EKSELANS BY ITS

USER MANUAL

CAP 2

335002

Controller for access points

V03

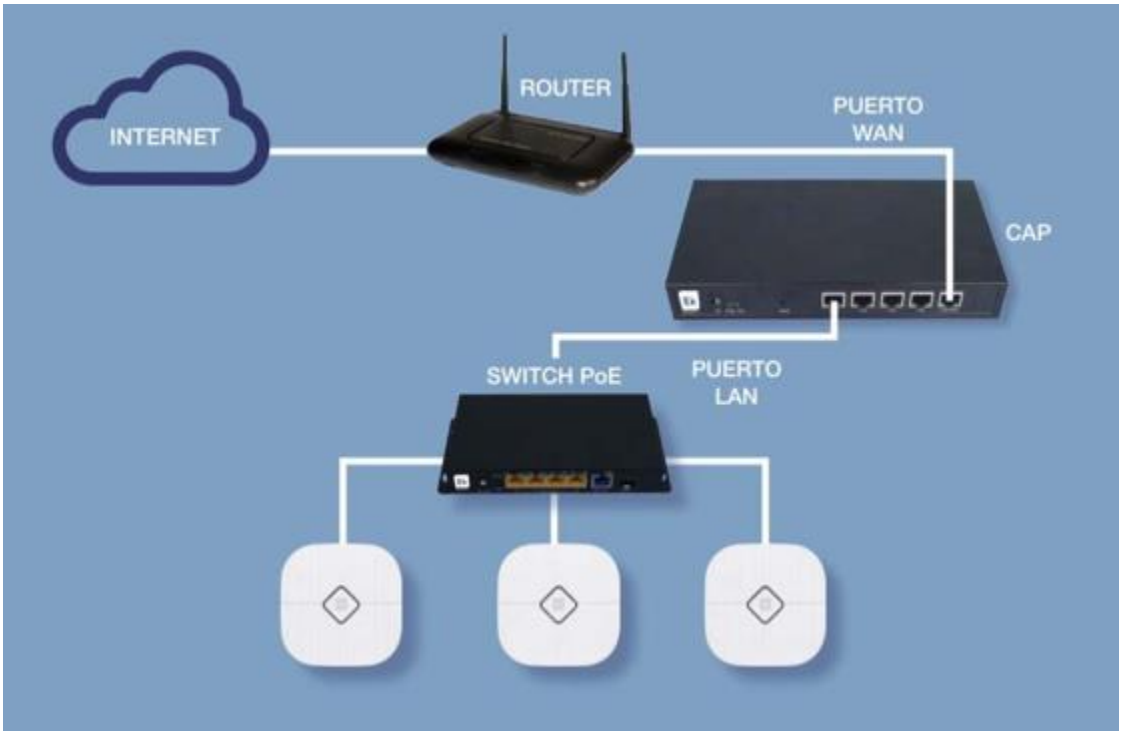
ITS Partner O.B.S S.L · Av. Cerdanyola 79-81 Local C
08172 Sant Cugat del Vallés · Barcelona (Spain)
Phone: +34935839543 · info@ek.plus · www.ek.plus

TABLE OF CONTENTS

Hardware

- RESET: Reset button. Press for 15 seconds for the device to restore to factory settings.
- WAN: WAN port. Connect to the internet provider's router.
- LAN: LAN port.
- DC: DC power supply.

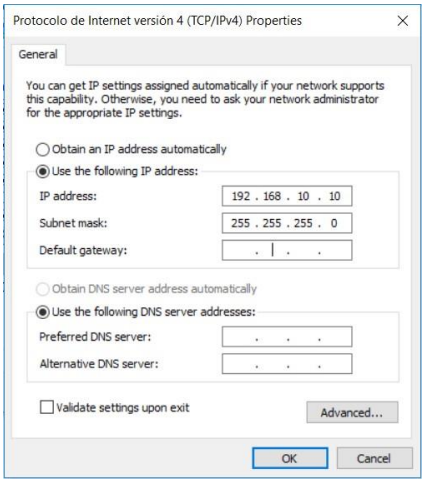
Example of installation diagram



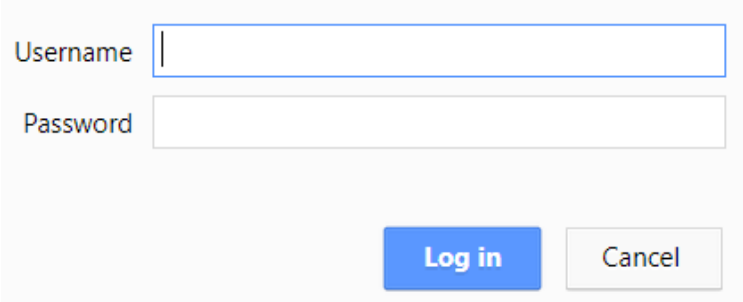
Access to CAP 2

To access the **CAP 2** follow the next steps:

1. Connect to **CAP 2** with a network cable or wireless configuration.
2. Connect to **CAP 2** with a network cable or wireless configuration (with an AP), **you always must be connected to its LAN port**. Configure your PC's network adapter with a static IP. In order to make the configuration easy, EK have the application **Ek NET Adapter,** you will be able to configure the network adapter easily. You can download from https://ek.plus/software/ you will find a new section "EK NET ADAPTER".



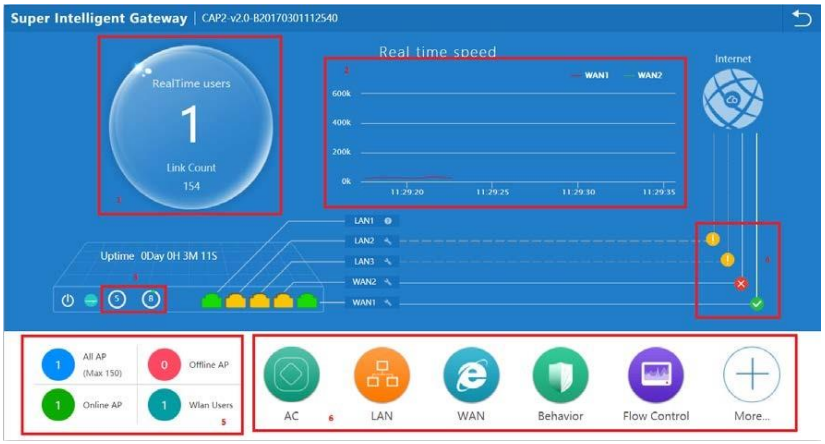
3. Open a web browser and go to the URL: http://192.168.10.1



4. Enter the user and password: **admin** / **admin**

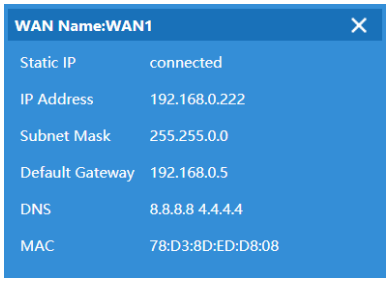
CAP 2 web interface

Once the password is entered, the following window will appear.



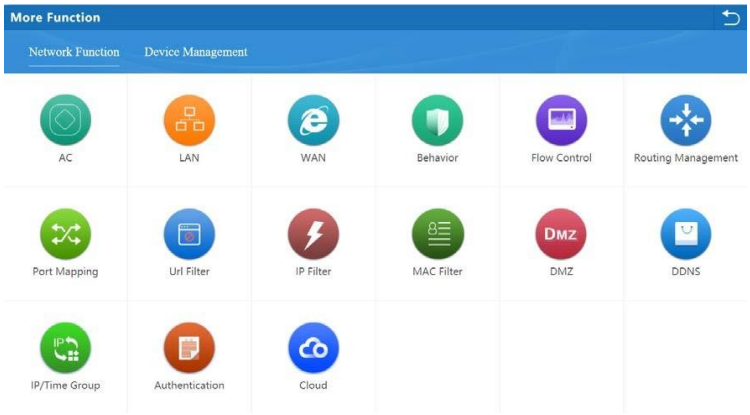
Then, it shows to us the next areas:

1. Shows the number of connected clients.
2. Displays the real-time bandwidth of each WAN network (provider).
3. Displays RAM and CPU usage information.
4. When clicked, it allows you to view the information of the selected WAN:



