

USER MANUAL

CAP 2 335002 Controller for access points



V03

TABLE OF CONTENTS

Hardware	4
Example of installation diagram	
Access to CAP 2	5
CAP 2 web interface	6
Network Function	7
AC Setting	7
Device Group	
Zero config	
Device Logs	14
Address Server	
LAN	
WAN	
WAN Setting	
Policy Routing	
Behavior	
Flow Control	
Smart Qos	
Speed Limit	
Routing Management	
Static Route	
Port Mapping	23
URL Filter	
IP Filter	
MAC Filter	
DMZ	
IP/Time Group	
IP Group	
Time Group	
Local auth	
Device Management	



USER MANUAL CAP 2

Management	30
Modify Password	30
Device Logs	31
Firmware Update	31
Examination	32
System Time	32



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".

Protocolo de Internet versión 4 ((TCP/IPV4) Properties	×			
General					
You can get IP settings assigned this capability. Otherwise, you n for the appropriate IP settings.	automatically if your network supports eed to ask your network administrator				
Obtain an IP address auton	natically				
• Use the following IP addres	is:				
IP address:	192 . 168 . 10 . 10				
Subnet mask:	255.255.255.0				
Default gateway:					
Obtain DNS server address	automatically				
• Use the following DNS serve	er addresses:				
Preferred DNS server:					
Alternative DNS server:					
Validate settings upon exit	Advanced				

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

Username			
Password			
		Log in	Cancel

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:

WAN Name:WAN	11	×
Static IP	connected	
IP Address	192.168.0.222	
Subnet Mask	255.255.0.0	
Default Gateway	192.168.0.5	
DNS	8.8.8.8 4.4.4.4	
MAC	78:D3:8D:ED:D8:08	

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



Network Function

Network Function	Device Management				+
	8	e			-*-
AC	LAN	WAN	Behavior	Flow Control	Routing Managemen
2%		F	8	Dmz	
Port Mapping	Url Filter	IP Filter	MAC Filter	DMZ	DDNS
PD	•				
IP/Time Group	Authentication	Cloud			

AC Setting

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

A	C Se	ttin	g											5
	II Devic	e List						0 Rosol		Zero Config	Device Gr	oup	Device Log	Address Server
	Select	SN	Location	Name		MAC	Users	Version	Channel	Txpower	Device Model	Uptime	Grou	ip Config
	٠	31	1		192.168.200.37	78:D3:8D:F7:E9:84	2 1	V2.0	9740	100%/100%	AP1200	0:00:50	N/A	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.

EKSELANS BY ITS

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

RealTim	e users							×
SN	Name		MAC	Tx bytes	Tx pkts	Rx bytes	Rx pkts	Link
1	pt-0	192.168.8.149	34:E6:AD:45:3A:53	4854	36	7448	33	21

- 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 Config			
Device Status	Device Model	XD4200	
	Uptime	22:49:02	
Device Network	MAC	44:D1:FA:39:09:50	
		192.168.200.103	
Wireless Basic	Software Name	XD4200-AP-OpenWrt-V4.0-Build20190904113604	
	Version		
Wireless Advanced	AC IP	192.168.200.1	
	SSID	Wireless 2.4G/Wireless 5.8G	
	BSSID	44:D1:FA:39:09:51/44:D1:FA:39:09:52	
Annala	Channel		
Арріу	Security	WPA/WPA2-PSK/WPA/WPA2-PSK	
	RF Output Power	100%/100%	
Close	Beacon Interval	100/100	
	Coverage Threshold	-90/-90	
	Time to restart	Disabled	

"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"

Wlan Device Config			×
Device Status	IP Setting IP Address	DHCP • 192 . 168 . 200 . 103	
Device Network	Subnet Mask	255 . <mark>255</mark> . <mark>252</mark> . 0	
Wireless Basic			
Wireless Advanced			
Apply			
Close			

"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.

