WLAN-64GM
Enterprise Wireless Controller & Gateway

WLAN-128GM
Enterprise Wireless Controller & Gateway

Web Manual

Ver. 1.0

CONTENTS

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

1.2 Product Specification WLAN-64GM

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

Model	WLAN64GM Enterprise Gateway & Wireless Controller

User Speed Limit

One Key Enable/Disabled
IP Group
Time Group
Up/Down
Remake

- **Firewall**:
  - IP Filter
  - Rule Name
  - Protocol
  - TCP/UDP
  - IP Address
  - Search
  - External Port
  - Internal Port
  - MAC Filter
  - Name
  - Time Group
  - Mac Address
  - Search Mac Address
  - URL Filter
  - Name
  - Time Group
  - URL Address
  - Port Map
  - Name
  - 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 Default Configure
  - Upgrade

Maintain

Remote Login
Remote Telnet
Reboot Regularly
DHCP Conflict Detection
Capture packet
Network
Protocol
Source Address
Target Address
Target Port
Number
Ping

Environment

Working Temperature: -20℃~55℃
Storage Temperature: -40℃ ~ 70℃
Working Humidity: 5% ~ 97%RH (No condensation)

Dimension

Package Size: 50 x 28.5 x 8 cm
Carton Package: 10PCS / 1 CTN
Carton Weight: G.W=10KGS
Carton Size: 54.5 x 32.5 x 23.5 cm

Ordering Information

Model Name: AirLive WLAN-64GM
Description: Enterprise Gateway & Wireless Controller

1.3 Product Specification WLAN-128GM

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

Model	WLAN-128GM Enterprise Gateway & Wireless Controller

User Speed Limit

One Key Enable/Disabled
IP Group
Time Group
Up/Down
Remake

- **Firewall**:
  - IP Filter
  - Rule Name
  - Protocol
  - TCP/UDP
  - IP Address
  - Search
  - External Port
  - Internal Port
  - MAC Filter
  - Name
  - Time Group
  - Mac Address
  - Search Mac Address
  - URL Filter
  - Name
  - Time Group
  - URL Address
  - Port Map
  - Name
  - 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 Default Configure
  - Upgrade

Maintain

Remote Login
Remote Telnet
Reboot Regularly
DHCP Conflict Detection
Capture packet
Network
Protocol
Source Address
Target Address
Target Port
Number
Ping

Environment

Working Temperature: -20℃~55℃
Storage Temperature: -40℃ ~ 70℃
Working Humidity: 5% ~ 97%RH (No condensation)

Dimension

Package Size: 50 x 28.5 x 8 cm
Carton Package: 5PCS / 1 CTN
Carton Weight: G.W=9KGS
Carton Size: 50.5 x 43.5 x 34.5 cm

Ordering Information

Model Name: AirLive WLAN-128GM
Description: Enterprise Gateway & Wireless Controller

Chapter 2. Hardware Installation

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

WLAN-64GM

WLAN-128GM

LED Description.

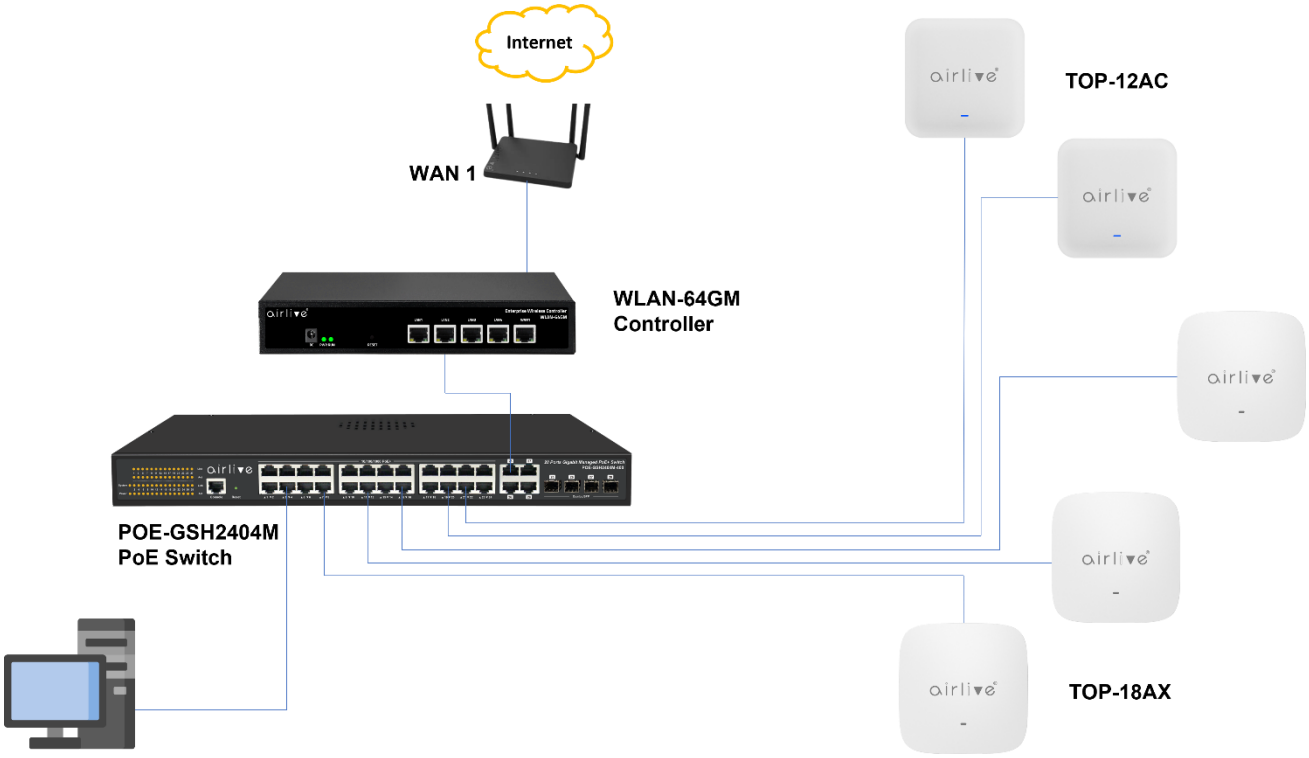
LED	Status	Function
PWR	On (Green)	Wireless Controller is powered on
	Off	System is off
Run	Blinking (Green)	Wireless Controller is working
	Off	No traffic
WAN/LAN	Blinking	Cable connected and Data Transfer

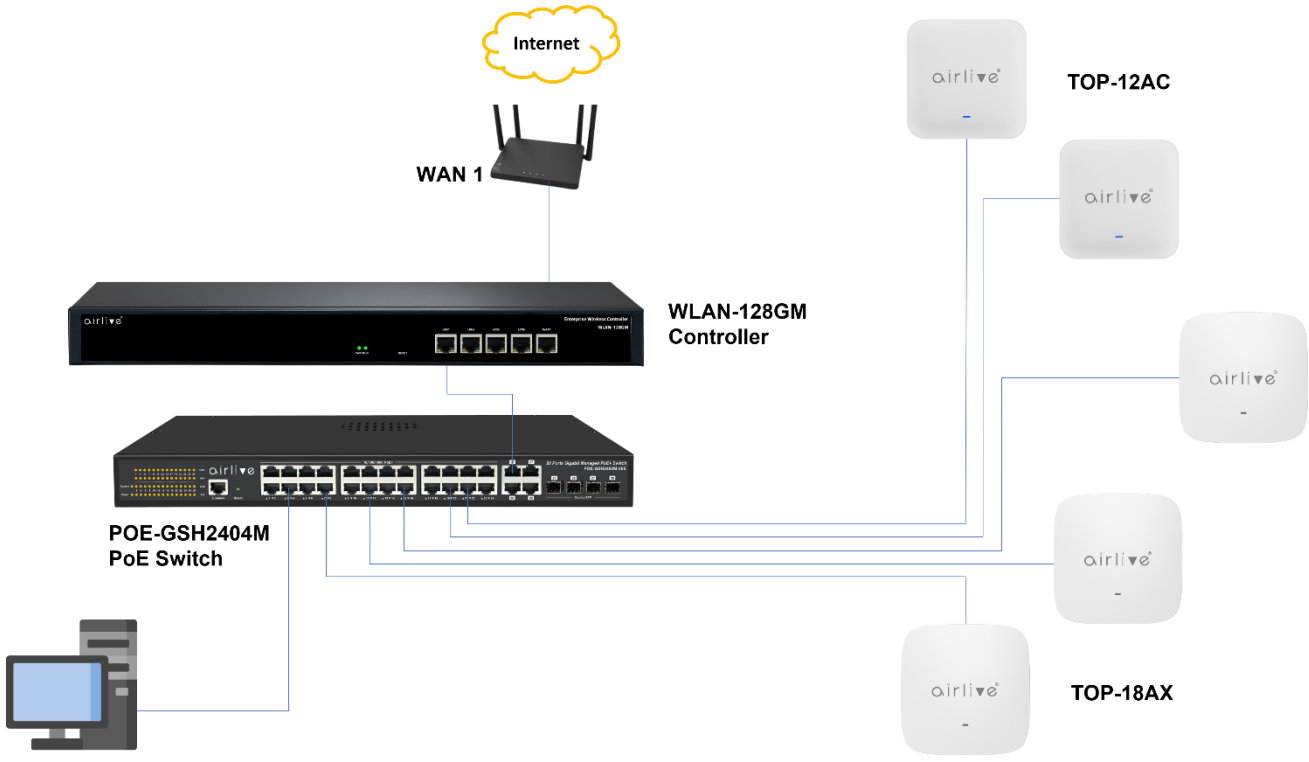
Port Description.

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.
Reset	To restore to the factory default setting, press and hold the Reset Button for 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

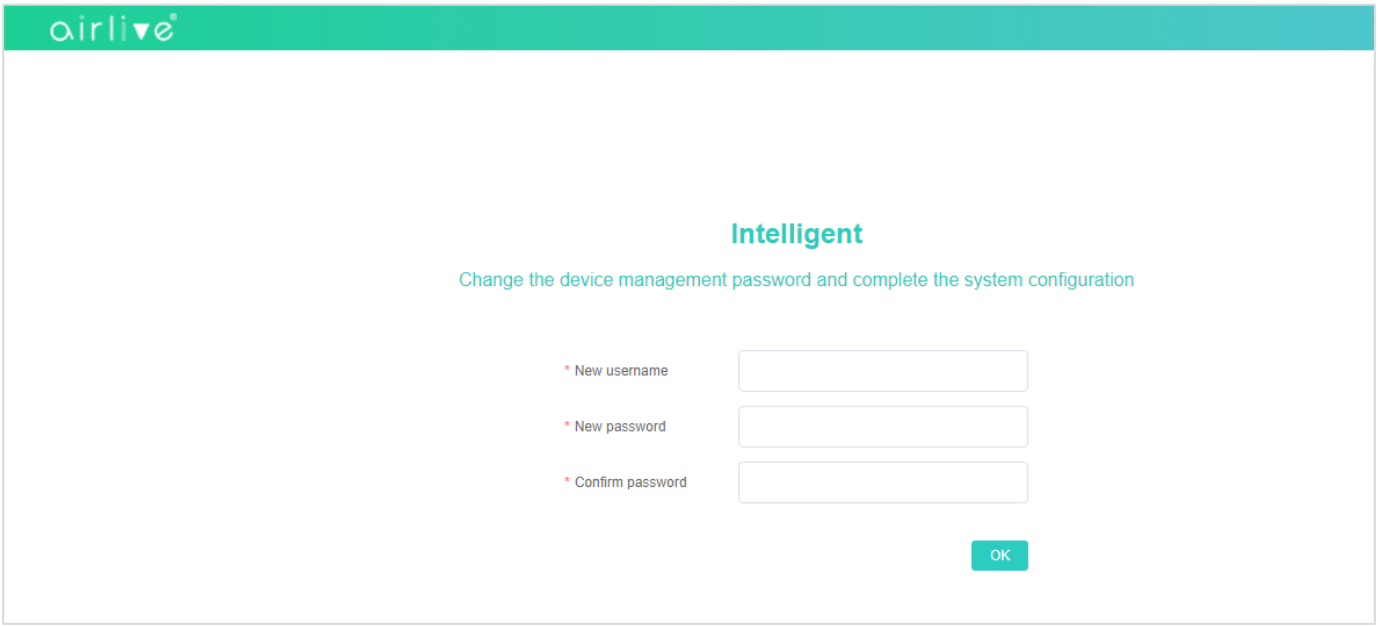
3.1 WLAN-64GM, WLAN-128GM , Web login Management.

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.

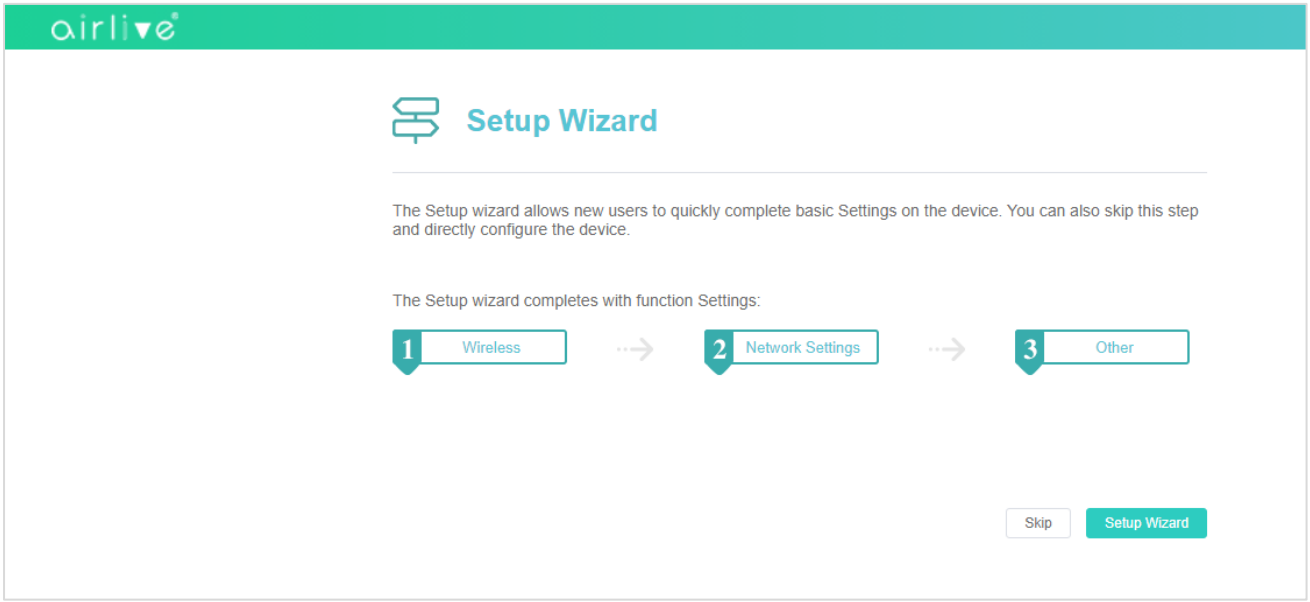
3.2 Initial Setup in the Web UI.