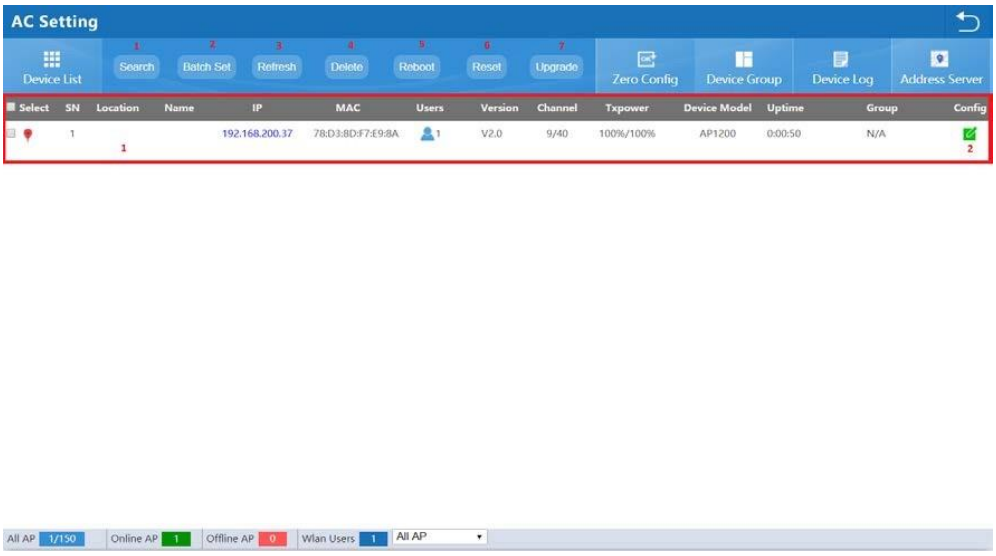
5. Displays relevant information about the number and status of Aps.
6. Menu

Network Function



AC Setting

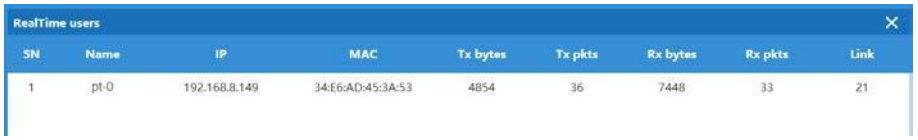
This section shows all the APs connected to the controller **CAP 2**.



1. Displays information regarding APs:

   - **SN:** ID assigned to the AP by CAP **2**.
   - **Location:** Location of the AP identified by the customer.
   - **Name:** AP name.
   - **IP:** IP assigned to the AP by **CAP 2**. If we connect to the NETWORK with the RANGE indicated on this IP, we will be able to access the WEB interface of the AP directly.

- **Users:** User number connected to the AP. Clicking will open a new window giving information about connected customers.

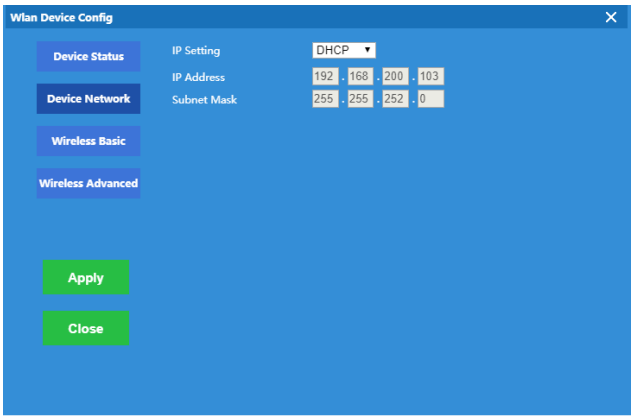


- **Channel:** Channel over which the AP is transmitting the SSID of the AP (2.4Ghz / 5.8Ghz according to model).
- **Tx power**: 2.4Ghz / 5.8Ghz frequency output power.
- **Online Time:** Shows how long the AP takes on.
- **Group:** Displays the name of the group to which the AP is assigned.

After pressing the CONFIG button of the desired AP, open a new window to configure the AP in question:

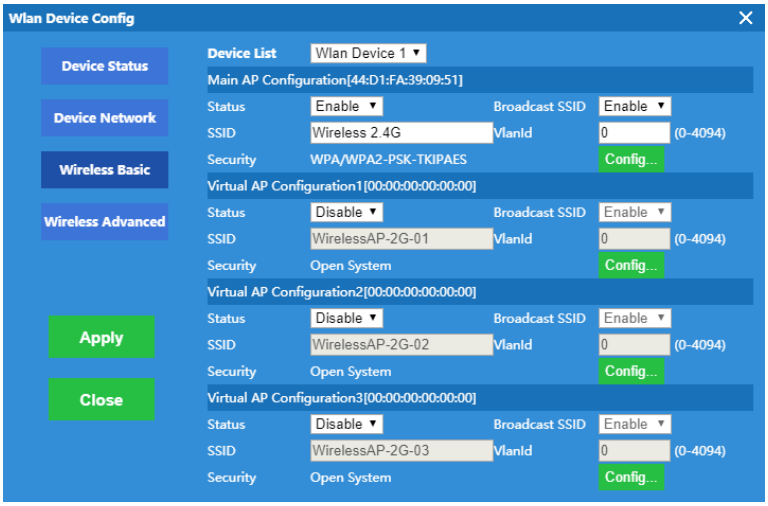
"Device Status" shows us relevant information about the AP:

- **Model:** Product name.
- **Online Time:** Shows how long the AP takes on.
- **MAC Device:** Displays MAC.
- **IP device:** IP assigned to the AP by CAP 1. If we connect to the NETWORK with the RANGE indicated on this IP, we will be able to access the WEB interface of the AP directly.
- **Software:** Displays the software version that the AP is currently using.
- **AC IP: CAP** 2 IP.
- **SSID:** SSID names.
- **BSSID:** Displays the MACs assigned to the different SSIDs.
- **Channel:** Channel on which the AP is transmitting the SSID of the 2.4Ghz / 5.8Ghz AP
- **Security:** Displays selected security for SSIDs.
- **RF Output Power:** Shows the emission power of the AP.
- **Beacon Interval:** Displays the selected "beacon interval" value.
- **Coverage Threshold**: Shows us the selected "threshold"



"Device Network " allows you to configure how the AP obtains IP:

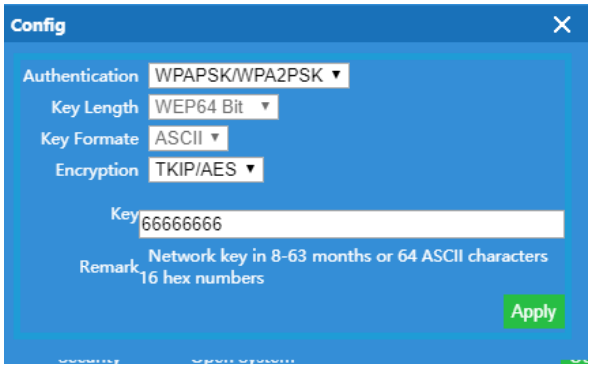
- DHCP: Gets the DHCP IP automatically from CAP 2.
- Static IP: Allows you to manually assign the desired IP to the AP.



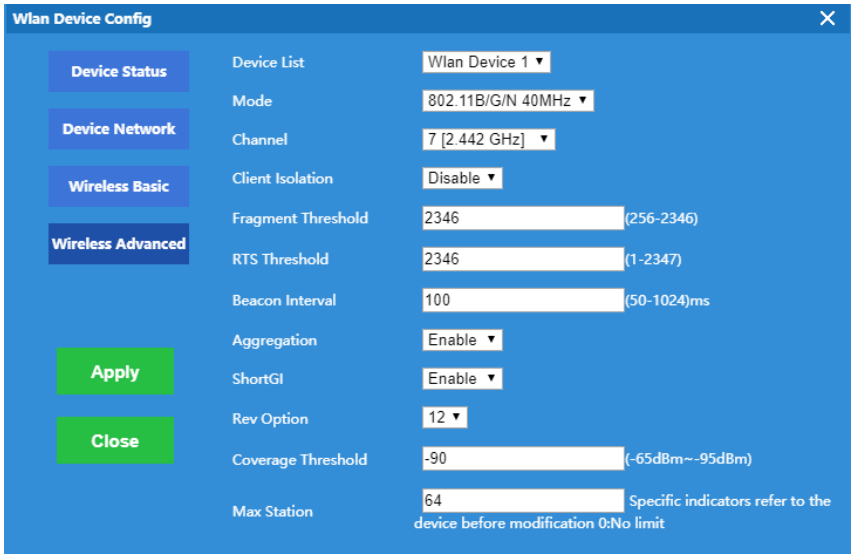
The "Wireless Basic" menu allows you to configure the basic options:

- Device list: If the AP has only a 2.4 or 5.8 broadcast band, it will correspond to WLAN 1, if on the contrary the AP has 2.4 and 5.8 the WLAN 1 will correspond to 2.4 GHz and WLAN 2 to 5.8 GHz.
- AP configuration: APs allow you to configure up to 4 SSIDs.
- Status: Enabled – Enables SSID, Disabled – Disables SSID.
- Broadcast SSID: Enabled - Emits SSID, Disabled – Hidden SSID,
- SSID: SSID Name.