n Device Config					
Device Status	Device List	Wlan Device 1 🔻			
Device Status	Main AP Confi	iguration[44:D1:FA:39:09:51]			
Device Network	Status	Enable 🔻	Broadcast SSID	Enable 🔻	
Device Network	SSID	Wireless 2.4G	VlanId	0	(0-4094)
Wireless Basic	Security	WPA/WPA2-PSK-TKIPAES		Config	
WITCHESS DUSIC	Virtual AP Cor	nfiguration1[00:00:00:00:00:0	0]		
Wireless Advanced	Status	Disable 🔻	Broadcast SSID	Enable 🔻	
Witchess Advanced	SSID	WirelessAP-2G-01	Vlanid	0	(0-4094)
	Security	Open System		Config	
	Virtual AP Cor	nfiguration2[00:00:00:00:00:0	0]		
	Status	Disable 🔻	Broadcast SSID	Enable 🔻	
Apply	SSID	WirelessAP-2G-02	Vlanid	0	(0-4094)
	Security	Open System		Config	
Close	Virtual AP Cor	nfiguration3[00:00:00:00:00:0	0]		
	Status	Disable 🔻	Broadcast SSID	Enable 🔻	
	SSID	WirelessAP-2G-03	VlanId	0	(0-4094)
	Security	Open System		Config	

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.

EKSELANS BY ITS

• 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.

Config	×
Authentication	WPAPSK/WPA2PSK V
Key Length	WEP64 Bit 🔻
Key Formate	ASCII T
Encryption	TKIP/AES V
Key	6666666
Remark 1	Network key in 8-63 months or 64 ASCII characters 6 hex numbers
	Apply

• VLAN: Allows you to assign a VLAN to the SSID.

Wlan Device Config			×
Device Status	Device List	Wlan Device 1 🔻	
	Mode	802.11B/G/N 40MHz 🔻	
Device Network	Channel	7 [2.442 GHz] 🔻	
Wireless Basic	Client Isolation	Disable <	
	Fragment Threshold	2346	(256-2346)
Wireless Advanced	RTS Threshold	2346	(1-2347)
	Beacon Interval	100	(50-1024)ms
	Aggregation	Enable v	
Apply	ShortGI	Enable v	
	Rev Option	12 🔻	
Close	Coverage Threshold	-90	(-65dBm~-95dBm)
	Max Station	64 device before modification 0	Specific indicators refer to the D:No limit

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.

AC Settin	ıg						≏
Device List		Zero Config	Device Group	Add Group Delete Group		Device Log	9 Address Server
Select	SN		Wlan Group	p Name	Contains AP		Config
	1		6K_TES	ST	€The group consists of AP (0)		4 🗹

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.

Wlan Group	Device	List					×
Select	SN	Location	Name	IP	MAC	Uptime	Group
	1			192.168.200.103	44:D1:FA:39:09:50	23:10:56	N/A
							Add AP
							- Add 7 d

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.



- 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. <u>Note: Allows you to select a certain time of the day when you want APs to be restarted</u>.
- 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.

AC Setting							
Device List	Zero Config	Device Group	Device Log		9 Address Server		
Device Log							
2018/02/14 17:0	5:10 Device192.10	58.200.37 MAC[7]	8:D3:8D:F7:E9:8A]	online			

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.

C Setting									
Device List	Zero Config	Device Group	Device Log	9 Address Server	Refresh	Apply			
AP Addres	s Server								
			Function	Enable	•				
			Server IP Address	192 . 168	. 200 . 1				
		Se	erver Address Count	150 (1-	1000)				
			Effective Time	1	▼Н				
		A	llocated AP number	0		1			
AP address	information list								_
	SN	N	ime	1	P		MAC	Lease Time	
									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

LAN			5
LAN Settings	Apply	Static	DHCP a
LAN Setting	js		
1 DHCP Serve	IP Address Subnet Mask Spanning Tree er Setting	is 192 . 168 . 10 . 1 ik 255 . 255 . 252 . 0 ie Enable	
	DHCP Server Setting	g Enable •	
	Initial allocation base address	15 2	
	Maximum DHCP address allocation	n 200	
	DHCP Lease Time	ie [24	
2	DHCP allocation quantity	y 0 DHCP List	

- 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.

