WLAN-64GM Enterprise Wireless Controller & Gateway

WLAN-128GM Enterprise Wireless Controller & Gateway

Web Manual



CONTENTS

Chapter	1 Product Introduction	1
	1.1 Package Contents WLAN-64GM and WLAN-128GM	1
	1.2 Product Specification WLAN-64GM	2
	1.3 Product Specification WLAN-128GM	4
Chapter	2 Hardware Installation	6
	2.1 WLAN-64GM and WLAN-128GM Port description	6
	2.2 WLAN-64GM, WLAN-128GM Hardware installation	7
Chapter	3 Quick Installation Guide	8
	3.1 WLAN-64GM, WLAN-128GM , Web login Management	8
	3.2 Initial Setup in the Web UI	8
	3.3 Wizard	8
	3.4 Wizard Wireless	9
	3.5 Wizard Network WAN	9
	3.6 Wizard Network LAN	10
	3.7 Wizard Network Other	10
	3.8 Starting Setup in the Web UI	11
Chapter	4 Configure the Wireless Controller	12
	4.1 Main Home Page	12
	4.2 Reboot and Password Change	13
	4.3 Device – AP List	14
	4.3.1 AP List - Position	14
	4.3.2 AP List - IP	14
	4.3.3 AP List - SSID	14
	4.3.4 AP List - Users	14
	4.3.5 AP – List Channel	15
	4.3.6 AP List – Config and Batch Config	15
	4.3.7 AP List – Config	16
	4.3.8 AP List – Config – Device Info	16
	4.3.9 AP List – Config – Wireless	17
	4.3.10 AP List – Config – Advanced	19
	4.3.11 AP List – Config - Other	20
	4.3.12 AP List – Batch Config	21
	4.3.13 AP List – Batch Config – Apply Template	21
	4.3.14 AP List – Batch Config – Country Code	22
	4.3.15 AP List – Batch Config – Reboot	22
	4.3.16 AP List – Batch Config – Reset	22
	4.3.17 AP List – Batch Config – Web Password	22
	4.3.18 AP List – Batch Config – Delete	22
	4.4 Device – Template	23
	4.4.1 Device – Template – Wireless	23
	4.4.2 Device – Template – Advanced	25
	4.4.3 Device – Template – Other	26
	4.4.4 Device – Template – List	26

4.5 Device – Upgrade	27
4.6 Device – Service	28
4.6.1 Device – Service – IP List	28
4.6.2 Device – Service – Static Binding	29
4.7 Device – IPTV Settings	29
4.8 Device – Auto Roaming	30
4.9 Network	31
4.9.1 Network – LAN Setting	31
4.9.2 Network – LAN Setting – IP List	32
4.9.3 Network – LAN Setting – Static Binding	32
4.9.4 Network – WAN Setting	33
4.9.5 Network – WAN Setting - DHCP	33
4.9.6 Network - WAN Setting - Static IP	34
4.9.7 Network - WAN Setting - PPPoE	35
4.9.8 Network – WAN Setting - Bypass	36
4.9.9 Network - Cloud	37
4.10 User	38
4.10.1 User - UserList	38
4.10.2 User – Speed Limit	38
4.11 Firewall	40
4.11.1 Firewall – IP Filter	40
4.11.2 Firewall – MAC Filter	41
4.11.3 Firewall – URL Filter	42
4.11.4 Firewall Port Map	43
4.11.5 Firewall – DMZ	44
4.12 System	45
4.12.1 System - Upgrade	45
4.12.2 System – Maintain - Telnet	46
4.12.3 System – Maintain – Reboot Regularly	46
4.12.4 System – Maintain – DHCP Conflict Detection	47
4.12.5 System – Maintain – Capture Packet	47
4.12.6 System – Maintain - Ping	48
4.12.7 System – Reboot	48
4.12.8 System – System Log	49
4.12.9 System – Manage – Backup Information	50
4.12.10 System – Manage – Restore Settings	50
4.12.11 System – Manage – Factory Settings	50
4.12.12 System – Manage – DHCP Cache Cleanup	50
4.12.13 System – System Time	51
4.12.14 System – IP Group	52
4.12.15 System – Time Group	53
4.12.16 System - Accelerate	53



Chapter 1. Product Introduction

1.1 Package Contents WLAN-64GM and WLAN-128GM

Before using this Wireless Controller, please check if there is anything missing in the package, and contact your dealer of purchase to claim for missing items:

- WLAN-64GM or WLAN-128GM Wireless Controller
- Power Adapter (WLAN-6GM)
- Power Cable (WLAN-128GM)
- Mounting Ears
- Installation Guide

airlive

1.2 Product Specification WLAN-64GM

Model	WLAN64GM Enterprise Gateway & Wireless Controller
Device Interface	Device Upgrade
Main Chip: MTK MT7621	Online upgrade
Flash:16MB	Local Upgrade
SSD :256MB	Firmware Upgrade
Ethernet (LAN): 4 x RJ45 10/100/1000mbps	Device Service
WAN: 1x RJ-45 10/100/1000mbps	AC Enable\Disable
Network Protocol: IEEE 802.3, 802.3u, 802.3ab,	DHCP Enable\Disable
TCP/IP, DHCP, ICMP, NAT, PPPoE, SNTP, HTTP,	Server IP Address
DDNS, IPsec, PPTP, L2TP, CAPWAP Protocol	Address Count
Heat Dissipate: Super silent ball fan	Lease Time
Power Input: 1 x 12VDC	Allocated IP
Power:AC:100-240V,50HZ	IP List
WAN	Static Binding
WAN: PPPoE, DHCP, Static IP, Bypass mode	IPTV Setting
irmware features	Enable IPTV mode
AP Management:	IPTV tags
Max to manage 64 PCS wireless AP	Topology Graph
Centrally and remotely to manage/configure	Device Auto Roaming
wireless AP	Auto Roaming
AP Template deploy	5G priority
View user's status	Network
Wireless Country Code	Lan Setting
Reboot/Reset	IP Address
Web Password	Subnet
Delete AP	DHCP Service
Online User List	Start/End IP
AP Configure	Primary/Secondary DNS
AP Template:	DHCP Lease Time
Device Add	DHCP Allocation Number
Device Configure	WAN Setting
Wireless Device	Internet Access: DHCP/Static IP/PPPoE/Bypass
Wireless Frequency: 2.4G/5.8G	MTU
Encryption	Line Detection
VLAN ID	Cloud
Virtual AP1~4	Cloud Enable/Disable
Country Code	Cloud Server
Max Station	Latitude/Longitude
User Isolation	Binding State
Short GI	User
Beacon Interval	User List
Coverage Threshold	Link
Fragment Threshold	Blacklist
RTS Threshold	
Reboot Regularly	
Device Web Password	

<u>oirlive®</u>

Model	WLAN64GM Enterprise Gateway & Wireless Controller
User Speed Limit	Maintain
One Key Enable/Disabled	Remote Login
IP Group	Remote Telnet
Time Group	Reboot Regularly
Up/Down	DHCP Conflict Detection
Remake	Capture packet
Firewall:	Network
IP Filter	Protocol
Rule Name	Source Address
Protocol	Target Address
TCP/UDP	Target Port
IP Address	Number
Search	Ping
External Port	Environment
Internal Port	Working Temperature: -20°C~55°C
MAC Filter	Storage Temperature: -40°C ~ 70°C
Name	Working Humidity: 5% ~ 97%RH (No condensation)
Time Group	Dimension
Mac Address	Package Size: 50 x 28 5 x 8 cm
Search Mac Address	Carton Package: 10PCS / 1 CTN
URL Filter	Carton Weight: G W=10KGS
Name	Carton Size: 54 5 x 32 5 x 23 5 cm
Time Group	Ordering Information
URL Address	Model Name: Airlive WI AN-64GM
Port Map	Description: Enterprise Gateway & Wireless Controller
Name	Beschption. Enterprise outeway a wheless controller
Protocol	
TCP/UDP	
IP Address	
Search	
External/Internal Port	
DMZ Host	
DMZ IP Address	
Search	
• System:	
System Time	
Current version	
Upgrade Type	
Online Upgrade	
Local Upgrade	
Upgrade Time	
Restore Detault Configure	
Upgrade	

