

CAP1300



Edimax Technology Co., Ltd.

No. 278, Xinhu 1st Rd., Neihu Dist., Taipei City, Taiwan Email: support@edimax.com.tw

Edimax Technology Europe B.V.

Fijenhof 2, 5652 AE Eindhoven, The Netherlands Email: support@edimax.nl

Edimax Computer Company

530 Technology Drive Suite 100, Irvine, CA 92618, USA Email: support@edimax.us

CONTENTS

OVER	VIEW	•••••••••••••••••••••••••••••••••••••••	1
1	Product I	nformation	2
	l-1 Pa	ackage Contents	2
		vstem Requirements	
	-	ardware Överview	
	I-4 LE	D Status	4
	I-5 Re	eset	4
	I-6 Sa	afety Information	5
11	Hardwar	e Installation	6
	ll-1 Ro	outer/PoE Switch	6
	II-2 M	ounting	7
	II-2-1	Wooden Ceiling	
	II-2-2	Other Ceiling	9
	II-2-3	T-Rail Mount	11
<i>III</i>	Quick	Setup & Mode Selection	13
	III-1 De	efault Mode: Access Point Mode	
	III-2 Re	epeater Mode	
	III-3 Cl	ient Bridge Mode	
	III-4 M	anaged AP Mode	22
AP, N	lanaged /	AP, Repeater & Client Bridge Modes	23
IV	Basic	Settings	24
V	Wi-Fi Pro	otected Setup (WPS)	29
VI	Brow	ser Based Configuration Interface	
	VI-1 In	formation	
	VI-1-1	System Information	
	VI-1-2	Wireless Clients	
	VI-1-3	Wireless Monitor	
	VI-1-4	DHCP Clients	
	VI-1-5	Log	
	VI-2 No	etwork Settings	

	VI-2-1	LAN-Side IP Address	40
	VI-2-2	LAN Port	42
	VI-2-3	IGMP Snooping	43
	VI-2-4	STP Management	44
	VI-2-5	VLAN	45
VI-3	3 Wi	reless Settings	46
	VI-3-1	Wireless Extender	46
	VI-3-2	Profile List	48
	VI-3-3	2.4GHz 11bgn	49
	VI-3	3-3-1 Basic	50
	VI-3	3-3-2 Advanced	52
	VI-3	3-3-3 Security	55
	VI-3	3-3-4 WDS	61
	VI-3	3-3-5 Guest Network	63
	VI-3-4	5GHz 11ac 11an	64
	VI-3	3-4-1 Basic	65
	VI-3	3-4-2 Advanced	67
	VI-3	3-4-3 Security	70
	VI-3	3-4-4 WDS	72
	VI-3	3-4-5 Guest Network	74
	VI-3-5	WPS	75
	VI-3-6	RADIUS	77
	VI-3	8-6-1 RADIUS Settings	78
	VI-3	3-6-2 Internal Server	80
	VI-3	8-6-3 RADIUS Accounts	82
	VI-3-7	MAC Filter	84
	VI-3-8	WMM	86
	VI-3-9	Schedule	
	VI-3-10	Traffic Shaping	90
	VI-3-11	Bandsteering	92
VI-4	4 Ma	inagement	93
	VI-4-1	Admin	93
	VI-4-2	Date and Time	96
	VI-4-3	Syslog Server	
	VI-4-4	Ping Test	
	VI-4-5	l'm Here	100
VI-	5 Adv	vanced	
	VI-5-1	LED Settings	
	VI-5-2	Update Firmware	102
	VI-5-3	Save / Restore Settings	
	VI-5-4	Factory Default	

		VI-5-5	Reb	oot	
	VI-6	5 Op	perati	on Mode	
Edima	y P	ro NM	лс		108
Lanne			//		
VII		Produ	ıct In	formation	
VII	1	Quick	Setu	p - NMS	
	VIII	-1 Ha	ardwa	re Deployment	
	VIII			e Setup	
IX		Wehn	nae	.ayout - NMS	118
		wcop	uge		
X	NN	1S Feat	tures		
	X-1		-	ogout & Restart	
	X-2			ard	
		X-2-1	-	em Information	
		X-2-2		ces Information	
		X-2-3		aged AP	
		X-2-4		aged AP Group	
		X-2-5 X-2-6		ve Clients ve Users	
	X-3	-			
	X-3	20 X-3-1		າກ u	
		X-3-1 X-3-2		u rol	
	X-4	-		onitor	
	A-4	X-4-1		ss Point	
		···-		Managed AP	
				Managed AP Group	
		X-4-2		N	
		~·-		Active WLAN	
				Active WLAN Group	
		х-4-3		its	
		-		Active Clients	
		X-4-4		S	
				Active Users	
				Users Log	
		X-4-5		ie Devices	
		X-4-6	•	mation	
		-		All Events/Activities	
				AP Monitoring	
		~ ~			

		X-4-(6-3	SSID Overview	155
X-5		NM	S Set	tings	156
	X-5-	1	Acce	ss Point	156
		X-5-:	1-1	Edit Access Point	157
		X-5-3	1-2	Add/Edit Access Point Group	166
	X-5-2	2	WLA	N	173
		X-5-2	2-1	Add/Edit WLAN	174
		X-5-2	2-2	Add/Edit WLAN Group	177
	X-5-	3	RAD	US	178
		X-5-3	3-1	Add/Edit External RADIUS Server	179
		X-5-3	3-2	Add/Edit Internal RADIUS Server	180
		X-5-3	3-3	Add/Edit/Import/Export RADIUS Accounts	181
		X-5-3	3-4	Add/Edit RADIUS Group	184
	X-5-4	4	Acce	ss Control	185
		X-5-4	4-1	Add/Edit MAC Access Control	187
		X-5-4	4-2	Add/Edit/Clone MAC Access Control Group	188
	X-5-	5	Gues	t Network	189
		X-5-!	5-1	Add/Edit Guest Network	190
		X-5-!	5-2	Add/Edit Guest Network Group	193
	X-5-	6	User	s	194
	X-5-	7	Gues	t Portal	196
		X-5-3	7-1	Free Guest Portal Type	197
		X-5-7	7-2	User Level Agreement Guest Portal Type	198
		X-5-3	7-3	Static Users Guest Portal Type	199
		X-5-3	7-4	Dynamic Users Guest Portal Type	200
		X-5-2	7-5	External Captive Portal Guest Portal Type	202
		X-5-2	7-6	Editing "Login Portal"	203
	X-5-	8	Zone	Edit	205
	X-5-	9	Sche	dule	207
	X-5-	10	Sma	rt Roaming	208
	X-5-	11	Devi	ce Monitoring	209
	X-5-	12	Firm	ware Upgrade	210
	X-5-	13	Adva	nced	211
		X-5-:	13-1	System Security	211
		X-5-:	13-2	Date & Time	211
		X-5-:	13-3	Google Maps	213
X-6		Loca	al Ne	twork	
	X-6-	1	Netv	vork Settings	214
		X-6- 2	1-1	LAN-Side IP Address	214
		X-6-:	1-2	LAN Port Settings	217
		X-6-:	1-3	VLAN	218

	X-6-2	2.40	GHz 11bgn	219
	X-6	-2-1	Basic	220
	X-6	-2-2	Advanced	223
	X-6	-2-3	Security	226
	X-6	-2-4	WDS	232
	X-6	-2-5	Guest Network	234
	X-6-3	5GH	lz 11ac 11an	235
	X-6	-3-1	Basic	236
	X-6	-3-2	Advanced	238
	X-6	-3-3	Security	241
	X-6	-3-4	WDS	243
	X-6	-3-5	Guest Network	245
	X-6-4	WPS	S	246
	X-6-5	RAD	DIUS	248
	X-6	-5-1	RADIUS Settings	249
	X-6	-5-2	Internal Server	251
	X-6	-5-3	RADIUS Accounts	253
	X-6-6	MA	C Filter	255
	X-6-7	WM	IM	257
	X-6-8	Sche	edule	259
X-7	Loo	cal Se	ettings	261
	X-7-1	Оре	ration Mode	261
	X-7-2	Net	work Settings	263
	X-7	-2-1	System Information	263
	X-7	-2-2	Wireless Clients	266
	X-7	-2-3	Wireless Monitor	267
	X-7	-2-4	Log	268
	X-7-3	Mar	nagement	270
	X-7	-3-1	Admin	270
	X-7	-3-2	Date and Time	272
	X-7	-3-3	Syslog Server Settings	274
	X-7	-3-4	Syslog E-mail Settings	275
	X-7	-3-5	I'm Here	276
	X-7-4	Adv	anced	277
	X-7	-4-1	LED Settings	277
	X-7	-4-2	Update Firmware	278
	X-7	-4-3	Save/Restore Settings	279
	X-7	-4-4	Factory Default	280
	X-7	-4-5	Reboot	281
X-8	То	olbo>	κ	282
	X-8-1	Net	work Connectivity	282

		X-8-1-1	Ping	282
		X-8-1-2	Trace Route	283
		X-8-1-3	IP Scan	284
XI	Ap	pendix		285
	XI-1	Configu	ring your IP address	
	XI-1	-1 Win	dows XP	
	XI-1	-2 Win	dows Vista	288
	XI-1	-3 Win	dows 7	290
	XI-1	-4 Win	dows 8	294
	XI-1	-5 Mad	·	298
	XI-2	Comma	nd Line Interface	
	XI-2	-1 Con	fig	
	XI-2	-2 LAN		
	XI-2	-3 Sho	w	
	XI-2	-4 Wla	n	
	XI-2	-5 Rad	ius	
	XI-2	-6 Exit		
	XI-2	-7 Qui	t	
	XI-2	-8 Con	າmand	
	XI-3	Setting	AP via ManageEngine MibBrowser with SNMPv3	- Example. 346
	XI-3	-1 Sett	ing in Web	
	XI-3	-2 Sett	ing Rule	
	XI-3	-3 Sett	ing in ManageEngine MibBrowser	347
XII	Bes	st Pract	ice	352
	XII-1	How to	Create and Link WLAN & Access Point Groups	
	XII-1	l-1 Crea	ate WLAN Group	352
	XII-1	L-2 Crea	ate Access Point Group	355
	XII-1	L-3 Assi	gn Access Point Group to use the SSID group settings	357

Your device can function in five different modes.

AP Mode is a regular access point for use in your wireless network. This is the default mode of the access point.

Repeater Mode is a wireless repeater (also called wireless range extender) that takes an existing signal from a wireless router or wireless access point and rebroadcasts it to create a second network.

Managed AP Mode acts as a "slave" AP within the AP array (controlled by the AP Controller "master").

AP Controller Mode acts as the designated master of an AP array (group of linked access points).

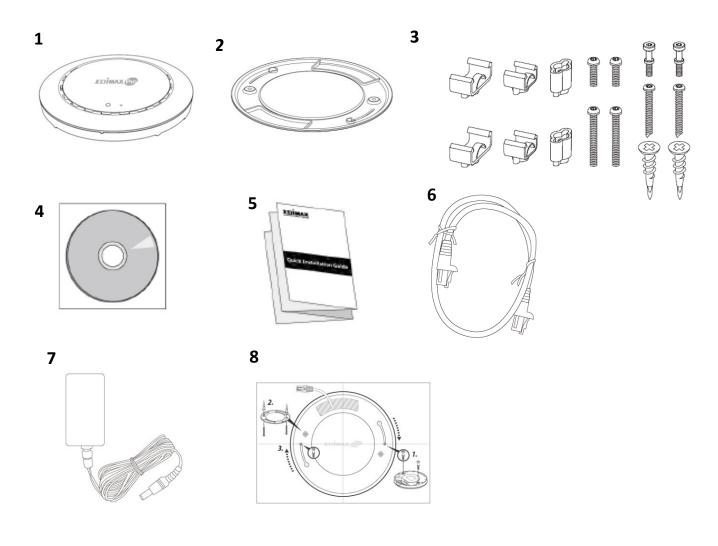
Client Bridge Mode determines the device to be a client bridge. The client bridge receives wireless signal and provides it to devices connected to the bridge via Ethernet cable.

Operation Mode		
Operation Mode	AP Mode Image: AP Mode Image: AP Mode 	
	AP Mode	
	Repeater Mode	
	AP Controller Mode	
	Managed AP mode	
	Client Bridge Mode	

This user manual is mainly split into two parts:

- AP Mode (blue) includes AP / Repeater / Managed AP / Client Bridge Mode settings
- Edimax Pro NMS (grey) includes AP Controller Mode settings

I-1 Package Contents



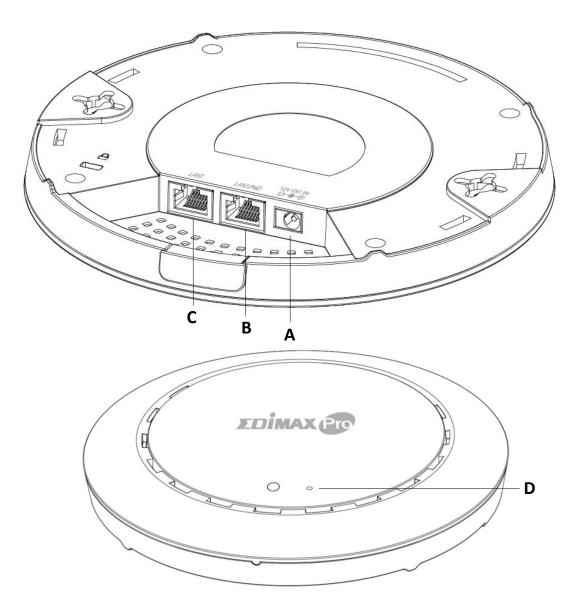
- 1. CAP1300 Access Point
- 2. Ceiling Mount Bracket
- 3. T-Rail Mounting Kit & Screws
- 4. CD

- 5. Quick Installation Guide
- 6. Ethernet Cable
- 7. Power Adapter
- 8. Ceiling Mount Screw Template

I-2 System Requirements

- Existing cable/DSL modem & router
- Computer with web browser for access point configuration

I-3 Hardware Overview



- A 12V DC IN
- **B** LAN 1 (PoE)
- C LAN 2
- LAN port with Power over Ethernet (PoE) IN LAN port

12V DC port to connect the power adapter

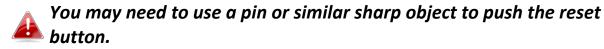
D Reset Reset the device to factory default settings

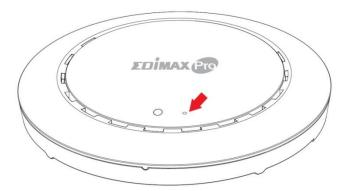
LED Color	LED Status	Description
	On	The device is on.
Blue	Flashing Slowly	Upgrading firmware.
	Flashing Quickly	Resetting to factory defaults.
A week a w	On	Starting up.
Amber	Flashing	Error.
Off	Off	The device is off.

I-5 Reset

If you experience problems with your device, you can reset it back to its factory settings. This resets all settings back to default.

1. Press and hold the reset button on the device for at least 10 seconds then release the button.





2. Wait for the device to restart. The device is ready for setup when the LED is blue.

I-6 Safety Information

In order to ensure the safe operation of the device and its users, please read and act in accordance with the following safety instructions.

- 1. The device is designed for indoor use only; do not place it outdoor.
- 2. Do not place the device in or near hot/humid places, such as in a kitchen or a bathroom.
- 3. Do not pull any connected cable with force; carefully disconnect it from the device.
- 4. Handle the device with care. Accidental damage will void the warranty of the device.
- 5. The device contains small parts which are a danger to small children under 3 years old. Please keep it out of reach of children.
- 6. Do not place the device on paper, cloth, or other flammable materials. The device may become hot during use.
- 7. There are no user-serviceable parts inside the device. If you experience problems with it, please contact your dealer of purchase and ask for help.
- The device is an electrical device and as such, if it becomes wet for any reason, do not attempt to touch it without switching the power supply off. Contact an experienced electrical technician for further help.
- 9. If smoke is visible or an obvious burning smell is coming from the device or the power adapter, disconnect the device and power adapter immediately as far as it is safe to do so. Call your dealer of purchase for help.

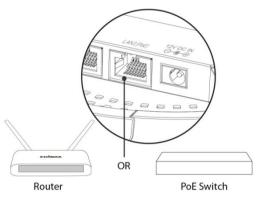
II Hardware Installation

II-1 Router/PoE Switch

1. If you need to, remove the cap from the underside of the device. This creates extra space for your cables to pass through.

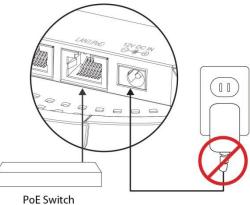


2. Connect a router or a PoE switch to the device's **LAN 1** port using an Ethernet cable.



- **3.** Power up the device:
 - a) If router is used, connect the power adapter to the device's 12V DC port and plug the power adapter into a power supply; or
 - b) If PoE (Power over Ethernet) switch is used, make sure the Ethernet cable is connected to
 LAN1 port from the switch. The device will be powered by the PoE switch.

Do not use the power adapter if



- you are using a PoE switch.
- **4.** Connect a local network client or switch to the device's **LAN 2** port as required.

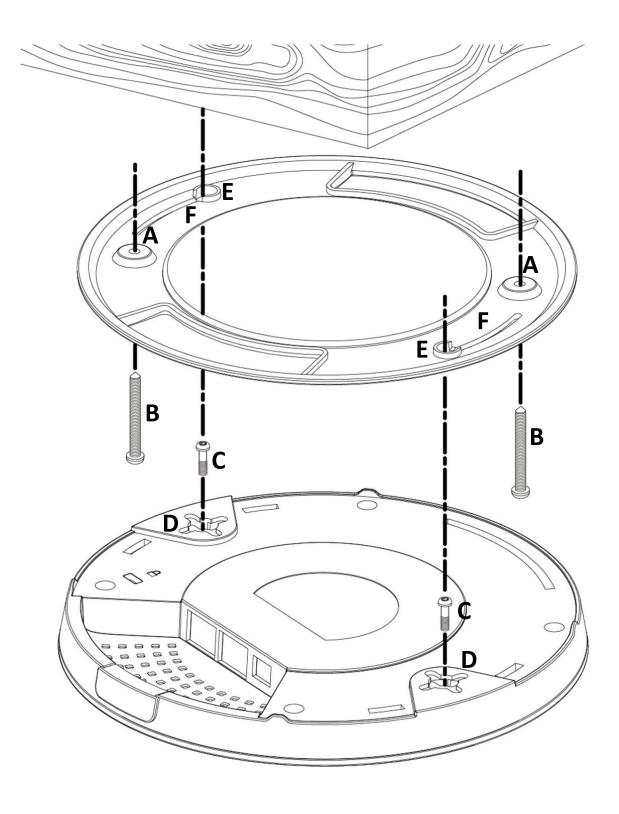
II-2 Mounting

To mount the device to a ceiling, please follow the instructions below and refer to diagram **A** & **B**.

II-2-1 Wooden Ceiling

Please refer to the figure below:

- **1.** By using the holes **A** on the ceiling bracket, identify and mark correct screw positions of the desired mounting location.
- 2. Where necessary, drill a hole (of radius smaller than the radius of the provided screws) on each of the marked screw positions.
- **3.** Fix the ceiling mount bracket to the desired location by inserting the ceiling fixing screws **B** through the bracket ceiling holes **A**. Tighten the ceiling fixing screws **B** to the marked screw position using a screw driver to fix the bracket in place.
- **4.** Fix the bracket rail screws **C** into the holes **D** on the device using a screw driver. The cap of the screws should be protruding outwardly from the holes **D**.
- **5.** Insert the bracket rail screws **C** into the device fixing holes **E**.
- 6. Twist the device as the bracket rail screws C slide through the bracket rail F.Twist the device all the way until you feel that it is fixed in position.