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



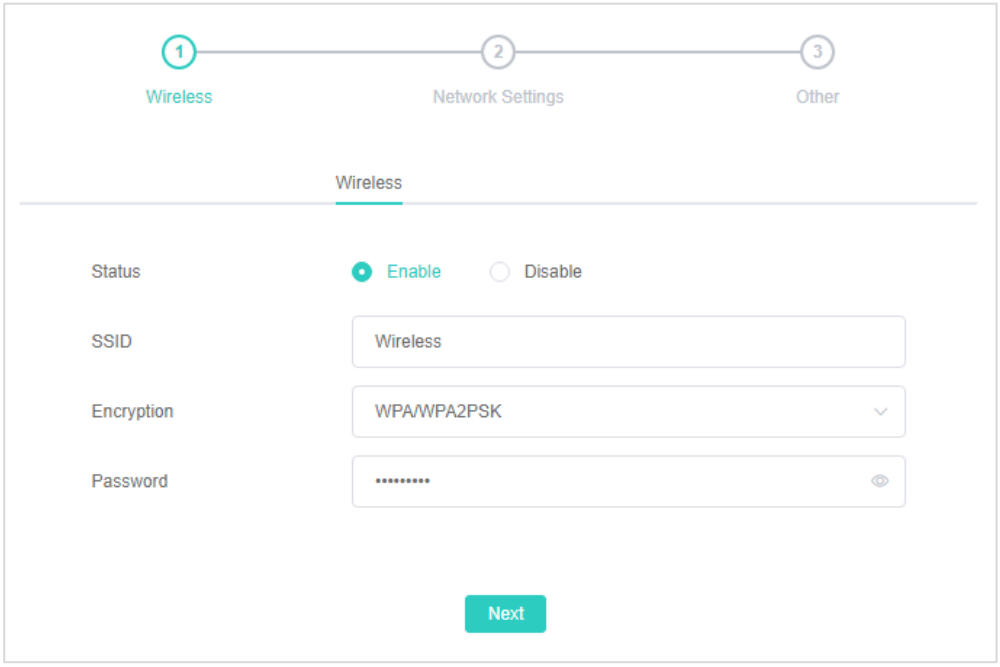
3.3 Wizard

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



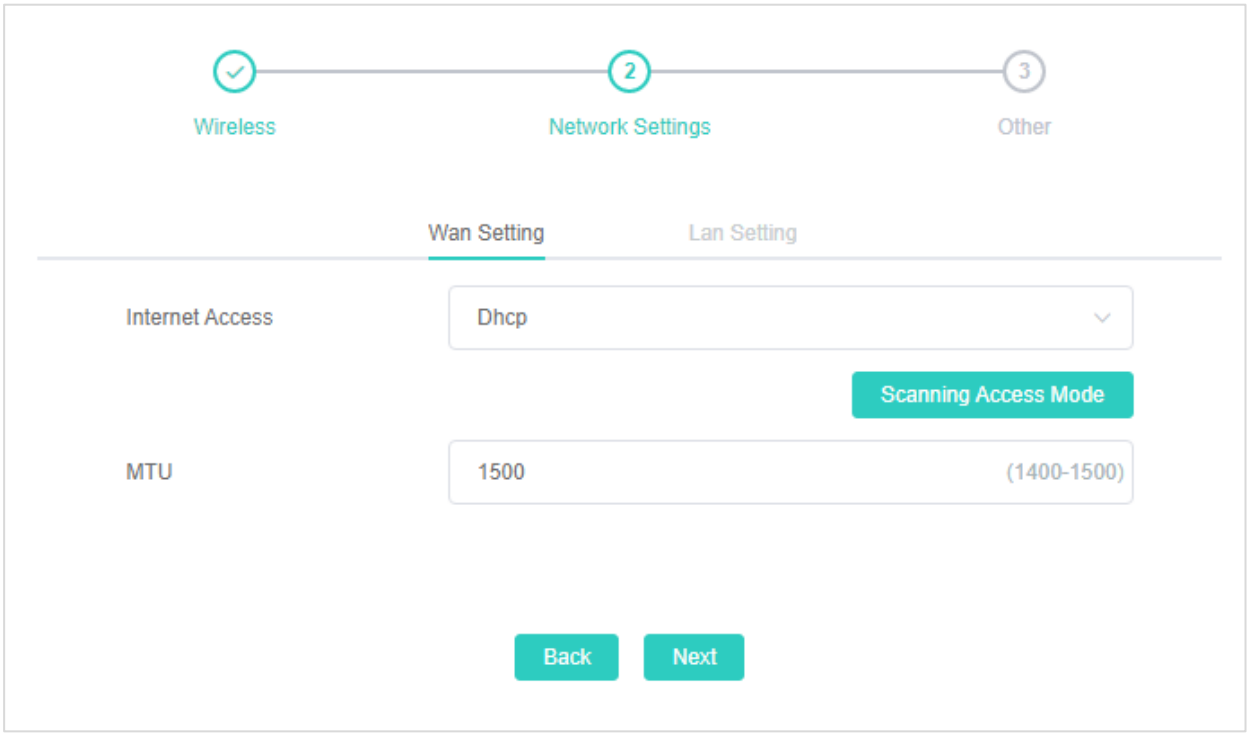
3.4 Wizard Wireless

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.



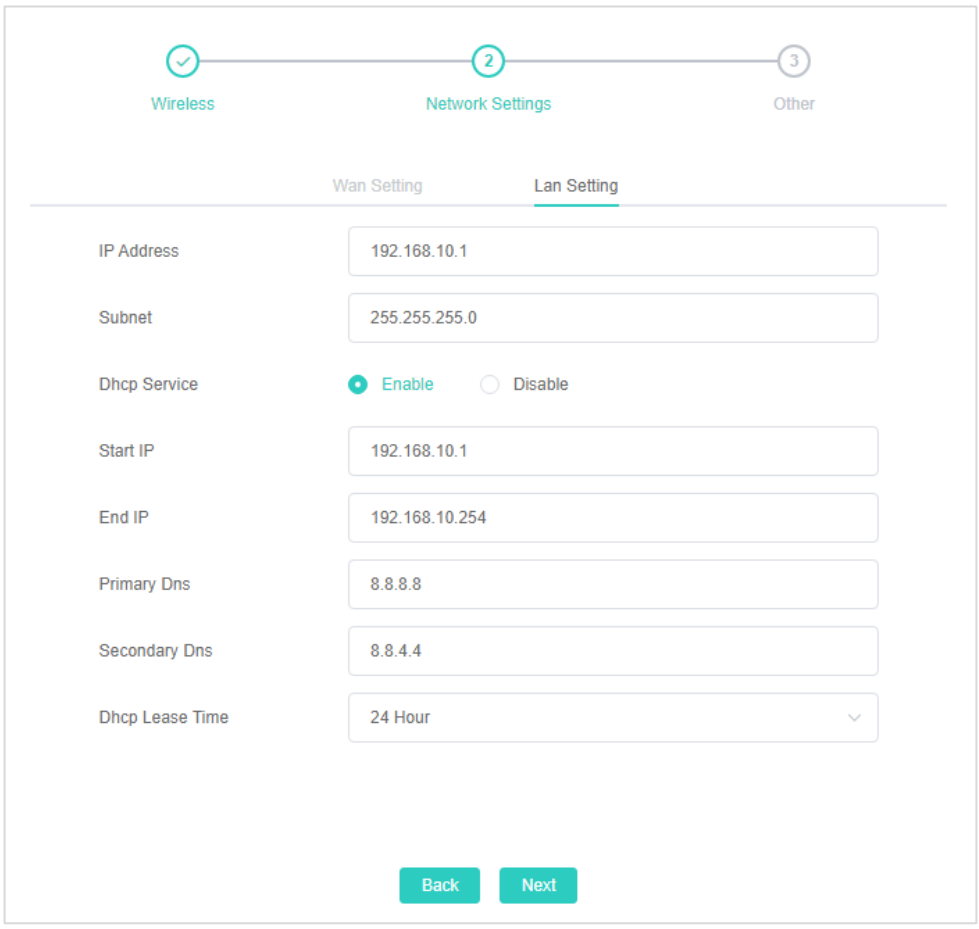
3.5 Wizard Network WAN

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.



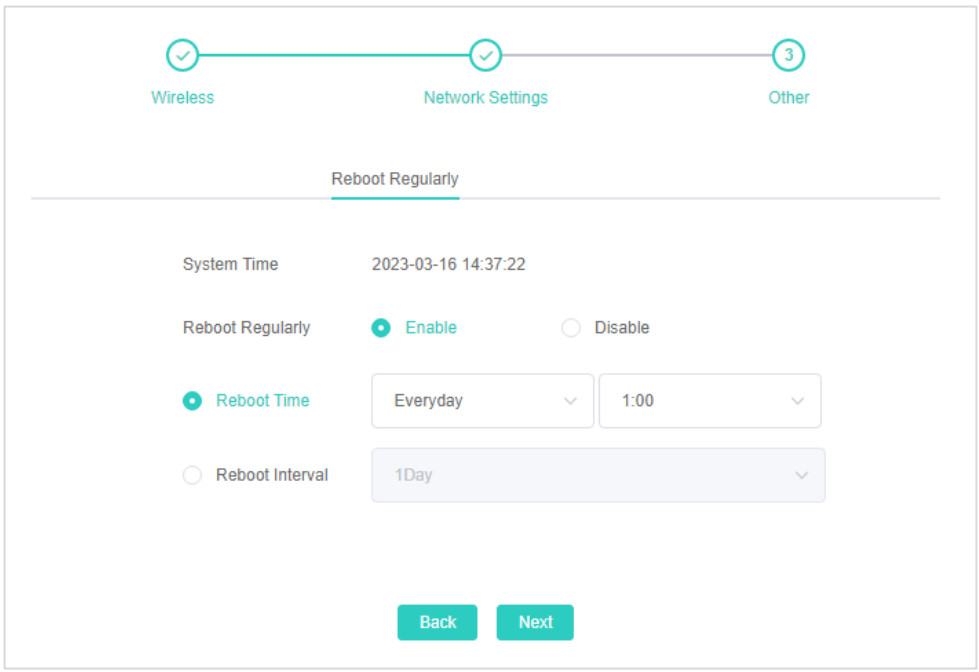
3.6 Wizard Network LAN

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



3.7 Wizard Network Other

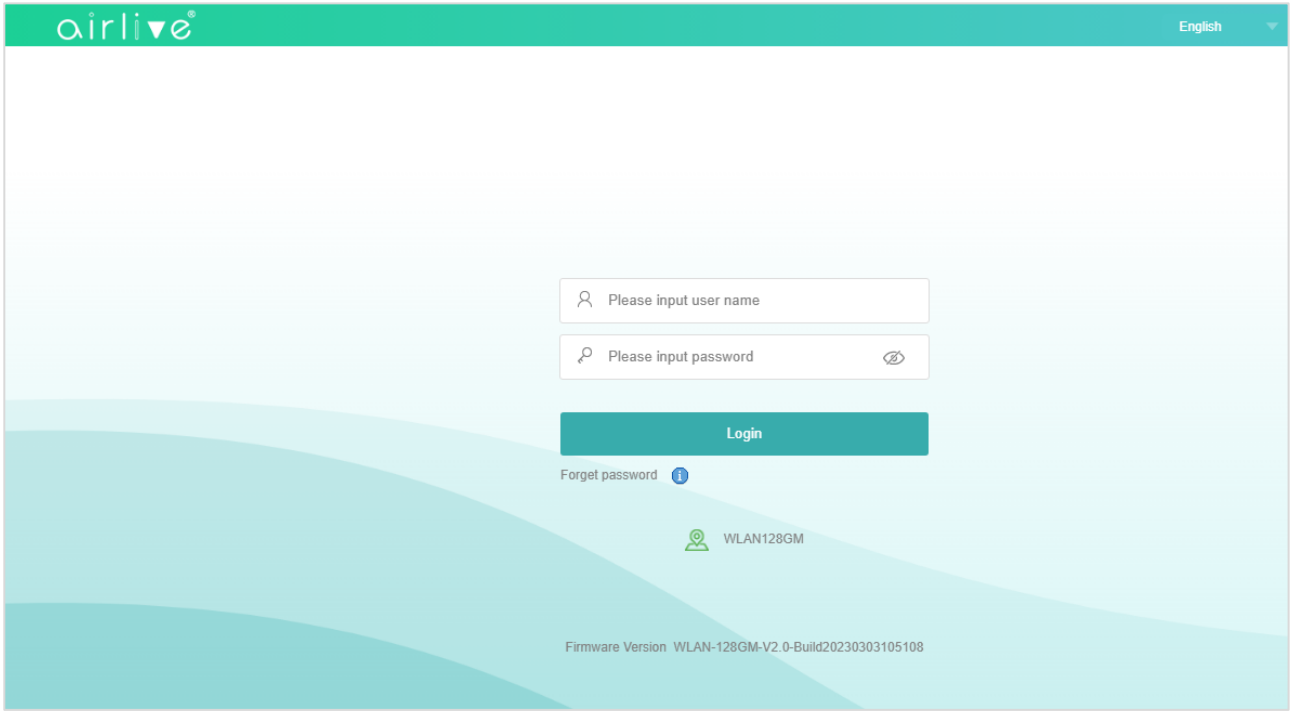
The Wireless Controller can automatically reboot on a fixed time. Select to Enable or Disable this function. After this select the Reboot Time and the Reboot Interval.



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.

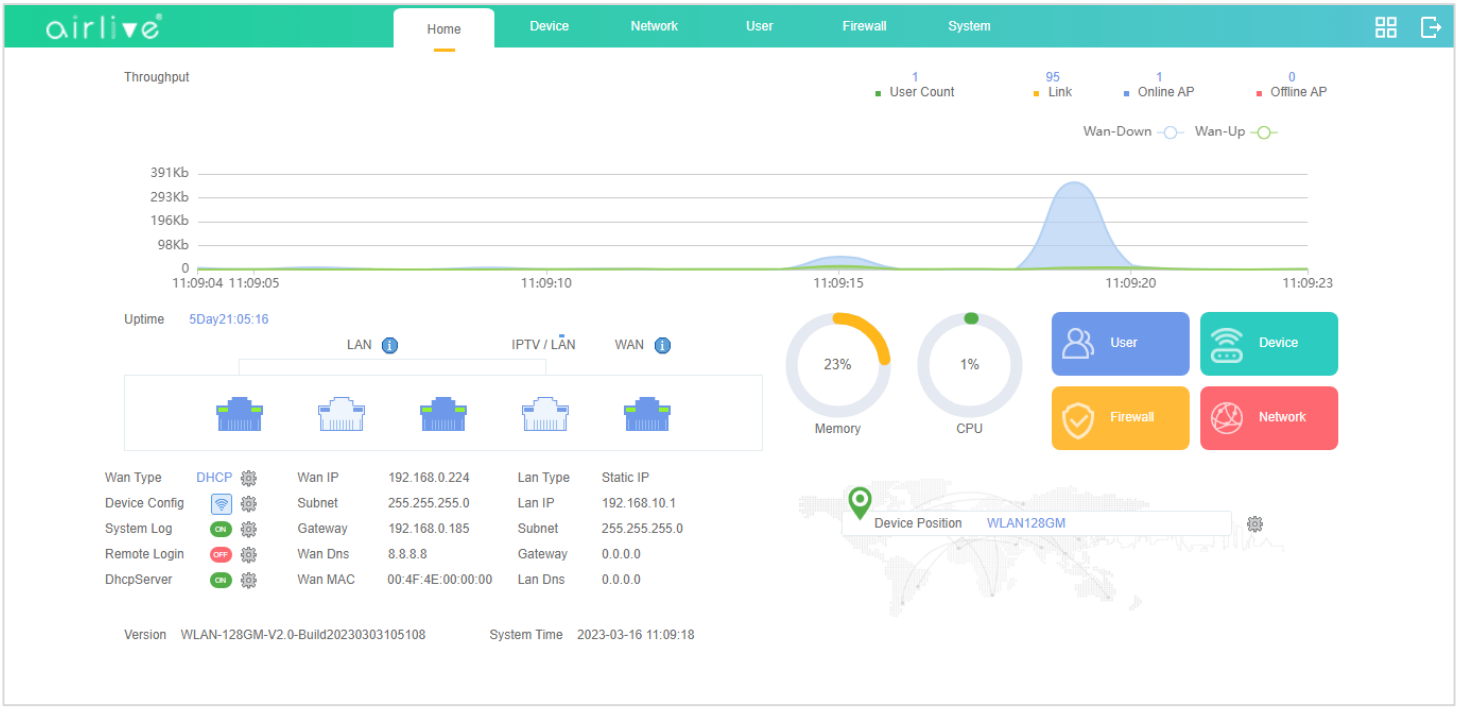
To change the language settings from English to Spanish click on the "v" to open the menu.



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:

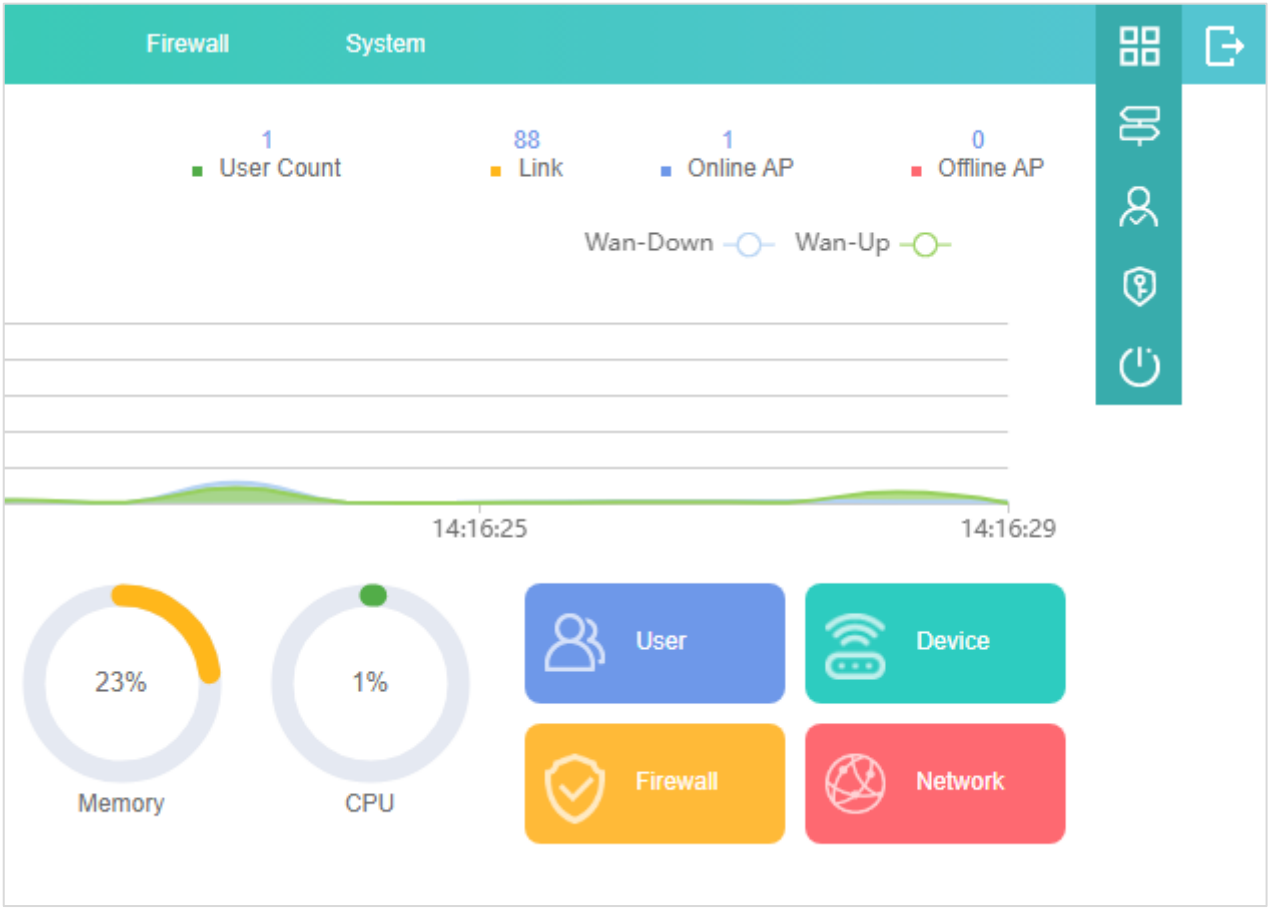
Object	Description
Throughput	Shows the current status of the WAN port UP and Downstream graph
LAN	Shows the current LAN status and IP information
WAN	Shows the current WAN status and IP information
Device Position	You can enter the device description.
Memory	Current % of internal memory in use
CPU	Current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

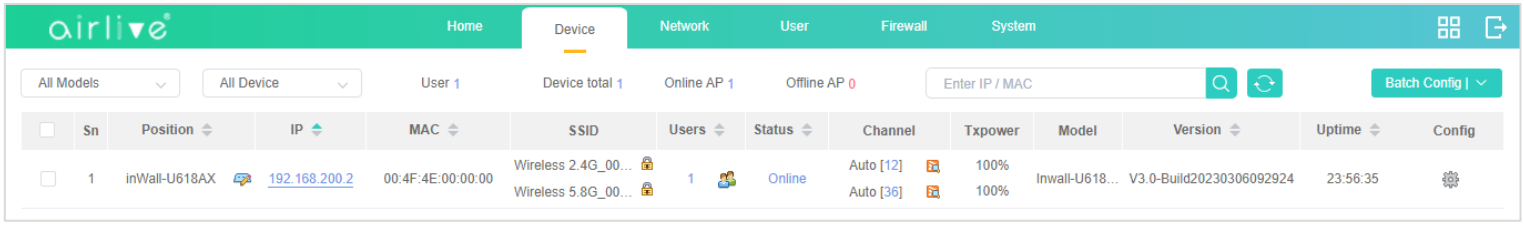
4.2 Reboot and Password Change

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.



