstream 100000 Kbps

DNS Priority High priority

Enable Web Server Access on WAN Port: 8080 (Port Range 1-65535)

Apply

Manage and integrate Access Point (AP)

2 methods :

- By Groupes
- Zero Config

Click on AC button, you will see all AP connected into this Wifi Controller.

AC Setting													
Device List		Search		Batch Set		Refresh		Delete		Reboot		Reset	
												Upgrade	
												Zero Config	
												Device Group	
												Device Log	
												Address Server	
Select	SN	Location	Name	IP	MAC	Users	Version	Channel	Txpower	Device Model	Uptime	Group	Config
☐	1			192.168.200.141	78:D3:8D:ED:F4:A4	0	V2.0	7	100%	A930-P48	0:00:38	N/A	☒

a) Creation of one or more groups

AC Setting

Device List Zero Config Add Group Delete Group Device Group Device Log Address Server

SSID Wireless Security Key Txpower Time to restart Config

Wireless Basic

Wireless Advanced

Automatic reboot at 3:00

Apply

Close

Device List: Wlan Device 1

Main AP Configuration Status: Enable Broadcast SSID: Enable

SSID: WLAN0 Vlanid: 0 (0-4094)

Wireless Security: Open System Config...

Virtual AP Configuration1 Status: Disable Broadcast SSID: Enable

SSID: WLAN1 Vlanid: 0 (0-4094)

Wireless Security: Open System Config...

Virtual AP Configuration2 Status: Disable Broadcast SSID: Enable

SSID: WLAN2 Vlanid: 0 (0-4094)

Wireless Security: Open System Config...

Virtual AP Configuration3 Status: Disable Broadcast SSID: Enable

Customize your Wifi Settings for this group :

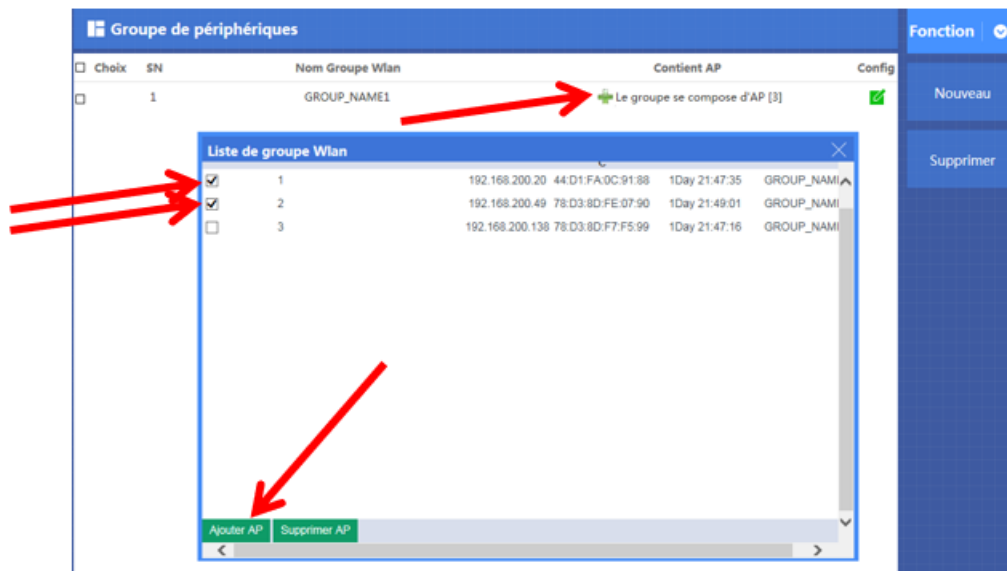
Status: Enable

SSID: Name of your Wifi

Security: Add a security Key

Add one or more Access Points: Click on 

- Select one or more Access Points to integrate
- Click on Add AP



b) Zero Config - Function Wireless Plug & Play

Zero Config function is the same as creation of groups.

Settings in **Zero Config** will be the same for all Access Points connected. (Same SSID, same Password, same channel).

Attention: it is recommended, first, to set the **Zero Config** before connecting all Access Points.