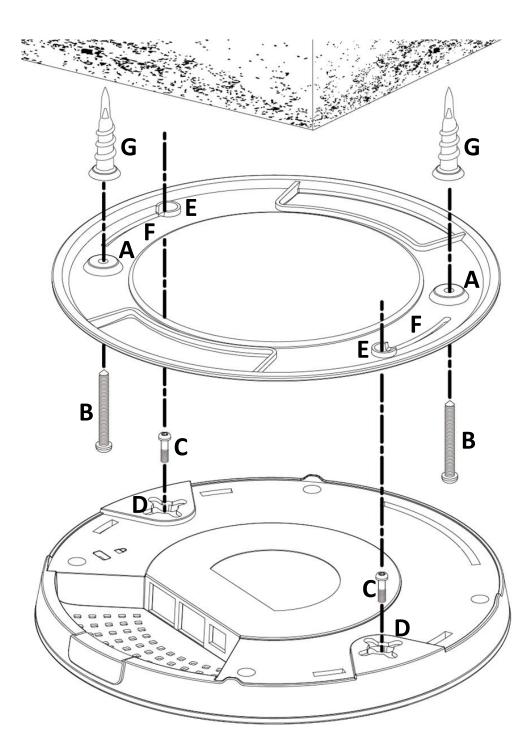


Other Ceiling II-2-2

Please refer to the figure below:

- 1. By using the holes **A** on the ceiling bracket, identify and mark correct screw positions of the desired mounting location.
- 2. Where necessary, drill a hole on each of the marked screw positions.
- 3. Insert the anchors **G** into the holes (use a screw driver where necessary) at the marked screw positions.
- 4. Fix the ceiling mount bracket to the desired location by inserting the ceiling fixing screws **B** through the bracket ceiling holes **A**. Tighten the ceiling fixing screws **B** onto the anchors **G** using a screw driver to fix the bracket to the ceiling.
- 5. Fix the bracket rail screws **C** into the holes **D** on the device using a screw driver. The cap of the screws should be protruding outwardly from the holes **D**.
- 6. Insert the bracket rail screws **C** into the device fixing holes **E**.
- 7. Twist the device as the bracket rail screws **C** slide through the bracket rail F.

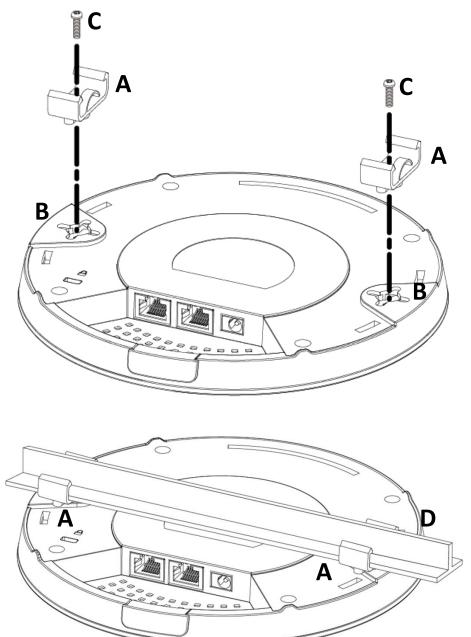
Twist the device all the way until you feel that it is fixed in position.



II-2-3 T-Rail Mount

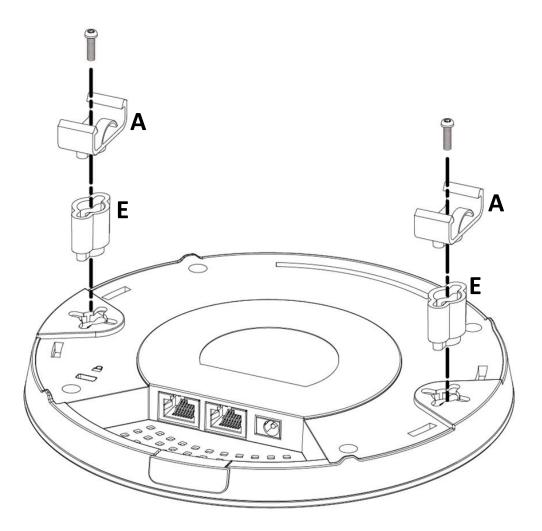
To mount the device to a T-Rail, please follow the instructions below and refer to the diagrams below.

- **1.** Select the correct size T-Rail bracket included in the package contents.
- 2. Attach the selected T-Rail brackets A to holes B using bracket fixing screws C.
- Clip the device onto the T-Rail D using the now attached T-Rail bracketsA.





If you need more space between the device and the T-Rail, additional **cushion bracket** E can be added between T-Rail brackets A and holes B (use the longer screws included).

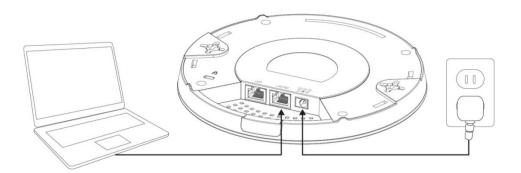


The device can function as a standalone access point (**AP Mode**), as a repeater (**Repeater Mode**), as an AP controller (**AP Controller Mode**), as part of an AP array (**Managed AP Mode**), or as a client bridge (**Client Bridge Mode**).

Follow the quick setup below before selecting the desired operation mode. For *AP Controller Mode*, please refer to viii **Quick Setup - NMS**.

III-1 Default Mode: Access Point Mode

- Set your computer's IP address to 192.168.2.x where x is a number in the range 3 100. If you are unsure how to do this, please refer xI-1.
 Please ensure there are no other active network connections on your computer by disabling Wi-Fi and other Ethernet connections.
- **2.** Connect the device to a computer via Ethernet cable.
- **3.** Connect the power adapter to the device's 12V DC port and plug the power adapter into a power supply.



- **4.** Please wait a moment for the device to start up. The device is ready when the LED is **blue**.
- 5. Enter the device's default IP address 192.168.2.2 into the URL bar of a web browser.

6. You will be prompted for a username and password. Enter the default username "**admin**" and the default password "**1234**".

Connect to 192.1	68.2.2	? ×
R		GET
The server 192.1 password.	.68.2.2 at localhost requ	ires a username and
User name:	🖸 admin	•
Password:	••••	
	🕅 Remember my p	bassword
	ОК	Cancel

7. "System Information" home screen will be shown:

EDİMAX 📴		Hor	ne Logout Global (English)
10000	Information Network Settin	gs Wireless Settings Management A	dvanced Operation Mode
Information	System Information		
> System Information			
> Wireless Clients	System		
> Wireless Monitor	Model	2017/01/s	
> wireless Monitor	Product Name	AP801F02F1968A	
> DHCP Clients	Uptime	0 day 00:07:24	
	System Time	2012/01/01 00:07:06	
> Log	Boot from	Internal memory	
	Firmware Version	1.8.1	
	MAC Address	80:1F:02:F1:96:8A	
	Management VLAN ID	1	
	IP Address	192.168.2.103 Refresh	
	Default Gateway	192.168.2.70	
	DNS	192.168.2.70	
	DHCP Server	192.168.2.70	
	Wired LAN Port Setting	15	
	Wired LAN Port	Status	VLAN Mode/ID
	LAN1	Connected (100 Mbps Full-Duplex)	Untagged Port / 1
	LAN2	Disconnected ()	Untagged Port / 1

8. By default, the device is in **AP Mode**.



If you do not wish to change the operation mode, switch your computer back to dynamic IP address now.

у 	•	•			
		•			
natically					
resses:					
			Ac	lvan	ced
		natically resses:	resses:	resses:	

9. If you wish to change to a different operation mode, go to "Operation Mode" to select the desired operation mode. Follow the steps in the following sections to change the operation mode.

100 C 4 10	Information Networ	k Settings Wireless Settin	gs Management	Advance	Operation Mode	e
Operation Mode Operation Mode	Operation Mode					
	Operation Mode	i de la companya de l				
	Operation Mode	AP Mode	• ▼			
	Wireless Mode					
	2.4GHz Mode 5GHz Mode	Access Access				
					Apply Ca	ancel
Operation Mode						
Operation Mode		P Mode ▼ P Mode				
	A	Repeater Mode P Controller Mode Janaged AP mode Client Bridge Mode				

III-2 Repeater Mode

From the quick setup above,

1. Select **Repeater Mode** from the operation mode drop down menu:

Operation Mode		
Operation Mode	AP Mode	
	AP Mode	
	Repeater Mode	
	AP Controller Mode	
	Managed AP mode	
	Client Bridge Mode	

2. Press "Apply" and wait for the device to reboot into Repeater Mode:

Operation Mode	
Rebooting	
Please wait for 48 seconds.	

3. When system page is displayed, go to Wireless Settings → Wireless Extender.

36K1/3F	Information Network S	Settings Wireless Settin	ngs Management	Advanced Operati	on Mode
Wireless Settings	Wireless Extender				
Wireless Extender					
Profile List	Wireless Extender				
> 2.4GHz 11bgn	Site Survey	Wirele	ess 2.4G / 5G 🔍 2.4G	5G Scan	
Basic					
Advanced	Wireless 2.4GHz				
Advanced Security	Wireless 2.4GHz				
Security	Wireless 2.4GHz Ch SSID	MAC Address	Security	Signal (%)	Туре
Security			Security k Scan button to start.	Signal (%)	Туре
Security				Signal (%)	Туре
Security > 5GHz 11ac 11an				Signal (%)	Туре
Security > 5GHz 11ac 11an Basic	Ch SSID			Signal (%) Signal (%)	Туре

4. Click Scan to search for and display available SSIDs

Site S	urve	ev.	Wireless 2.4G / 5G	○ 2.4G ○ 5G Sca	an	
		•)	• Wireless 2.407 50	0 2.40 0 30 000		
Wirel	ess	2.4GHz (37 Accesspo	ints)			
	000		into y			
Select	Ch	SSID	MAC Address	Security	Signal (%)	Туре
\bigcirc	1	edimax.setup	10 PALO-1940	NONE	100	b/g/n
\bigcirc	2	EdiPlug.Setup	> 251121, 0.16	NONE	94	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	ALC: NO REPORT	WPA2PSK/AES	100	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	SALES CONTRACTOR	WPA2PSK/AES	28	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	ALC: NO REPORT	WPA2PSK/AES	56	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	NAMES OF A DESCRIPTION OF	WPA2PSK/AES	92	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	A REAL PROPERTY OF	WPA2PSK/AES	92	b/g/n
			•			
Wirel	ess	5GHz (29 Accesspo	ints)			
Select	Ch	SSID	MAC Address	Security	Signal (%)	Туре
\bigcirc	40		10 PCL2-0910	NONE	28	a/n
\bigcirc	149	edimax.setup5G ce	N 261121, 324	NONE	36	ac
\bigcirc	40	Edimax_Guest	WE REAL PROPERTY.	WPA2PSK/AES	25	ac
\bigcirc	40	EdimaxHQ	NAMES OF A DESCRIPTION	WPA2PSK/AES	36	ac
\bigcirc	40	Edimax_Guest	WE REAL PROPERTY.	WPA2PSK/AES	15	ac
	40	EdimaxHQ	NUMBER OF STREET	WPA2PSK/AES	15	ac

5. Click the circle icon to connect to an available source SSID. SSIDs can be configured independently for each frequency 2.4GHz & 5GHz.

Wireless Create profile	
SSID	lol_24
Extended SSID	lcsl_2.4
Authentication Method	WPA-PSK 🔹
WPA Type	WPA2 Only 🔻
Encryption Type	AES V
Pre-shared Key Type	Passphrase v
Pre-shared Key	
Connect Cancel	

6. Edit the new **extended** SSID according to your preference and enter the security details for the source SSID (e.g. Pre-shared Key). Click "Connect" to proceed.

Wait for the configuration to take effect:

Wireless Extender
Configuration is complete. Reloading now
Please wait for 106 seconds.

7. The device (now in Repeater Mode) will establish a connection to the source SSID and repeat the extended SSID. The device will become a DHCP client of the router/root AP. Switch your computer back to dynamic IP address.

Internet Protocol Version 4 (TCP/IPv4	l) Properties X
General Alternative Configuration	
You can get IP settings assigned auto this capability. Otherwise, you need to for the appropriate IP settings.	
Obtain an IP address automatica	ally
O Use the following IP address:	
IP address:	
Subnet mask:	· · · · ·
Default gateway:	
Obtain DNS server address auto	matically
Use the following DNS server add	dresses:
Preferred DNS server:	
Alternative DNS server:	
Validate settings upon exit	Advanced
	OK Cancel

8. To access the web user interface, check your router/root AP's settings to determine the device's new IP address. Enter the new IP address into the browser for the web user interface.

If you wish to switch the operation mode, please reset the device to factory default (via web user interface or hardware reset).

III-3 Client Bridge Mode

From the quick setup above,

1. Select **Client Bridge Mode** from the operation mode drop down menu:

Operation Mode		
Operation Mode	AP Mode	
	AP Mode	
	Repeater Mode	
	AP Controller Mode	
	Managed AP mode	
	Client Bridge Mode	

2. Press "Apply" and wait for the device to reboot into Client Bridge Mode:

Operation Mode	
Rebooting	
Please wait for 48	seconds.

3. When system page is displayed, go to Wireless Settings → Wireless Extender.

3681.38	Information Network S	ettings Wireless Settin	igs Management	Advanced Operati	on Mode
Wireless Settings	Wireless Extender				
> Wireless Extender					
> Profile List	Wireless Extender				
> 2.4GHz 11bgn	Site Survey	Wirele	ss 2.4G / 5G 🔍 2.4G	5G Scan	
Basic					
Advanced	Wireless 2.4GHz				
Advanced Security	Wireless 2.4GHz				
Security	Wireless 2.4GHz Ch SSID	MAC Address	Security	Signal (%)	Туре
Security			Security k Scan button to start.	Signal (%)	Туре
Security			-	Signal (%)	Туре
Security > 5GHz 11ac 11an			-	Signal (%)	Туре
Security > 5GHz 11ac 11an Basic	Ch SSID		-	Signal (%)	Туре

4. Click Scan to search for and display available SSIDs

Site S	unve		Wireless 2.4G / 5G	○ 2.4G ○ 5G Sc	an	
Site S	urve	ey (Wireless 2.46 / 56		all	
37:1		2.4GHz (37 Accesspo				
wirei	ess	2.4GHz (37 Accesspo	ints)			
Select	Ch	SSID	MAC Address	Security	Signal (%)	Туре
\bigcirc	1	edimax.setup	10 PC40-0010	NONE	100	b/g/n
\bigcirc	2	EdiPlug.Setup	N 264 LLL 148	NONE	94	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	A DESCRIPTION OF A DESCRIPTION	WPA2PSK/AES	100	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	NAMES OF A DESCRIPTION	WPA2PSK/AES	28	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	 A state of the sta	WPA2PSK/AES	56	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	NAMES OF A DESCRIPTION OF	WPA2PSK/AES	92	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	A REAL PROPERTY OF A	WPA2PSK/AES	92	b/g/n
					1	
Wirel	ess	5GHz (29 Accesspo	ints)			
					Signal	
Select	Ch	SSID	MAC Address	Security	(%)	Туре
\bigcirc	40		10 P 010-09 10	NONE	28	a/n
\bigcirc	149	edimax.setup5G ce	N 244121, 324	NONE	36	ac
\bigcirc	40	Edimax_Guest	REPORT OF A	WPA2PSK/AES	25	ac
\bigcirc	40	EdimaxHQ	NUMBER OF STREET	WPA2PSK/AES	36	ac
\bigcirc	40	Edimax_Guest	Report States	WPA2PSK/AES	15	ac
		EdimaxHQ	NUMBER OF STREET	WPA2PSK/AES	15	ac

5. Click the circle icon to connect to an available source SSID. SSIDs can be configured independently for each frequency 2.4GHz & 5GHz.

Wireless Create profile	
SSID	NO.
Authentication Method	WPA-PSK •
WPA Туре	WPA2 Only 🔻
Encryption Type	AES V
Pre-shared Key Type	Passphrase
Pre-shared Key	
Connect Cancel	

6. Edit according to your preference and enter the security details for the source SSID (e.g. Pre-shared Key). Click "Connect" to proceed.

Wait for the configuration to take effect:

Configuration is complete. Reloading now	Wireless Extender	
Configuration is complete. Reloading now		
	Configuration is complete. Reloading now	
Please wait for 106 seconds.	Please wait for 106 seconds.	

7. The device (now in Client Bridge Mode) will receive wireless signal and provides it to devices connected to the bridge via Ethernet cable. The device will become a DHCP client of the router/root AP. Switch your computer back to dynamic IP address.

Internet Protocol Version 4 (TCP/IPv4) Properties						×	
General	Alternative Configuration						
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.							
() Ot	Obtain an IP address automatically						
OUs	e the following IP address: —						
IP ac	ldress:]	
Subn	et mask:]	
Defa	ult gateway:]	
() Ot	tain DNS server address auto	natically					
OUs	e the following DNS server add	resses:					
Prefe	erred DNS server:]	
Alter	native DNS server:]	
	alidate settings upon exit				Advar	nced	
		[OK		Cancel	

8. To access the web user interface, check your router/root AP's settings to determine the device's new IP address. Enter the new IP address into the browser for the web user interface.

If you wish to switch the operation mode, please reset the device to factory default (via web user interface or hardware reset).

III-4 Managed AP Mode

From the quick setup above,

1. Select **Managed AP Mode** from the operation mode drop down menu:

Operation Mode		
Operation Mode	AP Mode 🔻	
	AP Mode	
	Repeater Mode	
	AP Controller Mode	
	Managed AP mode	
	Client Bridge Mode	

2. Press "Apply" and wait for the device to reboot into Managed AP Mode:

Operation Mode
Rebooting
Please wait for 48 seconds.

For use a Managed AP in an AP array, the access point will automatically switch mode when an AP Controller is configured in the network.

The device can function as a standalone access point (AP Mode), as a repeater

(Repeater Mode), as an AP controller (AP Controller Mode), as part of an AP

array (Managed AP Mode), or as a client bridge (Client Bridge Mode).

Please refer to *Edimax Pro NMS* section for AP Controller Mode setting. For operation mode selection, please follow the quick setup in III *Quick Setup* & *Mode Selection*.

IV Basic Settings

Basic settings of the access point are:

- LAN IP Address; and
- 2.4GHz & 5GHz SSID & Security; and
- Administrator Name & Password; and
- Time & Date

It is recommended that these settings are configured before using the access point.

Whenever a new setting is applied to the access point, the webpage will reload, as shown below:

Configuration is complete. Reloading now					
Please wait for 1	19	seconds.			

Instructions below will help you configure these settings:

Changing IP Address:

1. Go to "Network Settings" > "LAN-side IP Address" for the screen below:

LAN-side IP Address	
IP Address Assignment	DHCP Client •
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	From DHCP V
Primary DNS Address	From DHCP v 0.0.0.0
Secondary DNS Address	From DHCP v 0.0.0.0
	Apply

If you are unable to configure any settings here, please make sure the operation mode of the Access Point is in "AP Mode". Please refer to VI-6 Operation Mode for more information. 2. Enter the IP address settings you wish to use for your access point. You can use a dynamic (DHCP) or static IP address, depending on your network environment. Click "Apply" to save the changes and wait a few moments for the access point to reload.

When you change your access point's IP address, you need to use the new IP address to access the browser based configuration interface instead of the default IP 192.168.2.2.

Changing SSID for 2.4GHz wireless network

- 1. Go to "Wireless Settings" > "2.4GHz 11bgn" > "Basic".
- **2.** Enter the new SSID for your 2.4GHz wireless network in the "SSID1" field and click "Apply".

NOT NOT	Information Network Settings	Wireless Settings Management Advanced Operation Mode
Wireless Settings 2.4GHz 11bgn Basic 	Basic 2.4GHz Basic Settings	
Advanced	Wireless Band	 ● Enable Disable 11b/g/n ▼
WDS	Enable SSID number	
Guest Network	SSID1	
Basic	Auto Channel Range	Ch 1 - 11 V
Advanced	Auto Channel Interval	One day Change channel even if clients are connected
WDS	Channel Bandwidth BSS BasicRateSet	Auto • all •
Guest Network > WPS		Apply Cancel

To utilize multiple 2.4GHz SSIDs, open the drop down menu labelled "Enable SSID number" and select how many SSIDs you require. Then enter a new SSID in the corresponding numbered fields below, before clicking "Apply".

Enable SSID number	2 •	
SSID1	400 00 00 00 Km	VLAN ID 1
SSID2	AND A REPORT	VLAN ID 1

Configuring Security Settings of 2.4GHz wireless network

- 1. Go to "Wireless Settings" > "2.4GHz 11bgn" > "Security".
- **2.** Select an "Authentication Method", enter or select fields where appropriate, and click "Apply".