4.3.1 AP List - Position

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

4.3.2 AP List - IP

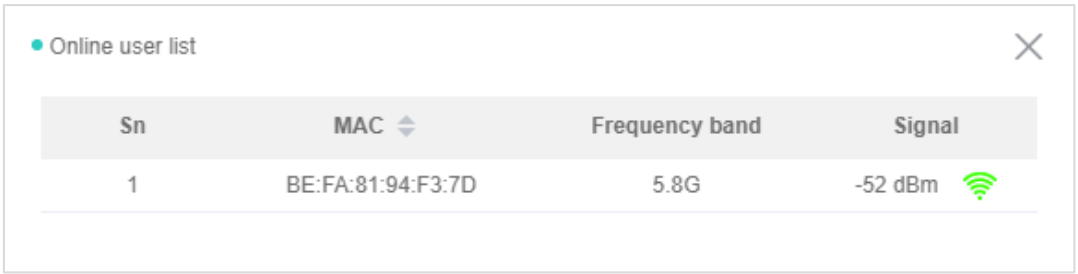
Click on the IP Address of the Access Point, the local webGUI of the Access Point will now open.
Note Wi-Fi changes which are made in the Access Point webGUI will be overruled by the Wi-Fi settings of the Wireless controller.

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.

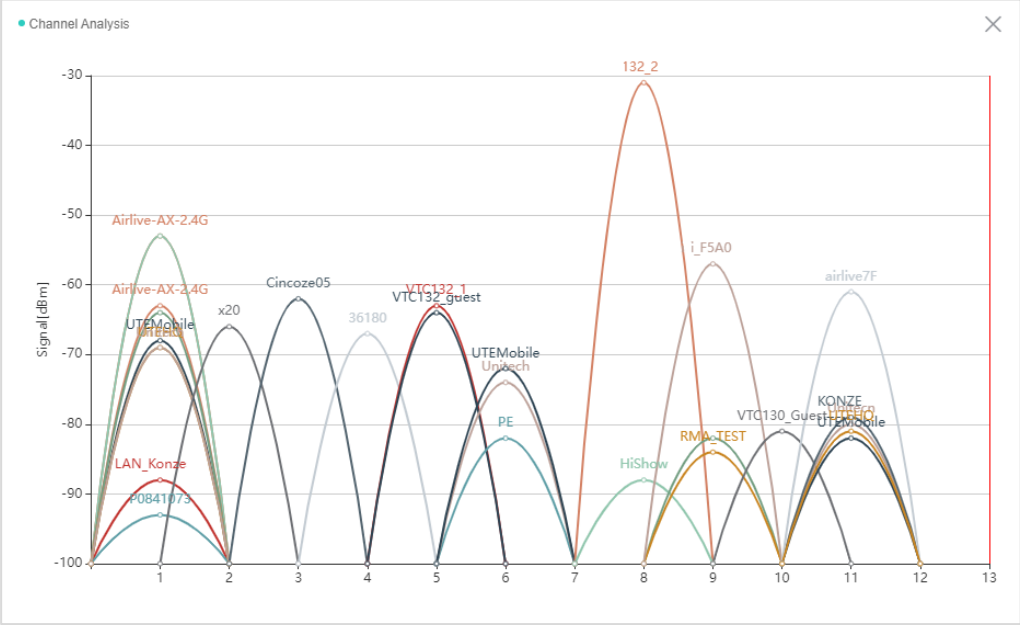
4.3.4 AP List - Users

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



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.

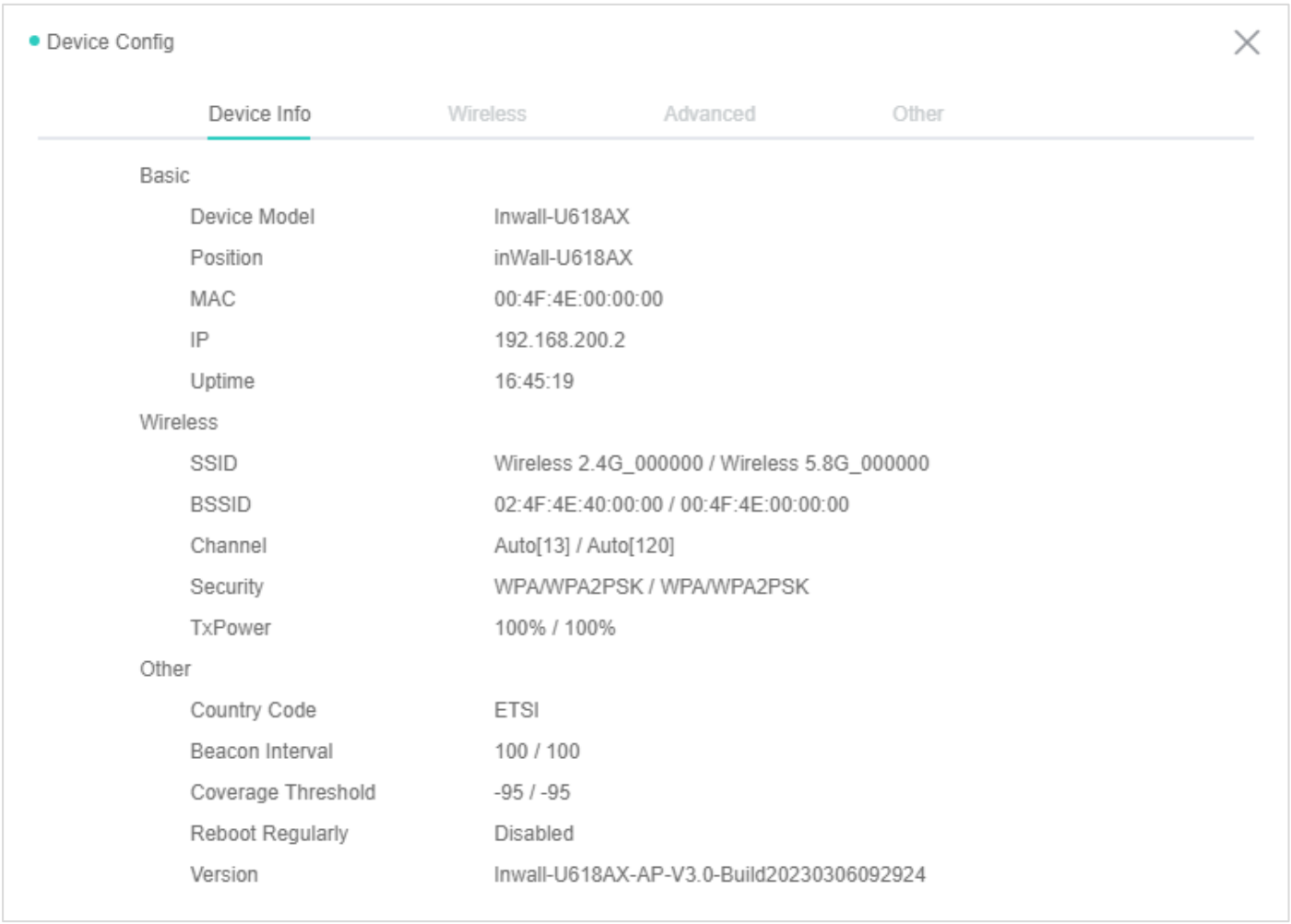
Batch Config: When using this function settings can be applied to multiple Access Points in one go. These can be the Wireless settings, Device Password, Reboot and Reset.

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.

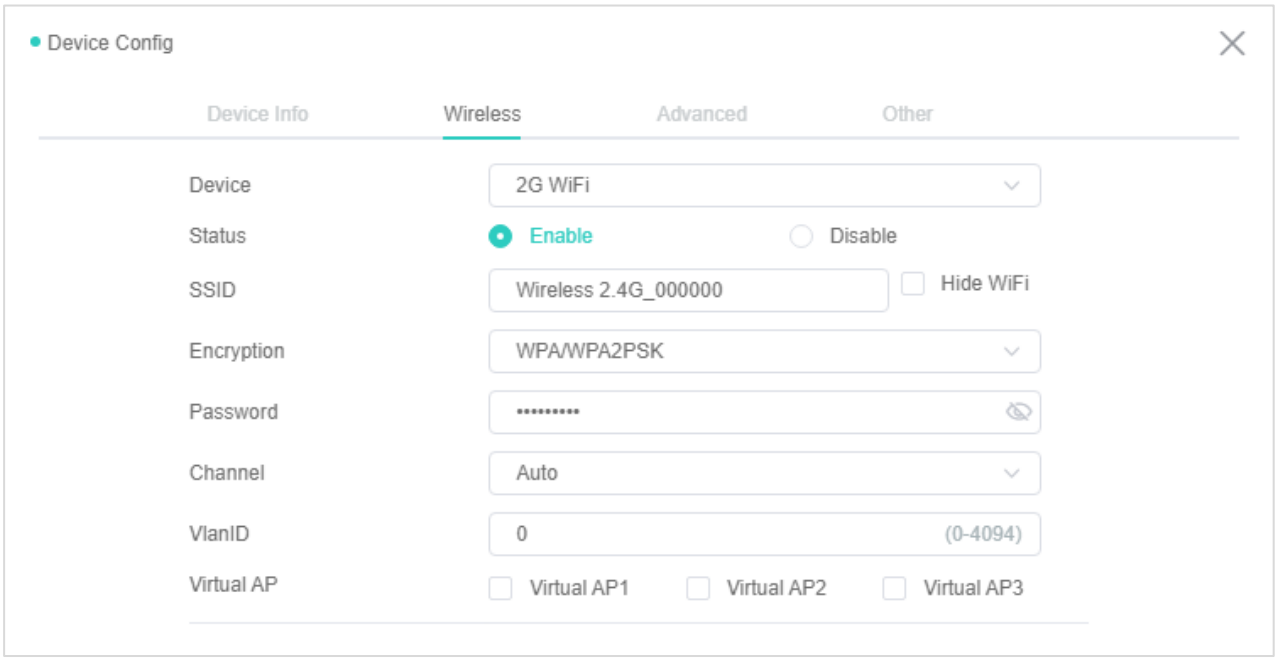
4.3.8 AP List – Config – Device Info

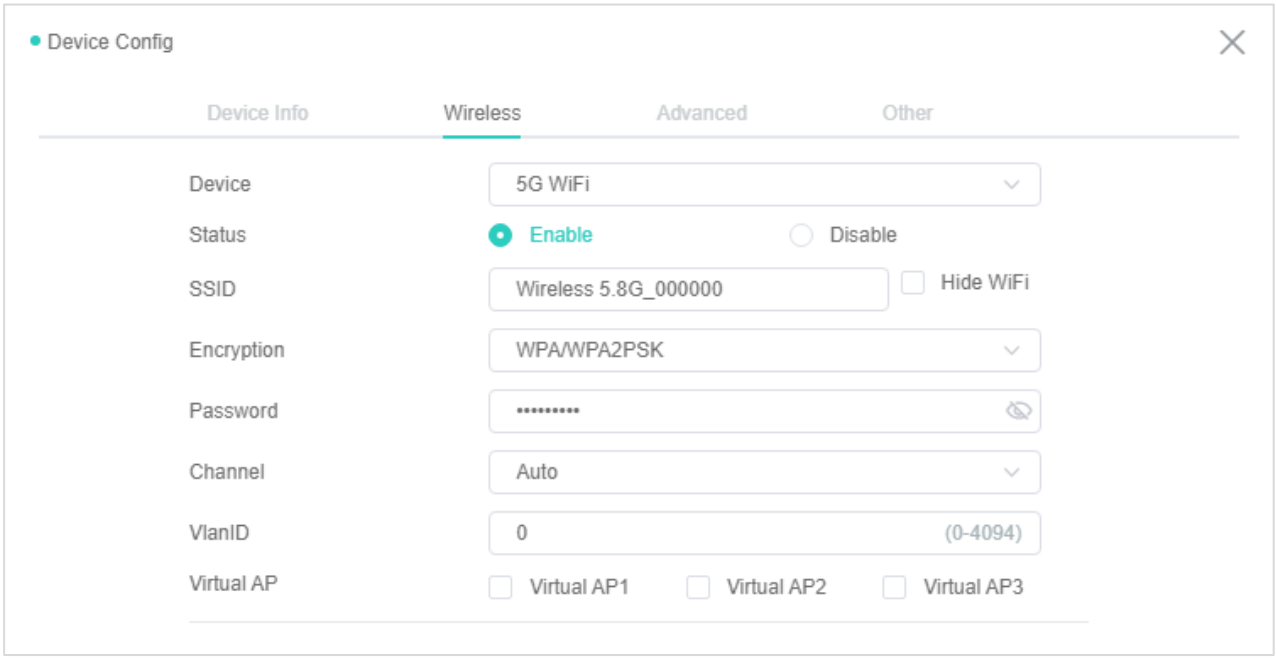
Device Info: This is an overview page which will display the current settings of the Access Point.