- **Wireless Security:** Displays the assigned security. To see more details and configure it, click on the **"Config" button.** A new window will open to set up wireless security.



- **VLAN:** Allows you to assign a VLAN to the SSID.



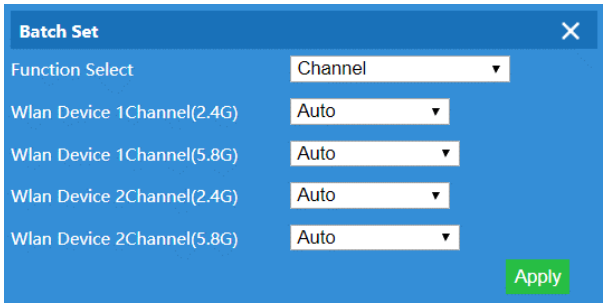
The **"Wireless Advanced"** menu shows more options for the most technical-level AP:

- **MODE:** Select the standard for wireless N/AC.
- **Channel:** Channel on which the AP is transmitting the SSID of the 2.4Ghz/ 5.8Ghz AP.
- **Client Isolation:** Enabled: Users are isolated and cannot be seen among themselves.
- **RTS Threshold:** Reduce this value if there are electromagnetic problems or traffic saturation in the network.

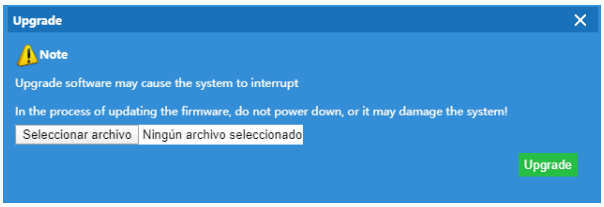
- **Beacon interval:** Interval for "beacon". The "beacon" is a packet that is sent to the client computer to notify if it is connected. If the time is reduced, more packets will be sent making the network slower. And if the value is too high, this will cause the equipment to disconnect more frequently.
- **Aggregation:** Allows for higher flow.
- **Short GI:** Improves flow rate. Use only for N mode and deactivate if mixed mode is used.
- **Coverage Threshold:** Indicates the maximum allowed power that the client can have to stay connected to the AP. Beyond this power the AP will disconnect the client.
- **MAX station:** Maximum number of clients that can be connected.

2. **Batch Set:** Selecting one or more APs and clicking on the Group function will open a new window. This feature allows one or more APs to configure a number of equal options:

    - Channels and Powers.
    - Time when APs reboot (watch dog).
    - Maximum users allowed when connecting.
    - Password.

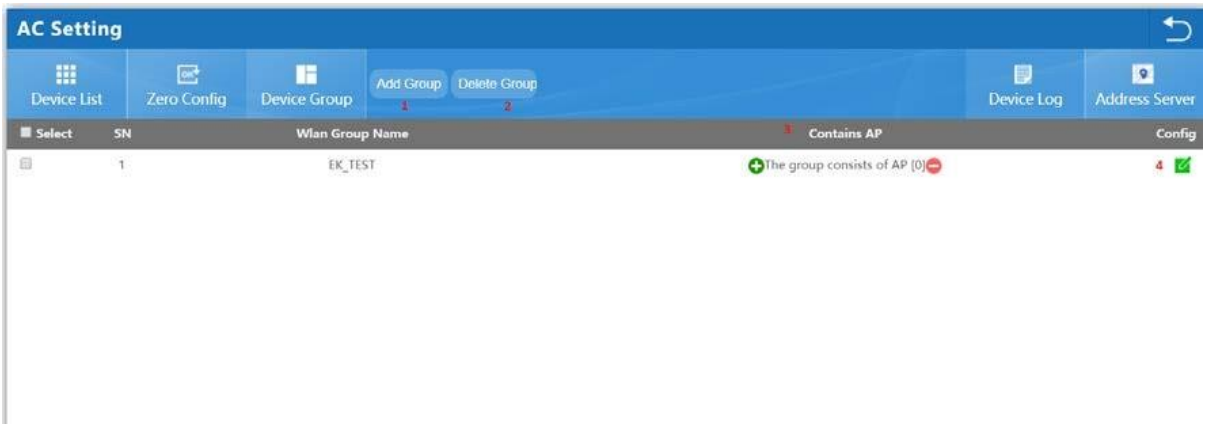


3. **Refresh:** Reapply the group configuration to the selected AP.
4. **Delete:** Remove ap from **CAP 2.**
5. **Reboot:** Restart the selected AP.
6. **Reset:** Empty the list.
7. **Reset:** Returns the selected AP to factory settings.
8. **Update:** Updates the firmware of the selected AP. Clicking opens a new window to select the firmware.

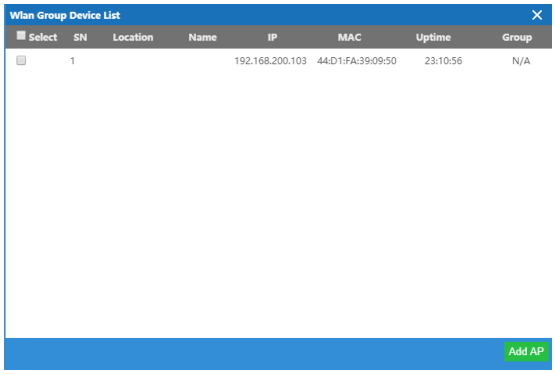


Device Group

This section lists all groups created in CAP 1. A group contains multiple APs that are set to the same setting.



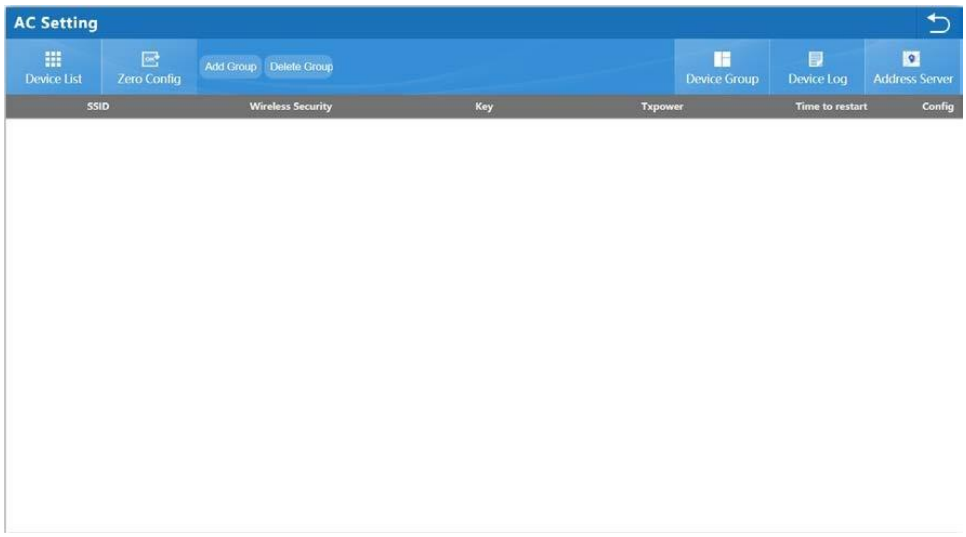
1. **Add Group:** Open the window to define the group settings. The form is the same as in point 2 of the "Equipment List" section.
   Note: Select a specific time of day when APs are restarted.
2. **Delete Group:** Deletes the group, but the configuration on the APs is still maintained.
3. **Contains AP:** Indicates the number of APs connected to the group. Pressing the + button displays a window with all the APs, allowing you to select the ones you want to add to the group.



4. **Config:** By clicking on the edit button in the corresponding group, you can carry out the configuration for the APs.