	Information Network Settings	Wireless Settings Management Advanced Operation Mode
Wireless Settings	Security	
> 2.4GHz 11bgn		
Basic	2.4GHz Wireless Security Se	ttings
Advanced	SSID	AND IN AN AVERAGE
> Security	Broadcast SSID	Enable v
WDS	Wireless Client Isolation	Disable •
Guest Network	802.11k	Disable v
Guest Network	Load Balancing	50 /50
5GHz 11ac 11an		
Basic	Authentication Method	No Authentication
Advanced	Additional Authentication	No additional authentication 🔹
Security		
WDS		
Guest Network	2.4GHz Wireless Advanced S	ettings
Guest Hetwork	Smart Handover Settings	
WPS	Smart Handover	Enable Disable
RADIUS	RSSI Threshold	-80 ▼ dB
RADIUS Settings		
Internal Server		Apply Cancel

For more information on authentication method, please refer to VI-3-3-3 **on page 55.**

If multiple SSIDs are used, specify which SSID to configure using the "SSID" drop down menu.

2.4GHz Wireless Security Set	tings
SSID	And the second sec
Broadcast SSID	
Wireless Client Isolation	
802.11k	Disable •
Load Balancing	50 /50
Authentication Method	No Authentication •
Additional Authentication	No additional authentication

<u>Changing SSID and Configuring Security Setting for 5GHz wireless network</u> Follow the steps outlined in "Changing SSID for 2.4GHz wireless network" and "Configuring Security Setting for 2.4GHz wireless network" but choose the 5GHz option instead.

Changing Admin Name and Password

1. Go to **"Management" > "Admin"** as shown below:

10000	Information Network Settings	Wireless Settings	Management	Advanced Operation Mode	
Management	Admin				
Date and Time	Account to Manage This D	evice			
> Syslog Server	Administrator Name	admin			
> Ping Test	Administrator Password	•••••		(4-32Characters)	
ring rest		•••••		(Confirm)	
> I'm Here	Apply				

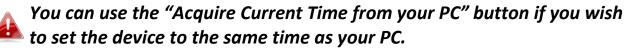
2. Complete the "Administrator Name" and "Administrator Password" fields and click "Apply".

Changing Date and Time

1. Go to "Management" > "Date and Time".

10000	Information Network Settings	Wireless Settings Management Advanced Operation Mode	
Management > Admin	Date and Time		
Date and Time	Date and Time Settings		
> Syslog Server> Ping Test	Local Time	2012 ▼ Year Jan ▼ Month 1 ▼ Day	
	0	D ▼ Hours 00 ▼ Minutes 00 ▼ Seconds	
> I'm Here	Acquire Current Time from Your PC		
	NTP Time Server		
	Use NTP	Enable	
	Auto Daylight Saving	Enable	
	Server Name	User-Defined v	
	Update Interval	24 (Hours)	
	Time Zone		
	Time Zone (G	MT+08:00) Taipei, Taiwan	
		Apply Cancel	

2. Set the correct time and time zone for your access point using the drop down menus. The access point also supports NTP (Network Time Protocol) so, alternatively, you can enter the host name or IP address of a time server. Click "Apply" when you are finished.



The basic settings of your access point are now configured.

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. You can use the configuration webpage to activate the device's WPS function.

- **1.** Go to **"Wireless Settings"** > **"WPS"** on your configuration webpage.
- **2.** Check the checkbox of "Enable" and click "Apply" to turn on WPS function.
- **3.** Within two minutes, activate WPS on your WPS-compatible wireless device. Please check the documentation of your wireless device for information regarding its WPS function.
- **4.** The devices will establish a connection.

Some functions of the browser based configuration interface are disabled for different mode settings, please refer to the sections applicable for your desired mode.



Please use Edimax Pro NMS on your Controller AP to configure your Managed AP(s).

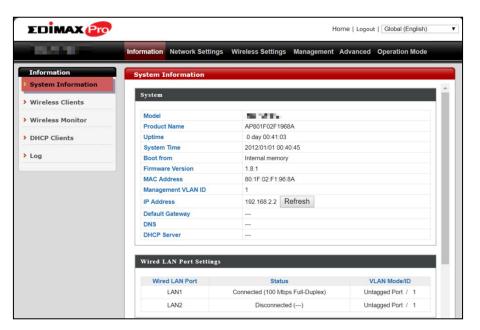
The browser-based configuration interface enables you to configure the device's advanced features. The CAP1300 features a range of advanced functions such as MAC filtering, MAC RADIUS authentication, VLAN configurations, up to 32 SSIDs and many more. To access the browser based configuration interface:

- 1. Connect a computer to your access point using an Ethernet cable.
- 2. Enter your access point's IP address in the URL bar of a web browser. The access point's default IP address is **192.168.2.2.**
- 3. You will be prompted for a username and password. The default username is "admin" and the default password is "1234", though it was recommended that you change the password during setup (see IV Basic Settings).



If you cannot remember your password, reset the access point back to its 📤 factory default settings. Refer to 1-5 Reset.

4. You will arrive at the "System Information" screen shown below.



5. Use the menu across the top and down the left side to navigate.

10000	Information	Network Settings	Wireless Settings	Management	Advanced	Operation Mode
Network Settings > LAN-side IP Address						
> LAN Port						
> IGMP Snooping						
STP Management						
> VLAN						
						Apply

6. Where applicable, click "Apply" to save changes and reload the access point, or "Cancel" to cancel changes.

Please wait a few seconds for the access point to reload after you "Apply" changes. A countdown will be shown as exemplified below.

Configuration is complete. Reloading now... Please wait for ²³ seconds.

7. Please refer to the following chapters for full descriptions of the browser based configuration interface.

VI-1 Information

Information Network Settings Wireless Settings Management Advanced Operation Mode

VI-1-1 System Information

"System Information" page displays basic system information.

System			
Model		ALVE:	
Product Name		AP801F02F1968A	
Uptime		1 day 23:51:09	
System Time		/01/02 23:53:07	
		Internal memory	
Firmware Version		1.8.1	
MAC Address		80:1F:02:F1:96:8A	
Management VLAN ID		1	
IP Address		192.168.2.103 Refresh	
Default Gateway		192.168.2.70	
DNS		192.168.2.70	
DHCP Server		192.168.2.70	
Wired LAN Port Settin	ngs		
	LAN Port	Status	VLAN Mode/ID
	AN1	Connected (100 Mbps Full-Duplex)	Untagged Port / 1
L	AN2	Disconnected ()	Untagged Port / 1
Wireless 2.4GHz			
Status		Enabled	
MAC Address		80:1F:02:F1:96:8A	
Channel		Ch 7 (Auto)	
Transmit Power		100% 28dbm	
RSSI		-63/-79/-80	
1351		-03-10-00	
Wireless 2.4GHz /WDS	SSID 5 Disabled	No Authentication No Encryption 1 No addition	I Authentication Wireless Client Isolation nal authentication Disabled nal authentication Disabled
	MAC Address	Encryption Type	VLAN Mode/ID
		No WDS entries.	
Wireless 5GHz			
Status		Enabled	
MAC Address		80:1F:02:F1:96:8B	
Channel		ov. iF.02.F 1.90.0D Ch 36 + 40 + 44 + 48 (Auto)	
Transmit Power		100% 24dbm	
RSSI		0/0	
K331		0/0	
Wireless 5GHz /SSID			
	S SID	Authentication Encryption VLAN ID Additional A	uthentication Wireless Client
		metiou Type	Isolation
AND ADDRESS		No Authentication No Encryption 1 No additional	authentication Disabled
	Disabled		
Wireless 5GHz /WDS D			
Wireless 5GHz /WDS D			
Wireless 5GHz /WDS D	MAC Address	Encryption Type	VLAN Mode/ID
Wireless 5GHz /WDS D	MAC Address	Encryption Type No WDS entries.	VLAN Mode/ID
Wireless 5GHz /WDS E	MAC Address		VLAN Mode/ID
Wireless 5GHz /WDS E	MAC Address		VLÂN Mode/ID
Wireless 5GHz /WDS D	MAC Address		VLÂN Mode/ID

System			
Model	Displays the model number of the access point.		
Product Name	Displays the product name for reference, which consists of		
	"AP" plus the MAC address.		
Uptime	Displays the total time since the device was turned on.		
System Time	Displays the system time.		
Boot From	Displays information for the booted hardware, booted from		
	internal memory.		
Firmware	Displays the firmware version.		
Version			
MAC Address	Displays the access point's MAC address.		
Management	Displays the management VLAN ID.		
VLAN ID			
IP Address	Displays the IP address of this device. Click "Refresh" to		
	update this value.		
Default	Displays the IP address of the default gateway.		
Gateway			
DNS	IP address of DNS (Domain Name Server)		
DHCP Server	IP address of DHCP Server.		

Wired LAN Port Settings			
Wired LAN	Specifies which LAN port (1 or 2).		
Port			
Status	Displays the status of the specified LAN port (connected or		
	disconnected).		
VLAN Mode/ID	e/ID Displays the VLAN mode (tagged or untagged) and VLAN ID		
	Displays the VLAN mode (tagged or untagged) and VLAN ID for the specified LAN port. See VI-2-5 VLAN.		

Wireless 2.4GHz (5GHz)				
Status	Displays the status of the 2.4GHz or 5GHz wireless (enabled			
	or disabled).			
MAC Address	Displays the access point's MAC address.			
Channel	Displays the channel number the specified wireless			
	frequency is using for broadcast.			
Transmit	Displays the wireless radio transmit power level as a			
Power	percentage.			

RSSI	Received Signal Strength Indicator (RSSI) is a measurement		
	of the power present in a received radio signal.		

Wireless 2.4GHZ	Wireless 2.4GHZ (5GHz) / SSID			
SSID	Displays the SSID name(s) for the specified frequency.			
Authentication	Displays the authentication method for the specified SSID.			
Method	See vi-3 Wireless Settings.			
Encryption	Displays the encryption type for the specified SSID. See VI-3			
Туре	Wireless Settings.			
VLAN ID	Displays the VLAN ID for the specified SSID. See VI-2-5 VLAN.			
Additional	Displays the additional authentication type for the specified			
Authentication	SSID. See vi-3 Wireless Settings.			
Wireless Client	Displays whether wireless client isolation is in use for the			
Isolation	specified SSID. See VI-2-5 VLAN.			

Wireless 2.4GHZ (5GHz) / WDS Status			
MAC Address	Displays the peer access point's MAC address.		
Encryption	Displays the encryption type for the specified WDS.		
Туре	See vi-3-3-4 WDS .		
VLAN Mode/ID	Displays the VLAN ID for the specified WDS. See VI-3-3-4 WDS.		

Select "Refresh" to refresh all information.

VI-1-2 Wireless Clients

"Wireless Clients" page displays information about all wireless clients connected to the device on the 2.4GHz or 5GHz frequency.

Refresh Tim	e		
Auto Refresh	n Time	● 5 seconds ○ 1 second ○ Disable	
Manual Refre	esh	Refresh	
2.4GHz WL	AN Client Table SSID	IP Address MAC Address Tx Rx Signal (%) RSSI (dbm) Connected Time Idle Time Vendor No wireless client	Kick
5GHz WLAN	N Client Table		
#	\$ \$ID	IP Address MAC Address Tx Rx Signal (%) RSSI (dbm) Connected Time Idle Time Vendor No wireless client	Kick

Refresh time				
Auto Refresh Select a time interval for the client table list to automatical				
Time	refresh.			
Manual	Click refresh to manually refresh the client table.			
Refresh				

2.4GHz (5GHz) V	VLAN Client Table			
SSID	Displays the SSID which the client is connected to.			
MAC Address	Displays the MAC address of the client.			
Тх	Displays the total data packets transmitted by the specified client.			
Rx	Displays the total data packets received by the specified client.			
Signal (%)	Displays the wireless signal strength for the specified client.			
Connected	Displays the total time the wireless client has been			
Time	connected to the access point.			
Idle Time	Client idle time is the time for which the client has not			
	transmitted any data packets i.e. is idle.			
Vendor	The vendor of the client's wireless adapter is displayed here.			

VI-1-3 Wireless Monitor

"Wireless Monitor" is a tool built into the device to scan and monitor the surrounding wireless environment. Select a frequency and click "Scan" to display a list of all SSIDs within range along with relevant details for each SSID.

Wireless Monitor					
Site Survey	• Wi	ireless 2.4G / 5G 🔍 2.4G 🔍 5G 🛛 Sc	an		
Channel Survey result	Expo	ort			
Wireless 2.4GHz					
Ch SSID	MAC Address	Security	Signal (%)	Туре	Vendor
		You can click Scan button to start.			
Wireless 5GHz					
Ch SSID	MAC Address	Security You can click Scan button to start.	Signal (%)	Туре	Vendor

Wireless Monitor				
Site Survey	Select which frequency (or both) to scan, and click "Scan" to			
	begin.			
Channel	After a scan is complete, click "Export" to save the results to			
Survey Result	local storage.			

Site Survey Res	ults
Ch	Displays the channel number used by the specified SSID.
SSID	Displays the SSID identified by the scan.
MAC Address	Displays the MAC address of the wireless router/access point
	for the specified SSID.
Security	Displays the authentication/encryption type of the specified
	SSID.
Signal (%)	Displays the current signal strength of the SSID.
Туре	Displays the 802.11 wireless networking standard(s) of the
	specified SSID.
Vendor	Displays the vendor of the wireless router/access point for the
	specified SSID.

VI-1-4 DHCP Clients

"DHCP Clients" shows information of DHCP leased clients.

DHCP Clients					
This table shows the assigned IP address, MAC address and expiration time for each DHCP leased client.					
DHCP Client Table	DHCP Client Table				
IP Address MAC Address Expiration Time					
No DHCP client					
Refresh					

"System log" displays system operation information such as up time and connection processes. This information is useful for network administrators. Older entries will be overwritten when the log is full

Search				🔲 Ma	tch whole words	
ID 🔻	Date and Time	Category 🔺	Severity 🔺	Users 🔺	Events/Activities	
186	/01/03 01:00:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
185	/01/03 00:30:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
184	/01/03 00:00:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
183	/01/02 23:30:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
182	/01/02 23:00:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
181	/01/02 22:30:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
180	/01/02 22:00:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
179	/01/02 21:30:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
178	/01/02 21:00:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
177	/01/02 20:36:40	SYSTEM	Low	admin	WLAN[5G], Best channel selection start, switch to channel 36 + 40 + 44 + 48	
176	/01/02 20:36:29	SYSTEM	Low	admin	Bandsteering, Stopping	
175	/01/02 20:36:18	SYSTEM	Low	admin	Bandsteering, Stopping	
174	/01/02 20:36:18	SYSTEM	Low	admin	Traffic Shaping ssid, Stopping	
173	/01/02 20:36:18	SYSTEM	Low	admin	SNMP, start SNMP server	
172	/01/02 20:36:18	SYSTEM	Low	admin	SNMP, stop SNMP server	
171	/01/02 20:36:18	SYSTEM	Low	admin	LAN, Firewall Disabled	
170	/01/02 20:36:18	SYSTEM	Low	admin	LAN, NAT Disabled	
169	/01/02 20:36:18	SYSTEM	Low	admin	LAN, stop Firewall	
168	/01/02 20:36:18	SYSTEM	Low	admin	LAN, stop NAT	
167	/01/02 20:36:18	SYSTEM	Low	admin	SCHEDULE, Schedule Stopping	

Save	Click to save the log as a file on your local computer.
Clear	Clear all log entries.
Refresh	Refresh the current log.

The following information/events are recorded by the log:



Mount & unmount

Wireless Client

Connected & disconnected Key exchange success & fail

Authentication
 Authentication fail or successful.

```
    Association
    Success or fail
```

WPS M1 - M8 messages WPS success Change Settings • System Boot Displays current model name NTP Client Wired Link LAN Port link status and speed status Proxy ARP Proxy ARP module start & stop ♦ Bridge Bridge start & stop. ♦ SNMP SNMP server start & stop. ♦ HTTP HTTP start & stop. ♦ HTTPS HTTPS start & stop. ♦ SSH SSH-client server start & stop. Telnet Telnet-client server start or stop. ◆ WLAN (2.4G) WLAN (2.4G] channel status and country/region status

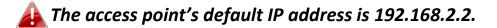
WLAN (5G)

WLAN (5G) channel status and country/region status

Information Network Settings Wireless Settings Management Advanced Operation Mode

VI-2-1 LAN-Side IP Address

"LAN-side IP address" page allows you to configure your access point on your Local Area Network (LAN). You can enable the access point to dynamically receive an IP address from your router's DHCP server or you can specify a static IP address for your access point, as well as configure DNS servers.



Address Assignment	DHCP Client The second s
P Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	From DHCP V
Primary DNS Address	From DHCP v 0.0.0.0
Secondary DNS Address	From DHCP ▼ 0.0.0.0

LAN-side IP Address				
IP Address	Select "DHCP Client" for your access point to be assigned a			
Assignment	dynamic IP address from your router's DHCP server.			
	Select "Static IP" to manually specify a static/fixed IP address			
	for your access point (below).			
	Select "DHCP Server" for your access point to assign a			
	dynamic IP address to your PC. You will have to set a Primary			
	DNS address and a Secondary DNS address. For example,			
	Google's Primary DNS address is 8.8.4.4 and Secondary DNS			

	address is 8.8.8.8.
	DHCP Client
	Static IP Address
	DHCP Client
	DHCP Server
IP Address	Specify the IP address here. This IP address will be assigned to
	your access point and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default	For DHCP users, select "From DHCP" to get default gateway
Gateway	from your DHCP server or "User-Defined" to enter a gateway
	manually. For static IP users, the default value is blank.
	From DHCP V
	User-Defined
	From DHCP

DHCP users can select to get DNS servers' IP address from DHCP or manually enter a value. For static IP users, the default value is blank.

Primary DNS	DHCP users can select "From DHCP" to get primary DNS			
Address	server's IP address from DHCP or "User-Defined" to manually			
	enter a value. For static IP users, the default value is blank.			
	From DHCP V			
	User-Defined			
	From DHCP			
Secondary	Users can manually enter a value when DNS server's primary			
DNS Address	address is set to "User-Defined".			
	From DHCP V			
	User-Defined			
	From DHCP			

VI-2-2 LAN Port

"LAN Port" page allows you to configure the settings for your access point's two wired LAN (Ethernet) ports.

Wired LAN Port	Settings				
Wired LAN Port	Enable	Speed & Duplex		Flow Control	802.3az
LAN1	Enabled •	Auto	▼	Enabled •	Enabled •
LAN2	Enabled •	Auto	▼	Enabled •	Enabled •

Wired LAN	Identifies IAN part 1 or 2				
	Identifies LAN port 1 or 2.				
Port					
Enable	Enable/disable specified LAN port.				
Speed &	Select a speed & duplex type for specified LAN port, or use				
Duplex	the "Auto" value. LAN ports can operate up to 1000Mbps and				
	full-duplex enables simultaneous data packets				
	transfer/receive.				
	Auto				
	Auto				
	10 Mbps Half-Duplex				
	10 Mbps Full-Duplex				
	100 Mbps Half-Duplex				
	100 Mbps Full-Duplex				
	1000 Mbps Full-Duplex				
Flow Control	Enable/disable flow control. Flow control can pause new				
	session request until current data processing is complete, in				
	order to avoid device overloads under heavy traffic.				
802.3az	Enable/disable 802.3az. 802.3az is an Energy Efficient				
	Ethernet feature which disables unused interfaces to reduce				
	power usage.				

VI-2-3 IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic. This page allows you to enable/disable this feature.

IGMP Snooping		
IGMP Snooping	Enable Disable	
		Apply Cancel

VI-2-4 STP Management

When enabled, STP ensures that you do not create loops when you have redundant paths in your network (as loops are deadly to a network). This page allows you to enable / disable STP management.

STP Management		
STP Management	Enable Disable	
		Apply Cancel

"VLAN" (Virtual Local Area Network) enables you to configure VLAN settings. A VLAN is a local area network which maps workstations virtually instead of physically and allows you to group together or isolate users from each other. VLAN IDs in the range 1 – 4095 are supported.