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



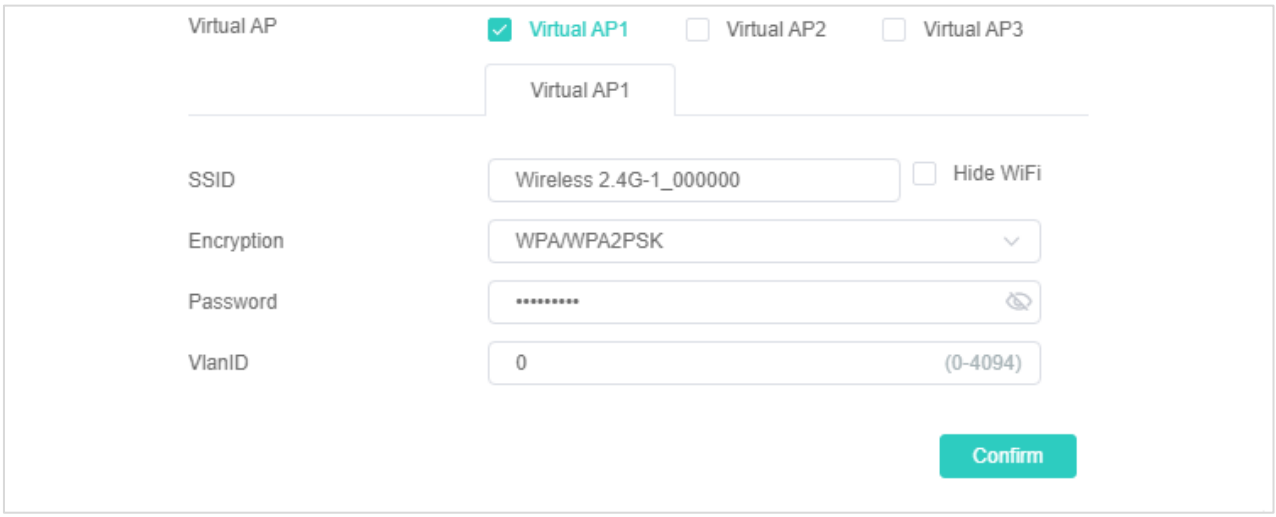


The page includes the following fields:

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

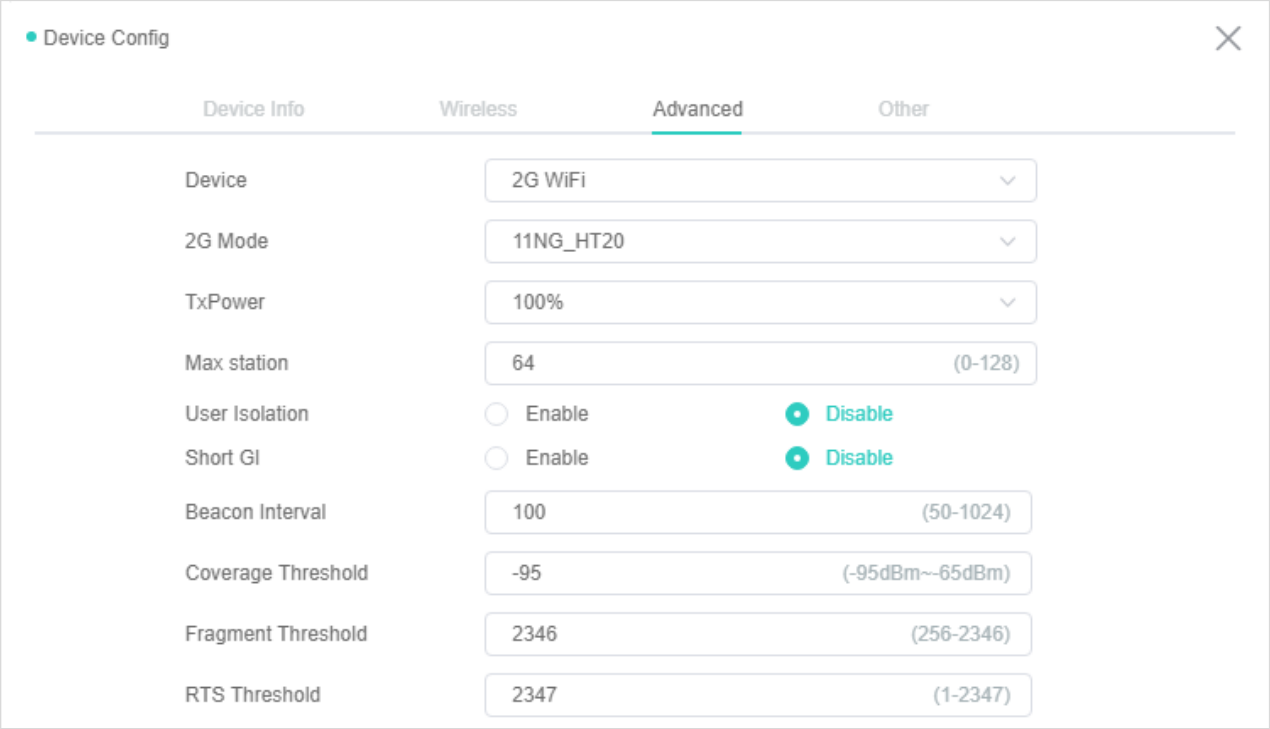


The page includes the following fields:

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.

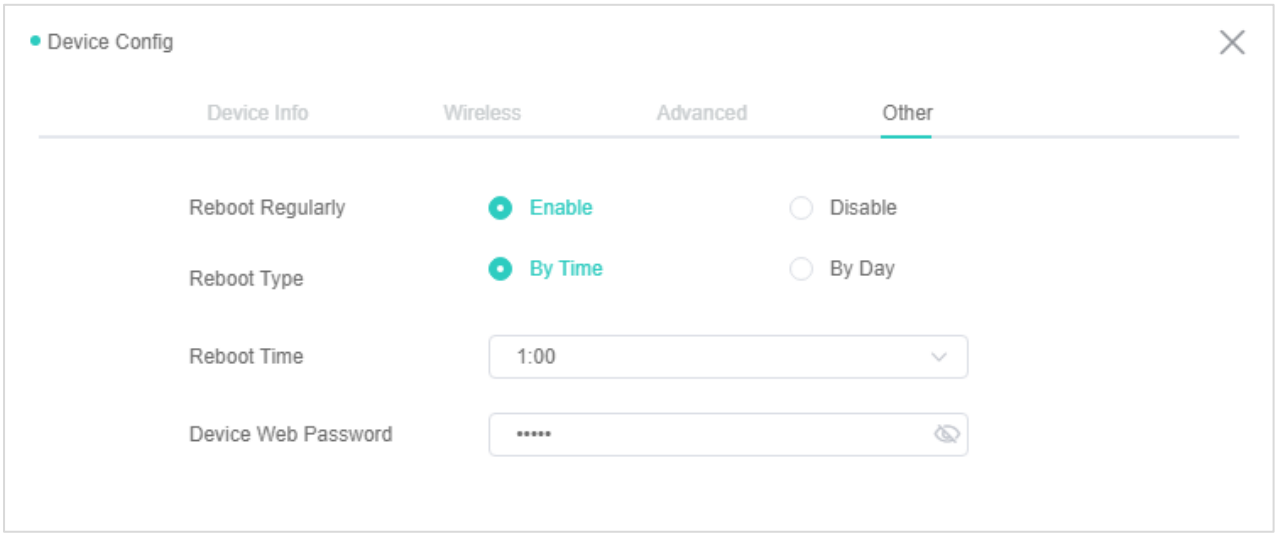


The page includes the following fields:

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.
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.

4.3.11 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.

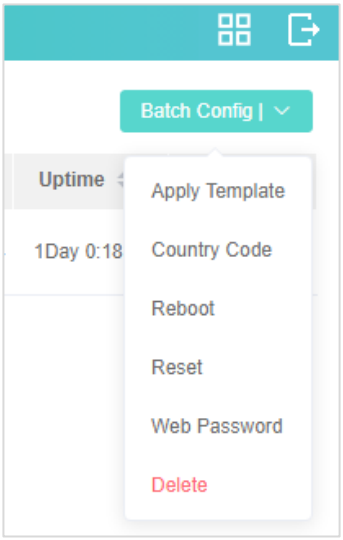


The page includes the following fields:

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

4.3.12 AP List – Batch Config

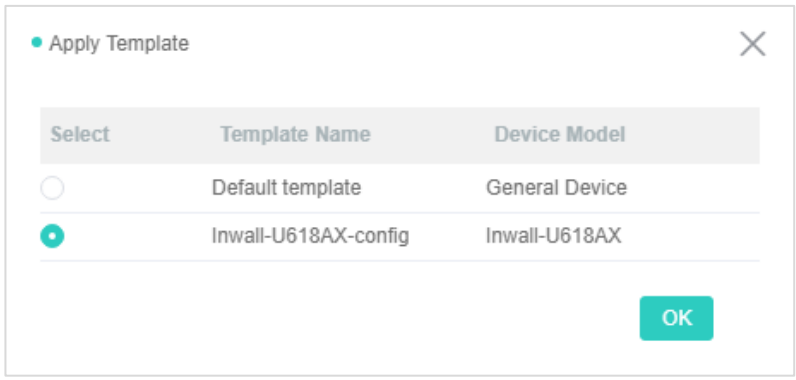
Batch Config: When using this function settings can be applied to multiple Access Points in one go. These can be the Wireless settings (Template), Device Password, Reboot and Reset.
To make a Template please see chapter 4.4
When the downward arrow is click for the Batch Config a pulldown menu will appear.



Object	Description
Apply Template	Apply the default Template or a made one
Country code	Select your region valid in your area of use.
Reboot	Reboot the Access Point
Reset	Reset the Access Point back to factory default
Web Password	Change the Access Point Password
Delete	Delete an Access Point from the AP List, Access Point must be offline

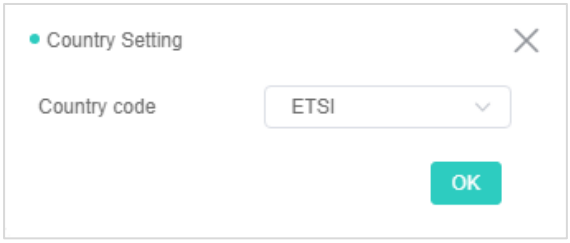
4.3.13 AP List – Batch Config – Apply Template

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.



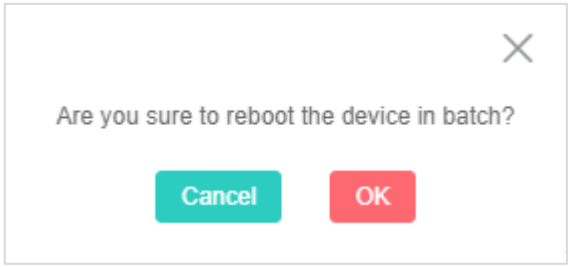
4.3.14 AP List – Batch Config – Country Code

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.



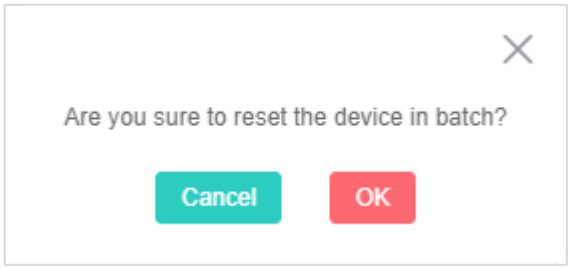
4.3.15 AP List – Batch Config – Reboot

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



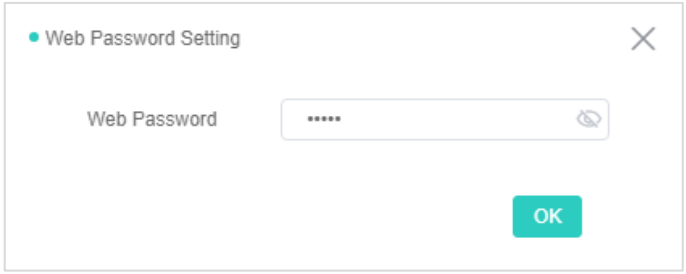
4.3.16 AP List – Batch Config – Reset

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.



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.

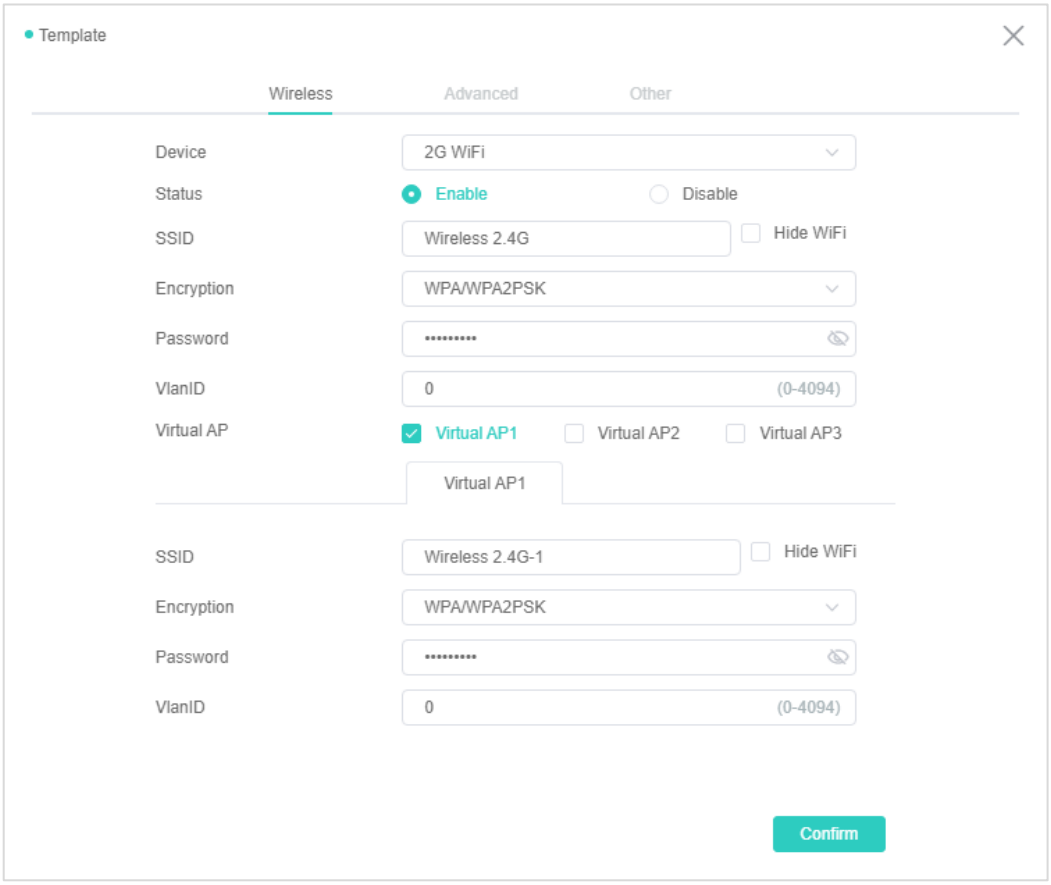
To make additional templates click on “Add” and enter a new Template Name.
For Device Model select the Model of Access Point for which the Template will be made. Only models which are active and online in the AP List will be displayed when different models are connected.

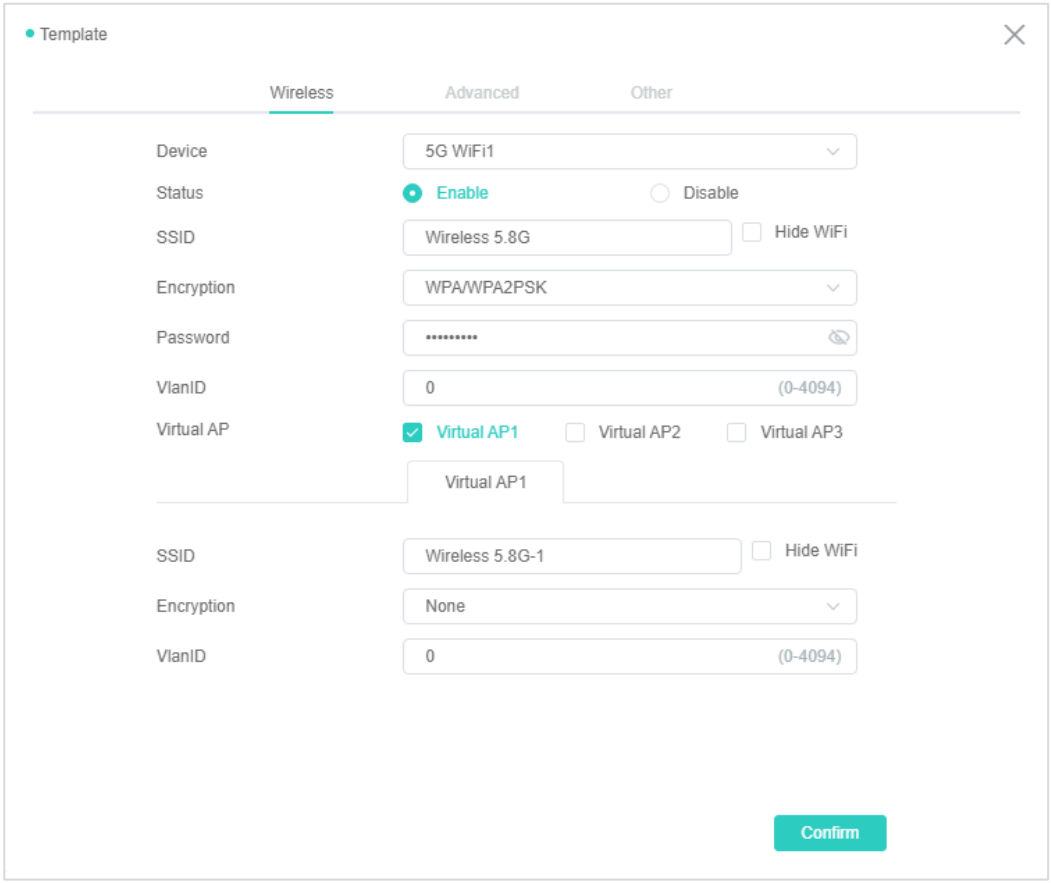
4.4.1 Device – Template – Wireless

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



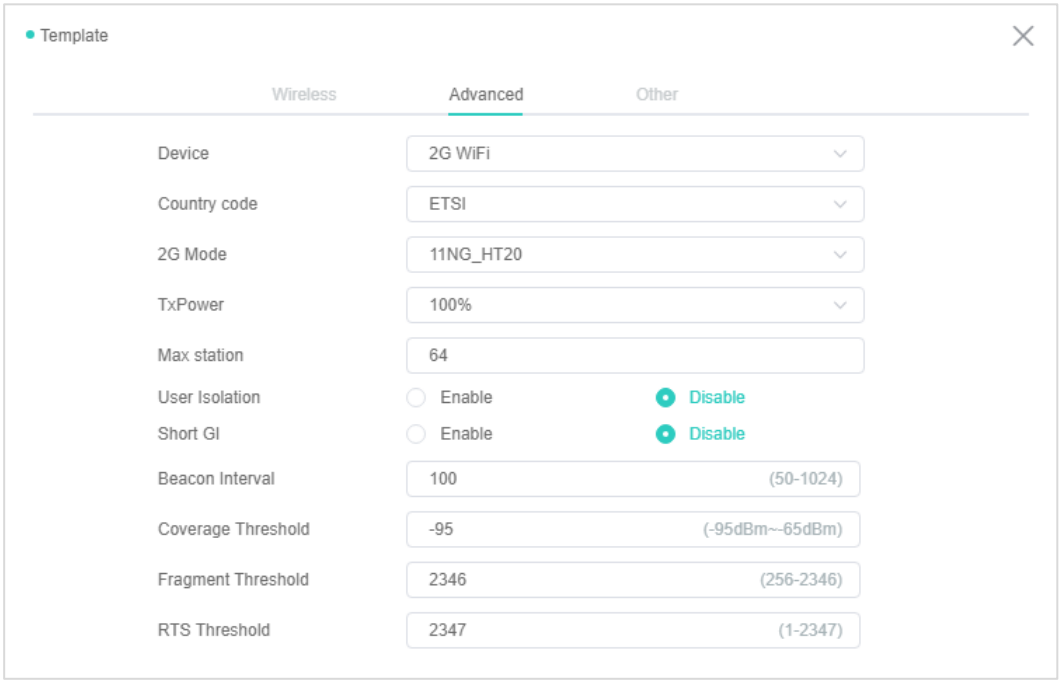


The page includes the following fields:

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	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.