Zero config

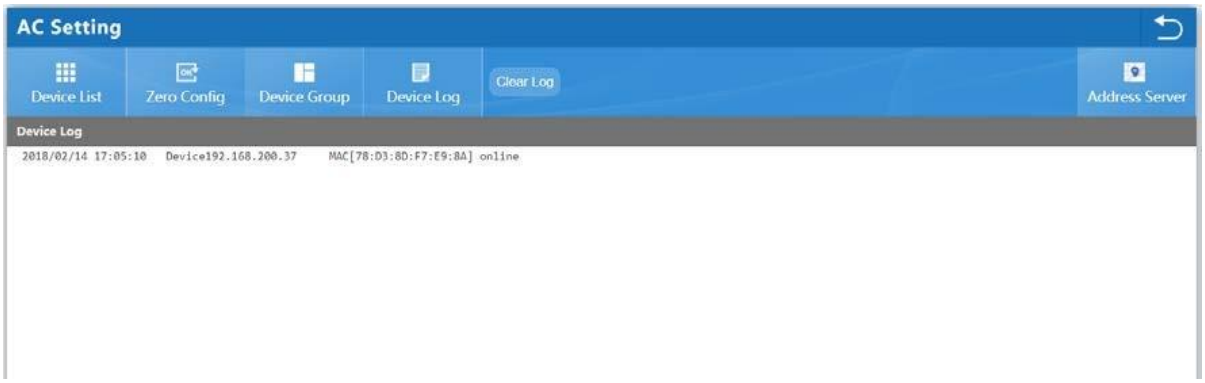
This function allows, before connecting any APs to **CAP 2** create a default configuration. There can only be one Zero configuration and once all the APs that are connected to **CAP 2** are created, they will be taking this default setting.



1. **Add Group:** Opens the window so that you can create the settings that will be used by the default APs. The form is the same as in **point 2 of the Teams List section**.
   Note: Allows you to select a certain time of the day when you want APs to be restarted.
2. **Delete Group:** Removes the default settings, but the settings on the APs are still maintained.
3. **Config:** By clicking on the edit button, you can create the default settings.

Device Logs

This section shows the activity event log for access points.



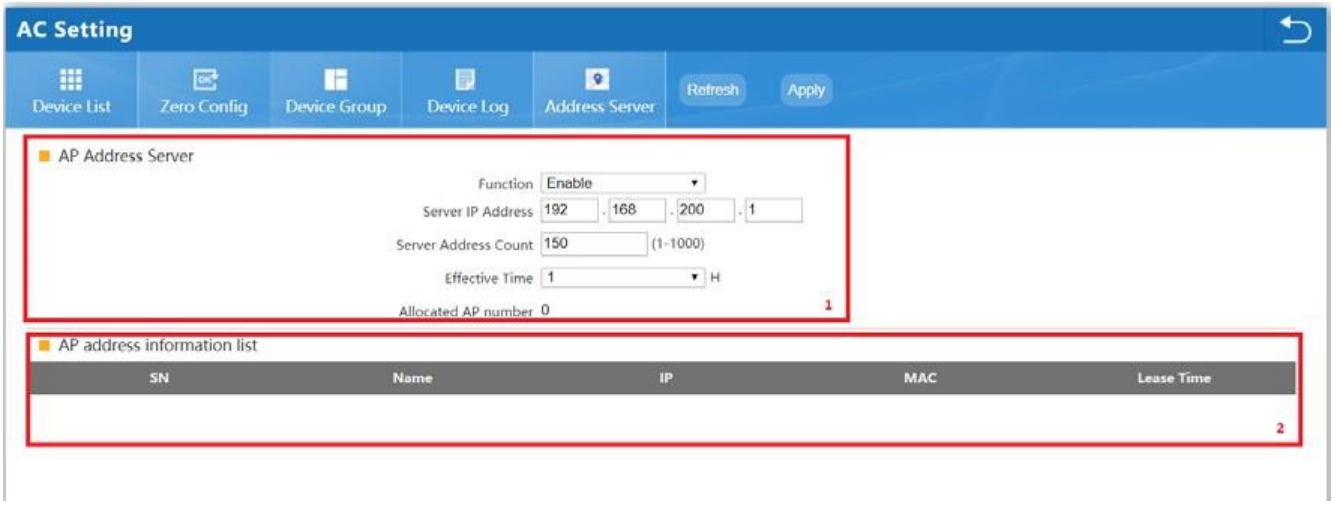
Date, computer ID and MAC are displayed for each event that is happening:

- On/ Off
- Deploying and configuring APs.
- Errors

The **"ClearLog"** button empty's the list of records.

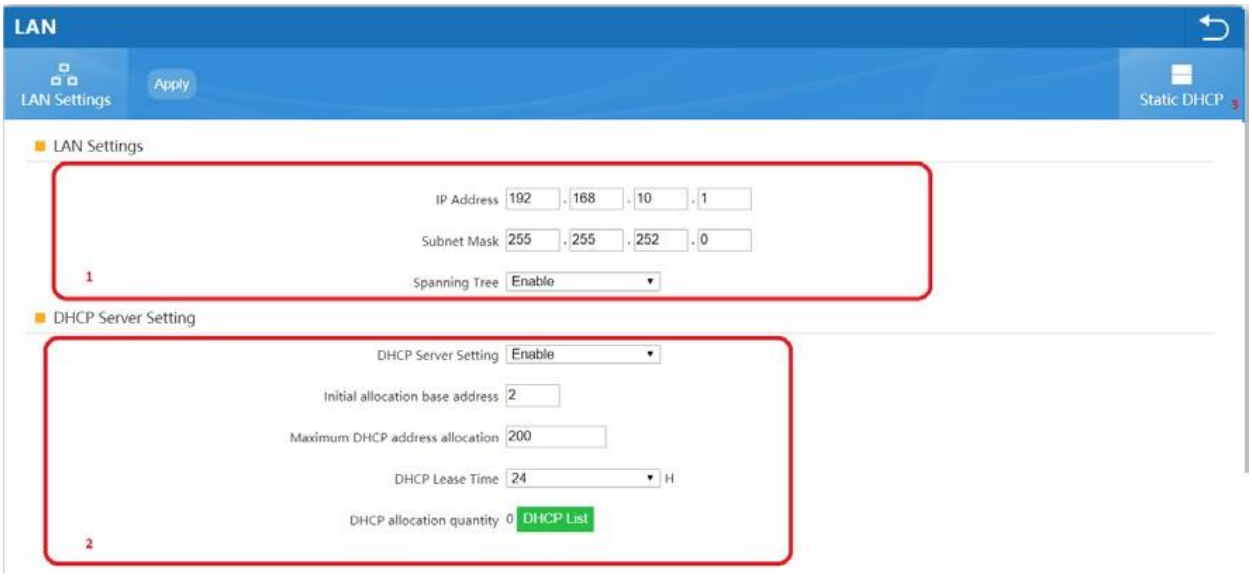
Address Server

This section configures DHCP that will assign IPs to different APs that connect to **CAP 2.**



1. **Server IP Address:** It shows the initial IP for DHCP as well as the IP that will link between the APs and **CAP 2** (IP Server is a second IP for CAP **2** in the range that the APs will be). The number of IPs that you can assign.
2. **Server Address Count** Displays the AP model, its assigned IP address, and its corresponding MAC. The remaining time for the IP to be updated is also shown.
3. **Refresh:** Refresh the page.
4. **Apply:** Apply the changes made.

LAN



1. **LAN Settings**: Configure the IP and subnet mask of **CAP 2.**
2. **DHCP Server Setting**: Turns DHCP on or off. Configure DHCP Initial IP and End IP.
3. **Static DHCP**: Allows you to assign fixed IPs to a MAC. This way the MAC will always have the same IP, which is ideal to be able to apply QoS.

WAN

WAN Setting

The CAP 2 allows you to change 3 of your LAN ports and enable them as WAN ports. In this way it is possible to have up to 4 WAN connections, 1 per ISP.

Clicking on the "Config" button on each WAN will open a sale to be able to configure:

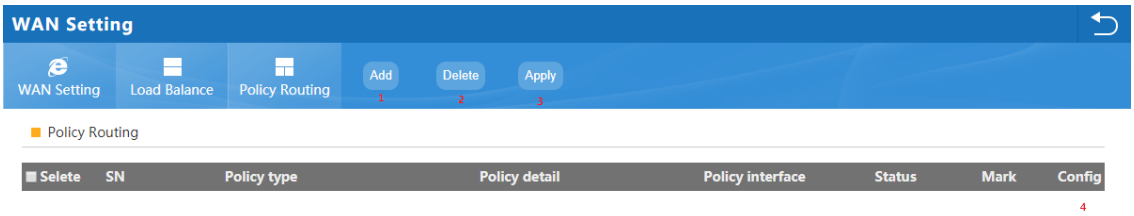
CAP 2 allows you to configure the WAN port in different ways; Static IP, DHCP, PPPoE, or disabled. If the WAN is disabled, the port will function as a LAN port.