VLAN Interface		
Wired LAN Port	VLAN Mode	VLAN ID
LAN1	Untagged Port V	1
LAN2	Untagged Port	1
Wireless 2.4GHz	VLAN Mode	VLAN ID
SSID [WWT 1763 - 108.4_1]	Untagged Port	
SSID (WAP 255-106CA, C, 2	Untagged Port	1
2210 [mill] - 2004 [Million] of [d	Unlagged Port	1
Wireless 5GHz	VLAN Mode	VLAN ID
SSID [WAP1700 F1006A_A]	Untagged Port	1
Management VLAN		
VLAN ID	1	
		Apply

VLAN Interface		
Wired LAN	Identifies LAN port 1 or 2 and wireless SSIDs.	
Port/Wireless		
VLAN Mode Select "Tagged Port" or "Untagged Port" for specified LAN		
	interface.	
VLAN ID	Set a VLAN ID for specified interface, if "Untagged Port" is	
	selected.	

Management VLAN		
VLAN ID Specify the VLAN ID of the management VLAN. Only the hosts		
belonging to the same VLAN can manage the device.		

Information Network Settings Wireless Settings Management Advanced Operation Mode

VI-3-1 Wireless Extender

This page allows you to scan for available wireless network (both 2.4GHz and 5GHz frequencies) to connect to for repeater / client bridge modes.

			-		
Site Su	irvey	Wirele	ess 2.4G / 5G 🔍 2.4G	5G Scan	
Virele	ss 2.4GHz				
					_
Ch	SSID	MAC Address	Security	Signal (%)	Туре
		You can clic	k Scan button to start.		
Virele	ess 5GHz				
Ch	SSID	MAC Address	Security	Signal (%)	Type

Click "Scan" to show available wireless network:

Site S	urve	v	Wireless 2 4G / 5G	24G 5G Sc	an	
one o	uive	-y	Villeless 2.407 30	0 2.40 0 30 00	an	
Virel	ess	2.4GHz (37 Accesspo	pints)			
elect	Ch.	SSID	MAC Address	Security	Signal	Туре
elect					(%)	
\bigcirc	1	edimax.setup	10 PCL04010	NONE	100	b/g/n
\bigcirc	2	EdiPlug.Setup	> 241121 (19)	NONE	94	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	87.1 (2010) No. 7 (2010)	WPA2PSK/AES	100	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	States and the	WPA2PSK/AES	28	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	 A second sec second second sec	WPA2PSK/AES	56	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	NAMES OF A DESCRIPTION OF	WPA2PSK/AES	92	b/g/n
\bigcirc	6	Edimax_Guest_2.4G	NUMBER OF STREET	WPA2PSK/AES	92	b/g/n
N7=1		5GHz (29 Accesspo	inta)			
virei	ess	SGHZ (29 Accesspo	ints)			
elect	Ch	SSID	MAC Address	Security	Signal (%)	Туре
\bigcirc	40		10 PC40-0010	NONE	28	a/n
	149	edimax.setup5G ce	N 241121, 244	NONE	36	ac
	40	Edimax_Guest	WEIGHT STREET	WPA2PSK/AES	25	ac
0	40	EdimaxHQ	NAMES OF A DESCRIPTION	WPA2PSK/AES	36	ac
\bigcirc	40	Edimax_Guest	WITH BUILDING STREET	WPA2PSK/AES	15	ac

Click the circle icon to connect to an available source SSID. SSIDs can be configured independently for each frequency 2.4GHz & 5GHz.

Repeater Mode source SSID connection page:

Wireless Create profile				
SSID	kol_24			
Extended SSID	lest_2.4			
Authentication Method	WPA-PSK V			
WPA Type	WPA2 Only 🔻			
Encryption Type	AES V			
Pre-shared Key Type	Passphrase •			
Pre-shared Key				
Connect Cancel				

Client Bridge Mode source SSID connection page:

Wireless Create profile				
SSID	5 Q 2			
Authentication Method	WPA-PSK •			
WPA Туре	WPA2 Only 🔻			
Encryption Type	AES •			
Pre-shared Key Type	Passphrase •			
Pre-shared Key				
Connect Cancel				

Edit the connection page according to your preference and enter the security details for the source SSID (e.g. Pre-shared Key). Click "Connect" to connect to the SSID.

For more information on setting up Repeater / Client Bridge Modes, please refer to III *Quick Setup & Mode Selection*.

VI-3-2 Profile List

Wireless 2.4GHz Current Setting				
SSID	Authentication Method	Encryption Type		
Wireless 2.4GHz I	Profile List			
Select SSID	Authentication Method	Encryption Type		
	No Profile List			
Wireless 5GHz Cu	rrent Setting			
SSID	Authentication Method	Encryption Type		
e La	WPA2-PSK	AES		
Wireless 5GHz Pr	ofile List			
Select SSID	Authentication Method	Encryption Type		
	WPA2-PSK	AES		
<u> </u>				
		Edit Connect		

To edit a connection, check the circle icon and press "Edit". The edit page is shown below:

📲 🖬 Wireless Security Set	tings
SSID	in the A
Authentication Method	WPA-PSK •
WPA Type	WPA2 Only 🔻
Encryption Type	AES V
Pre-shared Key Type	Passphrase v
Pre-shared Key	Sec. wa neg

Press "Save" to save the configuration, or "Cancel" to forfeit the changes.

If you wish to use a different source SSID connection, check the circle icon (of the source SSID) and press "Connect".

VI-3-3 2.4GHz 11bgn

The "2.4GHz 11bgn" menu allows you to view and configure information for your access point's 2.4GHz wireless network across five categories: Basic, Advanced, Security, WDS & Guest Network.

VI-3-3-1 Basic

The "Basic" screen displays basic settings for your access point's 2.4GHz Wi-Fi network (s).

2.4GHz Basic Settings	
Wireless	Enable 🖲 Disable
Band	11b/g/n ▼
Enable SSID number	2 🔻
SSID1	VLAN ID 1
SSID2	VLAN ID 1
Auto Channel	Enable Disable
Auto Channel Range	Ch 1 - 11 🔻
Auto Channel Interval	One day 🔻
Auto channel interval	Change channel even if clients are connected
Channel Bandwidth	Auto 🔻
BSS BasicRateSet	all
	Apply Cancel

Wireless	Enable or disable the access point's 2.4GHz wireless radio.			
	When disabled, no 2.4GHz SSIDs will be active.			
Band	Wireless standard used for the access point.			
	Combinations of 802.1	1b, 802.11g & 802.11	In can be selected.	
Enable SSID	Select how many SSIDs to enable for the 2.4GHz frequency			
Number	from the drop down menu. A maximum of 16 can be enabled.			
	Enable SSID number	1 🔻		
	SSID1	40 YO 10 YO 10 YO 10	VLAN ID 1	
	Enable SSID number	3 🔻		
	SSID1	an an an an Arith	VLAN ID 1	
	SSID2	2	VLAN ID 1	
	SSID3	1 1 1 1 1 1 1 1 1 1	VLAN ID 1	
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID			
	can consist of any combination of up to 32 alphanumeric			
	characters.			
VLAN ID	Specify a VLAN ID for each SSID.			
Auto	Enable/disable auto channel selection.			
Channel	Enable: Auto channel selection will automatically set the			
	wireless channel for th		,	
	on availability and pote	-		
	Disable: Select a chann	el manually as showi	h in the next table.	

Auto	Select a range to which auto channel selection can choose
Channel	from.
Range	
Auto	Select a time interval for how often the auto channel setting
Channel	will check/reassign the wireless channel.
Interval	Check/uncheck the "Change channel even if clients are
	connected" box according to your preference.
Channel	Select the channel bandwidth:
Bandwidth	20MHz (lower performance but less interference); or
	40MHz (higher performance but potentially higher
	interference); or
	Auto (automatically select based on interference level).
BSS	Set a Basic Service Set (BSS) rate: this is a series of rates to
BasicRateSet	control communication frames for wireless clients.

When auto channel is disabled, configurable fields will change. Select a wireless channel manually:

Auto Channel	Enable Disable
Auto Channel Range	Ch 1 - 11 🔻
Auto Channel Interval	One day Change channel even if clients are connected
Channel Bandwidth	Auto 🔻
BSS BasicRateSet	all

Auto Channel	
Channel	Ch 11, 2462MHz 🔻
Channel Bandwidth	Auto, +Ch 7 🔹
BSS BasicRateSet	all 🔹

Channel	Select a wireless channel from 1 – 11.	
Channel	Set the channel bandwidth:	
Bandwidth	20MHz (lower performance but less interference); or	
	40MHz (higher performance but potentially higher	
	interference); or	
	Auto (automatically select based on interference level).	
BSS	Set a Basic Service Set (BSS) rate: this is a series of rates to	
BasicRateSet	control communication frames for wireless clients.	

Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

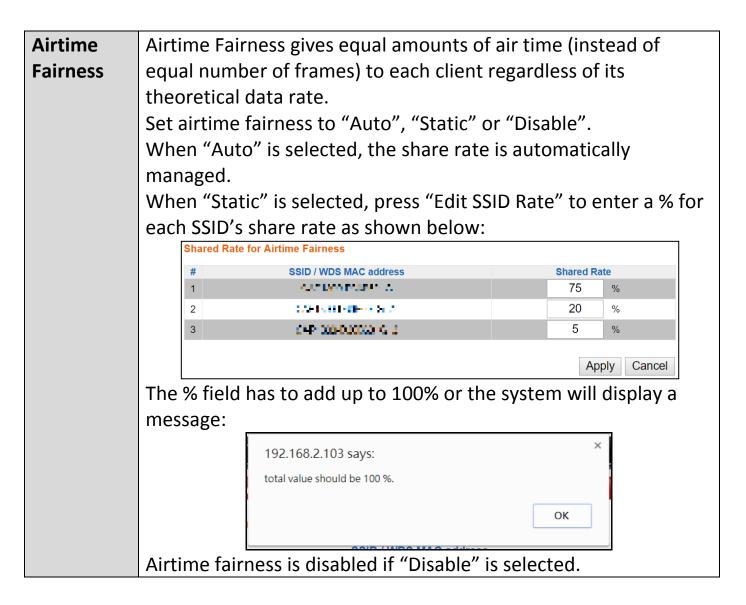
VI-3-3-2 Advanced

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

2.4GHz Advanced Settings		
Contention Slot	Obert T	
	Short ▼	
Preamble Type	Short •	
Guard Interval	Short GI ▼	
802.11g Protection	Enable	Disable
802.11n Protection	Enable	Disable
DTIM Period	1	(1-255)
RTS Threshold	2347	(1-2347)
Fragment Threshold	2346	(256–2346)
Multicast Rate	Auto 🔻	
Tx Power	100% 21dbm	▼
Beacon Interval	100	(40-1000 ms)
Station Idle Timeout	60	(30-65535 seconds)
Airtime Fairness	Disabled ▼	Edit SSID Rate

Contention	Select "Short" or "Long" – this value is used for contention
Slot	windows in WMM (see vi-3-8 WMM).
Preamble	Set the wireless radio preamble type. The preamble type in
Туре	802.11 based wireless communications defines the length of the
	CRC (Cyclic Redundancy Check) block for communication
	between the access point and roaming wireless adapters. The
	default value is "Short Preamble".
Guard	Set the guard interval. A shorter interval can improve
Interval	performance.

802.11g Enable/disable 802.1	1g protection, which increases reliability but
Protection reduces bandwidth (clients will send Request to Send (RTS) to
access point, and acc	ess point will broadcast Clear to Send (CTS),
before a packet is ser	nt from client).
802.11n Enable/disable 802.1	1n protection, which increases reliability
Protection but reduces bandwid	th (clients will send Request to Send (RTS)
to access point, and a	access point will broadcast Clear to Send
(CTS), before a packe	t is sent from client).
DTIM Set the DTIM (deliver	ry traffic indication message) period value of
Period the wireless radio. The	ne default value is 1.
RTS Set the RTS threshold	of the wireless radio. The default value is
Threshold 2347.	
Fragment Set the fragment three	eshold of the wireless radio. The default
Threshold value is 2346.	
Multicast Set the transfer rate	for multicast packets or use the "Auto"
Rate setting. The range of	the transfer rate is between 1Mbps to
54Mbps	
Tx Power Set the power output	t of the wireless radio. You may not require
100% output power.	Setting a lower power output may enhance
security since access	to your signal can be potentially prevented
from malicious/unkn	own users in distant areas.
Beacon Set the beacon interv	al of the wireless radio. The default value is
Interval 100.	
Station Set the interval for th	ne access point to send keepalive messages
idle to a wireless client to	o check if the station is still alive/active.
timeout	



Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

VI-3-3-3 Security

The access point provides various security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

It is essential to configure wireless security in order to prevent unauthorised access to your network.

SID	CA. 1304E36260_C v
Broadcast SSID	Enable v
Vireless Client Isolation	Disable •
802.11k	Disable v
oad Balancing	100 /100
Nuthentication Method	No Authontication V
Authentication Method	No Authentication
Additional Authentication	No additional authentication
Additional Authentication 4GHz Wireless Advanced S mart Handover Settings	■ No additional authentication ▼
Additional Authentication 4GHz Wireless Advanced S mart Handover Settings Smart Handover	► Mo additional authentication ■ Image: The second sec
Additional Authentication 4GHz Wireless Advanced S mart Handover Settings	■ No additional authentication ▼

SSID Selection	Select a SSID to configure its security settings.	
Broadcast SSID	Enable or disable SSID broadcast.	
	Enable: the SSID will be visible to clients as an available Wi-Fi	
	network.	
	Disable: the SSID will not be visible as an available Wi-Fi	
	network to clients – clients must manually enter the SSID in	
	order to connect. A hidden (disabled) SSID is typically more	
	secure than a visible (enabled) SSID.	
Wireless Client	Enable or disable wireless client isolation.	
Isolation	Wireless client isolation prevents clients connected to the	
	access point from communicating with each other and	
	improves security. Typically, this function is useful for	
	corporate environments or public hot spots and can prevent	
	brute force attacks on clients' usernames and passwords.	
Load Balancing	Load balancing limits the number of wireless clients	
	connected to an SSID. Set a load balancing value (maximum	
	100).	
Authentication	Select an authentication method from the drop down menu	
Method	and refer to the appropriate information below for your	
	method.	

VI-3-3-3-1 No Authentication / Additional Authentication

When "No Authentication" is selected in "Authentication Method", extra options are made available in the next line:

Additional	Select an additional authentication method from the drop
Authentication	down menu or select "No additional authentication" for no
	authentication, where no password/key is required to
	connect to the access point.
	For other options, refer to the information below.



"No additional authentication" is not recommended as anyone can connect to your device's SSID. Additional wireless authentication methods can be applied to all authentication methods:



WPS must be disabled to use additional authentication. See VI-3-5 WPS for WPS settings.

MAC Address Filter

Restrict wireless clients access based on MAC address specified in the MAC filter table.



See VI-3-7 MAC Filter to configure MAC filtering.

MAC-RADIUS Authentication

Restrict wireless clients access based on MAC address via a RADIUS server, or password authentication via a RADIUS server.



See VI-3-6 RADIUS to configure RADIUS servers.



WPS must be disabled to use MAC-RADIUS authentication. See VI-3-5 WPS for WPS settings.

Additional Authentication	MAC RADIUS authentication		
MAC RADIUS Password	 Use MAC address Use the following password 		

MAC Filter & MAC-RADIUS Authentication

Restrict wireless clients access using both of the above MAC filtering & **RADIUS** authentication methods.

Additional Authentication	MAC filter & MAC RADIUS authentication v
MAC RADIUS Password	 Use MAC address Use the following password

MAC RADIUS	Select whether to use MAC address or password	
Password	authentication via RADIUS server. If you select "Use the	
	following password", enter the password in the field below.	
	The password should match the "Shared Secret" used in VI-3-6	
	RADIUS.	

WEP (Wired Equivalent Privacy) is a basic encryption type. When selected, a notice will pop-up as exemplified below:

WPS 2.0 will be disabled if WEP is used.

Below is a figure showing the configurable fields:

Authentication Method	WEP 🔻
Key Length	64-bit 🔻
Кеу Туре	ASCII (5Characters) ▼
Default Key	Key 1 🔻
Encryption Key 1	
Encryption Key 2	
Encryption Key 3	
Encryption Key 4	

Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit
	and is recommended.
Кеу Туре	Choose from "ASCII" (any alphanumerical character 0-9, a-z
	and A-Z) or "Hex" (any characters from 0-9, a-f and A-F).
Default Key	Select which encryption key $(1 - 4 below)$ is the default key.
	For security purposes, you can set up to four keys (below)
	and change which is the default key.
Encryption Key	Enter your encryption key/password according to the format
1-4	you selected above.

For a higher level of security, please consider using WPA encryption.

VI-3-3-3-3 IEEE802.1x/EAP

Below is a figure showing the configurable fields:

Authentication Method	IEEE802.1x/EAP ▼
Key Length	64-bit ▼

Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit
	and is recommended.

VI-3-3-3-4 WPA-PSK

WPA-PSK is a secure wireless encryption type with strong data protection and user authentication, utilizing 128-bit encryption keys.

Below is a figure showing the configurable fields:

Authentication Method	WPA-PSK •
802.11r Fast Roaming	Enable Disable
WPA Туре	WPA/WPA2 Mixed Mode-PSK <
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)
Pre-shared Key Type	Passphrase v
Pre-shared Key	

Fast Roaming Settings will also be shown:

802.11r Fast Transition Roaming Settings		
mobility_domain		
Encryption Key		
Over the DS	Enable Disable	

802.11r Fast	When your device roams from one AP to another on the
Roaming	same network, 802.11r uses a feature called Fast Basic
	Service Set Transition (FT) to authenticate more quickly. FT
	works with both preshared key (PSK) and 802.1X
	authentication methods.
WPA Type	Select from WPA/WPA2 Mixed Mode-PSK, WPA2 or WPA
	only. WPA2 is safer than WPA, but is not supported by all
	wireless clients. Please make sure your wireless client
	supports your selection.
Encryption	Select "TKIP/AES Mixed Mode" or "AES" encryption type.
Key Renewal	Specify a frequency for key renewal in minutes.
Interval	
Pre-Shared	Choose from "Passphrase" (8 – 63 alphanumeric characters)
Кеу Туре	or "Hex" (up to 64 characters from 0-9, a-f and A-F).
Pre-Shared	Please enter a security key/password according to the
Кеу	format you selected above.

802.11r Fast Transition Roaming Settings		
Mobility_dom	Specify the mobility domain (2.4GHz or 5GHz)	
ain		
Encryption Key	Specify the encryption key	
Over the DS	Enable or disable this function.	

VI-3-3-3-5 WPA-EAP

Authentication Method	WPA-EAP 🔻
802.11r Fast Roaming	Enable Disable
WPA Туре	WPA/WPA2 mixed mode-EAP ▼
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)

Fast Roaming Settings will also be shown:

802.11r Fast Transition Roaming Settings		
mobility_domain		
Encryption Key		
Over the DS	Enable Disable	

WPA Туре	Select from WPA/WPA2 Mixed Mode-EAP, WPA2-EAP or WPA-EAP.
	WPA-EAP.
Encryption	Select "TKIP/AES Mixed Mode" or "AES" encryption type.
Туре	
Key Renewal	Specify a frequency for key renewal in minutes.
Interval	

WPA-EAP must be disabled to use MAC-RADIUS authentication.

802.11r Fast Transition Roaming Settings			
Mobility_dom	Specify the mobility domain (2.4GHz or 5GHz)		
ain			
Encryption Key	Key Specify the encryption key		
Over the DS	Enable or disable this function.		

Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

Wireless Distribution System (WDS) can bridge/repeat access points together in an extended network. WDS settings can be configured as shown below.

When using WDS, configure the IP address of each access point to be in the same subnet and ensure there is only one active DHCP server among connected access points, preferably on the WAN side.

WDS must be configured on each access point, using correct MAC addresses. All access points should use the same wireless channel and encryption method.

2.4GHz			
WDS Functionality	Disabled v		
Local MAC Address	80:1F:02:F1:96:8A		
WDS Peer Settings			
WDS #1	MAC Address		
WDS #2	MAC Address		
WDS #3	MAC Address		
WDS #4	MAC Address		
WDS VLAN			
VLAN Mode	Untagged Port V (Enter at least one MAC address.)		
VLAN ID	1		
WDS Encryption method			
Encryption	None (Enter at least one MAC address.)		
	Apply Reset		

2.4GHz			
WDS	Select "WDS with AP" to use WDS with access point or "WDS		
Functionality	Dedicated Mode" to use WDS and also block communication		
	with regular wireless clients. When WDS is used, each access		
	point should be configured with corresponding MAC addresses,		
	wireless channel and wireless encryption method.		
Local MAC	Displays the MAC address of your access point.		
Address			

WDS Peer Settings		
WDS #	Enter the MAC address for up to four other WDS devices you	
	wish to connect.	