LAN					5
LAN Settings	Static DHCP				
Select	SN	IP Address	MAC	Mark	modify info

IP Address	1			Search User
мас	-	1		
Mark				



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.

Setting			
e) Setting			Load Balance Policy Ro
WAN Setting			
	the second second second second		
vlocity the wan port number, please	manually reboot the device:		
WAN Name	manually report the device:	Connect Method	Config
WAN Name WAN Name	manually reboot the device: Status Configured	Connect Method Static IP	Config
WAN Name WAN 1 WAN1 WAN2	Status Configured Configured	Connect Method Static IP Dynamic IP	Config 24 24
WAN Name WAN Name WAN1 WAN2 WAN3	Configured Configured Configured Not Configured [Can serve as Lan port]	Connect Method Static IP Dynamic IP	Config Co

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

WAN Setting					×
WAN Setting					
Connect Method	Static I	•	•		
IP Address	172	1	1	1	
Subnet Mask	255	255	255	0	
Default Gateway	172	. 1	1	254	
	1500		_	(1400-1500)	
Primary DNS	8	8	8	8	
Secondary DNS	4	4	4	4	
Band Type	100M F	iber 🔹			
	100000			Kbps	
Upstream	100000			Kbps	
	High pr	iority 🔹			
	Enable W	leb Serve		n WAN Port <mark>8080</mark>	(Port
	Range 1-I				Apply

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.

WAN Setti	ng								1
C WAN Setting	Load Balance	Policy Routing	Add 1		Apply 3				
Policy Rou	ting								
Selete S	N	Policy type		Pol	icy detail	Policy interface	Status	Mark	Config
									4

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

Policy Routing		×
Status	Enable •	
Policy type	Source IP address V	
IP Address		
WAN	🗖 wan1 📮 wan2	
Identity binding	Identity binding timeout range[300-864000]	Identity binding timeout
Mark		
		Save

- 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.

ehavior								1
D Behavior	Add	Delete	Apoly					
Behavic	r Setting							
 Behavic Selete 	er Setting SN	Group Name	Time Group	Application Info	Action	Status	Mark	Config

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

Behavior Setting	×	
Status	Enable •	
IP Group	Any Add IP Group	
Time Group	Any Add Time Group	
Application Class	Instant messaging 🔻 💻 Select all the software in the class	
Application Info	QQ T	
Action	Reject •	
Mark		
	Apply	

- 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.

Flow Control -📕 Start up intelligent flow control 🗐 Custom priority bandwidth Application Class idth Ratio(%) Priority Instant messaging High priority • 20% 1 2 Network download Lowest priority • 5% 3 Network video Low priority · 10% Office 50% 4 Highest priority * Finance and other 15% Mid priority • 5

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

Custom priority bandw	vidth	×
SN	Priority	Bandwidth Ratio(%)
	Lowest priority	<mark>5</mark> %
2	Low priority	<mark>10</mark> %
	Mid priority	<mark>15</mark> %
4	High priority	<mark>20</mark> %
5	Highest priority	<mark>50</mark> %
		Apply

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



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:

IP speed limit set	tting	×
Status	Enable •	
IP Group	Victor PC Add IP Group	
Time Group	Any Add Time Group	
Limited Mode	Shared mode 🔻	
Downstream	Kbps	
Upstream	Kbps	
Mark		
		Apply

- 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.