It is also possible to limit the throughput of each WAN with the "Band Type", Downstream and Upstream.

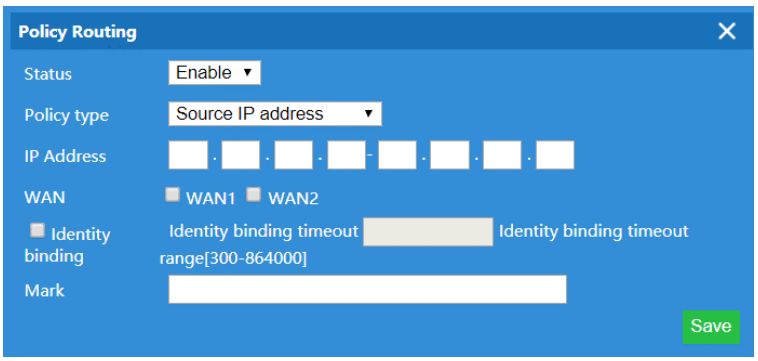
Allows you to configure access to the CAP 2 web interface over the WAN.

Policy Routing

This feature allows you to control and direct traffic through rules and routes to the WAN you want.



1. **Add**: Adds a route. Clicking will bring up the following window:

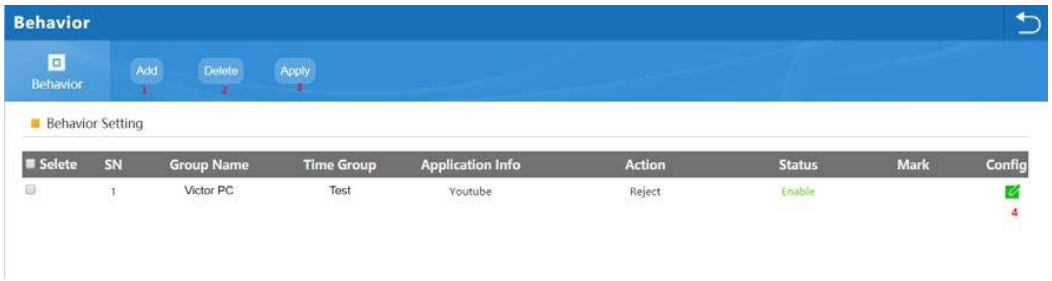


   - **Status:** Enables or disables the rule.
   - **Policy type:** Determines the type of font to use for the rule. Define: Source of an IP, destination of an IP, domain, a specific port, a MAC and an interface.
   - **WAN:** Determines the WAN where traffic will be redirected.
2. **Delete:** Deletes the selected route.
3. **Apply:** Applies routes that have been created.
4. **Config:** Allows you to edit the selected route.

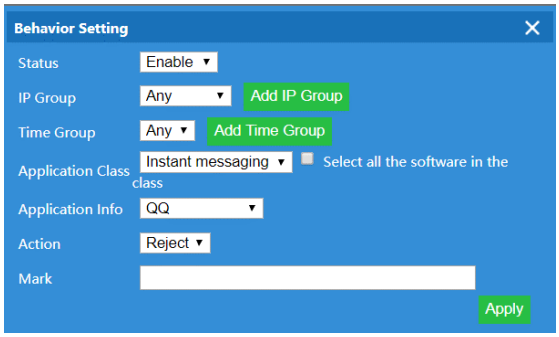
Behavior

CAP 2 allows you to control traffic behavior.

It allows you to identify different types of service and group them into different "Application Class" and give them a certain behavior.



1. **Add:** Allows you to add a behavior. Clicking will bring up the following window:



- **Status:** Enables or disables the speed limit.
- **IP Group:** Assigns a group of IPs to which the behavior in question will be applied.
- **Time Group:** Assign a "Time Group" so that the rule only applies in the given time zone.
- **Application Class:** Select the desired "Application" group to shit the related "Application Info". Check "Select all the software in the class" to block all services belonging to that class.
- **Application Info:** Select a particular "service".
- **Action:** Reject – Denies Application Class or Application Info traffic.

2. **Delete:** Delete selected behavior.
3. **Apply:** Applies behaviors that have been created.
4. **Config:** Allows you to edit the selected behavior.

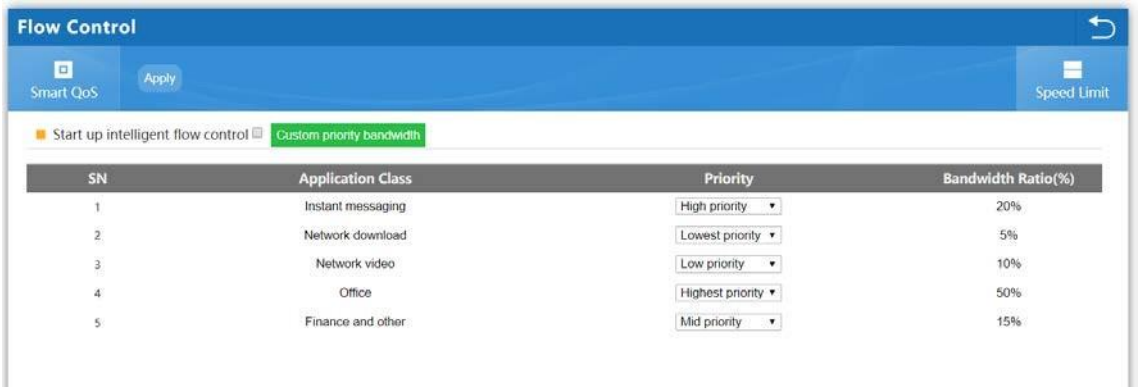
Flow Control

This function allows you to control the flow of traffic circulating through CAP 2.

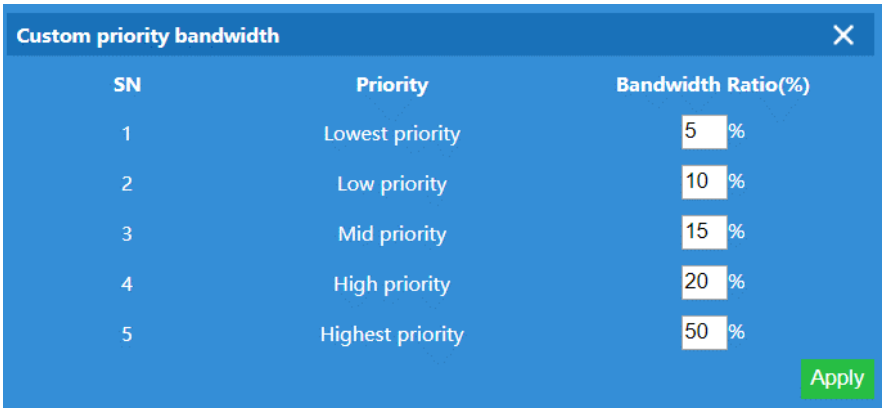
Smart Qos

It allows you to identify different types of service and group them into different "Application Class" and give them a priority over bandwidth.

It can be given more or less priority depending on our needs.

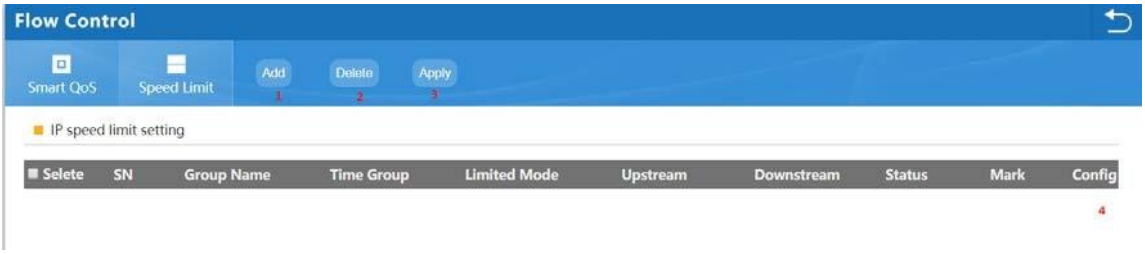


Pressing "Custom priority bandwidth" will open a window in which it will be possible to adjust the % on priorities:

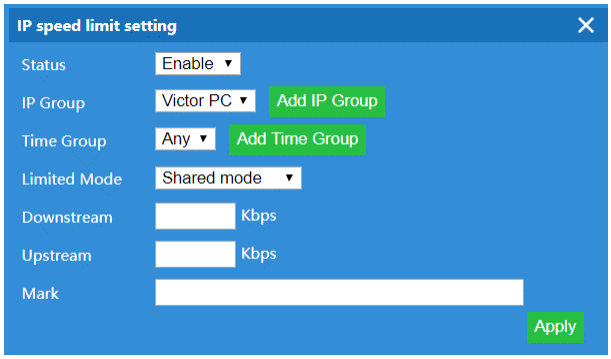


Speed Limit

This feature allows you to add speed limits to connected customers.