WDS VLAN		
VLAN Mode	Specify the WDS VLAN mode to "Untagged Port" or "Tagged Port".	
VLAN ID	Specify the WDS VLAN ID when "Untagged Port" is selected above.	

WDS Encryption method			
Encryption	Select whether to use "None" or "AES" encryption and enter a		
	pre-shared key for AES consisting of 8-63 alphanumeric		
	characters.		

Press "Apply" to apply the configuration, or "Reset" to forfeit the changes.

VI-3-3-5 Guest Network

Enable / disable guest network to allow clients to connect as guests.

Guest Network		
Guest Network	Enable Disable	
		Apply Cancel

VI-3-4 5GHz 11ac 11an

The "5GHz 11ac 11an" menu allows you to view and configure information for your access point's 5GHz wireless network across five categories: Basic, Advanced, Security, WDS & Guest Network.

VI-3-4-1 Basic

The "Basic" screen displays basic settings for your access point's 5GHz Wi-Fi network (s).

5GHz Basic Settings			
Wireless	Enable Disable		
Band	11a/n/ac ▼		
Enable SSID number	1 •		
SSID1	VLAN ID 1		
Auto Channel	Enable Disable		
Auto Channel Range	Band 1 🔹		
Auto Channel Interval	One day 🔻		
Auto channer interval	Change channel even if clients are connected		
Channel Bandwidth	Auto 80/40/20 MHz 🔻		
BSS BasicRateSet	all 🔹		
	Apply Cancel		
	Appry Cancer		

Wireless	Enable or disable the access point's 5GHz wireless radio. When			
	disabled, no 5GHz SSID	disabled, no 5GHz SSIDs will be active.		
Band	Wireless standard used	I for the access point		
	Combinations of 802.1	1a, 802.11n & 802.11	1ac can be selected.	
Enable SSID	Select how many SSIDs	to enable for the 2.4	4GHz frequency	
Number	from the drop down menu. A maximum of 16 can be enabled.			
	Enable SSID number	1 🔻		
	SSID1	ALC: NO REPORT.	VLAN ID 1	
	Enable SSID number	3 🔻		
	SSID1	ALL	VLAN ID 1	
	SSID2	2	VLAN ID 1	
	SSID3	***	VLAN ID 1	
SSID#	Enter the SSID name fo	Enter the SSID name for the specified SSID (up to 16). The SSID		
	can consist of any com	can consist of any combination of up to 32 alphanumeric		
	characters.	characters.		
VLAN ID	Specify a VLAN ID for e	ach SSID.		
Auto	Enable/disable auto channel selection. Auto channel selection			
Channel	will automatically set the wireless channel for the access			
	point's 5GHz frequency based on availability and potential			
	interference. When disabled, configurable fields will change as			
	shown below:			
Auto	Select a range to which auto channel selection can choose			

Channel	from.	
Range		
Auto	Select a time interval for how often the auto channel setting	
Channel	will check/reassign the wireless channel.	
Interval	Check/uncheck the "Change channel even if clients are	
	connected" box according to your preference.	
Channel	Select the channel bandwidth:	
Bandwidth	20MHz (lower performance but less interference); or	
	Auto 40/20 MHz; or	
	Auto 80/40/20 MHz (automatically select based on	
	interference level).	
BSS	Set a Basic Service Set (BSS) rate: this is a series of rates to	
BasicRateSet	control communication frames for wireless clients.	

When auto channel is disabled, configurable fields will change. Select a wireless channel manually:

Auto Channel	Enable Disable
Auto Channel Range	Band 1 🔹
Auto Channel Interval	One day Change channel even if clients are connected
Channel Bandwidth	Auto 80/40/20 MHz 🔻
BSS BasicRateSet	all 🔻

Auto Channel	Enable Disable
Channel	Ch 36, 5.18GHz 🔹
Channel Bandwidth	Auto 80/40/20 MHz •
BSS BasicRateSet	all 🔻

Channel	Select a wireless channel.	
Channel	Select the channel bandwidth:	
Bandwidth	20MHz (lower performance but less interference); or	
	Auto 40/20 MHz; or	
	Auto 80/40/20 MHz (automatically select based on	
	interference level).	
BSS	Set a Basic Service Set (BSS) rate: this is a series of rates to	
BasicRateSet	control communication frames for wireless clients.	

VI-3-4-2 Advanced

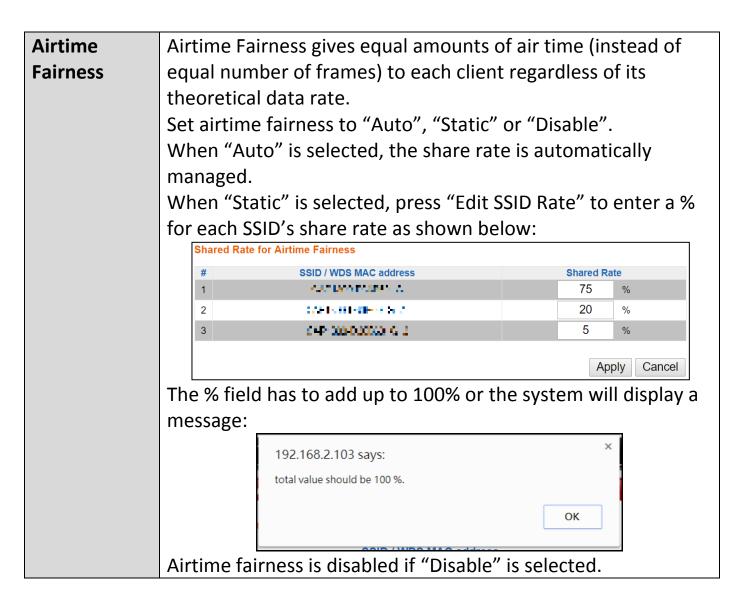
These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

Changing these settings can adversely affect the performation access point.	nce of your

802.11n ProtectionImage: Classible ClassibleDTIM Period1(1-255)RTS Threshold2347(1-2347)Fragment Threshold2346(256–2346)Multicast RateAutoTx Power100% 21 dbm <Beacon Interval100(40-1000 ms)Station Idle Timeout60(30-65535 seconds)BeamformingImage: ClassibleAirtime FairnessDisabled < Edit SSID Rate	Guard Interval	Short GI ▼		
RTS Threshold2347(1-2347)Fragment Threshold2346(256-2346)Multicast RateAutoTx Power100% 21dbm <Beacon Interval100(40-1000 ms)Station Idle Timeout60(30-65535 seconds)BeamformingImage: Enable Disable	802.11n Protection	Enable	Disable	
Fragment Threshold2346(256–2346)Multicast RateAutoTx Power100% 21dbm Beacon Interval100(40-1000 ms)Station Idle Timeout60(30-65535 seconds)BeamformingImage: Enable Disable	DTIM Period	1	(1-255)	
Multicast Rate Auto Tx Power 100% 21dbm ▼ Beacon Interval 100 Station Idle Timeout 60 Beamforming ● Enable	RTS Threshold	2347	(1-2347)	
Tx Power 100% 21dbm ▼ Beacon Interval 100 (40-1000 ms) Station Idle Timeout 60 (30-65535 seconds) Beamforming ● Enable Disable	Fragment Threshold	2346	(256–2346)	
Beacon Interval 100 (40-1000 ms) Station Idle Timeout 60 (30-65535 seconds) Beamforming Enable Disable 	Multicast Rate	Auto •		
Station Idle Timeout 60 (30-65535 seconds) Beamforming Enable Disable Image: Constraint of the second se	Tx Power	100% 21dbn	n ▼	
Beamforming Enable Disable	Beacon Interval	100	(40-1000 ms)	
	Station Idle Timeout	60	(30-65535 seconds)	
Airtime Fairness Disabled Edit SSID Rate	Beamforming	Enable	Disable	
	Airtime Fairness	Disabled ▼	Edit SSID Rate	

Guard	Set the guard interval. A shorter interval can improve	
Interval	performance.	
802.11n	Enable/disable 802.11n protection, which increases reliability	
Protection	but reduces bandwidth (clients will send Request to Send	
	(RTS) to access point, and access point will broadcast Clear to	
	Send (CTS), before a packet is sent from client.)	
DTIM Period	Set the DTIM (delivery traffic indication message) period value	
	of the wireless radio. The default value is 1.	
RTS	Set the RTS threshold of the wireless radio. The default value	
Threshold	is 2347.	
Fragment	Set the fragment threshold of the wireless radio. The default	
Threshold	value is 2346.	

Multicast	Set the transfer rate for multicast packets or use the "Auto"
Rate	setting.
Tx Power	Set the power output of the wireless radio. You may not
	require 100% output power. Setting a lower power output can
	enhance security since potentially malicious/unknown users in
	distant areas will not be able to access your signal.
Beacon	Set the beacon interval of the wireless radio. The default value
Interval	is 100.
Station idle	Set the interval for keepalive messages from the access point
timeout	to a wireless client to verify if the station is still alive/active.
Beamforming	Beamforming is a signal processing technique used in sensor
	arrays for directional signal transmission or reception.
	This is achieved by combining elements in an antenna array in
	such a way that signals at particular angles experience
	constructive interference while others experience destructive
	interference. Beamforming can be used at both the
	transmitting and receiving ends in order to achieve spatial
	selectivity. The improvement compared with omnidirectional
	reception / transmission is known as the directivity of the
	array.



The access point provides various security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

It's essential to configure wireless security in order to prevent unauthorised access to your network.

SID	CA(1)206-DC2DC0_A ×	
Broadcast SSID	Enable v	
Wireless Client Isolation	Disable v	
802.11k	Disable v	
Load Balancing	100 /100	
Authentication Method	No Authentication ▼	
Authentication Method Additional Authentication	No Authentication No additional authentication	
	No additional authentication	
Additional Authentication GHz Wireless Advanced Set	No additional authentication	
Additional Authentication GHz Wireless Advanced Set mart Handover Settings	No additional authentication	

SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will
	be visible to clients as an available Wi-Fi network. When
	disabled, the SSID will not be visible as an available Wi-Fi
	network to clients – clients must manually enter the SSID in
	order to connect. A hidden (disabled) SSID is typically more
	secure than a visible (enabled) SSID.

Wireless Client	Enable or disable wireless client isolation. Wireless client
Isolation	isolation prevents clients connected to the access point from communicating with each other and improves security.
	Typically, this function is useful for corporate environments or
	public hot spots and can prevent brute force attacks on clients'
	usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected
	to an SSID. Set a load balancing value (maximum 100).
Authentication	Select an authentication method from the drop down menu
Method	and refer to the appropriate information in vI-3-3-3 Security for
	your method.

Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

Please refer back to VI-3-3-3 **Security** for more information on authentication and additional authentication types.

Wireless Distribution System (WDS) can bridge/repeat access points together in an extended network. WDS settings can be configured as shown below.

When using WDS, configure the IP address of each access point to be in the same subnet and ensure there is only one active DHCP server among connected access points, preferably on the WAN side.

WDS must be configured on each access point, using correct MAC addresses. All access points should use the same wireless channel and encryption method.

5GHz WDS Mode	
WDS Functionality	Disabled •
Local MAC Address	80:1F:02:F1:96:8B
WDS Peer Settings	
WDS #1	MAC Address
WDS #2	MAC Address
WDS #3	MAC Address
WDS #4	MAC Address
WDS VLAN	
VLAN Mode	Untagged Port (Enter at least one MAC address.)
VLAN ID	1
Encryption method	
Encryption	None (Enter at least one MAC address.)
	Apply Reset

5GHz WDS Mode				
WDS	Select "WDS with AP" to use WDS with access point or "WDS			
Functionality	Dedicated Mode" to use WDS and also block communication			
	with regular wireless clients. When WDS is used, each access			
	point should be configured with corresponding MAC			
	addresses, wireless channel and wireless encryption method.			
Local MAC	Displays the MAC address of your access point.			
Address				

WDS Peer Settings		
WDS #	Enter the MAC address for up to four other WDA devices you	
	wish to connect.	

WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to "Untagged Port" or "Tagged Port".
VLAN ID	Specify the WDS VLAN ID when "Untagged Port" is selected above.

WDS Encryption		
Encryption	Select whether to use "None" or "AES" encryption and enter a	
	pre-shared key for AES with 8-63 alphanumeric characters.	

VI-3-4-5 Guest Network

Enable / disable guest network to allow clients to connect as guests.

Guest Network		
Guest Network	Enable Disable	
		Apply Cancel

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the compatible device or from within the compatible device's firmware / configuration interface (known as PBC or "Push Button Configuration"). When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. "PIN code WPS" is a variation of PBC which includes the additional use of a PIN code between the two devices for verification.

Please refer to manufacturer's instructions for your other WPS device.

WPS	Enable	
Apply		
WPS		
Product PIN	58327142 Generate PIN	
Push-button WPS	Start	
WPS by PIN	Start	
WPS Security		
WPS Status	Not Configured Release	

WPS	Check/uncheck this box to enable/disable WPS functionality.
	Press "Apply" to apply the settings.
	WPS must be disabled when using MAC-RADIUS
	authentication (see VI-3-6 RADIUS).

Press "Apply" to apply the configuration.

WPS	
Product PIN	Displays the WPS PIN code of the device, used for PIN code
	WPS. You will be required to enter this PIN code into another
	WPS device for PIN code WPS. Click "Generate PIN" to
	generate a new WPS PIN code.
Push-Button	Click "Start" to activate WPS on the device for approximately
WPS	2 minutes.
WPS by PIN	Enter the PIN code of another WPS device and click "Start" to
	attempt to establish a WPS connection. WPS function will last
	for approximately 2 minutes.

WPS Security	
WPS Status	WPS security status is displayed here. Click "Release" to clear
	the existing status.

RADIUS VI-3-6

The RADIUS menu allows you to configure the device's external RADIUS server settings.

A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

The device can utilize a primary and a secondary (backup) external RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz).



To use RADIUS servers, go to "Wireless Settings" → "Security" **and select** $\overset{\bullet}{\longrightarrow}$ "MAC RADIUS Authentication" \rightarrow "Additional Authentication" and select "MAC RADIUS Authentication" (see VI-3-3-3 or VI-3-4-3).

VI-3-6-1 RADIUS Settings

Configure the RADIUS server settings for 2.4GHz and 5GHz. Each frequency can use an internal or external RADIUS server.

RADIUS Server (2	2.4GHz)	
	Primary RADIUS Server	
RADIUS Type	Internal • External	
RADIUS Server		
Authentication Port	1812	
Shared Secret		
Session Timeout	3600 second(s)	
Accounting	Enable Disable	
Accounting Port	1813	
	Secondary RADIUS Server	
	Internal • External	
RADIUS Server	1812	
Authentication Port	1012	
Shared Secret	3600 second(s)	
Session Timeout		
Accounting	Enable Disable	
Accounting Port	1813	
RADIUS Server (5	5GHz)	
	Primary RADIUS Server	
RADIUS Type	Internal 🖲 External	
RADIUS Server		
Authentication Port	1812	
Shared Secret		
Session Timeout	3600 second(s)	
Accounting	Enable Disable	
Accounting Port	1813	
	Secondary RADIUS Server	
RADIUS Type	Internal • External	
RADIUS Server		
Authentication Port	1812	
Shared Secret		
Session Timeout	3600 second(s)	
Accounting	Enable Disable	
Accounting Port	1813	
3		
		Apply Cancel

RADIUS Type	Select "Internal" to use the access point's built-in RADIUS
	server or "external" to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication	Set the UDP port used in the authentication protocol of the
Port	RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in
	length. This should match the "MAC-RADIUS" password used
	in vi-3-3-3 or vi-3-4-3.
Session	Set a duration of session timeout in seconds between 0 –
Timeout	86400.
Accounting	Enable or disable RADIUS accounting.
Accounting	When accounting is enabled (above), set the UDP port used
Port	in the accounting protocol of the RADIUS server. Value must
	be between 1 – 65535.

Internal Server VI-3-6-2

The access point features a built-in RADIUS server which can be configured as shown below used when "Internal" is selected for "RADIUS Type" in the "Wireless Settings" \rightarrow "RADIUS" \rightarrow "RADIUS Settings" menu.



To use RADIUS servers, go to "Wireless Settings" → "Security" **and select** $\overset{\circ}{\longrightarrow}$ "MAC RADIUS Authentication" \rightarrow "Additional Authentication" and select "MAC RADIUS Authentication" (see VI-3-3-3 & VI-3-4-3).

Internal Server			
Internal Server	Enable		
EAP Internal Authentication	▼		
EAP Certificate File Format	PKCS#12(*.pfx/*.p12)		
EAP Certificate File	Upload		
Shared Secret			
Session-Timeout	3600	second(s)	
Termination-Action	 Reauthenication (RAD Not-Reauthenication (I Not-Send 		
		Apply Can	cel

Internal Server	Check/uncheck to enable/disable the access point's internal
	RADIUS server.
EAP Internal	Select EAP internal authentication type from the drop down
Authentication	menu.
EAP Certificate	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
File Format	
EAP Certificate	Click "Upload" to open a new window and select the location
File	of an EAP certificate file to use. If no certificate file is
	uploaded, the internal RADIUS server will use a self-made
	certificate.
Shared Secret	Enter a shared secret/password for use between the internal
	RADIUS server and RADIUS client. The shared secret should
	be 1 – 99 characters in length. This should match the

	"MAC-RADIUS" password used in vI-3-3-3 or vI-3-4-3.	
Session	Set a duration of session timeout in seconds between 0 –	
Timeout	86400.	
Termination	Select a termination-action attribute:	
Action	Reauthentication: sends a RADIUS request to the access	
	point; or,	
	Not-Reauthentication: sends a default termination-action	
	attribute to the access point; or	
	Not-Send: no termination-action attribute is sent to the	
	access point.	

VI-3-6-3 RADIUS Accounts

The internal RADIUS server can authenticate up to 256 user accounts. The "RADIUS Accounts" page allows you to configure and manage users.

RADIUS Accounts (Max: 256 users)			
User Name				
Example: USER1, USE	R2, USER3, USER4			
			1	
Add Reset				
User Registration L	ist			
Select	User Name	Password		Customize
	1	No user entries		
			Delete Se	Delete All

Enter a username in the box below and click "Add" to add the username.

User Registra	tion List		
Select	User Name	Password	Customize
	USER1	Not Configured	Edit
		Delet	te Selected Delete All

Select "Edit" to edit the username and password of the RADIUS account:

Edit User Registration	List	
User Name	USER1	(4-16Characters)
Password		(6-32Characters)

User Name	Enter the user names here, separated by commas.
Add	Click "Add" to add the user to the user registration list.
Reset	Clear text from the user name box.

Select	Check the box to select a user.
User Name	Displays the user name.
Password	Displays if specified user name has a password (configured) or
	not (not configured).
Customize	Click "Edit" to open a new field to set/edit a password for the
	specified user name (below).

Delete	Delete selected user from the user registration list.
Selected	
Delete All	Delete all users from the user registration list.

VI-3-7 MAC Filter

MAC filtering is a security feature that can help to prevent unauthorized users from connecting to your access point.

This function allows you to define a list of network devices permitted to connect to the access point. Devices are each identified by their unique MAC address. If a device which is not on the list of permitted MAC addresses attempts to connect to the access point, it will be denied.



To enable MAC filtering, go to "Wireless Settings" \rightarrow "2.4G Hz 11bgn" \rightarrow "Security" \rightarrow "Additional Authentication" and select "MAC Filter" (see VI-3-3-3 or VI-3-4-3).

The MAC address filtering table is displayed below:

Add MAC Addresses		
Enable Wireless Access Control Wireless Access Control Mode	 Enable Disable Blacklist 	
Apply		
Add MAC Addresses		
Add Reset		

Add MAC	Enter a MAC address of computer or network device manually
Address	e.g. 'aa-bb-cc-dd-ee-ff' or enter multiple MAC addresses
	separated with commas, e.g.
	'aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg'
Add	Click "Add" to add the MAC address to the MAC address
	filtering table.
Reset	Clear all fields.

MAC address entries will be listed in the "MAC Address Filtering Table". Select an entry using the "Select" checkbox.