Ek EKSELANS BY ITS

Routing Management

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

Routing M	Management				5
System Routin					Static Route
Routing	Management				
SN	Destination	Gateway	Subnet Mask	Metric	Network Interface
1	0.0.0.0	192.168.0.5	0.0.0.0	11	eth1
2	4,4,4,4	192.168.0.5	255.255.255.255	0	eth1
3	8.8.8	192.168.0.5	255.255.255.255	0	eth1
4	192.168.0.0	0.0.0.0	255.255.0.0	0	eth1
5	192.168.0.0	0.0.0.0	255.255.0.0	11	eth1
6	192.168.0.5	0.0.0.0	255.255.255.255	11	eth1
7	192.168.8.0	0.0.0.0	255.255.252.0	0	br0
8	192.168.200.0	0.0.0.0	255.255.252.0	0	br0

Static Route

stem Routing	Static Route	Add	Doloto 2	Apply 3			-76		
 Static Rou Selete Si 	ite Settings N Destinatio	on	Gateway	Subnet Mask	Metric	Network Inter	Status	Mark	Confi

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

Status	Enable •		
Subnet Mask			
Gateway			
Metric	0		
Network nterface	WAN1 V		
Mark			

- 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.

Port Mapping							5
Port Mapping Add Delete							
Enable port mapping function							
■ SN Rule Name Selete	L Port Mapping			×	Status	Mark	Config
	Status	Enable •					201
	Rule Class	User defined 🔹					
	Rule Name						
	Protocol	TCP+UDP *					
	Lan IP		Search User				
	External port	-	can not be empty, port range:1-65535				
	Internal port		can not be empty, port range:1-65535				
	Line	WAN1 •					
	Mark						
			A				

- 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.

				Add Deleta Anniv	In I
					Url Filter
				ilter function 🗉	Enable Url filte
Config	Mark	Status	URL	Rule Name Time Group	I Selete SN
	Mark	Status	URL	Rule Name Time Group	Selete SN

IP Filter

IP Filter							5
IP Filter Add Delete							
IP Filter Prohibit	•						
Selete SN Rule Name	Time Group	IP Address	Port Range	Protocol	Status	Mark	Config
	IP Filter			×			
	Status	Enable •					
	Rule Name						
	Time Group	Any Add Time Group					
	IP Address		Soarch U	sor			
	Port Range	- can no	ot be empty, port range:1-65!	535			
	Protocol	TCP+UDP ·					
	Mark						
				Apply			

- 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.

MAC Filter						5
MAC Filter						
MAC Filter	Prohibit					
Selete SN	Rule Name	Time Group	MAC	Status	Mark	Config

DMZ

DmZ allows redirecting all port requests to a particular IP.

DMZ		5
DMZ	(Apply)	
DMZ		
	Enable DMZ Function	
	DMZ Host 0 .0 .0 .0 Search	h User



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

/Time	Group				+
IP Group	Add	Delete	A second s		Time Grou
 IP Grou Selete 	p Managen SN	Group Name	IP Range	Mark	Config
3	1	Victor PC	192.168.8.149-192.168.8.149	123	1

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

IP Group					×
Group Name					
IP Range	- I	•	•		Search User
Mark					
					Apply

- 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

IP/Time	Group					
IP Group	Time Group	Add 1	Defete 2			
Time G	roup Managemen	it				
Selete	SN	Time Group	Time Range	Work date	Mark	Config
Selete	SN 1	Time Group Test	Time Range 16:20-16:45	Work date Monday Tuesday Wednesday Thursday Friday Saturday Sunday	Mark 456	Config
Selete	SN 1	Time Group Test	Time Range 16:20-16:45	Work date Monday Tuesday Wednesday Thursday Friday Saturday Sunday	Mark 456	Config Config

- 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.

Authentication			5
Authentication Apply			Local auth
Authentication			
Authentication Client Timeout	Local Authentication 20	Default:20 min Range(20-65535min) Add domain	
External domain white list	wifi.weixin.qq.com		
MAC white list		Scan MAC Add MAC	
Free authentication port	LAN1 LAN2 LAN3		

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

- Client Timeout: Maximum number of authentications allowed by the portal.
- External domain Whitelist: 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.