If not, configuration of Access Points will be enable after restarting it

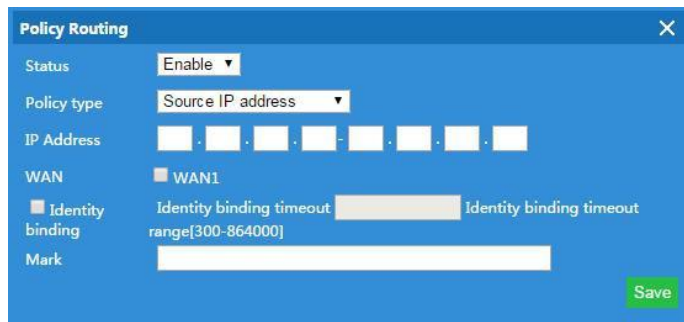
Manage Access Point

Here, you can use those functions:

- IP Filtering
- Port Filtering
- MAC Filtering
- QoS and Bandwidth Management

Policy Type:

Source IP Address: Policy based on source IP address



Policy Routing

Status:

Policy type:

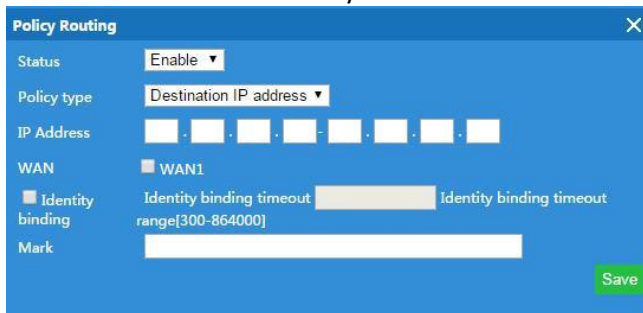
IP Address:

WAN: ☒ WAN1

☐ Identity binding: Identity binding timeout
range[300-864000]

Mark:

Destination IP address: Policy based on destination IP address



Policy Routing

Status:

Policy type:

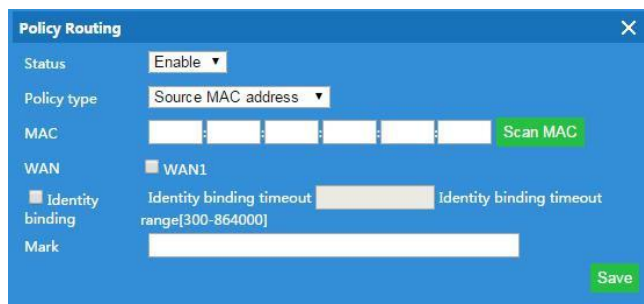
IP Address:

WAN: ☒ WAN1

☐ Identity binding: Identity binding timeout
range[300-864000]

Mark:

Source MAC address: Policy based on source MAC address



Policy Routing

Status:

Policy type:

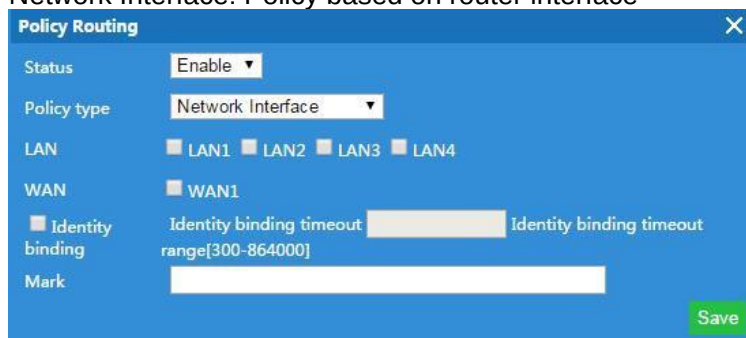
MAC:

WAN: ☒ WAN1

☐ Identity binding: Identity binding timeout
range[300-864000]

Mark:

Network Interface: Policy based on router interface



Policy Routing

Status:

Policy type:

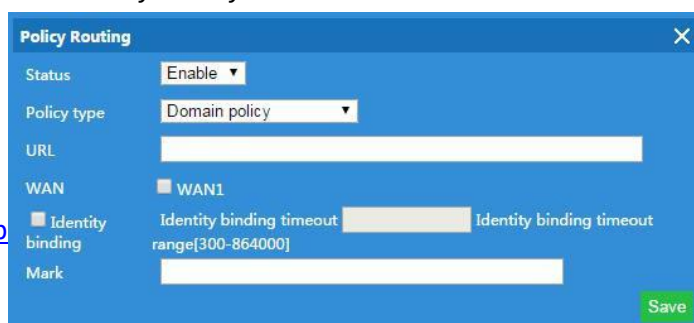
LAN: ☒ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4

WAN: ☒ WAN1

☐ Identity binding: Identity binding timeout
range[300-864000]

Mark:

Domain Policy: Policy based on router domain



Policy Routing

Status:

Policy type:

URL:

WAN: ☒ WAN1

☐ Identity binding: Identity binding timeout
range[300-864000]

Mark:

<http://>

Policy Routing

Status:

Policy type:

Destination port: can not be empty, port range:1-65535

WAN: ☒ WAN1

Identity binding: ☐ Identity binding timeout: Identity binding timeout range[300-864000]

Mark:

Flow Control

It is including smart QoS and Speed Limit in Flow Control.

Smart QoS

It is set priority bandwidth for application class to make it work freely.

Speed Limit

Speed Limit: Mean limit end users Ethernet speed;
Should add IP group first, then choose the limited mode.

Flow Control

IP speed limit setting

Select	SN	Group Name	Time Group	Limited Mode	Upstream	Downstream	Status	Mark	Config
☐	1	Sales	sales department	Shared mode	2000Kbps	1000Kbps	Enable		☒

IP speed limit setting

Status:

IP Group:

Time Group:

Limited Mode:

Downstream: Kbps

Upstream: Kbps

Mark:

Flow Control

Start up intelligent flow control: ☒ Custom priority bandwidth

SN	Application Class	Priority	Bandwidth Ratio(%)
1	Instant messaging	High priority	20%
2	Network download	Lowest priority	5%
3	Network video	Low priority	10%
4	Office	Highest priority	50%
5	Finance and other		15%

Custom priority bandwidth

SN	Priority	Bandwidth Ratio(%)
1	Lowest priority	5 %
2	Low priority	10 %
3	Mid priority	15 %
4	High priority	20 %
5	Highest priority	50 %

Routing

Management

Static Route: add the static router based on destination IP address.

Routing Management

System Routing Static Route Add Delete Apply

Static Route Settings

Select	SN	Destination	Gateway	Subnet Mask	Metric	Network Interface	Status	Mark	Config
Static Route Settings Status: Enable Destination: Subnet Mask: Gateway: Metric: 0 Network Interface: WAN1 Mark: Apply									

URL Filter

When enable URL filter, the router can reject users to visit the denied URL.

Url Filter

Url Filter Add Delete Apply

Enable Url filter function

Select	SN	Rule Name	Time Group	URL	Status	Mark	Config
☐	1	google	Any	www.google.com	Enable		☒

Url Filter

Status: Enable
Rule Name: google
Time Group: Any
URL: www.google.com
Mark:

Add Time Group
Apply

IP Filter

When enable this function, router will allow or limited this IP address to access into this router based on rules.

IP Filter

IP Filter Add Delete Apply

IP Filter Prohibit

Select	SN	Rule Name	Time Group	IP Address	Port Range	Protocol	Status	Mark	Config
IP Filter Status: Enable Rule Name: IP Filter Time Group: Any IP Address: 192.168.9.139 Port Range: Protocol: TCP+UDP Mark: Add Time Group Search User Apply									

MAC Filter

When enable MAC filter, router will allow or prohibit this MAC address to access into this router based on rules.

MAC Filter 

 **MAC Filter**   

☒ **MAC Filter** Allows the device to pass in the rule

Selete	SN	Rule Name	Time Group	MAC	Status	Mark	Config
--------	----	-----------	------------	-----	--------	------	--------

MAC Filter 

Status Enable

Rule Name

Time Group Any 

MAC 

Mark