<u>airlive</u>

1.3 Product Specification WLAN-128GM

Model	WLAN-128GM Enterprise Gateway & Wireless Controller
Device Interface	Device Upgrade
Main Chip: MTK MT7621	Online upgrade
• Flash:16MB	Local Upgrade
• SSD :256MB	Firmware Upgrade
• Ethernet (LAN): 4 x RJ45 10/100/1000mbps	Device Service
• WAN: 1x RJ-45 10/100/1000mbps	AC Enable\Disable
• Network Protocol: IEEE 802.3, 802.3u, 802.3ab,	DHCP Enable\Disable
TCP/IP, DHCP, ICMP, NAT, PPPoE, SNTP, HTTP,	Server IP Address
DDNS, IPsec, PPTP, L2TP, CAPWAP Protocol	Address Count
Heat Dissipate: Super silent ball fan	Lease Time
• Power Input: 1 x 12VDC	Allocated IP
• Power :AC:100-240V,50HZ	IP List
WAN	Static Binding
• WAN: PPPoE, DHCP, Static IP, Bypass mode	IPTV Setting
Firmware features	Enable IPTV mode
AP Management:	IPTV tags
Max to manage 128 PCS wireless AP	Topology Graph
Centrally and remotely to manage/configure	Device Auto Roaming
wireless AP	Auto Roaming
AP Template deploy	5G priority
View user's status	Network
Wireless Country Code	Lan Setting
Reboot/Reset	IP Address
Web Password	Subnet
Delete AP	DHCP Service
Online User List	Start/End IP
AP Configure	Primary/Secondary DNS
• AP Template:	DHCP Lease Time
Device Add	DHCP Allocation Number
Device Configure	WAN Setting
Wireless Device	Internet Access: DHCP/Static IP/PPPoE/Bypass
Wireless Frequency: 2.4G/5.8G	MTU
Encryption	Line Detection
VLAN ID	Cloud
Virtual AP1~4	Cloud Enable/Disable
Country Code	Cloud Server
Max Station	Latitude/Longitude
User Isolation	Binding State
Short GI	User
Beacon Interval	User List
Coverage Threshold	Link
Fragment Threshold	Blacklist
RTS Threshold	
Reboot Regularly	
Device Web Password	

<u>oirlive®</u>

Model	WLAN-128GM Enterprise Gateway & Wireless Controller
User Speed Limit	Maintain
One Key Enable/Disabled	Remote Login
IP Group	Remote Telnet
Time Group	Reboot Regularly
Jp/Down	DHCP Conflict Detection
Remake	Capture packet
Firewall:	Network
IP Filter	Protocol
Rule Name	Source Address
Protocol	Target Address
TCP/UDP	Target Port
IP Address	Number
Search	Ping
External Port	Environment
Internal Port	Working Temperature: -20°C~55°C
MAC Filter	Storage Temperature: -40°C ~ 70°C
Name	Working Humidity: 5% ~ 97%RH (No condensation)
Time Group	Dimension
Mac Address	Dimension Dackage Size: 50 x 28 5 x 8 cm
Search Mac Address	Carton Backage: 50CS / 1 CTN
URL Filter	Carton Weight: GW-9KGS
Name	Carton Vergin. $G.W = 3KGS$
Time Group	Carton Size, 50.5 x 45.5 x 54.5 cm
URL Address	
Port Map	Model Name: AirLive WLAN-128GM
Name	Description: Enterprise Gateway & Wireless Controller
Protocol	
TCP/UDP	
IP Address	
Search	
External/Internal Port	
DM7 Host	
DMZ IP Address	
Search	
System:	
System Time	
Current version	
Online Ungrade	
Upgrade Time	
Restore Default Configure	
Ungrade	
Upgrade	



Chapter 2. Hardware Installation

2.1 WLAN-64GM and WLAN-128GM Port description.



WLAN-64GM



WLAN-128GM

LED Description.

LED	Status	Function	
21112	On (Green)	Wireless Controller is powered on	
PWR	Off	System is off	
	Blinking (Green)	Wireless Controller is working	
Run	Off	No traffic	
WAN/LAN	Blinking	Cable connected and Data Transfer	

Port Description.

Port	Description
12V DC	12V DC port for WLAN-64GM only
WAN	WAN port connecting to Modem or Router
LAN 1~4	LAN port connecting to the network equipment.
	To restore to the factory default setting, press and hold the Reset Button for
Reset	about 10 seconds, and then release it.



2.2 WLAN-64GM, WLAN-128GM Hardware installation.

Connect the Wireless Controller via the WAN port to an Internet connection via a Modem or Router. To control the Access Points connect them direct to the LAN ports of the controller via a (PoE) Switch. The AirLive TOP-12AC, TOP-18AX and inWall-U618 as well as several outdoor CPE models are support by the Wireless controller.





Chapter 3. Quick Installation Guide

3.1 WLAN-64GM, WLAN-128GM , Web login Management.

This chapter will show you how to configure the basic functions of your Wireless Controller within minutes.

TCP/IP Configuration.

The default IP address of the Wireless Controller is 192.168.10.1. By default, the Wireless Controller has DHCP turned on and the device will give out IP addresses directly when a computer is connected to the LAN ports. No additional setup has to be done.

3.2 Initial Setup in the Web UI.

Input 192.168.10.1 into the browser, when this the first the time setup the Setup Wizard will start. Enter your own new Username and Password to start using the Wireless controller

airlive	
	Intelligent
Change the device management	password and complete the system configuration
* New username	
* New password	
* Confirm password	
	ок

3.3 Wizard

Continue with the Wizard or press Skip to go directly to the Home Page of the Wireless Controller.





3.4 Wizard Wireless

The settings which are entered in this field will be used as the default template for all the Access Points which will be connected to the Wireless Controller. Select Enable or Disable the wireless status, Enter your SSID name and wireless encryption.

Wireless	Network Settings	Other
	Wireless	
Status	• Enable Disable	
SSID	Wireless	
Encryption	WPA/WPA2PSK	~
Password	••••••	٢

3.5 Wizard Network WAN

For the WAN setup select the Internet Access type for your connection, this can be DHCP, Static IP, PPPoE or Bypass. Or press Scanning Access Mode to automatically select the Internet Access.

Wireless	Network Settings		3 Other	
	Wan Setting	Lan Setting		
Internet Access	Dhcp		~	
			Scanning Access Mode	
MTU	1500		(1400-1500)	
	Back	Next		



3.6 Wizard Network LAN

Change the LAN IP address of the Wireless Controller as well as the Start and End IP Address range and the DNS.

Wireless	Network Settings	Other	
	Wan Setting Lan Setting		
IP Address	192.168.10.1		
Subnet	255.255.255.0		
Dhcp Service	• Enable Disable		
Start IP	192.168.10.1		
End IP	192.168.10.254		
Primary Dns	8.8.8.8		
Secondary Dns	8.8.4.4		
Dhcp Lease Time	24 Hour	~	

3.7 Wizard Network Other

The Wireless Controller can automatically reboot on a fixed time. Select to Enable or Disable this function. After this select the Reboot Time and the Reboot Interval.

Wireless	Network Set	ttings	Other
R	eboot Regularly		
System Time	2023-03-16 14:37:2	22	
Reboot Regularly	Enable	Disable	
• Reboot Time	Everyday	× 1:00	~
Reboot Interval	1Day		~



3.8 Starting Setup in the Web UI.

It is easy to configure and manage the Wireless Controller with a web browser. Input 192.168.10.1 into the browser (When you changed the default IP address of the Wireless Controller in the Wizard, please use your new IP Address), When the Wireless Controller has been setup using the Wizard enter your own new Username and Password. When you clicked Skip in the Wizard setup, you would go directly to the Home Page of the Wireless Controller but with the next login the main login page as below will be shown.

To change the language settings from English to Spanish click on the "v" to open the menu.

airli√e°		English 🛛	
	A Please input user name		
	ℯ ^O Please input password ②		
	Login		
	Forget password		
	R WLAN128GM		
	Einmunn Marian MI AN 4390M V2 A Build20220203405400		



Chapter 4. Configure the Wireless Controller

4.1 Main Home Page.

The below web GUI and the topology used in this guide uses the WLAN-128GM as an example. It is easy to configure and manage the Controller with the web browser. The Home Page of the Wireless Controller shows an overview of the settings and several quick links.



The page includes the following fields:

Object	Description
Throughput	Shows the current status of the WAN port UP and Downstream graph
LAN	Shows the current LAN status and IP information
WAN	Shows the current WAN status and IP information
Device Position	You can enter the device description.
Memory	Current % of internal memory in use
СРU	Current CPU load
Version	Shows the current device firmware version.

Quick Links

Click on the cog icon 🎡 to directly go to the settings without going through the menu.

Quick Links

Click on the Blue, Green, Orange and Red Buttons to go direct to these settings, without going through the menu.



4.2 Reboot and Password Change

Click on the Green icon with the 4 squares in the top right corner and a pulldown menu will appear. The first icon will start the Setup Wizard.

- To change the Username, click on the person icon and enter your new Username.
- To change the Password, click on the lock icon and enter your new Password.