Authenticat	ion			
• Authentication	Local auth			
ELocal auth				
		Advertising	Pictures Upload first pictures Choose File No file chosen Update Picture Picture Picture (280	×280jpg) can not be more than 1M
	Firs	st pictures butto	on name Ek	
	F	irst pictures red	lirect un www.ekselansbyits.com	
	Secon	d pictures butto	on name	
	Seco	and pictures red	lirect url	
	Thir	d pictures butto	on name	
	Th	nird pictures red	lirect url [

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

				Device Management	Network Function
System Time	Examination	Modify Pass	Firmware Update	Device Log	management
					CO Reboot device
					Reboot device

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.

manageme	nt	D
nanagement		
Save/Reloa	ad Settings	
	Backup Save the configuration file to your computer	
	Restore Choose File No file chosen	
	Reset Default Restore the factory default settings, please press this button	

Modify Password

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

Modify Pass	word			 	
D Modify Password					
Modify Pass	word				
		Old password			
		New password]		
		Confirm new password			



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".

Device Log	5
Apply Refresh Delete Exoprt Log Device Log	
Device Log	
Device Log Enable •	
Remote log service 0 .0 .0	
Device Log	
<pre>Jan 1 00:00:11 CAP2 syslog.info syslogd started: BusyBox v1.22.1 Jan 1 00:00:11 CAP2 kern.notice kernel: klogd started: BusyBox v1.22.1 (2017-02-07 10:59:43 CST) Jan 1 00:00:11 CAP2 kern.nark kernel: [rtkn_scan_bbt, line 2077] block_v2r_num 400 Jan 1 00:00:11 CAP2 kern.nark kernel: M[rtk_scan_v2r_bb];969,block_v2r_num=3cd Jan 1 00:00:11 CAP2 kern.nark kernel: [rtk_scan_v2r_bb];969,block_v2r_num=3cd Jan 1 00:00:11 CAP2 kern.nark kernel: INFO: Stored BBI in D10 e0: block=8, block_status_p1=0xbb Jan 1 00:00:11 CAP2 kern.nark kernel: NMC+tscared BBI in D10 e0: block=8, block_status_p1=0xbb Jan 1 00:00:11 CAP2 kern.nark kernel: M[rtk_scan_v2r_bb] have created v2r bbt table:0 on block 8, just loads it !! Jan 1 00:00:11 CAP2 kern.nark kernel: M[rtk_scan_bbt, line 68B] men_page_num=1 bbt_page 704 Jan 1 00:00:11 CAP2 kern.nark kernel: NMC+table:0 RG Jan 1 00:00:11 CAP2 kern.nark kernel: NMC+table:0 Bage:704 Jan 1 00:00:11 CAP2 kern.nark kernel: M[rtk_had_scan_bbt] have created bbt table:0 on block 11, just loads it !! Jan 1 00:00:11 CAP2 kern.nark kernel: NMC+table:0 Bage:704 Jan 1 00:00:11 CAP2 kern.nark kernel: M[rtk_hand_scan_bbt] have created bbt table:0 on block 11, just loads it !! Jan 1 00:00:11 CAP2 kern.nark kernel: NMC+table:0 Bage:704 Jan 1 00:00:11 CAP2 kern.nark kernel: NMC+table:0 CK</pre>	
Jan 1 00:00:11 CAP2 kern.notice kernel: radlinepart partitions found on NID device rtk_nand Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk", nand": Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions J NID partitions on "rtk" Jan 1 00:00:11 CAP2 kern.notice kernel: cmainer J NID partitions J NID parti	•

Firmware Update

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

Upgrade		5
Upgrade		
	Firmware Version:CAP2-v2.0-B20170301112540	
	(L) Note	
	Upgrade software may cause the system to interrupt	
	In the process of updating the firmware, do not power down, or it may damage the system!	
	Choose File No file chosen Upgrade	



Examination

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

	5
Examination Enable •	
Reboot Time 17:00 •	
Reboot Time 17:00 • Device will be reset automatically according to the set time	

System Time

Manage CAP 2 time zone.

System Time	5
System Time	
System Time	
System Time 2018-02-09 11:31:23 Sync with host	
NTP Enable Enable •	
Time Zone Select (GMT+01:00)Barcolona, Madrid 🔹	
NTP Server time.windows.com	
Manual IP Setting 0 - 0 - 0	
Manually reset the device when you modify the system time zone!	