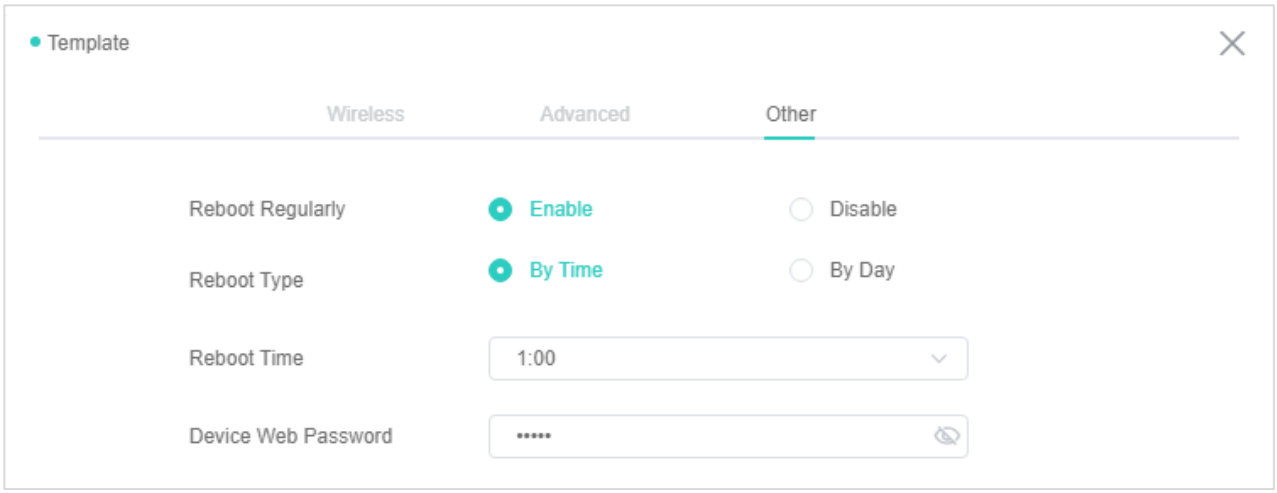


The page includes the following fields:

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 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.
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.

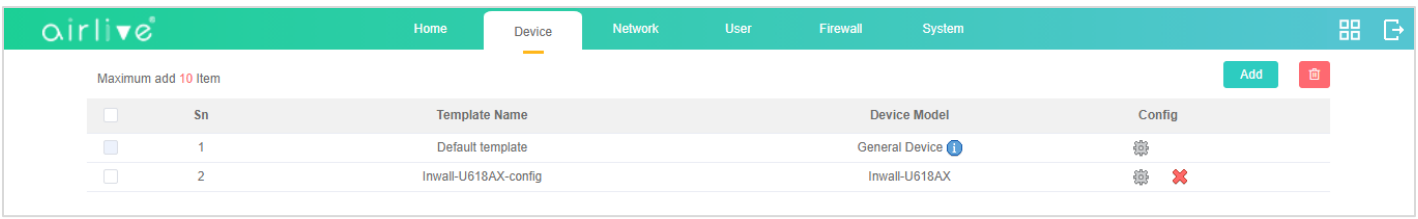


The page includes the following fields:

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

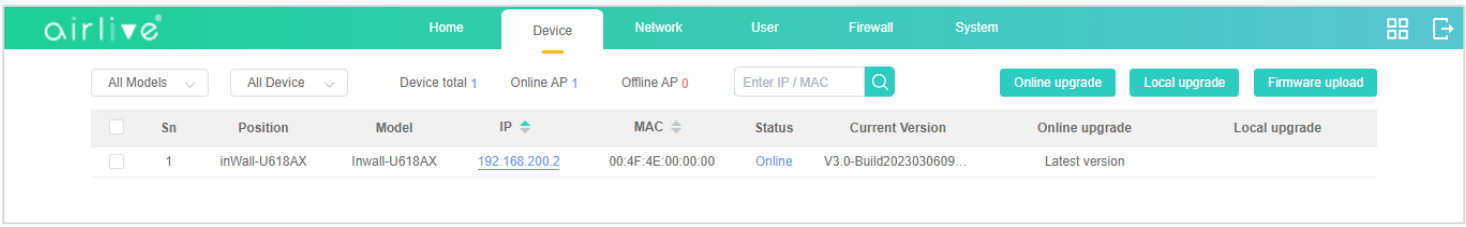
After the Template has been saved it will be displayed in the list.
To apply a Template please see Chapter 4.3.11 and 4.3.12

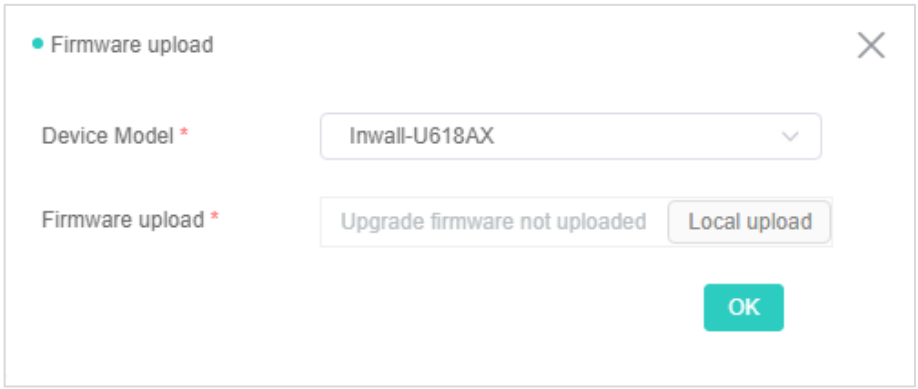


4.5 Device – Upgrade

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.

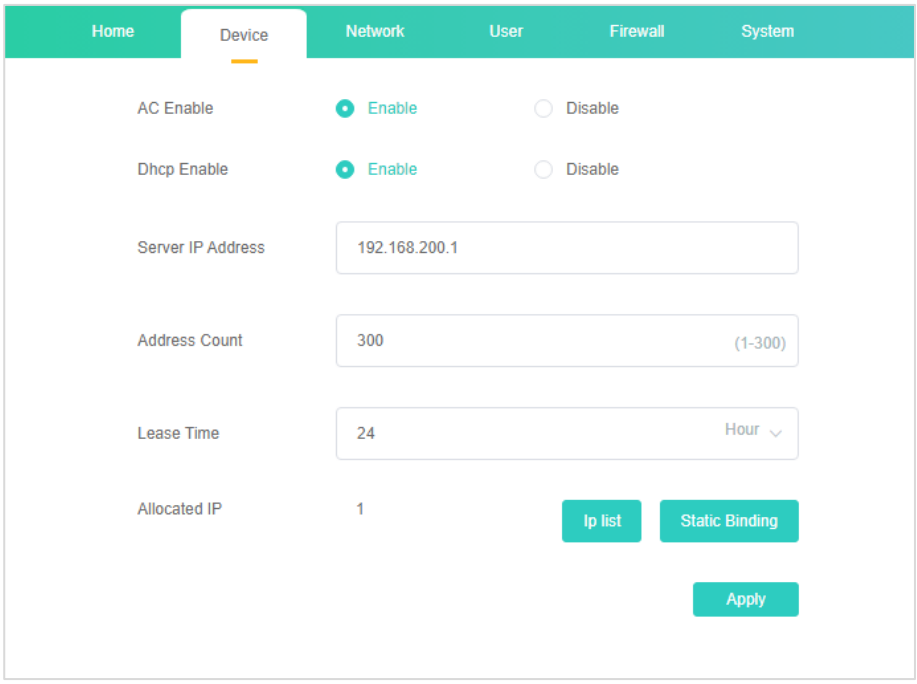
Online Upgrade: First check mark the Access Point you would like to Upgrade then click on Online Upgrade. When the Access Points already has the latest version of Firmware a notice will pop up. When the Firmware is not up to date you can select the latest version from the list which is displayed.
Local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





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.



The page includes the following fields:

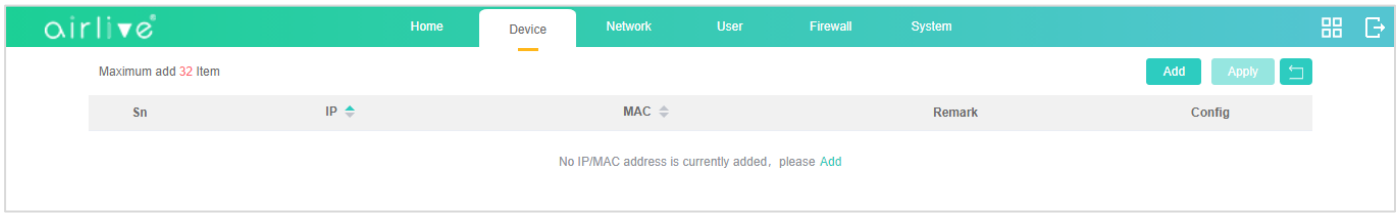
Object	Description
AC Enable	Enable or Disable the AC function of the Wireless Controller
DHCP Enable	Enable or Disable the DHCP
Server IP Address	IP Range for the Connected Access Points
Address Count	Number Addresses given
Lease Time	IP Address Lease Time
Allocated IP	Number of IP Addresses in use

4.6.1 Device – Service – IP List

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

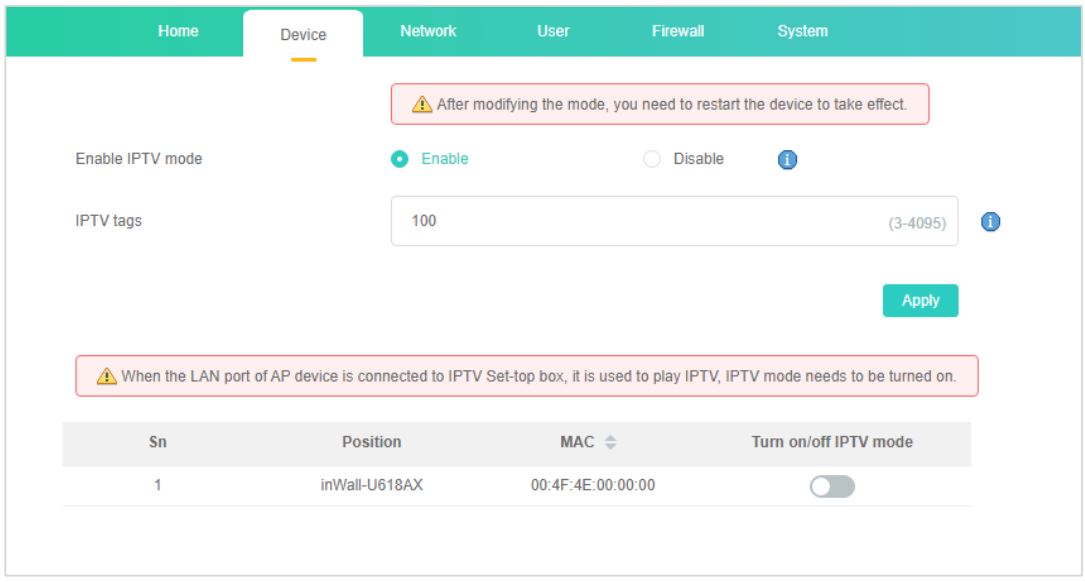
4.6.2 Device – Service – Static Binding

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.



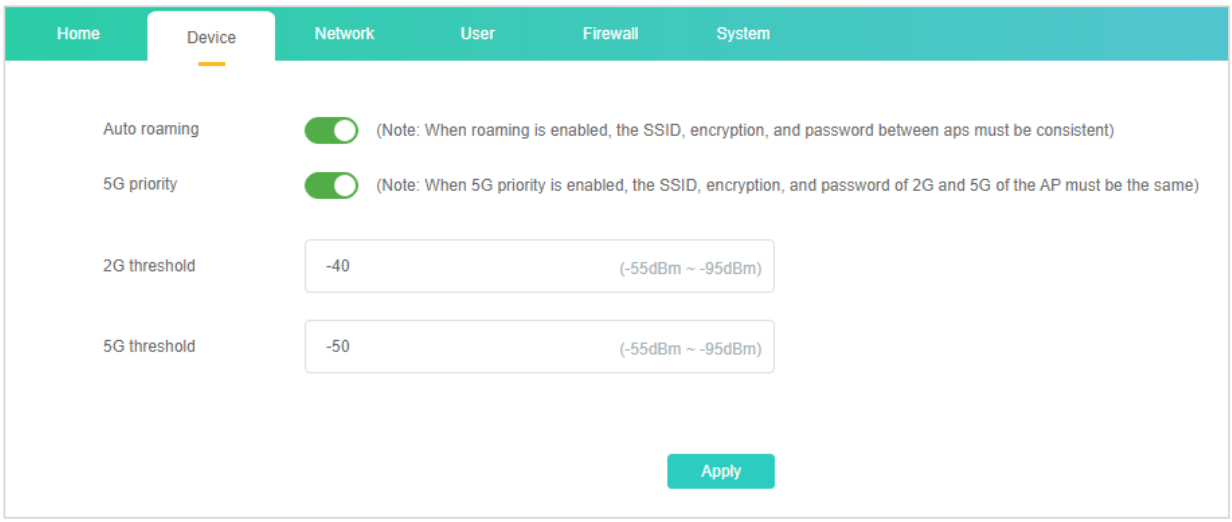
4.7 Device – IPTV Settings

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.



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.

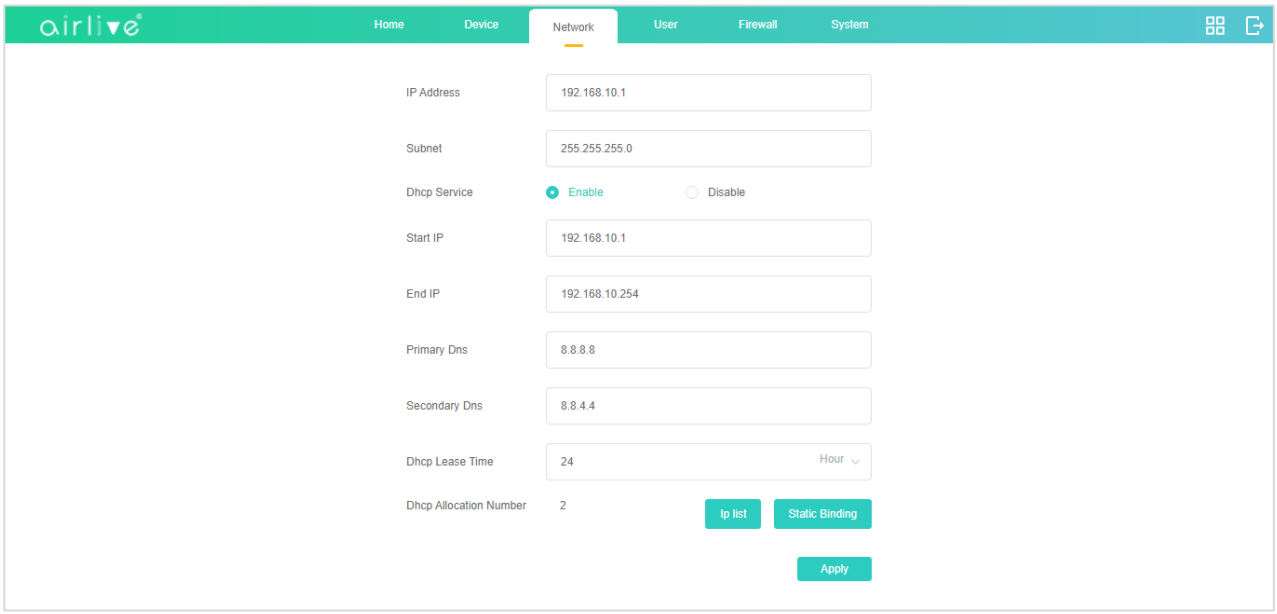


4.9 Network

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”

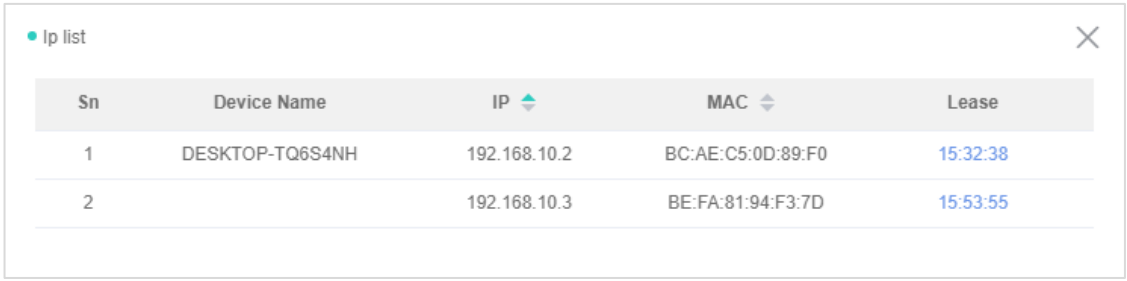


The page includes the following fields:

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

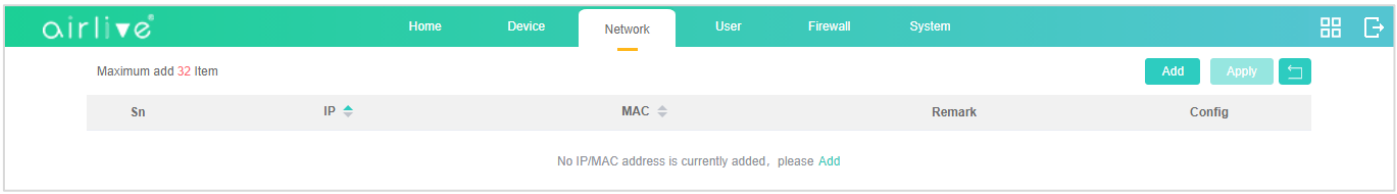
4.9.2 Network – LAN Setting – IP List

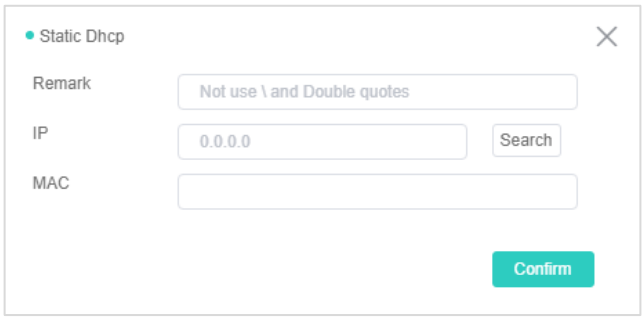
IP List shows the current connected Access Points to the Wireless Controller.