To Reboot the Access Point, click on the last icon





4.3 Device – AP List

AP list will show all the Access Points which are connected to the Wireless Controller. The Access Points will automatically appear when they are set to on "Get IP from AC" in their webGUI. When multiple different models of Access Points have been added they can be separated by model or by online/ offline devices. By default, All Models are shown, click on the All Models button and a single model can be selected, now only Access Points of the same model will be shown. Click on All Device to choose between Online and Offline device.

To search a selected Access Point enter it's IP or MAC Address in the search field and the device will be displayed.

air	li⊽e		Home	Device	Network	User	Firewall	Syste	m			88 €
All Models	 All Det 	vice 🗸	User 1	Device total 1	Online AP 1	Offline A	\P 0	Enter IP / MA	C	Q 😌	Bat	ich Config 🗸
Sn Sn	Position ≑	IP 🌲	MAC 🌲	\$ \$ID	Users ≑	Status ≑	Channel	Txpower	Model	Version 🌲	Uptime 🌲	Config
□ 1	inWall-U618AX 🧠	<u>192.168.200.2</u>	00:4F:4E:00:00:00	Wireless 2.4G_00 🛱 Wireless 5.8G_00 🛱	1 🏼 🛃	Online	Auto [12] Auto [36]	100%	Inwall-U618	V3.0-Build20230306092924	23:56:35	鏮

4.3.1 AP List - Position

Click on the pen icon to change the name of the Access Points

 Device Position 		\times
Position	inWall-U618AX	
	ок	

4.3.2 AP List - IP

Click on the IP Address of the Access Point, the local webGUI of the Access Point will now open. Note Wi-Fi changes which are made in the Access Point webGUI will be overruled by the Wi-Fi settings of the Wireless controller.

4.3.3 AP List - SSID

When the Lock icon is closed the SSID is using encryption, when the Lock icon is open there is no encryption.

4.3.4 AP List - Users

Click on the person icon to directly see which users are connected to the Access Point.

Online user list			\times
Sn	MAC ≑	Frequency band	Signal
1	BE:FA:81:94:F3:7D	5.8G	-52 dBm 🔶



4.3.5 AP – List Channel

Click on the channel icon to see the Channel analyze of the both the 2.4 and 5.8Ghz. The straight red vertical line shows the Channel which the Access Point is currently using.



4.3.6 AP List – Config and Batch Config

There are two different config's

Config: This is the setup up for the selected single Access Point, settings like SSID, Encryption, VAP and TX Power can be setup in this menu.

Batch Config: When using this function settings can be applied to multiple Access Points in one go. These can be the Wireless settings, Device Password, Reboot and Reset.



4.3.7 AP List - Config

Config: This is the setup up for the selected single Access Point, settings like SSID, Encryption, VAP and TX Power can be setup in this menu. These settings overrule any settings which may have been done before in the webGUI of the Access Point.

4.3.8 AP List - Config - Device Info

Device Info: This is an overview page which will display the current settings of the Access Point.

Device Info	Wireless	Advanced	Other	
Basic				
Device Model	Inwall-U61	8AX		
Position	inWall-U61	8AX		
MAC	00:4F:4E:0	0:00:00		
IP	192.168.20	0.2		
Uptime	16:45:19			
Wireless				
SSID	Wireless 2.	4G_000000 / Wireless 5.	8G_000000	
BSSID	02:4F:4E:4	0:00:00 / 00:4F:4E:00:00	:00	
Channel	Auto[13] / A	Auto[120]		
Security	WPA/WPA	2PSK / WPA/WPA2PSK		
TxPower	100% / 100	0%		
Other				
Country Code	ETSI			
Beacon Interval	100 / 100			
Coverage Threshold	-95 / -95			
Reboot Regularly	Disabled			



4.3.9 AP List – Config – Wireless

In Wireless setting you can setup the 2.4Ghz and 5Ghz setting

The 2.4Ghz settings are first when you need to do the 5Ghz settings click on the pulldown menu of the device and select 5Ghz.

Setup your own SSID, Encryption, Wi-Fi Password, Channel and VLAN

Device Info	Wireless	Advanced	Other	
Device	2G WiFi	i	~	
Status	• Enable	• 0	Disable	
SSID	Wireless	s 2.4G_000000	Hide WiFi	
Encryption	WPA/W	PA2PSK	~	
Password	•••••		Ś	
Channel	Auto		~	
VlanID	0		(0-4094)	

Device Info	Wireless	Advanced	Other	
Device	5G WiF	i	~	
Status	• Enable	e (Disable	
SSID	Wireless	s 5.8G_000000	Hide WiFi	
Encryption	WPA/W	PA2PSK	~	
Password	•••••			
Channel	Auto		~	
VlanID	0		(0-4094)	



The page includes the following fields:

Object	Description
Device	Select to setup either 2.4GHz or 5.8Ghz part of the Access Point
Status	Select ON (Green) or OFF (Gray) to enable or disable wireless LAN.
SSID	This is the wireless network name. The default SSID is Wireless 2.4G_XXXXXX and Wireless 5.8G_XXXXXX. X is the last 6 numbers of the AP MAC address.
Hide your SSID	Select ON (Green) or OFF (Gray) to hide wireless LAN or not.
Encryption	Select the wireless encryption
Password	Enter your wireless password
Channel	Select the operating channel you would like to use. The channel range will be changed by selecting a different domain.
VLAN	Set the VLAN-ID for the Access Point (between 3~4094)

Virtual AP (VAP)

Select VAP1~VAP3 to enable the virtual AP. Both the 2.4Ghz and 5Ghz have 3 virtual ap's

Virtual AP	Virtual AP1	Virtual AP2	Virtual AP3
	Virtual AP1		
SSID	Wireless 2.4G-1_0000	000	Hide WiFi
Encryption	WPA/WPA2PSK		~
Password	•••••		Ŵ
VlanID	0		(0-4094)
			Confirm

Object	Description
Virtual AP	Scheck mark VAP1~3 to enabled them
SSID	This is the wireless network name. The default SSID is Wireless 2.4G Vap1_XXXXXX and Wireless 5.8G Vap1_XXXXXX. X is the last 6 numbers of the AP MAC address. The SSID will have Vap2/3 in its name when Vap2 and 3 are enabled
Hide your SSID	Select ON (Green) or OFF (Gray) to hide wireless LAN or not.
Encryption	Select the wireless encryption. The default is "None"
VLAN	Set the VLAN-ID for the Access Point (between 3~4094)



4.3.10 AP List – Config – Advanced

Advanced Settings allows for the change of the Advanced parameters of the Access Points. 2.4Ghz will be shown first to switch to the Advanced parameters of the 5.8Ghz click on the pulldown menu in Device.

Device Config				
Device Info	Wireless	Advanced	Other	
Device	2G WiFi		~	
2G Mode	11NG_HT20		~	
TxPower	100%		~	
Max station	64		(0-128)	
User Isolation	Enable		• Disable	
Short GI	 Enable 		Disable	
Beacon Interval	100		(50-1024)	
Coverage Threshold	-95		(-95dBm~-65dBm)	
Fragment Threshold	2346		(256-2346)	
RTS Threshold	2347		(1-2347)	

Object	Description
Device	Select to setup either 2.4GHz or 5.8Ghz part of the Access Point
2G Mode/ 5G Mode	Select the Wireless mode and Channel bandwidth, "20MHz" or "40MHz" or "80MHz".
TX Power	Select the output power of the Access Point
Max Station	Set the maximum number of clients that can connect to the Access Point
User Isolation	Enable it to isolate each connected wireless client so that they cannot
	access mutually.
Short GI	Guard intervals are used to ensure that distinct transmissions do not
	interfere with one another. Enable or Disable
Beacon Interval	The Beacon Interval is the time between beacon frames transmitted by the Access Point. Default is 100
Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying
	session. The default is -95dBm.
Fragment Threshold	When the length of a data packet exceeds this value, the Access Point will
	send an RTS frame to the destination wireless node, and the latter will reply with a
	CTS frame, and thus they are ready to communicate. The default value is 2346.
RTSThreshold	Enable or Disable RTS/CTS protocol. It can be used in the following
	scenarios and used by Stations or Wireless AP.
	1)When medium is too noisy or lots of interferences are present. If the AP/Station
	cannot get a chance to send a packet, the RTS/CTS mechanism can be initiated to get
	the packet sent.
	2)In mixed mode, the hidden node problem can be avoided. The default
	value is 2347.



4.3.11 AP List – Config - Other

Set a schedule time on which the Access Point would reboot, this can be by time or by day. The password for the Access Point can also be changed here.