MAC Address Filtering	Table
Select	MAC Address
	No MAC Address entries.
	Delete Selected Delete All Export

Select	Delete selected or all entries from the table.	
MAC Address	The MAC address is listed here.	
Delete	Delete the selected MAC address from the list.	
Selected		
Delete All	Delete all entries from the MAC address filtering table.	
Export	Click "Export" to save a copy of the MAC filtering table. A new	
	window will pop up for you to select a location to save the file.	

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard, which provides Quality of Service (QoS) features to IEE 802.11 networks. WMM prioritizes traffic according to four categories: background, best effort, video and voice.

		ameters of Access F		
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	6	3	0
Video	3	4	1	94
Voice	2	3	1	47
	CWMin	CWMax	AIFSN	TxOP
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	10	3	0
Video	3	4	2	94
Voice	2	3	2	47

Configuring WMM consists of adjusting parameters on queues for different categories of wireless traffic. Traffic is sent to the following queues:

Background	Low Priority	High throughput, non time sensitive bulk data e.g. FTP
	Medium Priority	Traditional IP data, medium throughput and delay.
Video	High Priority	Time sensitive video data with minimum time delay.
Voice	High Priority	Time sensitive data such as VoIP and streaming media with minimum time delay.

Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can be adjusted further manually:

CWMin	Minimum Contention Window (milliseconds): This value is input to the initial random backoff wait time algorithm for retry of a data frame transmission. The backoff wait time will be generated between 0 and this value. If the frame is not sent, the random backoff value is doubled until the value reaches the number defined by CWMax (below). The CWMin value must be lower than the CWMax value. The contention window scheme helps to avoid frame collisions and determine priority of frame transmission. A shorter window has a higher probability (priority) of transmission.
CWMax	Maximum Contention Window (milliseconds): This value is the
	upper limit to random backoff value doubling (see above).
AIFSN	Arbitration Inter-Frame Space (milliseconds): Specifies additional time between when a channel goes idle and the AP/client sends data frames. Traffic with a lower AIFSN value has a higher priority.
ТхОР	Transmission Opportunity (milliseconds): The maximum interval of time an AP/client can transmit. This makes channel access more efficiently prioritized. A value of 0 means only one frame per transmission. A greater value means higher priority.

VI-3-9 Schedule

The schedule feature allows you to automate the wireless network for the specified time ranges. Wireless scheduling can save energy and increase the security of your network.

Check/uncheck the box "Enable" and select "Apply" to enable/disable the wireless scheduling function.

Enable the wireless network during the following schedules.					
This functio	on will not work unti	il date and time are set.	Settings		
Schedule		Enable			
Apply					
Schedule L	.ist				
#	SSID	Day of Week	Time	Select	
		No schedule entries			
Add Edit Delete Selected Delete All					

- **1.** Select "Add" to add a schedule.
- 2. Settings page will be shown if "Continue" is selected: Check/uncheck the box of the desired SSID network, day of schedule and select the Start Time and End Time (using the dropdown menu). Select "Apply" to apply the settings, or "Cancel" to forfeit the schedule.

Settings						
	2.4GHz SS	ID		-		
	- 200 PARA	100 C		5	GHz SSID	
					NAMES OF COMPANY	De la compañía de la
	- 10 March 10	an ta				
Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
Start Time	00 •: 00 •	End Time	00 • : 00 •	•		
					Арр	ly Cancel

Schedules will be shown in the Schedule List as exemplified below:

Sched	ule List			
#	SSID	Day of Week	Time	Select
1	an ann an Aire. An Ann an Aire	Mon.	07:00-16:00	
		Add	Edit Delete Selected D	elete All

3. Select "Add" to add more schedules; or Check the box of currently available schedule, select "Edit" to edit, or select "Delete Selected" to delete; or Select "Delete All" to delete all schedules.

VI-3-10 Traffic Shaping

Traffic shaping is used to optimize or guarantee performance, improve latency, or increase usable bandwidth for some kinds of packets by delaying other kinds.

Check the checkbox to enable traffic shaping, specify the down link and up link values, and click "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

Traffic Shaping for ssid(2.4GHz)				
Enable Unlimited : 0 Mbps Down Link/Up Link Maximum : 1024 Ml	ops			
SSID	Dov	vn Link	Up	Link
-F1968A_G	0	Mbps	0	Mbps
F1968A_G_2	0	Mbps	0	Mbps
F1968A_G_3	0	Mbps	0	Mbps
F1968A_G_4	0	Mbps	0	Mbps
F1968A_G_5	0	Mbps	0	Mbps
F1968A_G_6	0	Mbps	0	Mbps
F1968A_G_7	0	Mbps	0	Mbps
F1968A_G_8	0	Mbps	0	Mbps
F1968A_G_9	0	Mbps	0	Mbps
F1968A_G_10	0	Mbps	0	Mbps
F1968A_G_11	0	Mbps	0	Mbps
F1968A_G_12	0	Mbps	0	Mbps
F1968A_G_13	0	Mbps	0	Mbps
F1968A_G_14	0	Mbps	0	Mbps
F1968A_G_15	0	Mbps	0	Mbps
F1968A_G_16	0	Mbps	0	Mbps

Traffic Shaping for ssid(5GHz)

Enable

Unlimited : 0 Mbps

Down Link/Up Link Maximum : 1024 Mbps

SSID	Dow	n Link	Up	Link
F1968A_A	0	Mbps	0	Mbps
F1968A_A_2	0	Mbps	0	Mbps
F1968A_A_3	0	Mbps	0	Mbps
F1968A_A_4	0	Mbps	0	Mbps
F1968A_A_5	0	Mbps	0	Mbps
F1968A_A_6	0	Mbps	0	Mbps
F1968A_A_7	0	Mbps	0	Mbps
F1968A_A_8	0	Mbps	0	Mbps
F1968A_A_9	0	Mbps	0	Mbps
F1968A_A_10	0	Mbps	0	Mbps
F1968A_A_11	0	Mbps	0	Mbps
F1968A_A_12	0	Mbps	0	Mbps
F1968A_A_13	0	Mbps	0	Mbps
F1968A_A_14	0	Mbps	0	Mbps
F1968A_A_15	0	Mbps	0	Mbps
F1968A_A_16	0	Mbps	0	Mbps

Apply Cancel

VI-3-11 Bandsteering

Band steering detects clients capable of 5GHz operation and steers them there to make the more crowded 2.4 GHz band available for clients only capable of connecting to 2.4GHz band. This helps improve end user experience by reducing channel utilization, especially in high density environments.

Bandsteering	
Bandsteering	● Off ● 5G First ● Balanced ● User Define
	Apply Cancel

Bandsteering		
Bandsteering	Off	─ 5G First ─ Balanced ● User Define
2.4GHz Overload Threshold	0	(0-100%, suggest:70) Channel utilization percentage
5GHz Overload Threshold	0	(0-100%, suggest:70) Channel utilization percentage
Min RSSI	-95 🔻	dB

Information Network Settings Wireless Settings Management Advanced Operation Mode (Configurable for AP Mode only)

VI-4-1 Admin

You can change the password used to login to the browser-based configuration interface here. It is advised to do so for security purposes.

If you change the administrator password, please make a note of the new password. In the event that you forget this password and are unable to login to the browser based configuration interface, see 1-5 Reset for how to reset the access point.

Account to Manage This Device				
Administrator Name	admin			
Administrator Password	••••	(4-32Characters)		
Administrator Password	••••	(Confirm)		
Apply				

Account to Manage This Device				
Administrator	:or Set the access point's administrator name. This is used to log			
Name	in to the browser based configuration interface and must be			
	between 4-16 alphanumeric characters (case sensitive).			
Administrator	Set the access point's administrator password. This is used to			
Password	log in to the browser based configuration interface and must			
	be between 4-32 alphanumeric characters (case sensitive).			

Press "Apply" to apply the configuration.

Advanced Settings

Product Name	AP801F02F1968A	
HTTP Port	80	(80, 1024-65535)
HTTPS Port	443	(443, 1024-65535)
Management Protocol	 HTTP HTTP TELN SSH SNMF 	'S ET
Login Timeout	5 ▼ (n	nins)
SNMP Version	v1/v2c	T
SNMP Get Community	public	
SNMP Set Community	private	
SNMP V3 Name	admin	
SNMP V3 Password	••••	
SNMP Trap	Disable	d ▼
SNMP Trap Community	public	
SNMP Trap Manager		

Advanced Settin	gs	
Product Name	1e Edit the product name according to your preference	
	consisting of 1-32 alphanumeric characters. This name is used	
	for reference purposes.	
Management	Check/uncheck the boxes to enable/disable specified	
Protocol	management interfaces (see below). When SNMP is enabled,	
	complete the SNMP fields below.	
SNMP Version	Select SNMP version appropriate for your SNMP manager.	
SNMP Get	Enter an SNMP Get Community name for verification with the	
Community	SNMP manager for SNMP-GET requests.	
SNMP Set	Enter an SNMP Set Community name for verification with the	
Community	SNMP manager for SNMP-SET requests.	
SNMP Trap	Enable or disable SNMP Trap to notify SNMP manager of	
	network errors.	

SNMP Trap	Enter an SNMP Trap Community name for verification with
Community	the SNMP manager for SNMP-TRAP requests.
SNMP Trap	Specify the IP address or sever name (2-128 alphanumeric
Manager	characters) of the SNMP manager.

HTTP

Internet browser HTTP protocol management interface

TELNET

Client terminal with telnet protocol management interface

SNMP

Simple Network Management Protocol. SNMPv1, v2 & v3 protocol supported. SNMPv2 can be used with community based authentication. SNMPv3 uses user-based security model (USM) architecture.

Press "Apply" to apply the configuration.

VI-4-2 Date and Time

Configure the date and time settings of the access point here. The date and time of the device can be configured manually or can be synchronized with a time server.

Date and Time Settings	
Local Time	Year Jan Month 1 Day 0 Image: Hours 00 Image: Minutes 00 Image: Seconds
Acquire Current Time	from Your PC
NTP Time Server	
Use NTP	Enable
Auto Daylight Saving	Enable
Server Name	User-Defined •
Update Interval	24 (Hours)
Time Zone	
Time Zone	(GMT+08:00) Taipei, Taiwan ▼
	Apply Cancel

Date and Time Settings		
Local Time	Set the access point's date and time manually using the drop	
	down menus.	
Acquire	Click "Acquire Current Time from Your PC" to enter the	
Current Time	required values automatically according to your computer's	
from your PC	current time and date.	

NTP Time Server		
Use NTP	The access point also supports NTP (Network Time Protocol)	
	for automatic time and date setup.	
Server Name	Enter the host name or IP address of the time server if you	
	wish.	
Update	Specify a frequency (in hours) for the access point to	
Interval	update/synchronize with the NTP server.	

Time Zone	
Time Zone	Select the time zone of your country/region. If your country/region is not listed, please select another country/region whose time zone is the same as yours.

The system log can be sent to a server.

Syslog Server Settings		
Transfer Logs	Enable Syslog Server	
Syslog E-mail Settings		
E-mail Logs		
E-mail Subject		
SMTP Server Address		
SMTP Server Port		
Sender E-mail		
Receiver E-mail		
Authentication	Disable •	
		Apply Cancel

Syslog Server Settings	
Transfer Logs	Check the box to enable the use of a syslog server.
	Enter a host name, domain or IP address for the server,
	consisting of up to 128 alphanumeric characters.

Syslog E-mail Settings		
E-mail Logs	Check the box to enable/disable e-mail logs.	
E-mail Subject	Specify the subject line of log emails.	
SMTP Server	Specify the SMTP server address used to send log emails.	
Address		
SMTP Server	Specify the SMTP server port used to send log emails.	
Port		
Sender E-mail	Specify the sender email address.	
Receiver	Specify the email to receive log emails.	
E-mail		
Authentication	Disable or select authentication type: SSL or TLS. When using	
	SSL or TLS, enter the username and password.	

The access point includes a built-in ping test function. Ping is a computer network administration utility used to test whether a particular host is reachable across an IP network and to measure the round-trip time for sent messages.

Ping Test	
Destination Address	Execute
Result	

Destination Address	Enter the address of the host.
Execute	Click execute to ping the host.

The access point features a built-in buzzer which can sound on command using the "I'm Here" page. This is useful for network administrators and engineers working in complex network environments to locate the access point.

Duration of Sound
Duration of Sound 10 (1-300 seconds)



Duration of	Set the duration for which the buzzer will sound when the
Sound	"Sound Buzzer" button is clicked.
Sound Buzzer	Activate the buzzer sound for a duration specified above.

Information Network Settings Wireless Settings Management Advanced Operation Mode

VI-5-1 LED Settings

The access point's LEDs can be manually enabled or disabled according to your preference.

LED Settings		
Power LED	● On ● Off	
Diag LED	• On Off	
		Apply Concol
		Apply Cancel

Power LED	Select on or off.
Diag LED	Select on or off.

VI-5-2 Update Firmware

The "Firmware" page allows you to update the firmware of the system. Updated firmware versions often offer increased performance and security, as well as bug fixes. Download the latest firmware from the Edimax website.

Firmware Location			
Update firmware from	In a file on your PC		
Update Firmware from PC			
Firmware Update File	Choose File No file chosen		
Update			



Do not switch off or disconnect the access point during a firmware upgrade, as this could damage the device.

Firmware	Click "Choose File" to upload firmware from your local computer.
Location	

VI-5-3 Save / Restore Settings

The device's "Save / Restore Settings" page enables you to save / backup the device's current settings as a file to your local computer, and restore the device to previously saved settings.

Save/Restore Method	
Using Device	Using your PC
Save Settings to PC	
Save Settings	Encrypt the configuration file with a password.
Save	
Restore Settings from PC	
Restore Settings	Choose File No file chosen Open file with password.
Restore	

Save Settings to PC			
Save Settings	Encryption : If you wish to encrypt the configuration file with		
	a password, check the "Encrypt the configuration file with a		
	password" box and enter a password.		
	Click "Save" to save current settings. A new window will		
	open to allow you to specify a location to save to.		

Restore Settings from PC			
Restore	Click the "Choose File" button to find a previously saved		
Settings	settings file on your computer. If your settings file is		
	encrypted with a password, check the "Open file with		
	password" box and enter the password in the following field.		
	Click "Restore" to replace your current settings.		

VI-5-4 Factory Default

If the access point malfunctions or is not responding, rebooting the device (VI-5-5 **Reboot**) maybe an option to consider. If rebooting does not work, try resetting the device back to its factory default settings. You can reset the access point back to its default settings using this feature if the reset button is not readily accessible.

This will restore all settings to factory defaults.	
	Factory Default

FactoryClick "Factory Default" to restore settings to the factoryDefaultdefault. A pop-up window will appear and ask you to confirm.



After resetting to factory defaults, please wait for the access point to reset and restart.

If the access point malfunctions or is not responding, rebooting the device may be an option to consider. You can reboot the access point remotely using this feature.

This will reboot the product. Your settings will not be changed. Click "Reboot" to reboot the product now.

Reboot

Reboot	Click "Reboot" to reboot the device. A countdown will
	indicate the progress of the reboot.

Information Network Settings Wireless Settings Management Advanced Operation Mode

The access point can function in five different modes. Set the operation mode of the access point here.

- 1. AP Mode: The device acts as a standalone access point
- 2. Repeater Mode: The device acts as a wireless repeater (also called wireless range extender) that takes an existing signal from a wireless router or wireless access point and rebroadcasts it to create a second network.
- 3. AP controller Mode: The device acts as the designated master of the AP array
- 4. Managed AP Mode: The device acts as a slave AP within the AP array.
- 5. Client Bridge Mode: The device is now a client bridge. The client bridge receives wireless signal and provides it to devices connected to the bridge (via Ethernet cable).

Operation Mode		
Operation Mode	AP Mode Image: AP Mode 	
Wireless Mode		
2.4GHz Mode	Access Point	
5GHz Mode	Access Point	
		Apply Cancel
	AP Mode Image: AP Mode 	
	AP Mode	
	Repeater Mode	
	AP Controller Mode	
	Managed AP mode	
	Client Bridge Mode	



In Managed AP mode some functions of the access point will be disabled in this user interface and must be set using Edimax Pro NMS on the AP Controller.



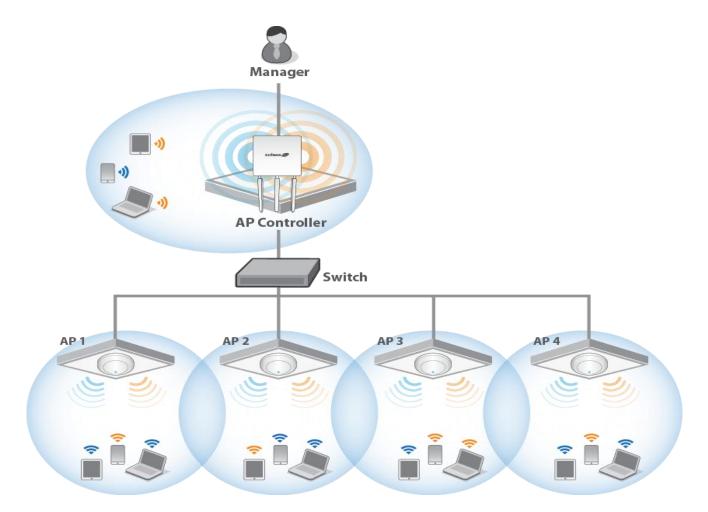
In AP Controller Mode the access point will switch to the Edimax Pro NMS user interface.

Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

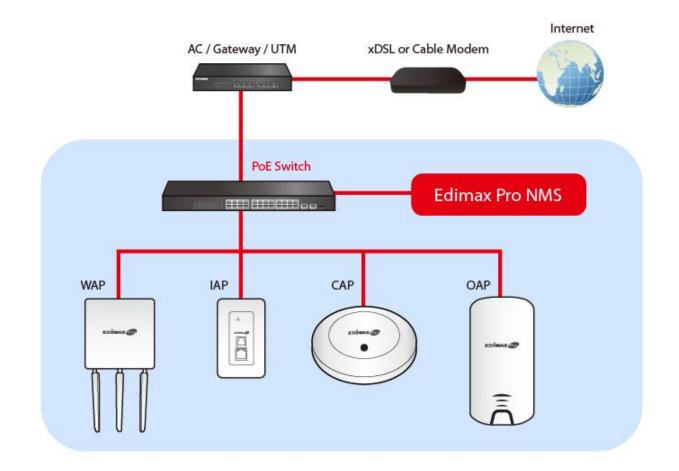
VII Product Information

Edimax Pro Network Management Suite (NMS) supports the central management of a group of access points, otherwise known as an AP Array. NMS can be installed on one access point and support up to 16 Edimax Pro access points with no additional wireless controller required, reducing costs and facilitating efficient remote AP management.

Access points can be deployed and configured according to requirements, creating a powerful network architecture which can be easily managed and expanded in the future, with an easy to use interface and a full range of functionality – ideal for small and mid-sized office environments. A secure WLAN can be deployed and administered from a single point, minimizing cost and complexity.



Edimax Pro NMS (AP Controller Mode) is simple to setup. An overview of the system is shown below:



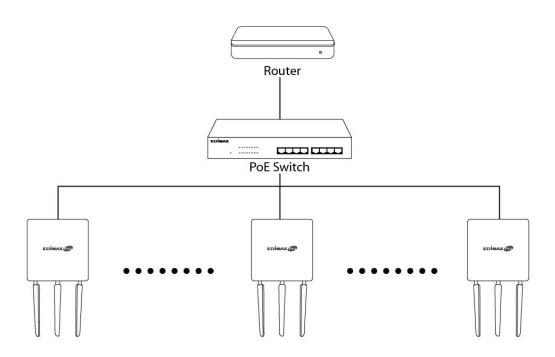
One AP (access point) is designated as the AP Controller (master) and other connected Edimax Pro APs are automatically designated as Managed APs (slaves). Using Edimax Pro NMS you can monitor, configure and manage all Managed APs (up to 16) from the single AP Controller.

Hardware Deployment VIII-1

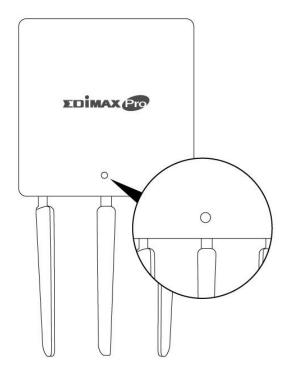


Ensure you have the latest firmware from the Edimax website for your Edimax Pro products.