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.



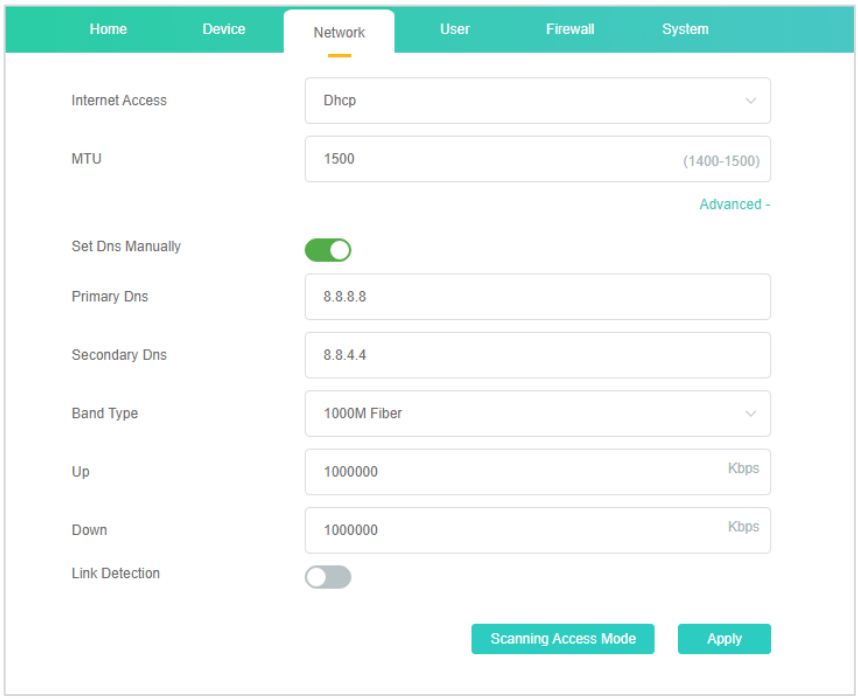


4.9.4 Network – WAN Setting

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.

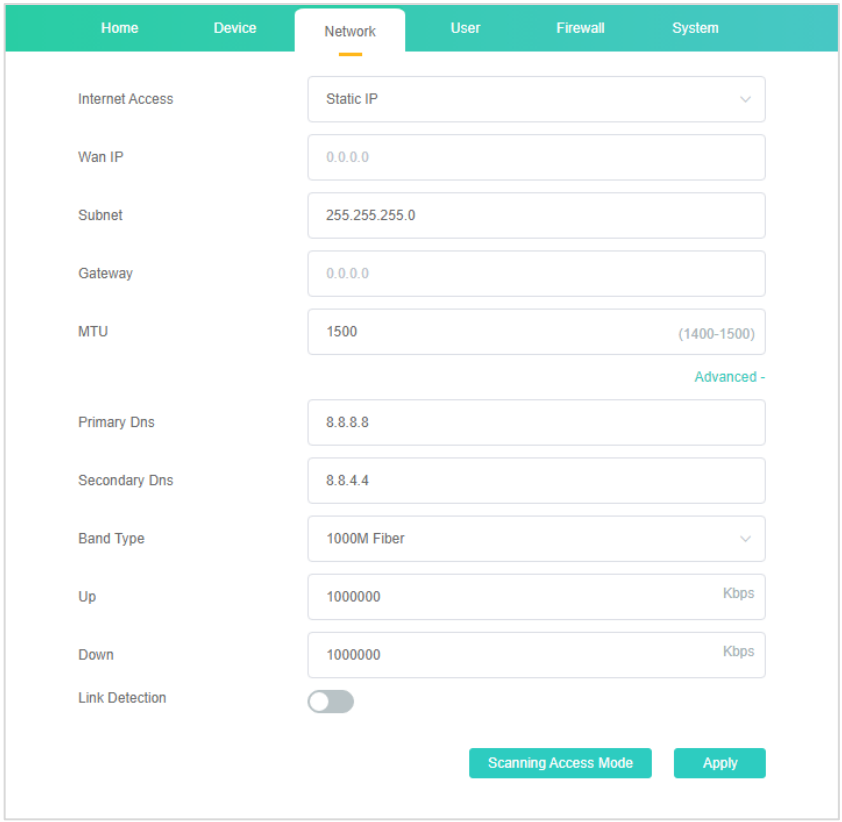


The page includes the following fields:

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.

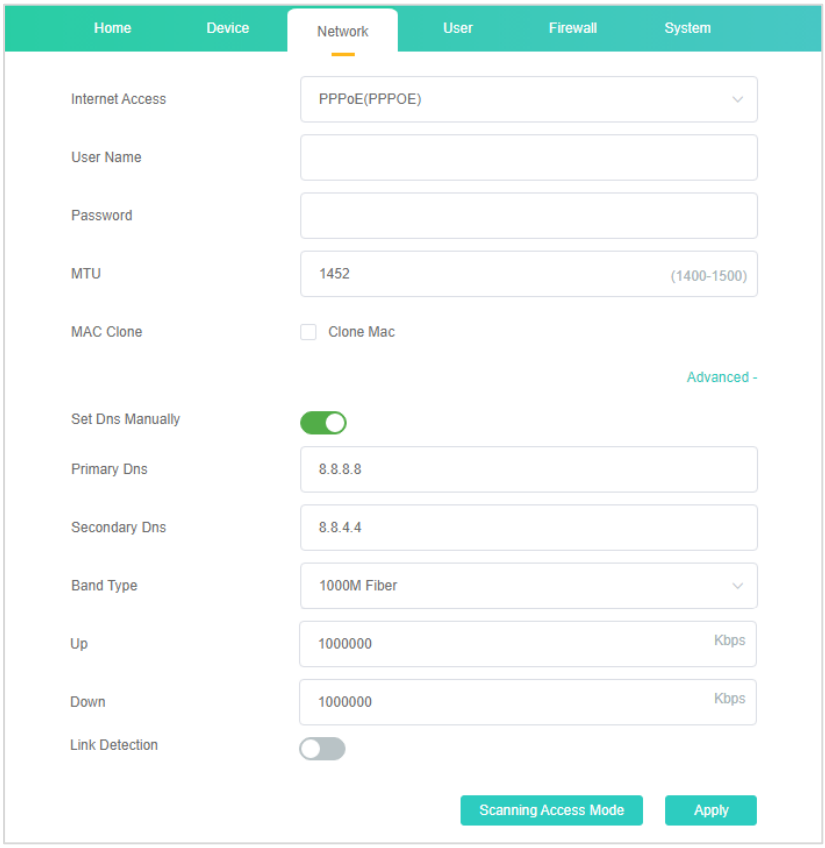


The page includes the following fields:

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.

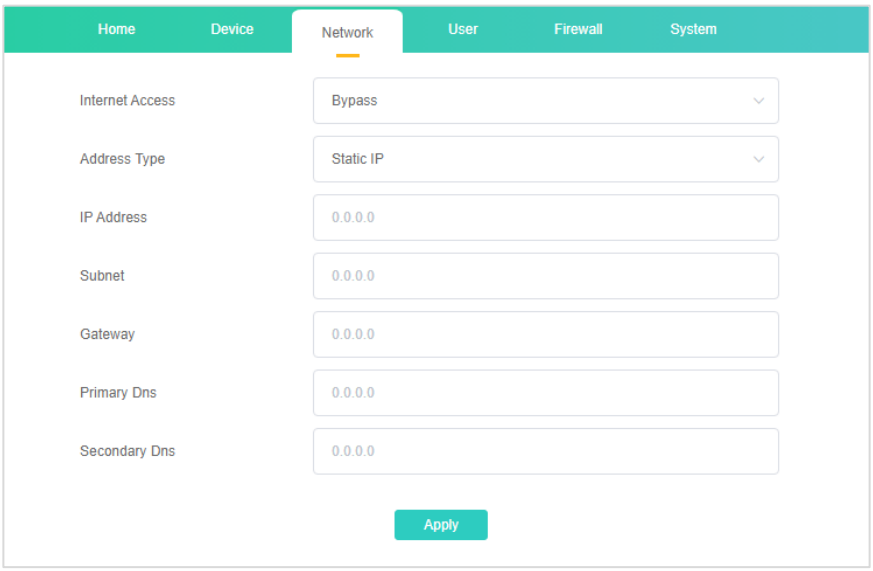


The page includes the following fields:

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.

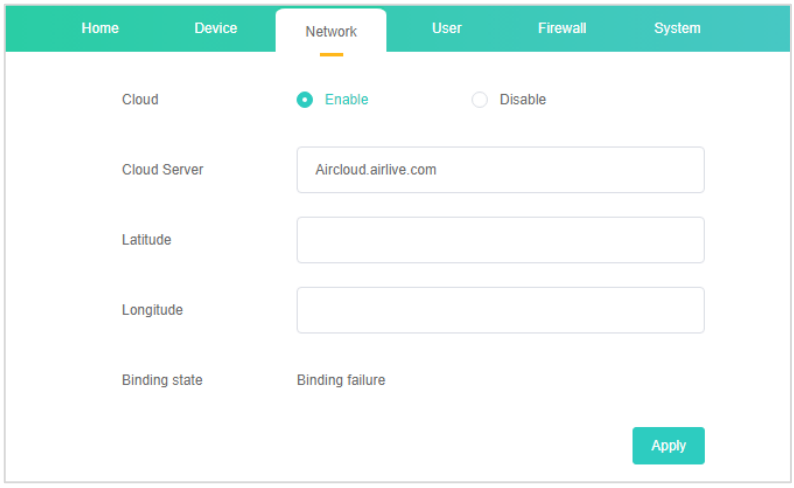


The page includes the following fields:

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.

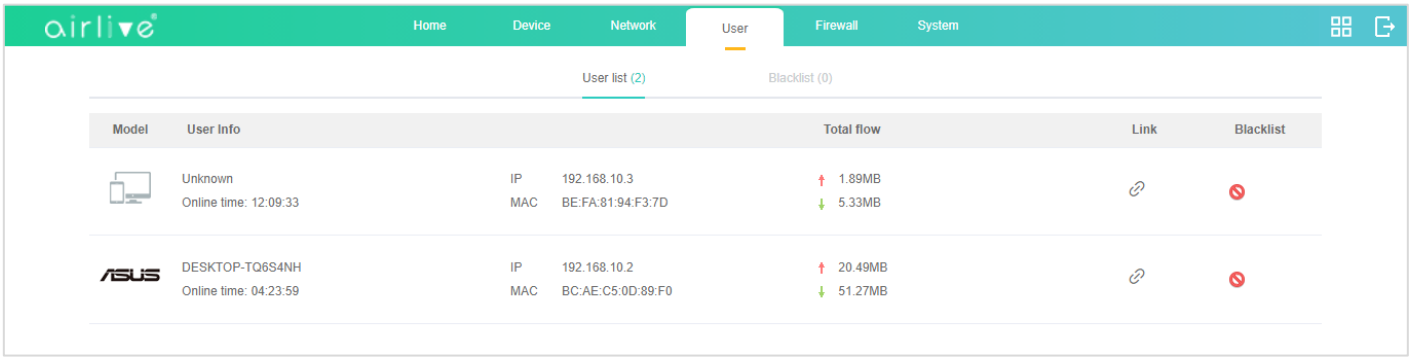


4.10 User

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

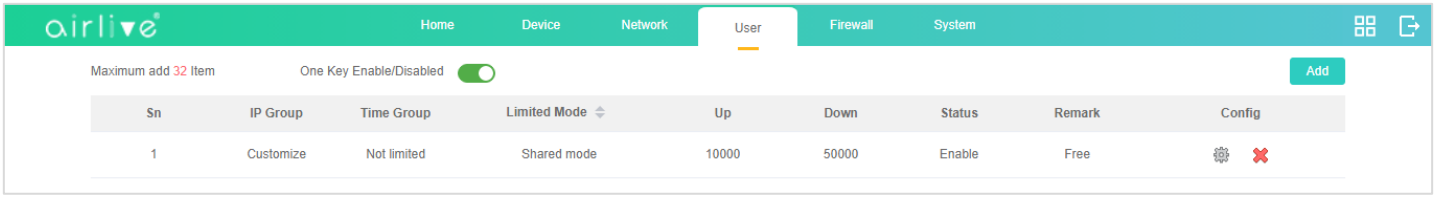
UserList shows the clients which are connected to the Access Points and their Total Flow information. Click on the Link icon to see more detailed information. To Blacklist a client, click on the Blacklist icon. To see all Blacklisted clients, click on Blacklist in the top bar.

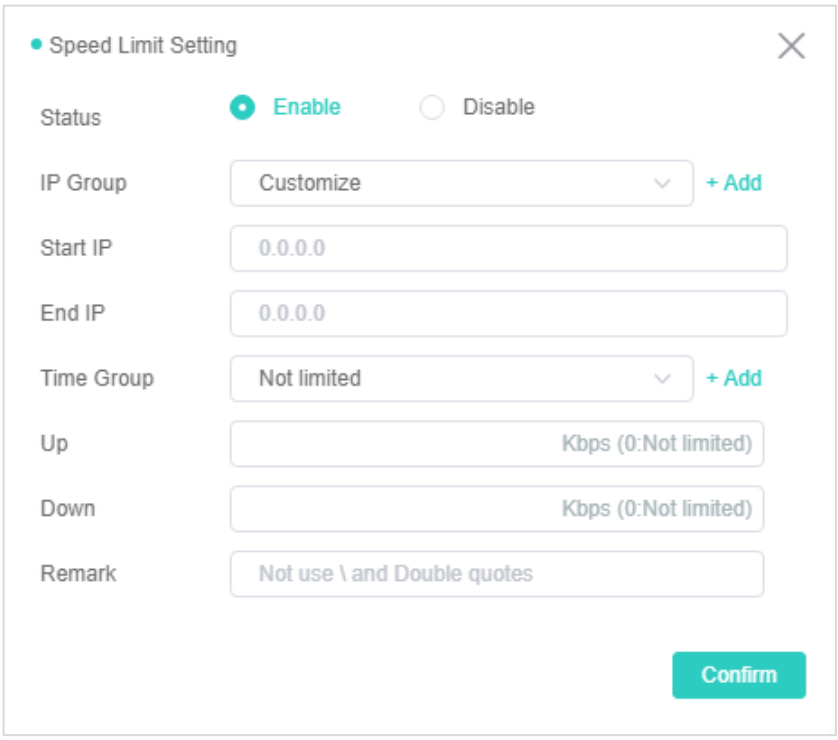


4.10.2 User – Speed Limit

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.