 Device Cor 	nfig			
	Device Info	Wireless	Advanced Other	
	Reboot Regularly	• Enable	Disable	
	Reboot Type	• By Time	O By Day	
	Reboot Time	1:00	~	
	Device Web Password	•••••	0	

Object	Description
Reboot Regularly	Select Enable or Disable to start schedule reboot
Reboot Type	Select reboot by Time or by Day
Reboot Time/Interval	Select reboot by Time or by Interval
Restart Interval	Select reboot duty by day
Device Web Password	Set the password for the Access Point
Confirm	Press confirm to save the settings



4.3.12 AP List – Batch Config

Batch Config: When using this function settings can be applied to multiple Access Points in one go. These can be the Wireless settings (Template), Device Password, Reboot and Reset.

To make a Template please see chapter 4.4

When the downward arrow is click for the Batch Config a pulldown menu will appear.

airli▼e	Ś	Home	Device	Network	User	Frewall	System											8
All Models	All Device		Us	er 1	Device total 1	Online AP	1	offi	ine AP 0			Enter IP / I	MAC		٩	0	1	Batch Config ~
Sn	Position 💠		IP 🚖	MAC ‡		S SID			Users	s \$	Status ≑	Channel		Txpower	Model	Version 💠	Uptime 🔅	Apply Template
1	inWall-U618AX	19 0	<u>192.168.200.2</u>	00:4F:4E:00:00:00		Wireless 2.4G_00000 Wireless 5.8G_00000	10 i	በ	1	8	Online	Auto [13] Auto [120]	63. 63.	100% 100%	Invall-U618AX	V3.0-Build20230306092924	16:56:00	Country Code
																		Reboot
																		Reset
																		Web Password
																		Delete

	88 ⊖		
	Batch Config 🗸	Object	Description
Uptime 🗧	Apply Template	Apply Template	Apply the default Template or a made one
1Day 0:18	Country Code	Country code	Select your region valid in your area of use.
	Reboot	Reboot	Reboot the Access Point
	Reset	Reset	Reset the Access Point back to factory default
	Web Password	Web Password	Change the Access Point Password
	Delete	Delete	Delete an Access Point from the AP List, Access Point must be offline

4.3.13 AP List – Batch Config – Apply Template

To Apply a Template, the default one can used which works with all models of the supported Access Points. An additional Template can also be made per model. For instructions on how to make a Template please see chapter 4.4. When using this function, the selected Template will be applied to all the selected (check marked) Access Points.

 Apply Templa 	ate		\times
Select	Template Name	Device Model	
	Default template	General Device	
0	Inwall-U618AX-config	Inwall-U618AX	
		OK	C



4.3.14 AP List – Batch Config – Country Code

Country Code lets you select the different Wi-Fi regions, please select the one which is valid in your country of use. This region code will be applied to all the selected (check marked) Access Points.

Country Setting		\times
Country code	ETSI	~
		ОК
1		

4.3.15 AP List – Batch Config – Reboot

All the selected (check marked) Access Points will be rebooted at the same time when using this function.

		\times
Are you sure to reboot	t the device in batcl	n?
Cancel	ок	

4.3.16 AP List – Batch Config – Reset

All the selected (check marked) Access Points will be rest back to factory default at the same time when using this function.



4.3.17 AP List – Batch Config – Web Password

Enter the webGUI Password which will be applied to all the selected (check marked) Access Points.

Web Password Setting			\times
Web Password	•••••	0	
		ОК	

4.3.18 AP List – Batch Config – Delete

Delete selected Access Points from the AP List. Note Access Points can only be deleted ones they show Offline in the AP List, else they cannot be deleted.



4.4 Device – Template

A Template can be made and applied to all or a selected number of Access Points. This way time can be saved as not every Access Points need to be configured one by one. The Default Template is the one which is made when at the first startup the Wizard was used. This default template can be used for all supported Access Points. To change the default template, click on the cog icon.

To make additional templates click on "Add" and enter a new Template Name.

For Device Model select the Model of Access Point for which the Template will be made. Only models which are active and online in the AP List will be displayed when different models are connected.

 Add configuration template 		\times
Template Name *	Inwall-U618AX-config	
Device Model *	Inwall-U618AX V	
	ок	

4.4.1 Device – Template – Wireless

In Wireless setting you can setup the 2.4Ghz and 5Ghz setting

The 2.4Ghz settings are first when you need to do the 5Ghz settings click on the pulldown menu of the device and select 5Ghz. Setup your own SSID, Encryption, Wi-Fi Password, Channel and VLAN

Virtual AP (VAP)

Select VAP1~VAP3 to enable the virtual AP. Both the 2.4Ghz and 5Ghz have 3 virtual ap's

W	ireless Advanced	Other	
Device	2G WiFi		~]
Status	• Enable	 Dis 	able
SSID	Wireless 2.4	G	Hide WiFi
Encryption	WPA/WPA2	PSK	~
Password			Ø
VlanID	0		(0-4094)
Virtual AP	Virtual AP1	Virtual AP2	Virtual AP3
	Virtual AP	1	
SSID	Wireless 2.4	G-1	Hide WiFi
Encryption	WPA/WPA2	PSK	~
Password	•••••		\otimes
VlanID	0		(0-4094)

<u>airlive</u>

Wireless	Advanced (Other
Device	5G WiFi1	~]
tatus	• Enable	Disable
SID	Wireless 5.8G	Hide WiFi
cryption	WPA/WPA2PSK	~
assword	*******	Ø
lanID	0	(0-4094)
firtual AP	Virtual AP1 Virtua	al AP2 Virtual AP3
	Virtual AP1	
SID	Wireless 5.8G-1	Hide WiFi
ncryption	None	~]
anID	0	(0-4094)

Object	Description
Device	Select to setup either 2.4GHz or 5.8Ghz part of the Access Point
Status	Select ON (Green) or OFF (Gray) to enable or disable wireless LAN.
SSID	This is the wireless network name. The default SSID is Wireless 2.4G_XXXXXX and Wireless 5.8G_XXXXXX. X is the last 6 numbers of the AP MAC address.
Hide your SSID	Select ON (Green) or OFF (Gray) to hide wireless LAN or not.
Encryption	Select the wireless encryption
Password	Enter your wireless password
Channel	Select the operating channel you would like to use. The channel range will be changed by selecting a different domain.
VLAN	Set the VLAN-ID for the Access Point (between 3~4094)
Virtual AP	Scheck mark VAP1~3 to enabled them
SSID	This is the wireless network name. The default SSID is Wireless 2.4G Vap1_XXXXXX and Wireless 5.8G Vap1_XXXXXX. X is the last 6 numbers of the AP MAC address. The SSID will have Vap2/3 in its name when Vap2 and 3 are enabled
Hide your SSID	Select ON (Green) or OFF (Gray) to hide wireless LAN or not.
Encryption	Select the wireless encryption. The default is "None"



4.4.2 Device – Template – Advanced

Advanced Settings allows for the change of the Advanced parameters of the Access Points.

2.4Ghz will be shown first to switch to the Advanced parameters of the 5.8Ghz click on the pulldown menu in Device.

Template		
Wireless	Advanced	Other
Device	2G WiFi	~
Country code	ETSI	~
2G Mode	11NG_HT20	~
TxPower	100%	~
Max station	64	
User Isolation	 Enable 	 Disable
Short GI	Enable	 Disable
Beacon Interval	100	(50-1024)
Coverage Threshold	-95	(-95dBm~-65dBm)
Fragment Threshold	2346	(256-2346)
RTS Threshold	2347	(1-2347)

Object	Description
Device	Select to setup either 2.4GHz or 5.8Ghz part of the Access Point
Country Code	Select your region valid in your area of use.
2G Mode/ 5G Mode	Select the Wireless mode and Channel bandwidth, "20MHz" or "40MHz" or "80MHz".
TX Power	Select the output power of the Access Point
Max Station	Set the maximum number of clients that can connect to the Access Point
User Isolation	Enable it to isolate each connected wireless client so that they cannot
	access mutually.
Short Gl	Guard intervals are used to ensure that distinct transmissions do not
	interfere with one another. Enable or Disable
Beacon Interval	The Beacon Interval is the time between beacon frames transmitted by the Access Point. Default is 100
Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying
	session. The default is -95dBm.
Fragment Threshold	When the length of a data packet exceeds this value, the Access Point will
	send an RTS frame to the destination wireless node, and the latter will reply with a
	CTS frame, and thus they are ready to communicate. The default value is 2346.
RTS Threshold	Enable or Disable RTS/CTS protocol. It can be used in the following
	scenarios and used by Stations or Wireless AP.
	1)When medium is too noisy or lots of interferences are present. If the AP/Station
	cannot get a chance to send a packet, the RTS/CTS mechanism can be initiated to get
	the packet sent.
	2)In mixed mode, the hidden node problem can be avoided. The default
	value is 2347.



4.4.3 Device – Template – Other

Set a schedule time on which the Access Point would reboot, this can be by time or by day. The password for the Access Point can also be changed here.