1. **Add:** Adds a speed limit. Clicking will bring up the following window:

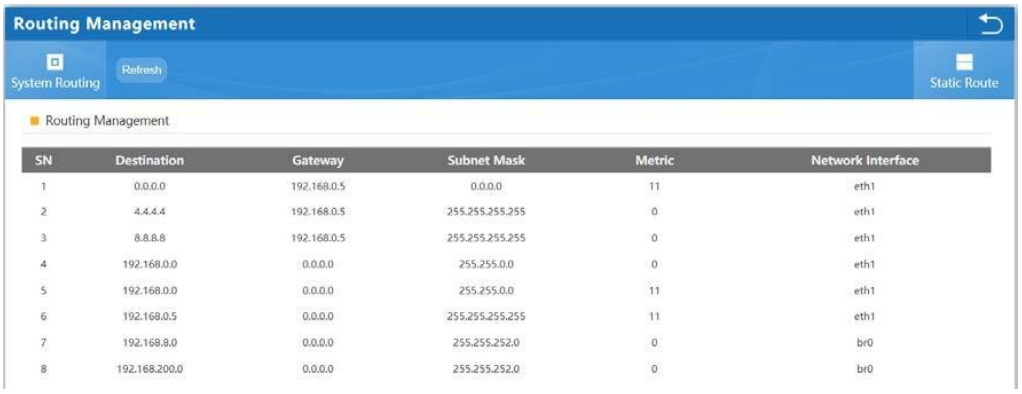


- **Status:** Enables or disables the speed limit.
- **IP Group:** Assigns a group of IPS to which the speed limit will be applied.
- **Time Group:** Assign a "Time Group" so that the rule only applies in the given time zone.
- **Limited Mode**: Shared Mode shares the designated speed between all IPs. Exclusive mode assigns each IP the designated speed.
- **Downstream:** Download speed limit.
- **Upstream:** Upload speed limit.

2. **Delete:** Removes the selected speed limit.
3. **Apply:** Applies speed limits that have been created.
4. **Config:** Allows you to edit the speed limit.

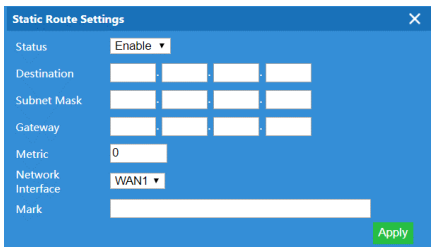
Routing Management

This section shows all the routes that **CAP 2** is currently using.



Static Route

1. **Add:** Adds a static route. Clicking will bring up the following window:

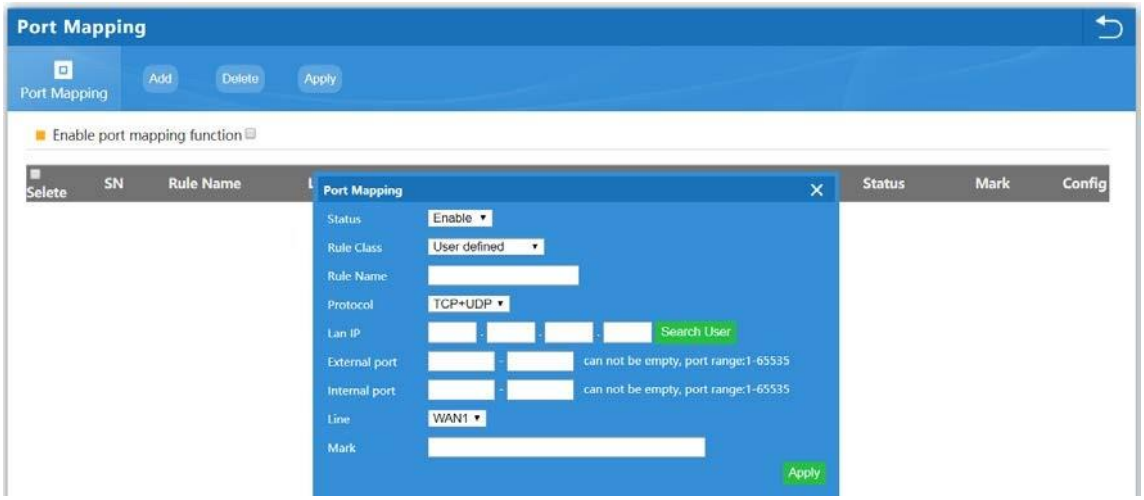


   - **Destination**: Sets the destination IP address.
   - **Subnet Mask:** Set the subnet mask.
   - **Gateway:** Set the gateway.
   - **Network Interface:** Identifies on which interface the static route is applied.
2. **Delete:** Deletes static routes that have been selected.
3. **Apply:** Applies static routes that have been created.

Port Mapping

In this section it is possible to open certain ports to the IPs of the desired devices. This allows certain services of the assigned devices to be viewed from the **CAP 2** WAN.

Note: **CAP 2** allows you to work with different WANs.



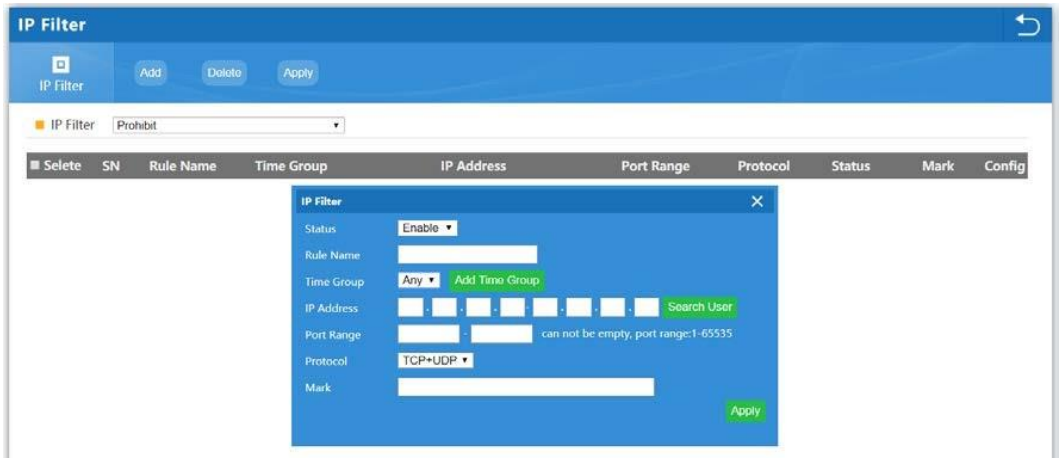
- **Status:** Enable or disable the rule.
- **Rule Name:** Name to identify the rule.
- **Protocol:** TCP / UDP.
- **Lan IP**: IP address of the device to which you want to open the port.
- **External port:** Port where the petition will enter.
- **Internal port:** Device port where the request will enter.
- **Line:** WAN on which the rule will apply.

Once you have entered all the data, click "**Apply**

URL Filter

The URL Filter allows you to deny all those URLs added to the list.