The page includes the following fields:

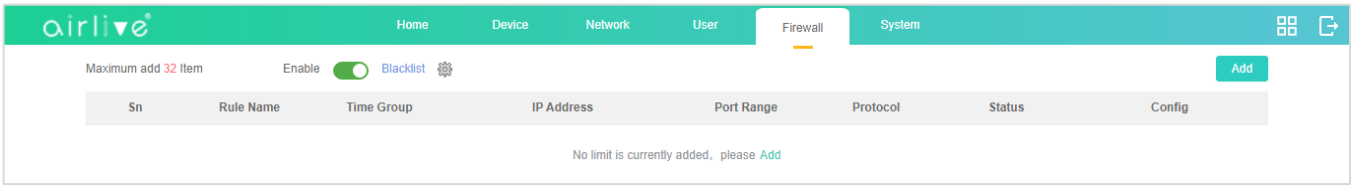
Object	Description
Status	Select enable or disable Speed Limit rule
IP Group	Select Custom or Add an IP group
Start IP	Enter a Start IP Address for the range
End IP	Enter an End IP Address for the range
Time Group	Select any or Custom or Add a Time group
Up	Enter the upstream limited for kbps
Down	Enter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

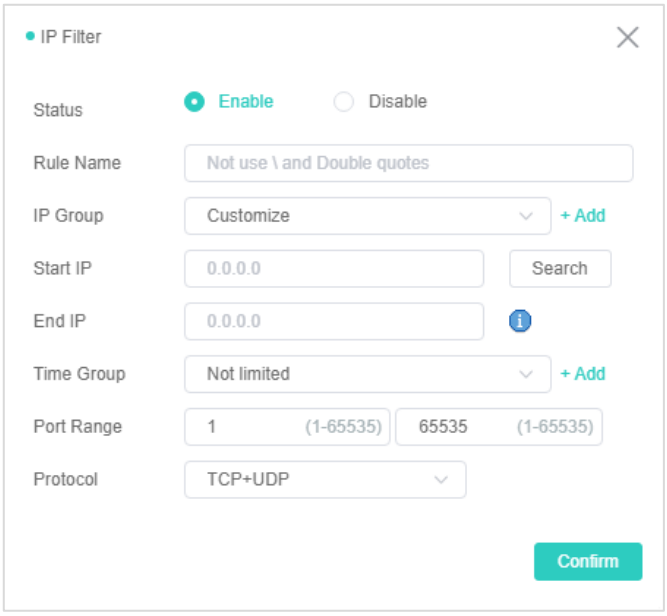
4.11 Firewall

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.



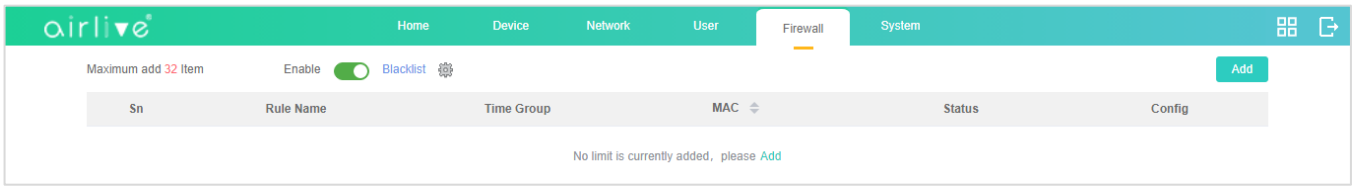


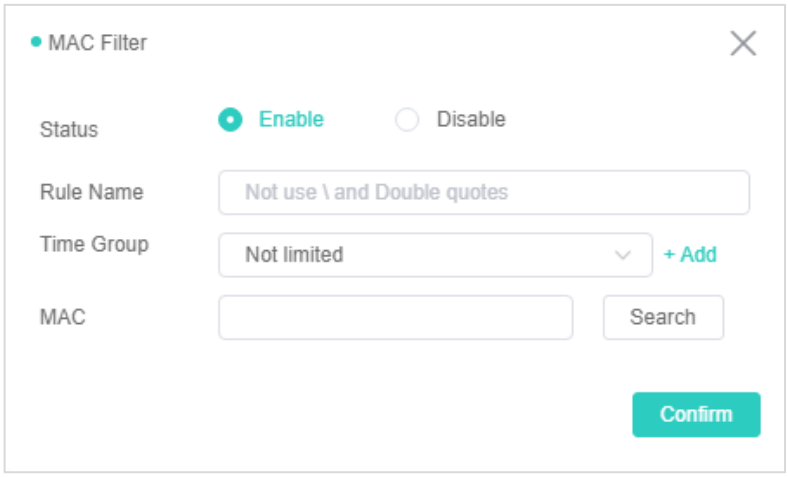
The page includes the following fields:

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.



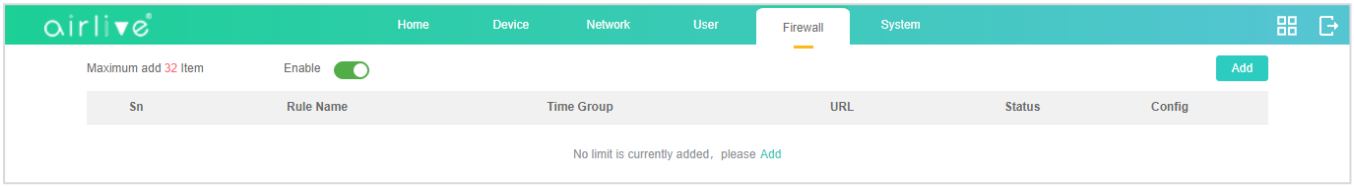


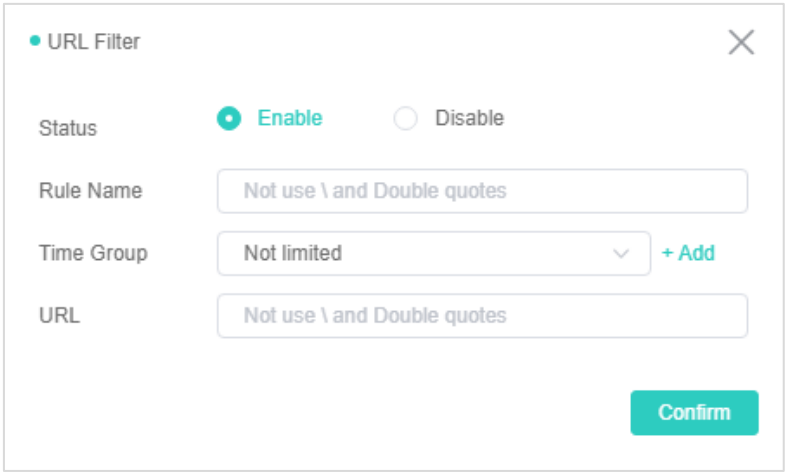
The page includes the following fields:

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.





The page includes the following fields:

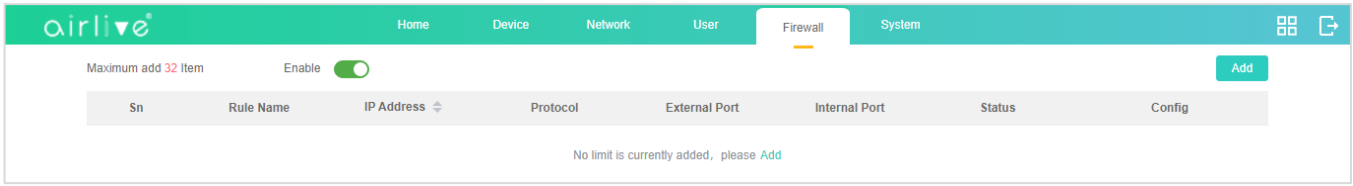
Object	Description
Status	Select ON (Green) or OFF (Gray) to enable or disable
Rule Name	Enter the rule name, e.g. Black list
Time Group	Select to Customize or Add a Time Group and setup time range and work data.
URL	Enter the URL that you need to put in black list
Confirm	Press Save to save the settings

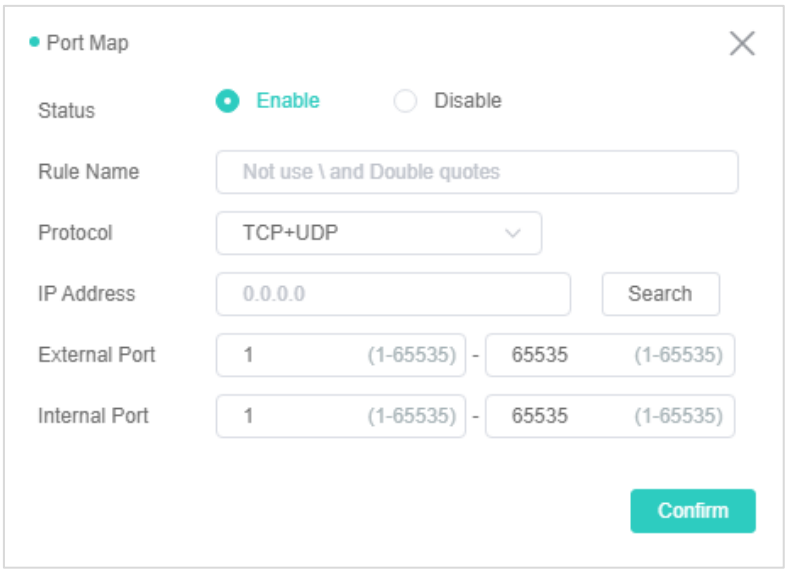
4.11.4 Firewall Port Map

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.



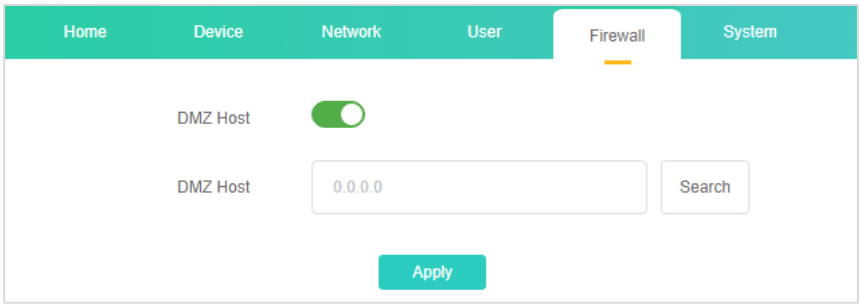


The page includes the following fields:

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.



The page includes the following fields:

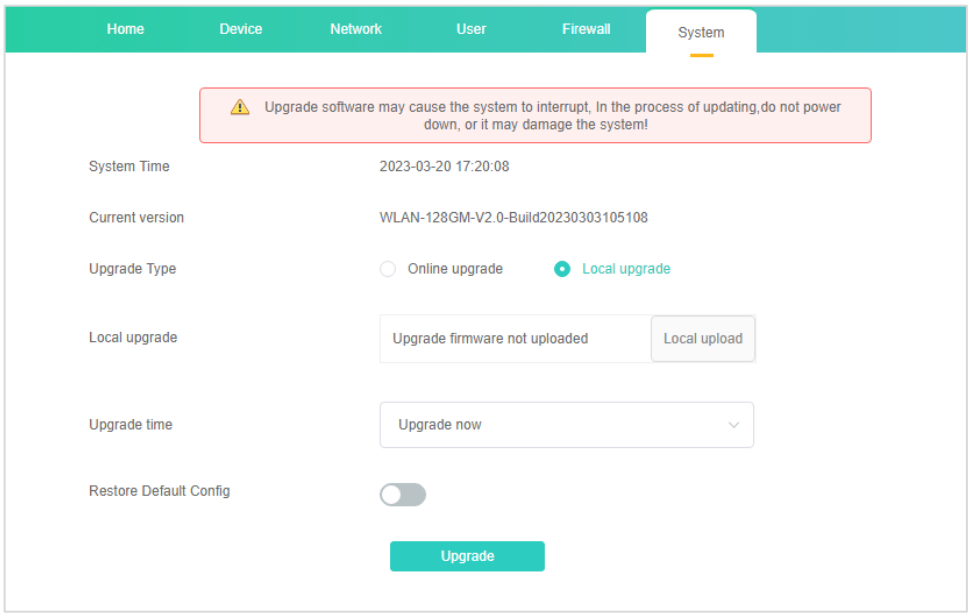
Object	Description
Enable DMZ	Select Enable DMZ Host or Disable
DMZ Host IP	Enter the DMZ LAN IP for which you would like to open DMZ
Apply	Save the setting.

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.



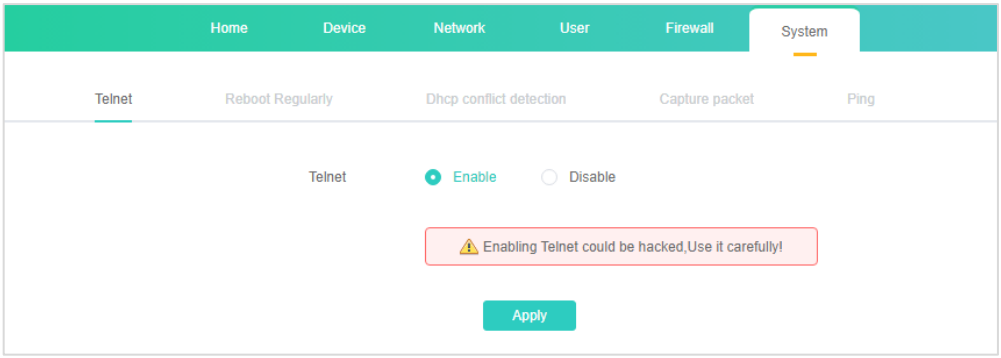
The page includes the following fields:

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!!

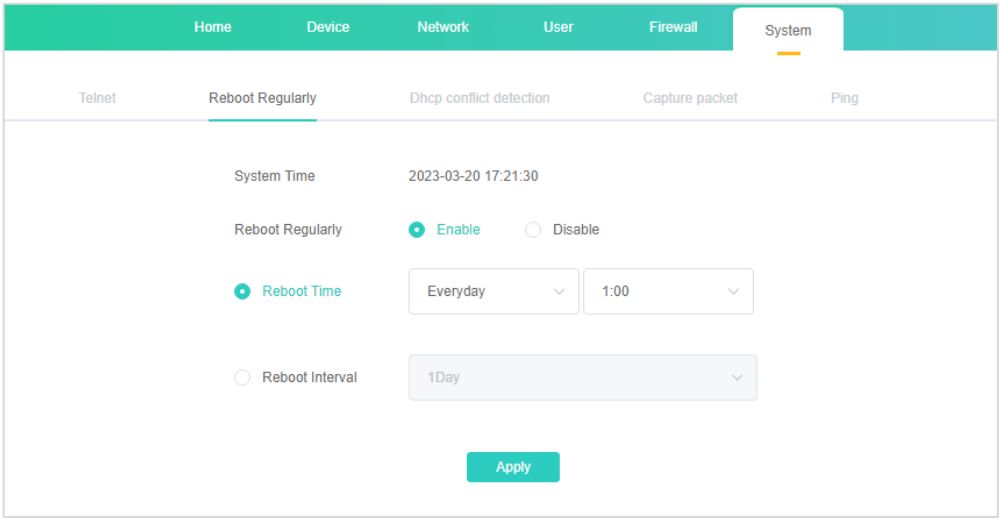
4.12.2 System – Maintain - Telnet

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.



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.

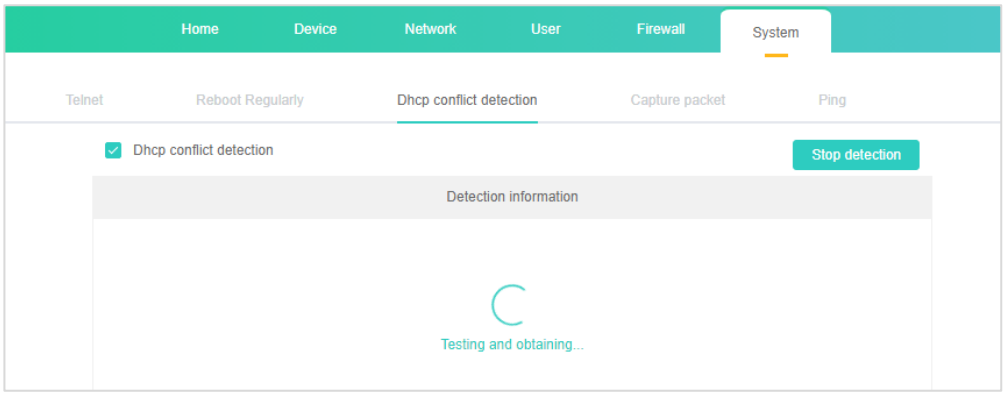


The page includes the following fields:

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

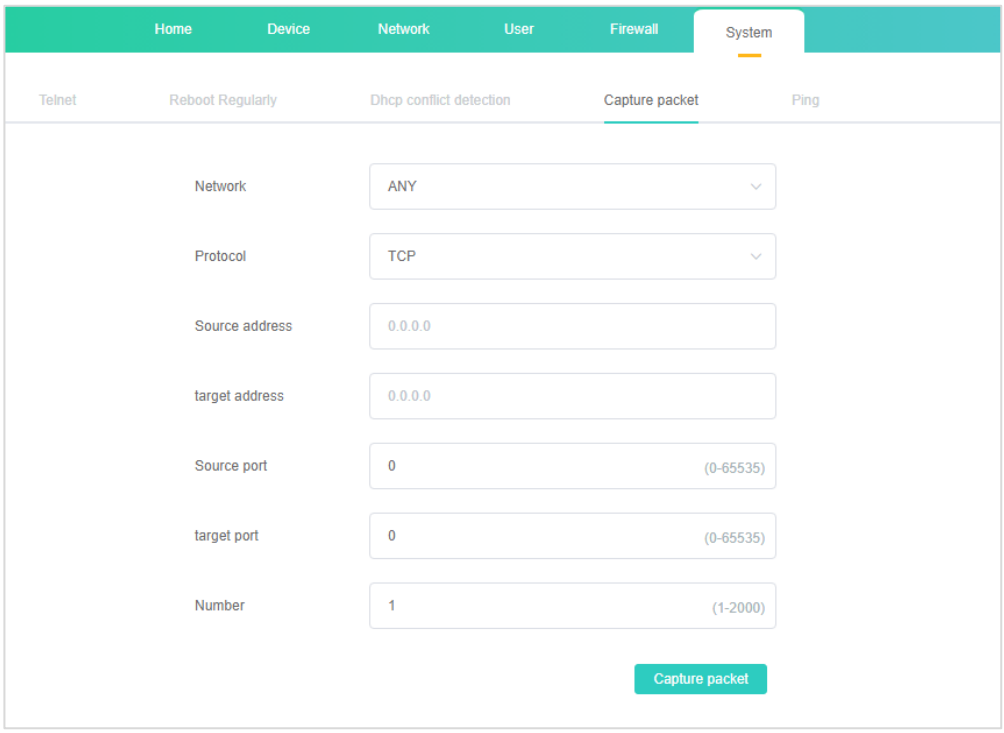
4.12.4 System – Maintain – DHCP Conflict Detection

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



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..