•	Template				\times
		Wireless	Advanced	Other	
		Reboot Regularly	• Enable	Disable	
		Reboot Type	• By Time	🔵 Ву Дау	
		Reboot Time	1:00	~	
		Device Web Password		Ŵ	

The page includes the following fields:

Object	Description			
Reboot Regularly	Select Enable or Disable to start schedule reboot			
Reboot Type	Select reboot by Time or by Day			
Reboot Time/Interval	Select reboot by Time or by Interval			
Restart Interval	Select reboot duty by day			
Device Web Password	Set the password for the Access Point			
Confirm	Press confirm to save the settings			

4.4.4 Device – Template – List

After the Template has been saved it will be displayed in the list. To apply a Template please see Chapter 4.3.11 and 4.3.12

air	live°		Home	Device	Network	User	Firewall	System			88	Ð
	Maximum a	idd 10 Item								Add	J	
		Sn	Templat	e Name			Devi	ce Model	Config			
		1	Default t	emplate			Genera	al Device 🕕	御			
		2	Inwall-U618	BAX-config			Inwa	II-U618AX	÷ 🗱			



4.5 Device – Upgrade

To Upgrade a single or multiple of Access Points of the same model, select (check mark) the Access Points that need to be Upgraded. To search an Access Point you can also enter the IP or MAC Address of the Access Point in the search field.

Online Upgrade: First check mark the Access Point you would like to Upgrade then click on Online Upgrade. When the Access Points already has the latest version of Firmware a notice will pop up. When the Firmware is not up to date you can select the latest version from the list which is displayed.

Local Upgrade: To use this function first you need to upload the firmware via the button "Firmware Upload" This will put the firmware file into the memory of the Wireless Controller. Ones this is done it can be used multiple times.

Firmware Upload: To use the Local Upgrade function, a firmware file must first be uploaded. Ones it has been Uploaded to the Wireless Controller it can be used via the Local Upgrade function.

xirli⊽e°	Home	Device	Network				
All Models \lor All Device \lor	Device total 1	Online AP 1	Offline AP 0	Enter IP / MAC	Q	Online upgrade	Local upgrade Firmware upload
Sn Position	Model I	Р ≑	MAC ≑	Status	Current Version	Online upgrade	Local upgrade
1 inWall-U618AX I	nwall-U618AX 192.	168.200.2 0	0:4F:4E:00:00:00	Online	V3.0-Build2023030609	Latest version	

Device Model *
Firmware upload * Upgrade firmware not uploaded Local upload
ОК



4.6 Device – Service

Service is the function that gives the connected Access Points there IP Addresses. Also, it makes sure that the Access Points are automatically detected and shown in the AP List.

Home Device	Network	Firewall	System	
AC Enable	• Enable	Disable		
Dhcp Enable	 Enable 	Disable		
Server IP Address	192.168.200.1			
Address Count	300		(1-300)	
Lease Time	24		Hour 🗸	
Allocated IP	1	lp list	Static Binding	
			Apply	

The page includes the following fields:

Object	Description
AC Enable	Enable or Disable the AC function of the Wireless Controller
DHCP Enable	Enable or Disable the DHCP
Server IP Address	IP Range for the Connected Access Points
Address Count	Number Addresses given
Lease Time	IP Address Lease Time
Allocated IP	Number of IP Addresses in use

4.6.1 Device – Service – IP List

IP List shows the current connected Access Points to the Wireless Controller.

•	Ip list				×
	Sn	Device Name	IP 🌩	MAC 🌲	Lease
	1	Inwall-U618AX	192.168.200.2	00:4F:4E:00:00:00	14:19:32



4.6.2 Device – Service – Static Binding

Allocate a fixed Static IP Address to a connected Access Point.

Click on the Add to enter the Static DHCP for the Access Point.

In the new pop-up Window Click on "Online AP" to select an Access Point or manually enter the Access Point IP and MAC Address.

air	rli▼e°	Home	Device	Network	User	Firewall	System		88	G	
	Maximum add 32 Item							Add Apply			
	Sn	IP ≑		MAC \$			Remark	Config			
	No IP/MAC address is currently added, please Add										

Remark	Not use \ and Double quotes	
IP	0.0.0.0	Online AP
MAC		

4.7 Device – IPTV Settings

The IPTV mode can be used when the Access Point is connected to an IPTV Set-top box. Note that by default this functions is Disabled.

After the Mode is turned on, the IPTV port can only be used for the IPTV function, not as an ordinary Internet port. IPTV tags: The default value is 100, which only needs to be modified when VLAN conflicts.

Home	Device	Network	User Fi	rewall	System	
		🛕 After mo	difying the mode, you nee	ed to restart the o	device to take effect.	
Enable IPTV mode		• Enable		Disable	0	
IPTV tags		100			(3-409	5)
					App	lv
						~
\Lambda When the LAN port	of AP device is co	onnected to IPTV S	et-top box, it is used to pl	ay IPTV, IPTV m	node needs to be turned	on.
Sn	Pos	ition	MAC 🌲	Tu	m on/off IPTV mode	
1	inWall-0	J618AX	00:4F:4E:00:00:00			



4.8 Device – Auto Roaming

Enable Auto Roaming for a better connection between the Access Points in a single large network. Note that the SSID, Encryption and Wireless Password of both the 2.4 and 5.8Ghz of the Access Point must be the same.

5G Priority: Clients connected to the Access Point will be connected to 5.8G first. Note when 5G priority is enabled, the SSID, encryption, and password of 2G and 5G of the AP must be the same Change the value of the 2/5G threshold.

Home	Device	Network	User	Firewall	System	
Auto ro 5G pric	paming	(Note	: When roaming is : When 5G priority	enabled, the SSID, is enabled, the SSII	encryption, an D, encryption, a	d password between aps must be consistent) and password of 2G and 5G of the AP must be the same)
2G thre	eshold	-40		(-55dBm /	~ -95dBm)	
5G thre	eshold	-50		(-55dBm ⁄	~ -95dBm)	
					Apply	



4.9 Network

The Network menu allows you to setup the LAN, WAN and Cloud connection of the Wireless Controller.

4.9.1 Network – LAN Setting

Setup the LAN settings for the Wireless Controller. This setup is for the local IP Address of the Wireless Controller and the IP Range for all the connected clients to the Access Points. To see the connected clients, click on "IP List" to enter a static binding to a client connected to an Access Point click on "Static Binding"

airlive°	Home Device	Network User Firewall System	G
	ID Address		
	IP Address	192. 105. 10. 1	
	Subnet	255.255.255.0	
	Dhcp Service	Enable Disable	
	Start IP	192.168.10.1	
	End IP	192.168.10.254	
	Primary Dns	8.8.8.8	
	Secondary Dns	8.8.4.4	
	Dhcp Lease Time	24 Hour 🗸	
	Dhcp Allocation Number	2 Ip list Static Binding	
		Apply	

Object	Description
IP Address	Enter the Static IP Address of the Wireless Controller
Subnet	Enter the Subnet Mask.
DHCP Server	Enable or Disable the Access Point DHCP Server (Default is on)
Start IP	Start IP Address of DHCP Server
End IP	End IP Address of DHCP Server
Primary DNS	Enter the primary DNS IP Address, or not.
Secondary DNS	Enter the secondary DNS IP Address, or not.
DHCP Lease Time	Lease time of a given IP Address
DHCP Allocation Number	Number of active clients
IP List	Detail list of active clients
Static Binding	Bind a Static IP Address to a Client



4.9.2 Network – LAN Setting – IP List

IP List shows the current connected Access Points to the Wireless Controller.

•	lp list				×	<
	\$n	Device Name	IP ≑	MAC 🌲	Lease	
	1	DESKTOP-TQ6S4NH	192.168.10.2	BC:AE:C5:0D:89:F0	15:32:38	
	2		192.168.10.3	BE:FA:81:94:F3:7D	15:53:55	

4.9.3 Network – LAN Setting – Static Binding

Allocate a fixed Static IP Address to a connected Client.

Click on the Add to enter the Static DHCP for the Client.

In the new pop-up Window Click on "Search" to select a Client or manually enter the Access Point IP and MAC Address.

air	'li▼e"		Network	User				88	Đ
	Maximum add 32 Item		_				Add Apply 🗂		
	Sn	IP 🗢	MAC \$			Remark	Config		
			No IP/MAC address	is currently added,	please Add				

		\times
Not use \ and Double quotes		
0.0.0.0	Search	
	Confirm	
	Not use \ and Double quotes	Not use \ and Double quotes 0.0.0 Search Confirm



4.9.4 Network – WAN Setting

WAN Settings allows you setup the Internet Mode of the Wireless Controller, When using the WAN settings make sure your WAN port is connected to your Modem. The Wireless Controller has 4 WAN settings, DHCP, Static IP, PPPOE and Bypass

4.9.5 Network – WAN Setting - DHCP

The default setting for the WAN port is DHCP. Choose "DHCP" and the Wireless Controller will automatically obtain an IP Address, Subnet Mask and Gateway Address from your ISP. Click on Advanced to further setup the connection when needed.