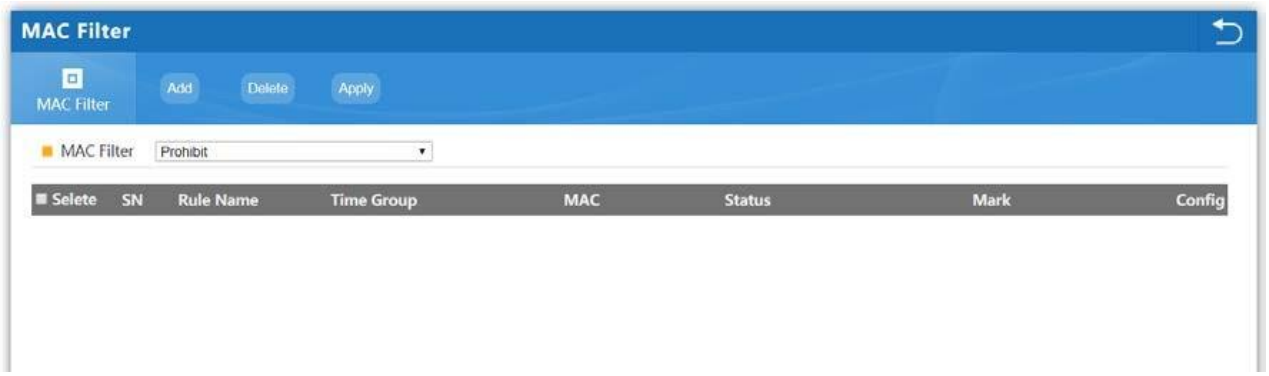
IP Filter



- **Status:** Enables or disables the rule.
- **Rule Name:** Filter name.
- **Time Group:** Select the rule in case that is applied over any particular time group.
- **IP Address:** Range of IPs in which the filter was applied.
- **Protocol:** TCP / UDP, TCP, UDP
- **Port Range:** Determines the port we want to filter. Once you have entered all the data, click "Add"

MAC Filter

Mac Filter allows you to authorize or deny devices identified by the MAC.



DMZ

DmZ allows redirecting all port requests to a particular IP.

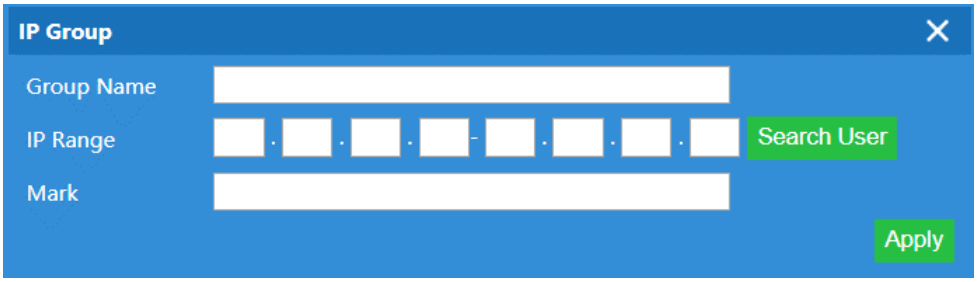
IP/Time Group

In this section you can create IP groups and time zones.

Note: It is important to remember that IPs are granted through DHCP and are variable. It is recommended to use fixed IPs assigned through the MAC in DHCP.

IP Group

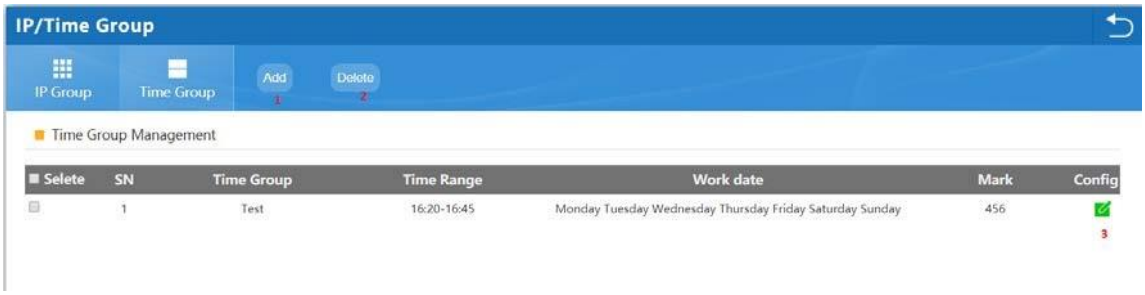
1. **Add:** Add a group of IPs. Pressing will open a new window.



- **Group Name:** Name of the IP group
- **IP Range**: IPs address range for the group.

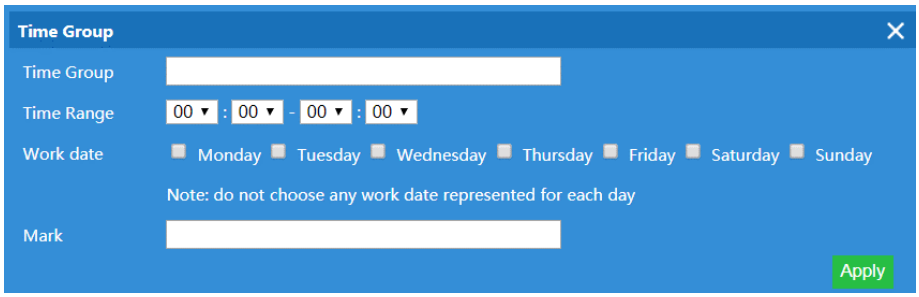
2. **Delete:** Select the group of IPs you want to delete.
3. **Config:** Allows you to edit the selected IP group.

Time Group



1. **Add:** Add a "Time Group". Clicking will open a new window.

   - **Time Group:** Name of "Time Group"

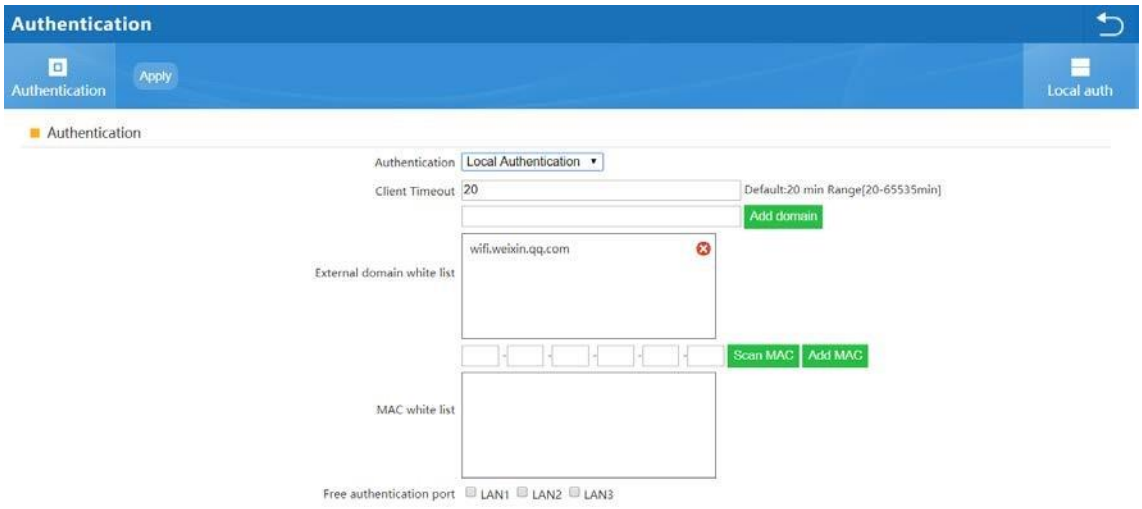


   - **Time Range:** Time range.
   - **Work date:** Select the days of the week.
     "Example: 8:00 to 12:00 only on Saturdays and Sundays. **THE CAP 2** options for assigning a "Time Group" will use the time and day provided to perform the action".

1. **Delete:** Select the "Time Group" you want to delete.
2. **Config:** Allows you to edit the selected "Time Group".

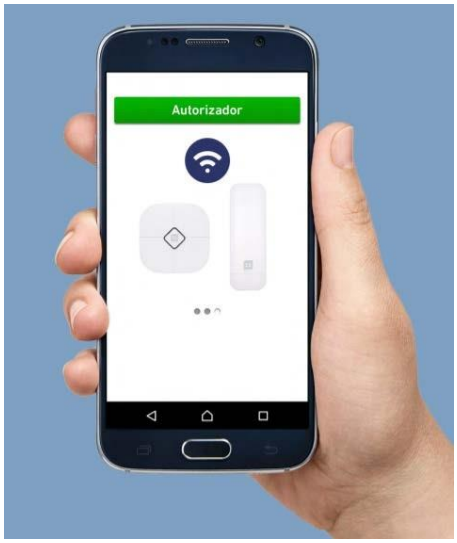
Authentication

This section of **CAP 2** activates the simple captive portal.