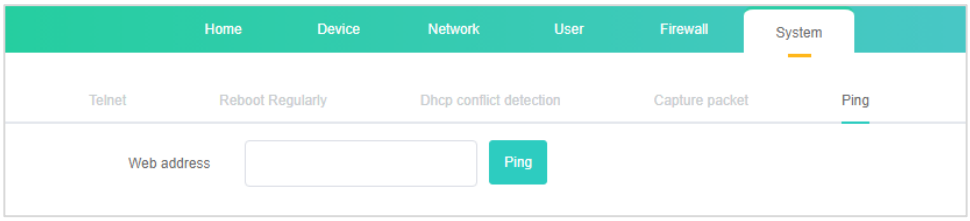


The page includes the following fields:

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

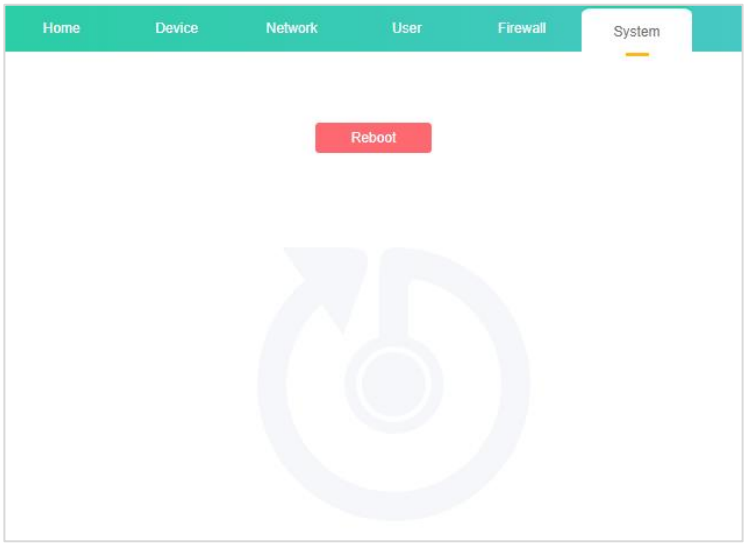
4.12.6 System – Maintain - Ping

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



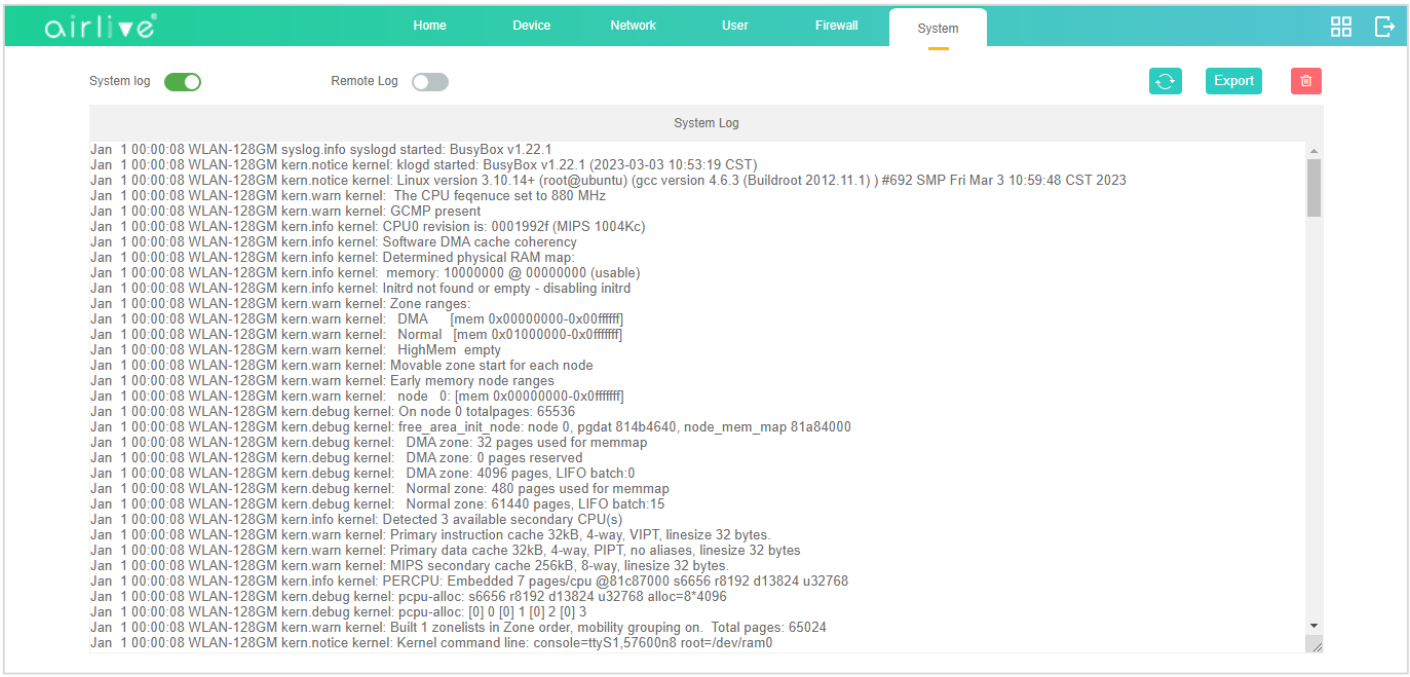
4.12.7 System – Reboot

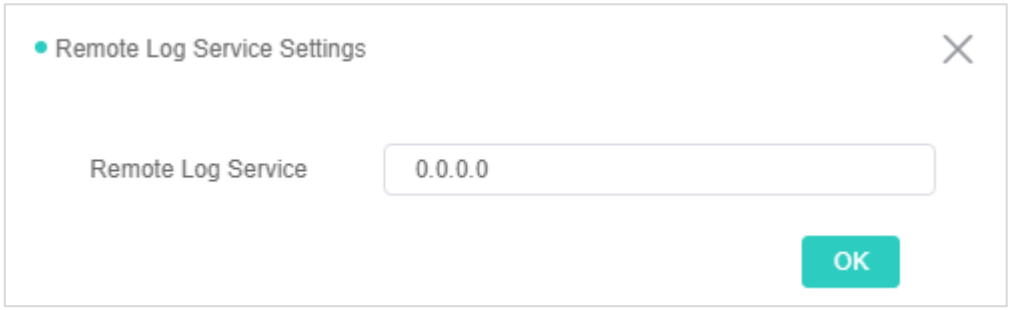
Enable Reboot to Reboot the Wireless Controller directly.



4.12.8 System – System Log

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



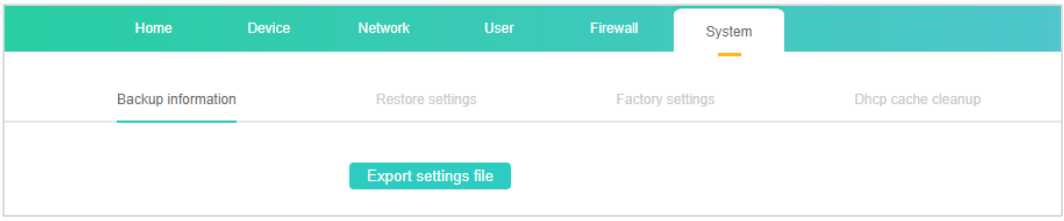


The page includes the following fields:

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

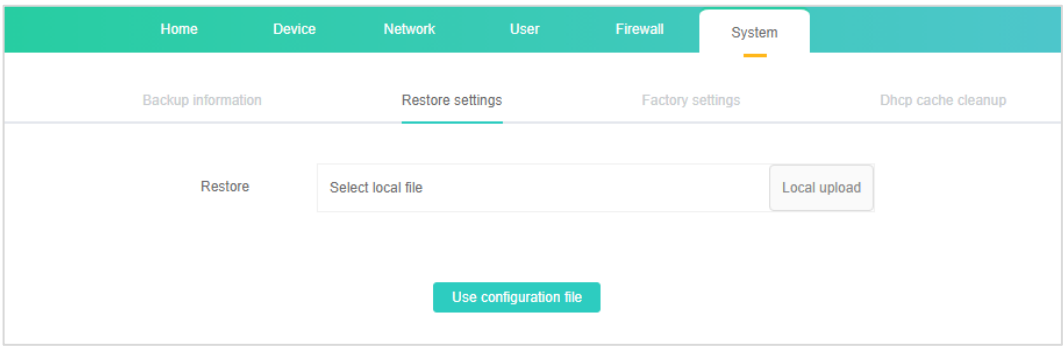
4.12.9 System – Manage – Backup Information

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



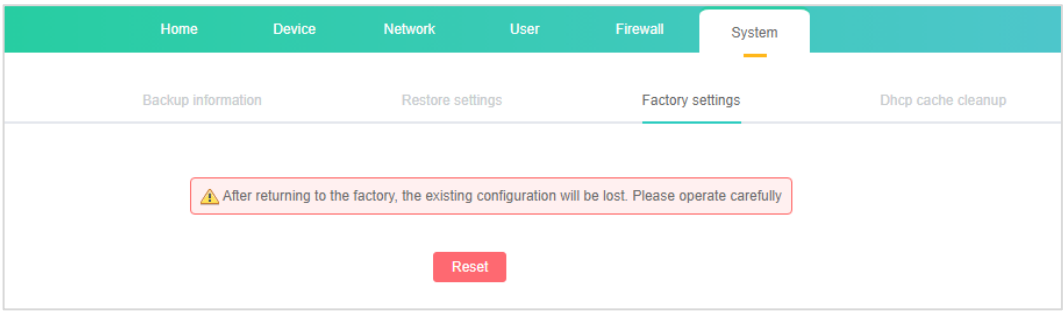
4.12.10 System – Manage – Restore Settings

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!!



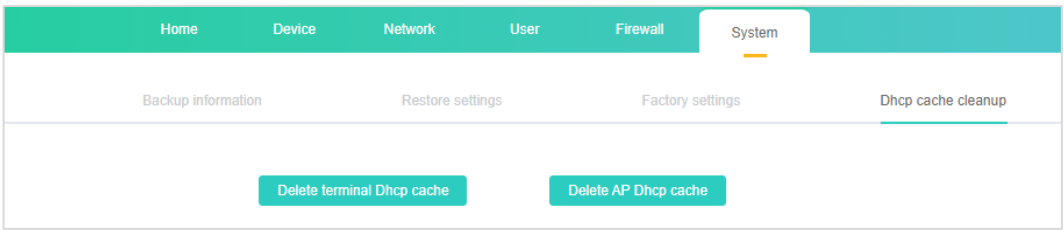
4.12.11 System – Manage – Factory Settings

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



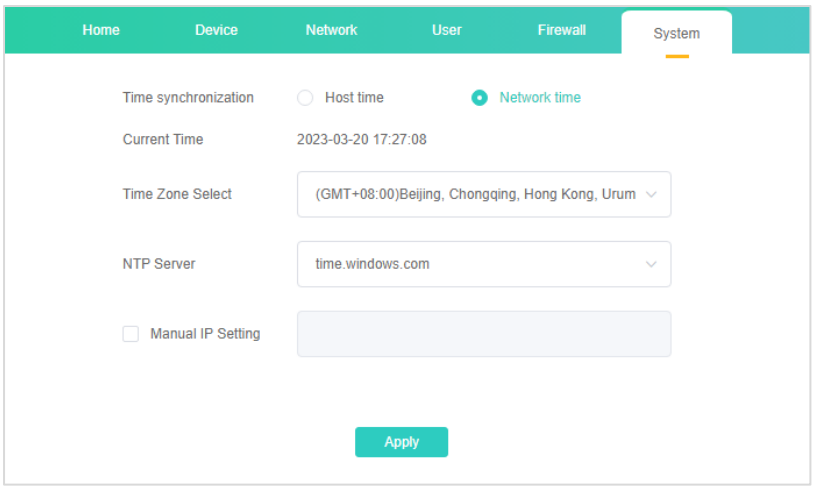
4.12.12 System – Manage – DHCP Cache Cleanup

Delete the Terminal and AP Cache from the Wireless Controller.



4.12.13 System – System Time

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



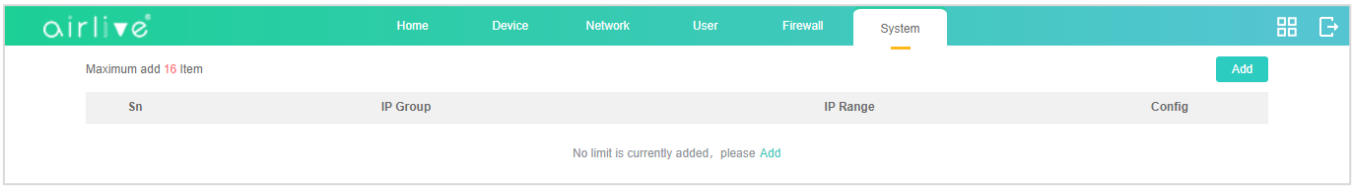
The page includes the following fields:

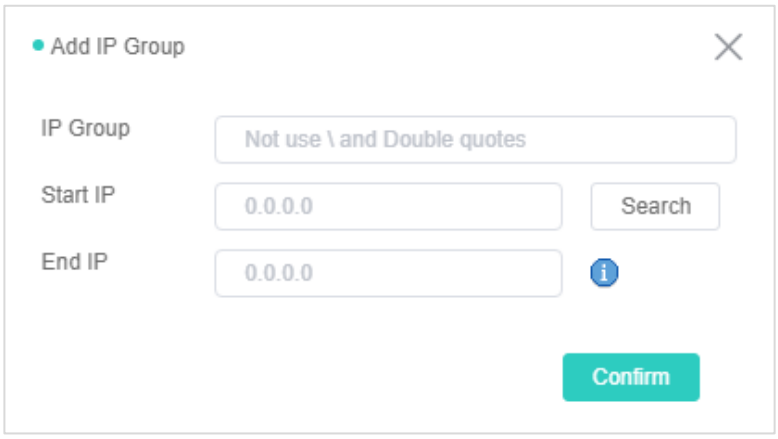
Object	Description
Time Synchronization	Select either Host Time or Network Time
Current Time	Show system time of the Wireless Controller
Time Zone Select	Select Time Zone
NTP Server	Select NTP server
Manual IP Setting	Enter manual IP for NTP server

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.



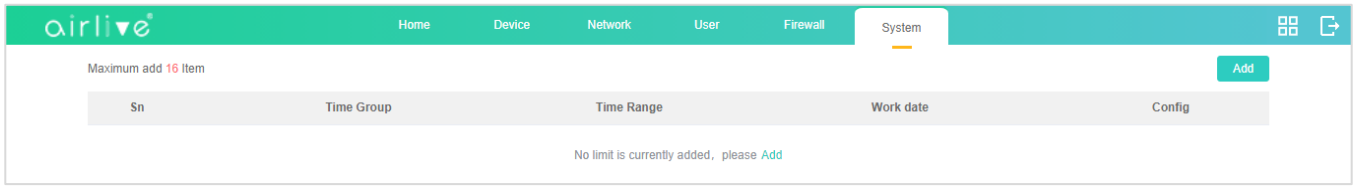


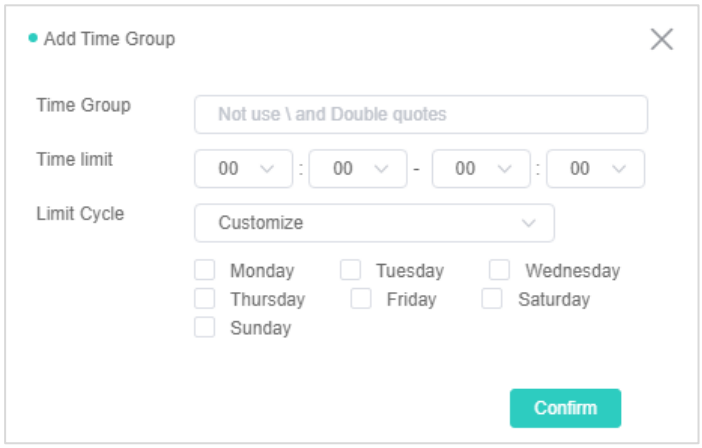
The page includes the following fields:

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.





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.