Internet Access			
	Dhcp		~
МТО	1500		(1400-1500)
Set Dns Manually			Advanced
Primary Dns	8.8.8.8		
Secondary Dns	8.8.4.4		
Band Type	1000M Fibe	r	~
Up	1000000		Kbps
Down	1000000		Kbps
Link Detection			

Object	Description
Internet Access	Select DHCP, Static IP, PPPoE or Bypass
MTU	Maximum Transmission Unit. Default is 1500.
Set DNS Manually	Enable/Disable DNS Manually. Default is Enabled
Primary DNS	Enter the necessary DNS address provided by your ISP.
Secondary DNS	Enter the secondary DNS address provided by your ISP.
Band Type	Select the band type provided by your ISP.
Upstream	Enter limited upstream throughput, default is 1000000 Kbps.
Downstream	Enter limited downstream throughput, default is 1000000 Kbps.
Link Detection	Enable to ping Host 1 and Host 2 IP. If ping fails, the WAN will be disconnected.
Scanning Access Mode	When you do not know your Access Type you can press Search and the Wireless Controller will search the correct Access connection type.



4.9.6 Network - WAN Setting - Static IP

The default setting for the WAN port is DHCP. If your ISP offers you static IP Internet connection type, select "Static IP" and then enter IP address, subnet mask, default gateway and primary DNS information provided by your ISP in the corresponding fields. Click on Advanced to further setup the connection when needed.

Home	Device	Network	User	Firewall		
Internet Access		Static IP			~	
Wan IP		0.0.0				
Subnet		255.255.255	.0			
Gateway		0.0.0				
MTU		1500			(1400-1500)	
					Advanced -	
Primary Dns		8.8.8.8				
Secondary Dns		8.8.4.4				
Band Type		1000M Fiber	r		~	
Up		1000000			Kbps	
Down		1000000			Kbps	
Link Detection						
			Sca	nning Access Mode	Apply	

Object	Description
Internet Access	Select DHCP, Static IP, PPPoE or Bypass
WAN IP	Enter the WAN IP provided by your ISP.
Subnet	Enter the Subnet Mask.
Gateway	Enter the Gateway IP Address provided by your ISP.
MTU	Maximum Transmission Unit. Default is 1500.
Primary DNS	Enter the necessary DNS address provided by your ISP.
Secondary DNS	Enter the secondary DNS address provided by your ISP.
Band Type	Select the band type provided by your ISP.
Upstream	Enter limited upstream throughput, default is 1000000 Kbps.
Downstream	Enter limited downstream throughput, default is 1000000 Kbps.
Link Detection	Enable to ping Host 1 and Host 2 IP. If ping fails, the WAN will be disconnected.
Scanning Access Mode	When you do not know your Access Type you can press Search and the Wireless Controller will search the correct Access connection type.



4.9.7 Network - WAN Setting - PPPoE

The default setting for the WAN port is DHCP. Select PPPOE if your ISP is using a PPPoE connection and provided you with a PPPoE username and password. Click on Advanced to further setup the connection when needed.

Home	Device	Network			System
Internet Access		PPPoE(PPP	OE)		~
User Name					
Password					
MTU		1452			(1400-1500)
MAC Clone		Clone Mac			
					Advanced -
Set Dns Manually					
Primary Dns		8.8.8.8			
Secondary Dns		8.8.4.4			
Band Type		1000M Fiber			~
Up		1000000			Kbps
Down		1000000			Kbps
Link Detection					
			Scar	nning Access Mode	Apply

Object	Description
Internet Access	Select DHCP, Static IP, PPPoE or Bypass
Username	Enter the PPPoE Username provided by your ISP.
Password	Enter the PPPoE Password provided by your ISP.
MTU	Maximum Transmission Unit. Default is 1452.
Clone MAC	Enable and Search to clone the MAC address
Set DNS Manually	Enable/Disable DNS Manually. Default is Enabled
Primary DNS	Enter the necessary DNS address provided by your ISP.
Secondary DNS	Enter the secondary DNS address provided by your ISP.
Band Type	Select the band type provided by your ISP.
Upstream	Enter limited upstream throughput, default is 1000000 Kbps.
Downstream	Enter limited downstream throughput, default is 1000000 Kbps.
Link Detection	Enable to ping Host 1 and Host 2 IP. If ping fails, the WAN will be disconnected.
Scanning Access Mode	When you do not know your Access Type you can press Search and the Wireless Controller will search the correct Access connection type.



4.9.8 Network – WAN Setting - Bypass

This the Bridge/Transparent mode for the WAN Port.

Home Device	Network	User	Firewall	System
Internet Access	Bypass			~
Address Type	Static IP			~
IP Address	0.0.0.0			
Subnet	0.0.0.0			
Gateway	0.0.0.0			
Primary Dns	0.0.0.0			
Secondary Dns	0.0.0.0			
	A	pply		

Object	Description
Internet Access	Select DHCP, Static IP, PPPoE or Bypass
Address Type	Select Static IP or DHCP
IP Address	Enter the IP Address for the WAN port
Subnet	Enter the Subnet Mask
Gateway	Enter the Gateway IP Address
Primary DNS	Enter the necessary DNS address provided by your ISP.
Secondary DNS	Enter the secondary DNS address provided by your ISP.



4.9.9 Network - Cloud

By default, the Cloud setting is turned on. When this settings is turned on the Wireless Controller can be added to the AirCloud platform. The AirCloud platform allows you to remote control the Access Points which are connected to the Wireless Controller via the Cloud.

See www.airlive.com for more information about the AirCloud.

Home	Device	Network	User	Firewall	System	
Cloud		Enable	0	Disable		
Cloud	Server	Aircloud.airl	ive.com			
Latitud	le					
Longit	ude					
Bindin	g state	Binding failure				
					Apply	



4.10 User

The User menu shows the User List and Speed Limit which can be set for the clients. Note that the Speed Limit function will only work correctly when the Accelerate function has been set to normal. The Accelerate function can be found in the System Menu.

4.10.1 User - UserList

UserList shows the clients which are connected to the Access Points and their Total Flow information. Click on the Link icon to see more detailed information. To Blacklist a client, click on the Blacklist icon. To see all Blacklisted clients, click on Blacklist in the top bar.

air	live°		Home	Device	Network	User		Firewall	System			88	Ð
					User list (2)		Black						
	Model	User Info						Total flow		Link	Blacklist		
		Unknown Online time: 12:09:33		IP MAC	192.168.10.3 BE:FA:81:94:F3:7D			† 1.89MB ↓ 5.33MB		Ð	0		
	/isus	DESKTOP-TQ6S4NH Online time: 04:23:59		IP MAC	192.168.10.2 BC:AE:C5:0D:89:F0			↑ 20.49MB ↓ 51.27MB		Ũ	0		

4.10.2 User - Speed Limit

Speed Limit can limit the UP and Downstream speed per client or client group. This can be done by settings limit for a single IP address or for an IP Group. An additional time function can also be setup to limit the speed for the client(s) for a certain time frame. Note that the Speed Limit function will only work correctly when the Accelerate function has been set to normal. The Accelerate function can be found in the System Menu.

Click Add to open the Pop-up window to enter the IP and Time information. To Delete a Rule, select the Rule which was made before and check mark it, then press the X to Delete it.

To Enable the Rule(s) click on the "One Key Enable/Disable" when its Green the function is active.

airli	re"		Home		Network	User	Firewall				88	Ð
Maxim	ium add 32 Item	One K	ey Enable/Disabled	D		_				Add		
	Sn	IP Group	Time Group	Limited Mode 🔶		Up	Down	Status	Remark	Config		
	1	Customize	Not limited	Shared mode		10000	50000	Enable	Free	帶 🗙		

Status	• Enable Disable	
IP Group	Customize	~ + Add
Start IP	0.0.0.0	
End IP	0.0.0.0	
Time Group	Not limited	+ Add
Up		Kbps (0:Not limited)
Down		Kbps (0:Not limited)
Remark	Not use \ and Double quotes	

Object	Description
Status	Select enable or disable Speed Limit rule
IP Group	Select Custom or Add an IP group
Start IP	Enter a Start IP Address for the range
End IP	Enter an End IP Address for the range
Time Group	Select any or Custom or Add a Time group
Up	Enter the upstream limited for kbps
Down	Enter the downstream limited for kbps
Remark	Enter the Remark string, or not
Confirm	Save Settings



4.11 Firewall

IP Filter, MAC Filter, URL Filtering, Port Mapping and DMZ are the functions which can be set under the Firewall menu. Setup for the IP Group and Time Group which can be used in some of the Firewall features can been done in the System menu (see chapter 4.12.14 and 4.12.15).