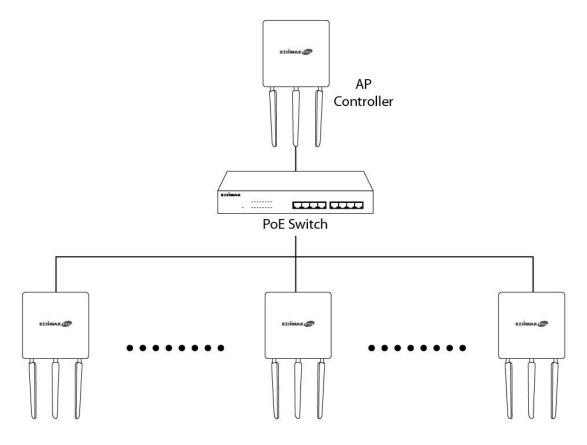
1. Connect all APs to an Ethernet or PoE switch which is connected to a gateway/router.



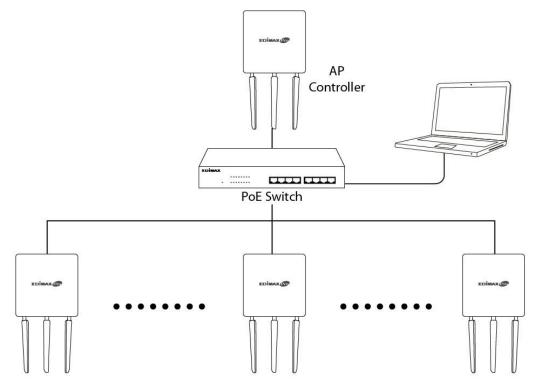
2. Ensure all APs are powered on (check their LEDs).



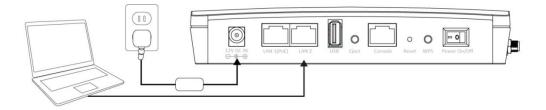
3. Designate one AP as the *AP Controller* which will manage all other connected APs (up to 16).



4. Connect a computer to the designated AP Controller using an Ethernet cable.



- Set your computer's IP address to 192.168.2.x where x is a number in the range 3 100. If you are unsure how to do this, please refer XI-1.
 Please ensure there are no other active network connections on your computer by disabling Wi-Fi and other Ethernet connections.
- **2.** Disconnect the designated AP Controller from the PoE switch and connect it to your computer via Ethernet cable.
- **3.** Connect the power adapter to the device's 12V DC port and plug the power adapter into a power supply.



- **4.** Please wait a moment for the device to start up. The device is ready when the LED is **blue**.
- 5. Enter the device's default IP address **192.168.2.2** into the URL bar of a web browser.



6. You will be prompted for a username and password. Enter the default username "**admin**" and the default password "**1234**".

Connect to 192.1	58.2.2 ? ×
R	GA
The server 192.1 password.	58.2.2 at localhost requires a username and
User name:	🖸 admin 👻
Password:	•••••
	Remember my password
	OK Cancel

7. "System Information" home screen will be shown:

EDİMAX 📴		Hor	ne Logout Global (English)
10000	Information Network Settin	gs Wireless Settings Management A	dvanced Operation Mode
Information	System Information		
> System Information	System		
> Wireless Clients	system		
	Model	2017/01/s	
> Wireless Monitor	Product Name	AP801F02F1968A	
> DHCP Clients	Uptime	0 day 00:07:24	
	System Time	2012/01/01 00:07:06	
> Log	Boot from	Internal memory	
	Firmware Version	1.8.1	
	MAC Address	80:1F:02:F1:96:8A	
	Management VLAN ID 1		
	IP Address	192.168.2.103 Refresh	
	Default Gateway	192.168.2.70	
	DNS	192.168.2.70	
	DHCP Server	192.168.2.70	
	Wired LAN Port Setting		
	Wired LAN Port	Status	VLAN Mode/ID
	LAN1	Connected (100 Mbps Full-Duplex)	Untagged Port / 1
	LAN2	Disconnected ()	Untagged Port / 1

- **8.** By default, the device is in **AP Mode**.
- **9.** Go to "Operation Mode" to select AP Controller Mode.

WAP1750	Information Network Settings	Wireless Settings Managemer	nt Advanced Operation Mode
Operation Mode Operation Mode	Operation Mode		
	Operation Mode		
	Operation Mode	AP Mode •]
	Wireless Mode		
	2.4GHz Mode 5GHz Mode	Access Point ▼ Access Point ▼	
			Apply Cancel
Operation Mode			
Operation Mode	AP Mode	V	
[AP Mode Repeater M AP Control Managed A Client Bridg	ller Mode AP mode	

- **10.** Once selected, press "Apply" to apply the settings. Wait for the device to reboot.
- **11.** Edimax Pro NMS includes a wizard to quickly setup the SSID & security for Managed APs. Go back to the web user interface, locate and click "Wizard" in the top right corner to begin the wizard.



12. Follow the on-screen instructions to complete **Steps 1-6** and click **"Finish"** to save the settings.

Step 1 2 3 4 5 6 Finish	Step 1 2	3 4 5 6 Finish
Installation	Local LAN-side IP Addre	\$\$
Before start, please power on the managed APs and plug	IP Address Assignment	DHCP Client ~
into the same Ethernet network with this AP Controller.	IP Address	192.168.2.2
This Setup Wizard will guide you through a basic procedure to	Subnet Mask	255.255.2
configure AP Controller system.	Default Gateway	From DHCP ~
	Primary DNS Address	From DHCP ~
Next >> Cancel	Secondary DNS Address	From DHCP ~
		<< Back Next >> Cancel
Step 1 2 3 4 5 6 Finish	Step 1 2	3 4 5 6 Finish
Date and Time Settings	Account to Manage This	Device
	Administrator Name	admin
Local Time		(6-32 Characters)
0 ~ Hours 00 ~ Minutes 00 ~ Seconds	Administrator Password	••••• (Confirm)
Acquire Current Time from Your PC		
		<< Back Next >> Cancel
NTP Time Server		
Use NTP Enable		
Saving Enable		
Server Name User-Defined ~		
Update Interval 24 (Hours)		
Time Zone		
Time Zone (GMT+08:00) Taipei, Taiwan		
Time Zone (GMT+08:00) Taipei, Taiwan v		
<< Back Next >> Cancel		

Step 1 2 3	4 5 6	Finish	Step '	1 2	3 4 5	6	Finish
Select Free AP(s)			2.4GHz Se	ettinas			
			SSID				
	Match whole words		Security Ke	ey			
MAC Address Device Name Image: The second sec		IP Address Statu 192.168.2.101 O		ork O Enable Disa	able		
			Guest SSI				
Managed AP(s)			Security Ke	≥y			
Search	Match whole words						
MAC Address Device Name		P Address Status	5GHz Sett	ings			
No	Access Point List		Clone 2.4	4GHz Settings			
Rescan	<< Back	Next >> Can	cel				
			Security Ke				
			Guest Netw	ork O Enable Disa	able		
			Guest SSI				
			Security Ke	≥y			
					<< Ba	nck Next >>	> Cancel
	Step 1	2 3	4 5	6	Finish		
-							
	Confirmati	on					
	Comman						
	Management IP						
	IP Address Assignme	ent DHCP	Client				
	Date and Time						
	Local Time	2012/0	1/01 00:00:00				
	Time Zone	(GMT+	08:00) Taipei, Taiwan				
	Administrator Ac	count					
	Administrator Name	admin					
	Managed AP(s)						
	MAC Address 74:DA:38:1D:26:4E	Device Name AP74DA381D264E	Model WAP1200	IP Address 192.168.2.101	Status		
	11.07.00.10.20.1E		11200	102.100.2.101			
	2.4GHz Settings						
	SSID		100 Bar				
	Security Key	123456	378				
	ECU- Cottingo						
	5GHz Settings						
	SSID		2010 - C				
	Security Key	123456	378				
			<< B	ack Finish	Cancel		

If any of your Managed APs cannot be found, reset it to its factory default settings.

13. Your AP Controller & Managed APs should be fully functional. Use the top menu to navigate around Edimax Pro NMS.

Dashboard Zone Plan NMS Monitor NMS Settings Local Network Local Settings Toolbox

Use **Dashboard**, **Zone Plan**, **NMS Monitor** & **NMS Settings** to configure Managed APs.

Use *Local Network & Local Settings* to configure your AP Controller.

Use **Toolbox** to diagnose network status including *Ping*, *Traceroute*, and *IP Scan*.

The top menu features 7 panels: *Dashboard, Zone Plan, NMS Monitor, NMS Settings, Local Network, Local Settings & Toolbox.*

Dashboard



The **Dashboard** panel displays an overview of your network and key system information, with quick links to access configuration options for Managed APs and Managed AP groups. Each panel can be refreshed, collapsed or moved according to your preference.

										Auto Re	fresh Time 🗆	1 minute 🔍	30 seconds 🔘	Disable
APs Information	© –	Managed	AP											C
	0 1	Search				M	atch whole wo	ords						
Managed Ad	ctive Offline													
0		📄 Index 🔺	MAC Address	Device Name A	Model 🔺	IP Address	2.4G Channel	45G Channel 4	 Clients A 	2.4G Domain	▲5G Domain ▲	🖌 Status 🔺	Act	on
Discovered		1	74:DA:38:1D:26: 4E	AP74DA381D26 4E	WAP1200	<u>192.168.2.101</u>	N/A	N/A	0	FCC	FCC	0	<u>8</u> 73	
System Informatio	on CO													
Product Name	WAP1750													-
Host Name	AP801F02F1968A	Managed	AP Group											(0)
MAC Address	80:1F:02:F1:96:8A													
IP Address	192.168.2.2	Search				— M	atch whole wo	ords						
Firmware Version System Time	1.8.1 2012/01/01 19:53:06		iroup Name	MAC Add		Device Name	Mo	del I	P Address	Clients	\$	atus	Actio	
Uptime	0 day 19:53:25	System D		INAC AUG	633	Device Name	inio	uer r	r Address	Glients	51	atus	Actio	
CPU Usage	3%	System D	relatit (0)											(
Memory / Cache Us								Empty						
age	63%	Wizard A	P Group 2 (1)	•										(
484														
		Active Cli												
		Active ch	ients											
Devices Informati	on CO													
Device	Number	Search				M	atch whole wo	ords						
Device Access Points	Number 1	P	Client MAC Add	AP MAC Addres										
Device	Number	Search	Client MAC Add	AP MAC Addres	v		atch whole wo		Signal(%	Connected	Time Idle Tim	ne Tx(KB)	Rx(KB)	Vendor

Zone Plan

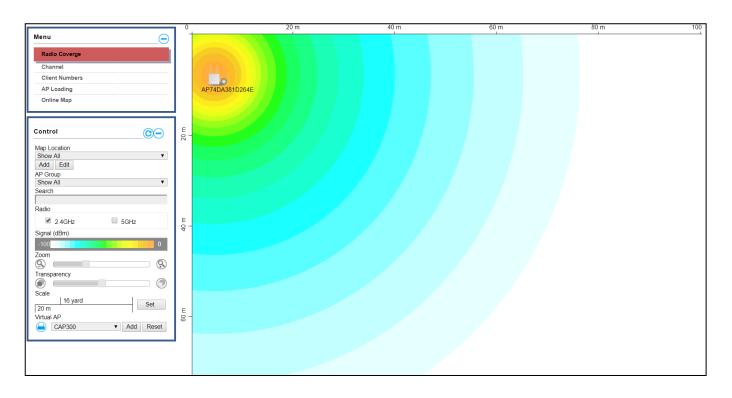
Dashboard

Zone Plan

Local Settings

Toolbox

Zone Plan displays a customizable live map of Managed APs for a visual representation of your network coverage. Each AP icon can be moved around the map, and a background image can be uploaded for user-defined location profiles using NMS Settings \rightarrow Zone Edit. Options can be configured using the menu on the right side and signal strength is displayed for each AP.



NMS Monitor

Dashboard Zone Plan NMS Monitor NMS Settings Local Network Local Settings Toolbox

The **NMS Monitor** panel provides more detailed monitoring information about the AP Array than found on the Dashboard, grouped according to categories in the menu down the left side.

Access Point	Managed Al									
Managed AP										
Managed AP Group	Search				Match whole wo	as				
WLAN	Index 🔺 1	MAC Address 🗻 74:DA:38:1D:26:4E	Device Name AP74DA381D264E	Model 🔺 WAP1200	IP Address 🔺 192.168.2.101	2.4G Channel 🔺 N/A	5G Channel 🗻 N/A	Clients 🔺 0	Status 🔺	Action
Active WLAN										000000
Active WLAN Group										
Clients										
Active Clients										
Users										
Active Users										
Users Log										
Rogue Devices										
Information										
All Events/Activities										
AP Monitoring										
SSID Overview										

NMS Settings

Dashboard Zone Plan NMS Monitor NMS Settings Local Network Local Settings Toolbox

NMS Settings provides extensive configuration options for the AP Array. You can manage each access point, assign access points into groups, manage WLAN, RADIUS & guest network settings as well as upgrade firmware across multiple access points. The Zone Plan can also be configured using "Zone Edit".

Access Point	Access	Point										
WLAN	Search				🗆 Ma	tch whole w	vords					
RADIUS		Index 🔺	MAC Address 🔺	Device Name 🔺	Model 🔺	AP Grou	up 🔺 2.4G Channel 🔺	5G Channel 🔺	2.4G Tx Power	▲ 5G Tx Power	Status	Action
Access Control		1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	Wizard AP 0	Group N/A	N/A	N/A	N/A	0	0
Guest Network						2						
Users	Refr	esh Ed	lit Delete Selecte	ed Delete All								
Guest Portal												
Zone Edit		Point Gr	oup									
Schedule	Search					tch whole w	vords					
Smart Roaming			Group Name	AP Mem			2.4G Guest Network Profile	5G Guest Network	Profile RADIU	IS Profile Acco	ss Control	Profile
Device Monitoring			System Default	0	Disable	ed Disabled	Disabled	Disabled	Dis	abled	Disabled	
Firmware Upgrade			Wizard AP Group 2	1		d Wizard N WLAN	Disabled	Disabled	Dis	abled	Disabled	
Advanced					2.4G		Disubica	Disabled	00	abica	Disabled	
System Security					Group	1 Group 2						
Date and Time	Add	Edit	Clone Delete S	Selected Delete	All							
Google Maps	Access	Point Set	ttings									
	Auto	pprove	• E	nable 🔍 Disable								
	Appl	1										

Local Network



Local Network settings are for your AP Controller. You can configure the IP address and DHCP server of the AP Controller in addition to 2.4GHz & 5Ghz Wi-Fi and security, with WPS, RADIUS server, MAC filtering and WMM settings also available.

Network Settings	LAN-side IP Address	
> LAN-side IP Address		
LAN Port Settings	IP Address Assignment	DHCP Client
VLAN	IP Address	192.168.2.2
	Subnet Mask	255.255.255.0
> 2.4GHz 11bgn	Default Gateway	From DHCP
Basic	Primary DNS Address	From DHCP 0.0.0
Advanced	Secondary DNS Address	From DHCP V 0.0.0
Security		
WDS		
Guest Network		Apply
> 5GHz 11ac 11an		
Basic		
Advanced		
Security		
WDS		
Guest Network		
> WPS		
> RADIUS		
RADIUS Settings		
Internal Server		
RADIUS Accounts		
> MAC Filter		
> WMM		
> Schedule		

Local Settings

Zone Plan

NMS Monitor

Dashboard

Local Settings are for your AP Controller. You can set the operation mode and view network settings (clients and logs) specifically for the AP Controller, as well as other management settings such as date/time, admin accounts, firmware and reset.

NMS Settings

Local Network

Local Settings

Toolbox

> Operation Mode	Operation Mode		
 System Settings System Information 	Operation Mode	AP Controller Mode 🔻	
Wireless Clients	Wireless Mode		
Wireless Monitor			
Log	2.4GHz Mode	Access Point V	
> Management	5GHz Mode	Access Point	
Admin	Management		
Date and Time			
Syslog Server Settings	Self AP Management Mode	Disable 🔻	
Syslog E-mail Settings			
I'm Here		A	Apply Cancel
> Advanced			
LED Settings			
Update Firmware			
Save/Restore Settings			
Factory Default			
Reboot			

<u>Toolbox</u>

Dashboard	Zone Plan	NMS Monitor	NMS Settings	Local Network	Local Settings	Toolbox
Dashbuaru	ZUIIE Flatt		NWO Settings	LOCAL NELWORK	Local Settings	TOOIDOX

The Toolbox panel provides network diagnostic tools: *Ping, Traceroute,* and *IP Scan*.

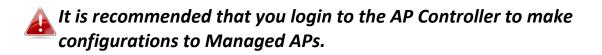
> Network Connectivity	Ping Test	
> Ping		
Trace Route	Destination Address	Execute
IP Scan	Result	

X NMS Features

Descriptions of the functions of each main panel can be found below. When using Edimax NMS, click "Apply" to save changes:

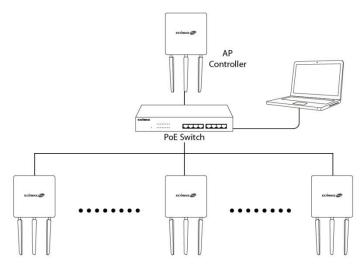


X-1 Login, Logout & Restart



<u>Login</u>

1. Connect a computer to the designated AP Controller using an Ethernet cable:



2. Open a web browser and enter the AP Controller's IP address in the address field. The default IP address is **192.168.2.2**





Your computer's IP address must be in the same subnet as the AP Controller. Refer to XI-1 Configuring your IP address for more help.



If you changed the AP Controller's IP address, or if your gateway/router uses a DHCP server, ensure you enter the correct IP address. Refer to your gateway/router's settings.



If a DHCP server is used in the network, it is advised to use your DHCP server's settings to assign the AP Controller a static IP address.

3. Enter the username & password to login. The default username & password are **admin** & **1234**.

<u>Logout</u>

To logout from Edimax NMS, click "Logout" in the top right corner:



Restart

You can restart your AP Controller or any Managed AP using Edimax NMS. To restart your AP Controller go to Local Settings \rightarrow Advanced \rightarrow Reboot and click "Reboot".

This will reboot the product. Your settings will not be changed. Click "Reboot" to reboot the product now.



To restart Managed APs click the Restart icon for the specified AP on the Dashboard:



X-2 Dashboard



The dashboard displays an overview of your AP array:

										Auto Re	efresh Time 🔍	1 minute 🔍	30 seconds	Disable
APs Information		Managed	AP											0-
	0 1 ctive Offline	Search				ПМ	atch whole wo	ords						
0		Index 🔺	MAC Address	Device Name 🔺	Model 🔺	IP Address	2.4G Channel	45G Channel 4	Clients 🔺	2.4G Domain	▲5G Domain 🔺	Status 🔺		Action
Discovered		1	74:DA:38:1D:26: 4E	AP74DA381D26 4E	WAP1200	<u>192.168.2.101</u>	N/A	N/A	0	FCC	FCC	0		30000
System Informatio	on CO													
Product Name Host Name	WAP1750 AP801F02F1968A	Managed	AP Group											© –
MAC Address	80:1F:02:F1:96:8A													
IP Address	192.168.2.2	Search				— м	atch whole wo	ords						
Firmware Version	1.8.1	-												
System Time	2012/01/01 19:53:06		roup Name	MAC Addr	ess	Device Name	Mo	del IF	P Address	Clients	Sta	tus	Ac	tion
Uptime	0 day 19:53:25	System E)efault (0)											
CPU Usage	3%							Empty						
Memory / Cache Us age	63%	Wizard A	P Group 2 (1)	Ð										
Devices Informati	on CO	Active Cl	ients											©—
Device Access Points	Number 1	Search				M	atch whole wo	ords						
Client Devices	0	Index		AP MAC Addres	v	/LAN	User Nam	e Radio	Signal(%) Connected	Time Idle Time	Tx(KB)	Rx(KB)	Vendor
Rogue Devices	0		ress	S				Empty						
								Empty						

\bigcirc

Use the blue icons above to refresh or collapse each panel in the dashboard. Click and drag to move a panel to suit your preference. You can set the dashboard to auto-refresh every 1 minute, 30 seconds or disable auto-refresh:



X-2-1 System Information

System Information displays information about the AP Controller: *Product Name (model), Host Name, MAC Address, IP Address, Firmware Version, System Time and Uptime (time the access point has been on).*

System Information	
Product Name	WAP1750
Host Name	AP801F02F1968A
MAC Address	80:1F:02:F1:96:8A
IP Address	192.168.2.2
Firmware Version	1.8.1
System Time	2012/01/01 19:53:06
Uptime	0 day 19:53:25
CPU Usage	3%
Memory / Cache Us age	63%

X-2-2 Devices Information

Devices Information is a summary of the number of all devices in the local network: *Access Points, Clients Connected, and Rogue (unidentified) Devices.*

Devices Informat	evices Information							
Device	Number							
Access Points	1							
Client Devices	0							
Rogue Devices	0							

X-2-3 Managed AP

This page displays information about the Managed APs in the local network: Index (reference number), MAC Address, Device Name, Model, IP Address, 2.4GHz & 5GHz Wireless Channel Number, No. of Clients connected to each access point, and Status (connected, connecting or disconnected).