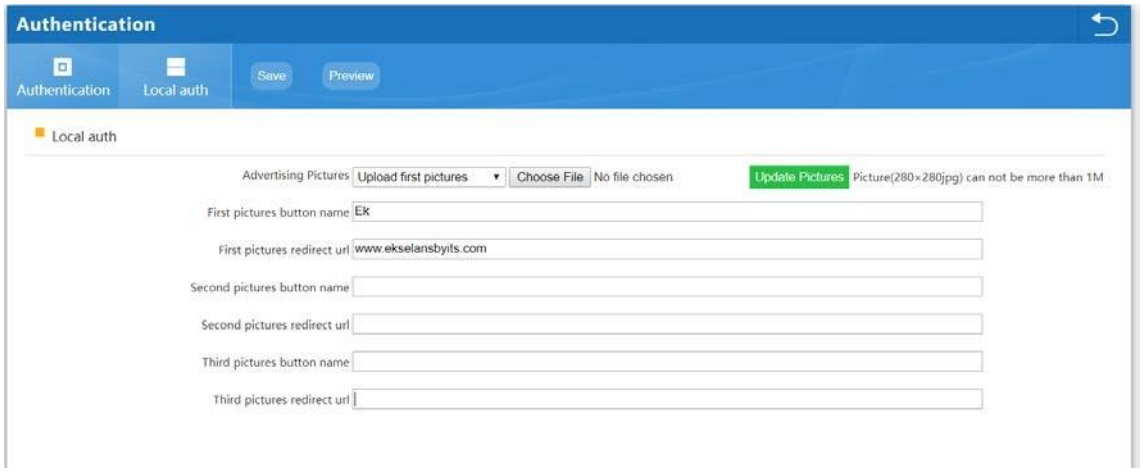
To activate the portal, the "authentication" must be in **"local authentication" mode.**

- **Client Timeout:** Maximum number of authentications allowed by the portal.
- **External domain White**list: List of domains that can be accessed without authentication.
- **MAC White list:** MACs of devices that do not need to authenticate to the portal.



Local auth

In this section we will be able to configure the portal page.

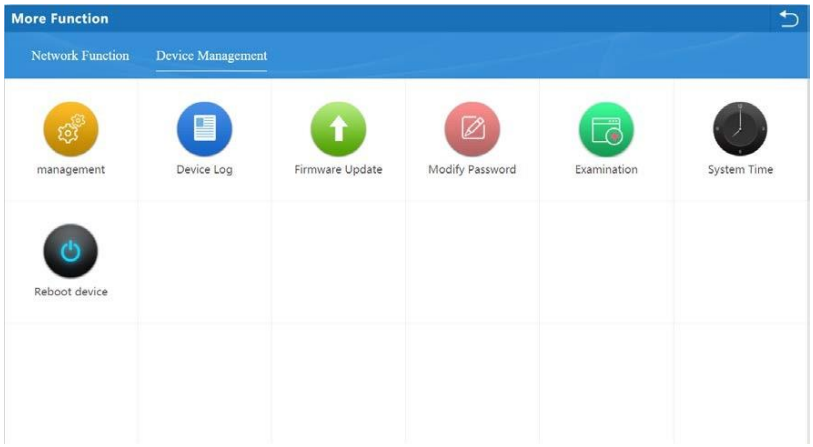


The portal consists of a slide show with 3 images and 3 buttons.

- Advertising pictures: Select the position of the image you want to change, select the file and press "Update Pictures".
- First pictures button name: Name for first button.
- First pictures redirect url: After pressing the button the device will go to the URL indicated.

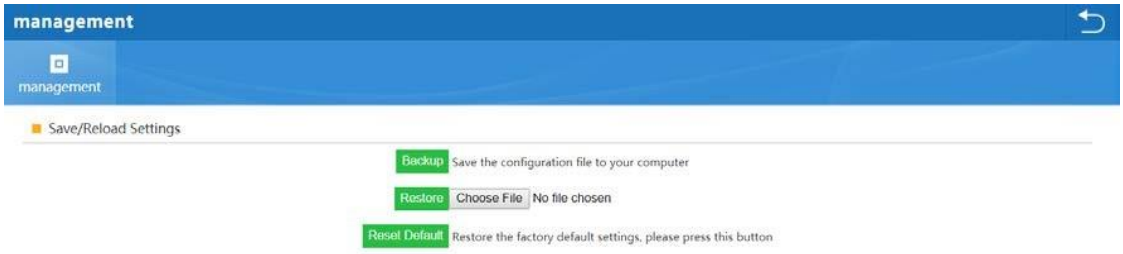
The "Preview" button will show a preview of the configured portal.

Device Management



Management

In this section you can export the CAP 2 settings as well as restore it. You can also restore the equipment with factory settings.

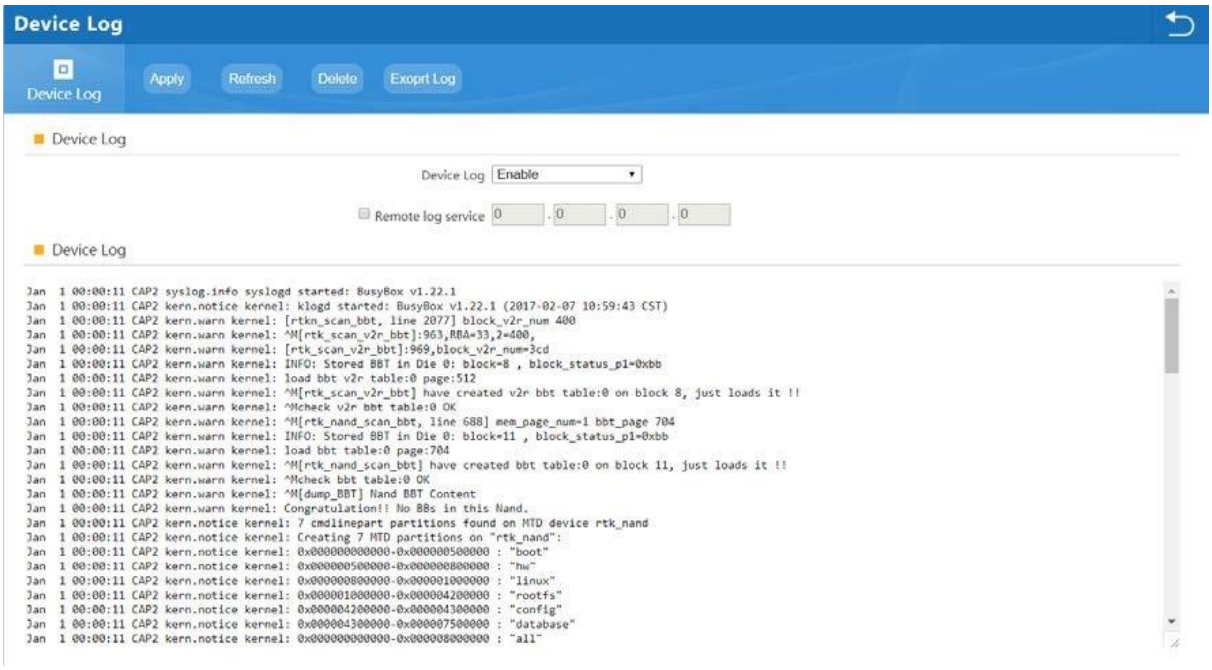


Modify Password

Allows you to configure the user and password to access the CAP 2.

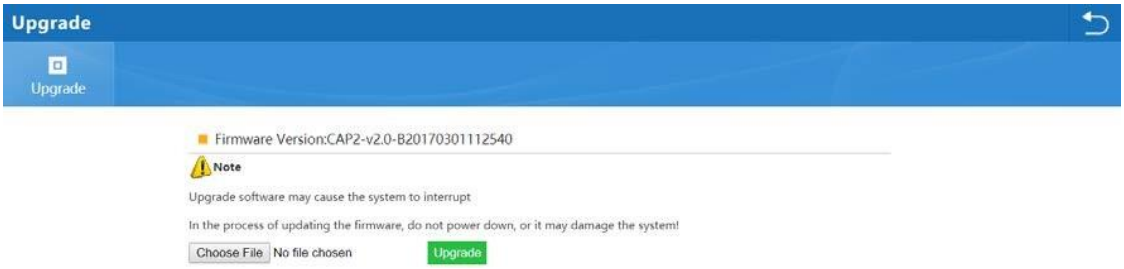
Device Logs

Displays all **CAP 2** events. It is also possible to store the logs on an external server by entering the IP and clicking on "Apply".



Firmware Update

Select the file with which to update the **cap 2** firmware and press "Upgrade"



Examination

Allows you to assign a daily time for **CAP 2** to restart.

System Time

Manage **CAP 2** time zone.