4.11.1 Firewall – IP Filter

IP Filtering can block or allow certain clients based on the IP Address, also a port or port range can be set for the IP Address together with the Protocol.

Click Add to open the Pop-up window to enter the IP and Time information. To Delete an IP Filter, select the IP Filter which was made before and check mark it, then press Delete.

To Enable the Rule(s) for Black or Whitelist click on "Enable" in the top bar when its Green the function is active.

			Device	Network	User	Firewall	System			器
Maximum add 32 Item	Enable	🔵 Blacklist 虊							Add	
Sn Ru	ule Name	Time Group	IP Add	Iress	Port Rar	nge	Protocol	Status	Config	
				No limit is currently	added, please	Add				

Status	Enable Uisa	ible	
Rule Name	Not use \ and Double que	otes	
IP Group	Customize		~ + Add
Start IP	0.0.0.0		Search
End IP	0.0.0.0		0
Time Group	Not limited		~ + Add
Port Range	1 (1-65535)	65535	(1-65535)
Protocol	TCP+UDP	~	

Object	Description
Status	Select ON (Green) or OFF (Gray) to enable or disable
Rule Name	Enter the rule name, e.g. Black list
IP Group	Select IP Group for adding IP by entering IP range or by searching devices
Start IP	Enter a Start IP Address for the range or click Search
End IP	Enter an End IP Address for the range
Time Group	Select to Customize or Add a Time Group and setup time range and work data.
Port Range	Enter the web port to access
Protocol	Select TCP, UDP orTCP+UDP
Confirm	Save the settings



4.11.2 Firewall – MAC Filter

MAC Filtering can block or allow certain clients based on the MAC Address.

Click Add to open the Pop-up window to enter the MAC and Time information. To Delete an MAC Filter, select the MAC Filter which was made before and check mark it, then press Delete.

To Enable the Rule(s) for Black or Whitelist click on "Enable" in the top bar when its Green the function is active.

air	rli▼e®		Home	Device	Network	User	Firewall	System		88	C
	Maximum add 32 Item	Enable 🚺	Blacklist 🔅						Add		
	Sn	Rule Name		Time Group		MAC 🌲		Status	Config		
					No limit is currer	ntly added, please	Add				

MAC Filter		\times
Status	• Enable Disable	
Rule Name	Not use \ and Double quotes	
Time Group	Not limited	→ + Add
MAC		Search
		Confirm

Object	Description
Status	Select ON (Green) or OFF (Gray) to enable or disable
Rule Name	Enter the rule name, e.g. Black list
Time Group	Select to Customize or Add a Time Group and setup time range and work data.
MAC	Enter the MAC address that you need to put in black or white list
Confirm	Save the settings.



4.11.3 Firewall – URL Filter

URL Filtering can block certain webpage for the clients. When enabled clients connected to the network will not be able to browse webpages which have been added to the URL Filter.

Click Add to open the Pop-up window to enter the URL and Time information. To Delete a URL Filter, select the URL Filter which was made before and check mark it, then press Delete.

To Enable the Rule(s) click on "Enable" in the top bar when its Green the function is active.

airli▼e	Hon	ie Device	Network	User	Firewall	System			88 C
Maximum add 32 Item	Enable				_			Add	
Sn	Rule Name		Time Group		URL	5	Status Config		
			No limit is curre	ently added,please	Add				

 URL Filter 		×
Status	• Enable Disable	
Rule Name	Not use \ and Double quotes	
Time Group	Not limited	✓ + Add
URL	Not use \ and Double quotes	
		Confirm

Object	Description
Status	Select ON (Green) or OFF (Gray) to enable or disable
Rule Name	Enter the rule name, e.g. Black list
Time Group	Select to Customize or Add a Time Group and setup time range and work data.
URL	Enter the URL that you need to put in black list
Confirm	Press Save to save the settings



4.11.4 Firewall Port Map

Port mapping allows extranet access to an intranet server. Enter the IP Address of the client for which you would like to open the External and Internal port.

Click Add to open the Pop-up window to enter the Port information. To Delete a Port Mapping, select the Port Mapping which was made before and check mark it, then press Delete.

To Enable the Rule(s) click on "Enable" in the top bar when its Green the function is active.

airli▼e		Home	Device	Network	User	Firewall	System			88
Maximum add 32 Item	Enable					_			Add	
Sn	Rule Name	IP Address 🌲	Proto	col	External Port	Interna	I Port	Status	Config	
				No limit is curr	rently added, please	Add				

Status	Enabl	e Disab	le	
Rule Name	Not use	> \ and Double quote	IS	
Protocol	TCP+U	DP	~	
IP Address	0.0.0.0			Search
External Port	1	(1-65535) -	65535	(1-65535)
Internal Port	1	(1-65535) -	65535	(1-65535)

Object	Description
Status	Select ON (Green) or OFF (Gray) to enable or disable
Rule Name	Enter the rule name, e.g. Black list
Protocol	Select TCP, UPD or TCP+UDP
IP Address	Enter the IP Address or click Search for the IP Address you need for Port Forwarding
External Port	Enter the external port range
Internal Port	Enter the internal port range
Save	Save the settings.



4.11.5 Firewall – DMZ

Open the DMZ for a client IP Address.

Home	Device	Network	User	Firewall	System
	DMZ Host				
	DMZ Host	0.0.0.0			Search
		A	oply		

Object	Description
Enable DMZ	Select Enable DMZ Host or Disable
DMZ Host IP	Enter the DMZ LAN IP for which you would like to open DMZ
Apply	Save the setting.



4.12 System

The System Menu page offers several functions including Upgrade, Backup, IP Group, Time Group, Log, Reset and more. The IP Group and Time Group functions are used in the Firewall (Chapter 4.11)

4.12.1 System - Upgrade

Browse the firmware file and click on upgrade. Wait till the upgrade is successful. The device will reboot automatically after successful firmware upgrade. You can also turn on the Restore to Default after the Firmware Upgrade has been completed.

When selecting "Online Upgrade" the Wireless Controller when connected to Internet will automatically search the latest firmware. When there is no newer Firmware file the Wireless Controller will give a notice.

Select Local Upgrade to update the Wireless Controller via the computer.

Current Version will show which firmware is currently on the Wireless Controller.

Home	Device	Network	User	Firewall	System	
	🔥 Upg	rade software may ca	ause the system t down, or it may o	o interrupt, In the pr lamage the system!	ocess of updating	,do not power
System Time		2023-0	03-20 17:20:08			
Current version		WLAN	l-128GM-V2.0-Bu	ld20230303105108		
Upgrade Type		0 0	nline upgrade	Local upgr	ade	
Local upgrade		Upg	rade firmware not	uploaded	Local upload	
Upgrade time		Up	grade now		~	
Restore Default Co	onfig	0				
			Upgrade			

The page includes the following fields:

Object	Description
Local Upload	Press to select the firmware file
Upgrade Time	Select the Time to Update the Firmware of the Wireless Controller
Restore Default Config	Enable Factory Reset after firmware upgrade has been done
Upgrade	Press to upgrade the firmware

Note: Do not power off during the process of upgrading!!



4.12.2 System – Maintain - Telnet

Enable the Telnet function for the Wireless Controller, Note use this function with care!! When Enabled the device is open and could be hacked. Default this function is Disabled.

	Home	Device	Network	User	Firewall	System
Teinet	Reboot Re	egularly	Dhcp conflict d	etection	Capture packet	Ping
		Telnet	Enable	Disable		
			🚹 Enab	ing Telnet could b	e hacked,Use it care	fully!
				Apply		
				4993		

4.12.3 System – Maintain – Reboot Regularly

Set a schedule time on which the Wireless Controller would reboot, this can be every day or on an interval.

	Home	Device	Network	User	Firewall	System
Telnet	Reboot R	egularly	Dhcp conflict de	tection	Capture packet	Ping
	Syste	m Time	2023-03-20 17:2	21:30		
	Rebo	ot Regularly	Enable	 Disable 		
	O R	leboot Time	Everyday	~ 1 :	00 ~	
	O R	eboot Interval	1Day		~	
			A	pply		

Object	Description
Reboot Regularly	Select Enable or Disable to start schedule reboot
Reboot Time	Select reboot time form clock
Reboot Interval	Select reboot duty by day

4.12.4 System – Maintain – DHCP Conflict Detection

Enable this function to automatically detect a DHCP conflict on the network.

		Home	Device	Network	User	Firewall	System
Teln	et	Reboot Regu	larly	Dhcp conflict dete	ection	Capture packet	Ping
	🔽 Dhcp	conflict detection					Stop detection
				Detection	information		
				Testing and	d obtaining		
				resting un	a obtaining		

4.12.5 System – Maintain – Capture Packet

The Capture Packet enable the capture of a packet from a source IP address, this can be Any network or fixed on only LAN or WAN with different protocol TCP, UDP, ARP ect..

	Home	Device	Network	User	Firewall	System		
Telnet	Reboot Regula	ırly	Dhcp conflict del	ection	Capture packet		Ping	
	Network		ANY			~		
	Protocol		ТСР			~		
	Source ad	dress	0.0.0.0					
	target addı	ess	0.0.0.0					
	Source po	rt	0			(0-65535)		
	target port Number		0		(0-65535)			
			1			(1-2000)		
					Capture	packet		

Object	Description
Network	Select ANY, LAN or WAN as network
Protocol	Select the Protocol, TCP, UDP, ARP, IP or ICMP
Source Address	Enter the Source IP Address
Target Address	Enter the Target IP Address
Source Port	Enter the Source Port
Target Port	Enter the Target Port
Number	Number of Packets Captured



4.12.6 System – Maintain - Ping

Enable the Ping function by entering a Web Address which you would like to Ping. To start the Ping function, press the Ping button.

	Home	Device	Network	User	Firewall	System
Telnet	Reboot R	egularly	Dhcp conflict de	etection	Capture packet	Ping
Web add	iress		P	ng		

4.12.7 System – Reboot

Enable Reboot to Reboot the Wireless Controller directly.

Home	Device	Network	User	Firewall	System
		_			
			Reboot		



4.12.8 System – System Log

Review the Wireless Controller log, you can also enable Remote Log Service or export the log file.

rli▼e	Home	Device	Network	User	Firewall	System					88	Ð
System log Remote Lo	g							Ð	Export	Ē		
			S	ystem Log								
Jan 1 00:00:08 WLAN-128GM syslog.info syslog Jan 1 00:00:08 WLAN-128GM kern.notice kernel Jan 10:00:08 WLAN-128GM kern notice kernel Jan 10:00:08 WLAN-128GM kern warn kernel: Jan 10:00:08 WLAN-128GM kern info kernel: C Jan 10:00:08 WLAN-128GM kern warn kernel: Jan 10:00:08 WLAN-128GM kern debug kerne Jan 10:00:08 WLAN-128GM kern mernel: Jan 10:00:08 WLAN-128GM kern	d started: Busyl klogd started: Linux version The CPU feque GCMP present PU0 revision is fotware DMA c. letermined phys memory: 10000 Zone ranges: DMA [mem Normal [men HighMem em Normal [men HighMem em Novable zone : Early memory t Movable zone : Early memory t is DMA zone: 0 is DMA zone: 0 is DMA zone: 4 is DM	Box v1.22.1 BusyBox v1.22.1 BusyBox v1.22.1 S10.14+ (root@ nuce set to 880 Å s: 0001992f (MIP: ache coherency sical RAM map: 000 @ 00000000 or empty - disabili o 0x00000000-0x m 0x00000000-0x start for each nod node ranges m 0x00000000-0x japges sesef to 0366 pages, LIFC o pages reserved 10366 pages, LIFC s: 61440 pages sues diode 7 pages/cp 6666 r6192 d1362, v1 cache 266KB, i v1 cache 2	(2023-03-03 10) jubintu) (gcc vers Hz S 1004Kc) I (usable) ng initrd onfiffff] offiffff] ide cofffffff] gdat 814b4640, r memmap P batch:0 f for memmap P batch:0 f for memmap P batch:15 iFO batch:	:53:19 CST) sion 4.6.3 (Build node_mem_maj esize 32 bytes. s, linesize 32 by bytes. 5656 r8192 d138 8*4096 on. Total pages oot=/dev/ram0	oot 2012.11.1)) # o 81a84000 tes i24 u32768 : 65024	4692 SMP Fri Mar 3	10:59:48 CST 202	3				

 Remote Log Service Settings 		\times
Remote Log Service	0.0.0.0	
	ок	

Object	Description
Log	Select ON/OFF to record log or not
Remote Log Service	Enable remote log server and enter the server IP Address
Export	Export a log.bin file to you PC
Delete	Press the trashcan icon to delete all the system log
Refresh	Press the refresh icon to refresh the system log



4.12.9 System – Manage – Backup Information

Click "Export Settings File" to save the configuration file of the Wireless Controller to your local computer.

Home	e [Device	Network	User	Firewall	System	
Backup	information		Restore settings		Factory settings		Dhcp cache cleanup
		I	Export settings	file			

4.12.10 System – Manage – Restore Settings

To Restore a saved Configuration file, select a previous saved configuration from your computer and Click "Use Configuration File" This will now load the settings which you saved before. Note the current configuration will be overwritten!!

Home Devic	e Network	User	Firewall	System	
Backup information	Restore setti	ngs	Factory se	ettings	Dhcp cache cleanup
Restore	Select local file			Loc	al upload
	Use	configuration f	ile		

4.12.11 System – Manage – Factory Settings

Reset will return the Wireless Controller back to its factory default settings. All current settings will be lost!! Use this function with care.

i	Home	Device	Network	User F	-irewall	System		
Bac	kup information		Restore settings		Factory se	ettings	Dhcp cache cleanup	
	After returning to the factory, the existing configuration will be lost. Please operate carefully							
			Reset					

4.12.12 System – Manage – DHCP Cache Cleanup

Delete the Terminal and AP Cache from the Wireless Controller.

Home	Device	Network	User	Firewall	System	
Backup informat	ion	Restore se	ttings	Factory s	ettings	Dhcp cache cleanup
	Delete term	inal Dhcp cache		Delete AP Dhcp cach	e	



4.12.13 System – System Time

Setup the system time, enable NTP Server and select the Time Zone for the Wireless Controller.

Home	Device	Network	User	Firewall	System
Time	synchronization	 Host time 	0	letwork time	_
Curre	ent Time	2023-03-20 17:2	7:08		
Time	Zone Select	(GMT+08:00)	Beijing, Chongqir	ng, Hong Kong, Uru	m ~
NTP	Server	time.windows	.com		~
	Manual IP Setting				
		Ар	ply		

The page includes the following fields:

Object	Description
Time Synchronization	Select either Host Time or Network Time
Current Time	Show system time of the Wireless Controller
Time Zone Select	Select Time Zone
NTP Server	Select NTP server
Manual IP Setting	Enter manual IP for NTP server

Note: If you want to use any function that needs scheduling, must enable NTP function.



4.12.14 System – IP Group

IP Group, Setup up an IP Group which can be used in the Firewall menu.

Click Add to open the Pop-up window to enter the IP information. To Delete an IP Group, select the IP Group which was made before and check mark it, then press Delete.

air	rli▼e°	Home	Device	Network	User	Firewall	System		88	Đ
	Maximum add 16 Item						_	Add		
	Sn	IP Group				IP Ran	ige	Config		
				No limit is current	ly added, pleas	e Add				

 Add IP Group 		\times
IP Group	Not use \ and Double quotes	
Start IP	0.0.0.0	Search
End IP	0.0.0.0	1
		Confirm

Object	Description
IP Group	Enter an IP group description
Start IP	Enter a start IP Address for the range or use Search to select
End IP	Enter an End IP Address for the range.
Confirm	Save the settings.



4.12.15 System – Time Group

Time Group, Setup up a Time Group which can be used in the Firewall menu.

Click Add to open the Pop-up window to enter the Time information. To Delete a Time Group, select the Time Group which was made before and check mark it, then press Delete.

airli∎e			Network		Firewall	System			88	G
Maximum add 16 Item								Add		
Sn	Time Group		Time Range			Work date		Config		
			No limit is current	lly added,please	Add					
	 Add Time Group 						×			
	Time Group	Not	use \ and Dou	ible quotes						
	Time limit	00	~ : 00	~]-[00 ~ :	00 ~				
	Limit Cycle	Cus	tomize		~					
		Mc	onday ursday	Tuesday Friday	We Satu	dnesday Irday				
		Jou	inuay							
					Co	onfirm				

The page includes the following fields:

Object	Description				
Time Group	Enter a Time Group description				
Time Limit	Select Start Time and End Time for time range				
Limit Cycle	Select Workday by option table				
Confirm	Save the settings.				

4.12.16 System - Accelerate

This function can greatly improve the network forwarding ability of the Wireless Controller. Note: When this function is enabled (Hard Fast NAT) the Speed Limit function of the Wireless Controller will not f function correctly. Switch the Accelerate function back to "Normal" when the Speed Limit function needs to be used.

Method Hard Fast NAT ~	Home	Device	Network		Firewall	System	
After setting, network forwarding ability will be greatly improved, firewall function will be disable	Method	Hard Fast NAT		~		_	
	(After setting,	network forwarding a	bility will be great	ly improved,fire	wall function will b	e disable
		_	_				