Managed	AP										0
Search				M	latch whole wo	ords					
📄 Index 🔺	MAC Address	Device Name 🔺	Model 🔺	IP Address	2.4G Channel	45G Channel 4	Clients 🔺	2.4G Domain	▲5G Domain 🔺	Status 🔺	Action
1	74:DA:38:1D:26: 4E	AP74DA381D26 4E	WAP1200	<u>192.168.2.101</u>	N/A	N/A	0	FCC	FCC	0	

The **search** function can be used to locate a specific Managed AP. Type in the search box and the list will update:

-	
Search 1	Match whole words
Course II	

The **Status** icon displays *grey* (disconnected), *yellow* (connecting) or *green* (connected) for each Managed AP.

Each Managed AP has "Action" icons with the following functions:



1. Disallow

Remove the Managed AP from the AP array and disable connectivity.

2. Edit

Edit various settings for the Managed AP (refer to x-5-1 *Access Point)*.

3. Blink LED

The Managed AP's LED will flash temporarily to help identify & locate the access point.

4. Buzzer

The Managed AP's buzzer will sound temporarily to help identify/locate the access point.

5. Network Connectivity

Go to the "Network Connectivity" panel to perform a ping or traceroute.

6. Restart

Restarts the Managed AP.

Status lo	Status Icons										
lcon	Color	Status	Definition								
	Grey	Disconnected	Managed AP is disconnected. <i>Please check</i> the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.								
	Red	Authentication Failed	System security must be the same for all access points in the AP array. <i>Please check security settings (refer to</i> x-5-13-1 System Security).								
	Red	Or Incompatible NMS Version	All access points must have the same firmware version. <i>Please use the AP</i> <i>Controller's firmware upgrade function</i> <i>(refer to</i> x-5-12 Firmware Upgrade).								
0	Orange	Configuring or Upgrading	<i>Please wait while the Managed AP makes configurations or while the firmware is upgrading.</i>								
	Yellow	Connecting	Please wait while Managed AP is connecting.								
	Green	Connected	Managed AP is connected.								
0	Blue	Waiting for Approval	Managed AP is waiting for approval. Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.								

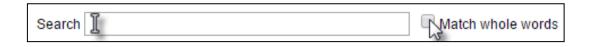
X-2-4 Managed AP Group

Managed APs can be grouped according to your requirements. **Managed AP Group** displays information about each Managed AP group in the local network: *Group Name, MAC Address, Device Name, Model, IP Address, 2.4GHz* & 5GHz Wireless Channel Number, No. of Clients connected to each access point, and Status (connected or disconnected).

To edit Managed AP Groups go to NMS Settings \rightarrow Access Point (refer to x-5-1 Access Point).

Manag	ed AP Group									
Search	Search Match whole words									
	Group Name		MAC Address	Device Name	Model	IP Address	Clients	Status	Action	
Syste	m Default (0)									
					E	mpty				
Wizar	d AP Group 2 (1)	•								

The search function can be used to locate a specific Managed AP Group. Type in the search box and the list will update:



The **Status** icon displays *grey* (disconnected), *yellow* (connecting) or *green* (connected) for each individual Managed AP.

Each Managed AP Group has "Action" icons with the following functions:



1. Disallow

Remove the Managed AP Group from the AP array and disable connectivity.

2. Edit

Edit various settings for the Managed AP Group (refer to x-5-1 **Access Point**)

3. Blink LED

The LED of all Managed APs in the group will flash temporarily to help identify & locate the access points.

4. Buzzer

The buzzer of all Managed APs in the group will sound temporarily to help identify & locate the access points.

5. Network Connectivity

Go to the "Network Connectivity" panel to perform a ping or traceroute.

6. Restart

Restarts all Managed APs in the group.

Status lo	Status Icons									
lcon	Color	Status	Definition							
	Grey	Disconnected	Managed AP is disconnected. <i>Please check</i> the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.							
		Authentication Failed	System security must be the same for all access points in the AP array. <i>Please check security settings (refer to</i> x-5-13-1 System Security).							
	Red	Or Incompatible NMS Version	All access points must have the same firmware version. <i>Please use the AP</i> <i>Controller's firmware upgrade function</i> <i>(refer to</i> X-5-12 Firmware Upgrade).							
	Orange	Configuring or Upgrading	<i>Please wait while the Managed AP makes configurations or while the firmware is upgrading.</i>							
	Yellow	Connecting	Please wait while Managed AP is connecting.							
	Green	Connected	Managed AP is connected.							

0	Blue	Waiting for Approval	Managed AP is waiting for approval. Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.
---	------	-------------------------	---

X-2-5 Active Clients

Active Clients displays information about each client in the local network: Index (reference number), Client MAC Address, Device Name, Model, IP Address, 2.4GHz & 5GHz Wireless Channel Number, No. of Clients connected to each access point, and Status (on or off).

Active Clients										<u>©</u> _	
Search	Match whole words										
Index	Client MAC Add ress	AP MAC Addres s	WLAN	User Name	Radio	Signal(%)	Connected Time	Idle Time	Tx(KB)	Rx(KB)	Vendor
					Empty						

The search function can be used to locate a specific client. Type in the search box and the list will update:

Search [Match whole words

X-2-6 Active Users

Active Users displays information about users currently connected to the AP Array: User Name, MAC Address, IP Address, SSID, Creator, Create Time, Expire Time, Usage Percentage, Vendor, Platform and Action.

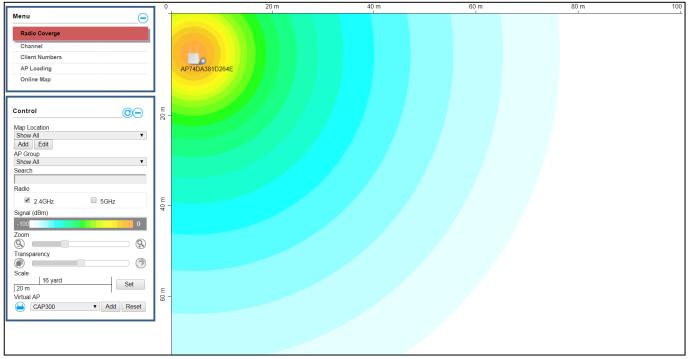
Active Users											<u>C</u> -
Search				Match who	Match whole words						
□ _{Index}	User Name	MAC Address	IP Address	SSID	Creator	Create Time	Expire Time	Usage Percentag e	Vendor	Platform	Action
	Empty										

The search function can be used to locate a specific user. Type in the search box and the list will update:

Search 📱	Match whole words
	15



The Zone Plan can be fully customized to match your network environment. You can move the AP icons and select different location images (upload location images in **NMS Settings** \rightarrow **Zone Edit**) to create a visual map of your AP array.



Use the menu on the left side to make adjustments and mouse-over an AP icon in the zone map to see more information. Click an AP icon in the zone map to select it and display action icons:



Menu allows you to keep track of the access points' information. Select between *Radio Coverage, Channel, Client Numbers, AP Loading,* and *Online Map.* When an option is selected, the zone plan and Control section will change accordingly.

Menu)
Radio Coverge	
Channel	
Client Numbers	
AP Loading	
Online Map	

Radio Coverage

Below is displayed as Radio Coverage is selected:

	0	20 m	40 m	60 m	80 m	100
Menu Radio Coverge Channel Client Numbers AP Loading Online Map		AP74DA381D264E				
Control © Map Location Show All Add Edit AP Group Show All Show All	20 m -					
Radio 2.4GHz 5GHz Signal (dBm) 100 0 Zoom Scale Scale Scale	40 m -					
Scale 16 yard Set 20 m Virtual AP Image: CAP300 Image: Add Reset	ш – 99					

<u>Channel</u>

Below is displayed as Channel is selected:

	0	20 m	40 m	60 m	80 m	100
Radio Coverge						
Radio Coverge Channel Client Numbers AP Loading Online Map	AP74	4DA381D264E				
Control	20 H					
Map Location Show All T Add Edit						
AP Group Show All Search						
Radio	_					
Channel	40 - E					
Zoom S Transparency						
Scale 16 yard Set						
	E -					

Client Numbers

Below is displayed as Client Numbers is selected:

	0	20 m	40 m	60 m	80 m 100
Menu 😑		1			
Radio Coverge					
Channel					
Client Numbers					
	0				
AP Loading	AP74DA381D264E				
Online Map					
Control	E				
Control	E - 28				
Map Location					
Show All Add Edit					
AP Group					
Show All 🔹					
Search					
Radio					
	c				
	64 - E				
Clients Numbers 0 50					
Zoom					
§					
Transparency					
Scale					
20 m Set	-				
1	E 00 -				
	-				

AP Loading

Below is displayed as AP Loading is selected:

	0		20 m	40 m	60 m	80 m	100
Menu	1		I	I	I		L
Radio Coverge							
Channel							
Client Numbers							
AP Loading		AP74DA381D264E					
Online Map							
Control	20 m						
Map Location	Ñ						
Show All							
Add Edit							
AP Group Show All							
Show All							
AP Loading							
CPU V	40 H						
CPU Loading (%) 0 100	40.						
S S							
Transparency							
Scale							
20 m Set							
	_						
	а 1900 -	-					
	_						

Online Map

When Online Map is selected, the message below is displayed:

192.168.2.2 says:		×
Please click "OK" to enter Google Maps API	key.	
	ОК	Cancel

Click "OK" and the interface will bring you to the page shown below to allow API key entry:

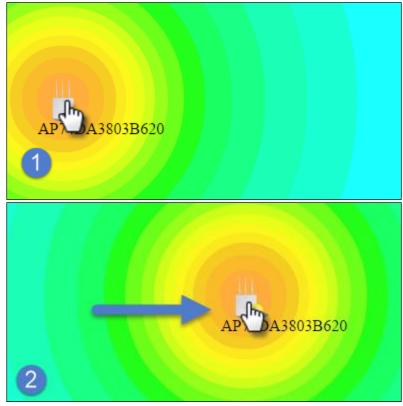
Google Maps	
АРІ Кеу	(Please go to <u>https://console.developers.google.com/flows/enableapi?</u> apiid=maps_backend&keyType=CLIENT_SIDE&reusekey=true to apply for an API key.)
Apply Cancel	

X-3-2 Control

The Control section will change according to the selection in the Menu section.

Map Location	Select a pre-defined location from the drop down menu.				
	When you upload a location image in NMS Settings \rightarrow Zone				
	Edit, it will be available for selection here.				
AP Group	You can select an AP Group to display in the zone map. Edit				
	AP Groups in NMS Settings → Access Point.				
Search	Use the search box to quickly locate an AP.				
Radio	Use the checkboxes to display APs according to 2.4GHz or				
	5GHz wireless radio frequency.				
Signal	When Radio Coverage is selected in Menu, signal strength is				
	shown in the Control section below the "Radio" option.				
	Signal strength chart displays the signal strength in dBm,				
	and is also shown around each AP in the zone map.				
Channel	When Channel is selected in Menu, channel is shown in the				
	Control section below the "Radio" option.				
Client Numbers	When Client Numbers is selected in Menu, client numbers is				
	shown in the Control section below the "Radio" option.				
AP Loading	When AP Loading is selected in Menu, AP loading is shown				
	in the Control section below the "Search" option. Two				
	options are available: "CPU" or "Traffic (Tx + Rx)".				
CPU Loading	This shows the CPU loading of the AP.				
Traffic (Tx + Rx)	This shows the Traffic (Tx+Rx) loading.				
Zoom	Use the slider to adjust the zoom level of the map.				
Transparency	Use the slider to adjust the transparency of location images.				
Scale	Zone map scale.				
Device/Number	Displays number and type of devices in the zone map.				

Click and drag an AP icon to move the icon around the zone map. The signal strength for each AP is displayed according to the "Signal" key in the menu on the right side:



X-4 NMS Monitor



X-4-1 Access Point

X-4-1-1 Managed AP

Displays information about each Managed AP in the local network: *Index* (reference number), MAC Address, Device Name, Model, IP Address, 2.4GHz & 5GHz Wireless Channel Number, No. of Clients connected to each access point, and Status (connected, connecting or disconnected).

Managed A	Managed AP								
Search				Match whole wo	ords				
Index 🔺	MAC Address	Device Name 🔺	Model 🔺	IP Address 🔺	2.4G Channel 🔺	5G Channel 🔺	Clients 🔺	Status 🔺	Action
1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	N/A	N/A	0	0	

The **search** function can be used to locate a specific Managed AP. Type in the search box and the list will update:

0	
Search][Match whole words
	15

The **Status** icon displays the status of each Managed AP.

Status Icons						
lcon	Color	Status	Definition			
			Managed AP is disconnected. <i>Please check</i>			
	Grey	Disconnected	the network connection and ensure the			
			Managed AP is in the same IP subnet as the			
			AP Controller.			
		Authentication	System security must be the same for all			
	Red	Failed	access points in the AP array. <i>Please check</i>			
			security settings (refer to x-5-13-1 System			

		Or	Security).
		Incompatible NMS Version	All access points must have the same firmware version. <i>Please use the AP</i> <i>Controller's firmware upgrade function</i> <i>(refer to</i> x-5-12 Firmware Upgrade).
	Orange	Configuring or Upgrading	Please wait while the Managed AP makes configurations or while the firmware is upgrading.
	Yellow	Connecting	Please wait while Managed AP is connecting.
	Green	Connected	Managed AP is connected.
0	Blue	Waiting for Approval	Managed AP is waiting for approval. Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.

Each Managed AP has "Action" icons with the following functions:



1. Disallow

Remove the Managed AP from the AP array and disable connectivity.

2. Edit

Edit various settings for the Managed AP (refer to x-5-1 *Access Point)*.

3. Blink LED

The Managed AP's LED will flash temporarily to help identify & locate access points.

4. Buzzer

The Managed AP's buzzer will sound temporarily to help identify & locate access points.

5. Network Connectivity

Go to the "Network Connectivity" panel to perform a ping or traceroute.

6. Restart

Restarts the Managed AP.

X-4-1-2 Managed AP Group

Managed APs can be grouped according to your requirements. Managed AP Group displays information about each Managed AP group in the local network: *Group Name, MAC Address, Device Name, Model, IP Address, 2.4GHz* & 5GHz Wireless Channel Number, No. of Clients connected to each access point, and Status (connected or disconnected).

To edit Managed AP Groups go to NMS Settings \rightarrow Access Point (refer to x-5-1 Access Point).

Managed AP Group								
Search		Match	whole words					
Group Name	MAC Address	Device Name	Model	IP Address	Clients	Status	Action	
System Default (0)								
			En	npty				
Wizard AP Group 2 (1)	Θ							
	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	0	0	◙₿₿₽€⊘	

The search function can be used to locate a specific Managed AP Group. Type in the search box and the list will update:

Search	↓ Match whole words
--------	------------------------

The **Status** icon displays the status of each Managed AP.

Status lo	cons		
lcon	Color	Status	Definition
			Managed AP is disconnected. <i>Please check</i>
	Grou	Disconnected	the network connection and ensure the
	Grey	Disconnected	Managed AP is in the same IP subnet as the
			AP Controller.
		Authentication	System security must be the same for all
		Failed	access points in the AP array. <i>Please check</i>
			security settings (refer to x-5-13-1 System
	Red	Or	Security).
		Incompatible	All access points must have the same
		NMS Version	firmware version. Please use the AP

			Controller's firmware upgrade function (refer to x-5-12 Firmware Upgrade).
	Orange	Configuring or Upgrading	<i>Please wait while the Managed AP makes configurations or while the firmware is upgrading.</i>
	Yellow	Connecting	Please wait while Managed AP is connecting.
	Green	Connected	Managed AP is connected.
0	Blue	Waiting for Approval	Managed AP is waiting for approval. Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.

Each Managed AP has "Action" icons with the following functions:



1. Disallow

Remove the Managed AP Group from the AP array and disable connectivity.

2. Edit

Edit various settings for the Managed AP Group (refer to x-5-1 *Access Point)*

3. Blink LED

The LED of all Managed APs in the group will flash temporarily to help identify & locate the access points.

4. Buzzer

The buzzer of all Managed APs in the group will sound temporarily to help identify & locate the access points.

5. Network Connectivity

Go to the "Network Connectivity" panel to perform a ping or traceroute.

6. Restart

Restarts all Managed APs in the group.

X-4-2 WLAN

X-4-2-1 Active WLAN

Displays information about each SSID in the AP Array: *Index (reference number), Name/SSID, VLAN ID, Authentication, Encryption, IP Address and Additional Authentication.*

To configure encryption and VLANs for Managed APs go to NMS Settings \rightarrow WLAN.

The search function can be used to locate a specific SSID. Type in the search box and the list will update:

Search I	N Matab whale words
Search I	Match whole words
	45

Active WLAN					
Search		Mat	ch whole words		
Index	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
1	wap1750	1	WPA2PSK	AES	No additional authentication

X-4-2-2 Active WLAN Group

WLAN groups can be created according to your preference. Active WLAN Group displays information about WLAN group: *Group Name, Name/SSID, VLAN ID, Authentication, Encryption, IP Address and Additional Authentication.*

The search function can be used to locate a specific Active WLAN Group. Type in the search box and the list will update:

	Search					n whole words
Active V	WLAN Group					
Search			Match whole words			
	Group Name	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
Wizard	WLAN 2.4G Group 1 (1)					
		wap1750	1	WPA2PSK	AES	No additional authentication
Wizard	WLAN 5G Group 2 (1)					
		wap1750	1	WPA2PSK	AES	No additional authentication

X-4-3 Clients

X-4-3-1 Active Clients

Displays information about clients currently connected to the AP Array: *Index* (*reference number*), *Client MAC Address, AP MAC Address, WLAN (SSID), Radio* (2.4GHz or 5GHz), Signal Strength received by Client, Connected Time, Idle Time, Tx & Rx (Data transmitted and received by Client in KB), and the Vendor of the client device.

You can set or disable the auto-refresh time for the client list or click "Refresh" to manually refresh.

The search function can be used to locate a specific client. Type in the search box and the list will update:

	Search						latch wh	ole word	s	
Clients										
Manual Refresh	Refresh									
Active Clients										
Search		□ N	atch whole words							
Index Client MA	AC Address AP MAC Add	dress 🔻 WLAN 🔻	User Name 🔻	Radio 🕶 Empty	Signal(%) 🔻	Connected Time 💌	Idle Time 🔻	Tx(KB) ▼	Rx(KB) ▼	Vender

X-4-4 Users

X-4-4-1 Active Users

Displays information about users currently connected.

Active	Users										
Search				Mat	tch whole word	is					
Index	User Name	MAC Address	IP Address	SSID	Creator	Create Time	Expire Time	Usage Percentage	Traffic progress	Vendor	Platform Action
						Empty					

X-4-4-2 Users Log

Displays the log information about users currently connected.

Search

Users Log		
Search	Match whole words	
ID Date and Time Category Severity	Users Events/	Activities
Refresh		

X-4-5 Rogue Devices

Rogue access point detection can identify any unauthorized access points which may have been installed in the network.

Click "Start" to scan for rogue devices:



Unknown Rogue Devices area displays information about rogue devices discovered during the scan: Index (reference number), Channel, SSID, MAC Address, Security, Signal Strength, Type, Vendor and Action.

The search function can be used to locate a known rogue device. Type in the search box and the list will update:

	5	Search				Ma	tch whole words	
Rogue Do	evices							
Scan		Start						
Unknown	a Rogue Dev	ices						
Search			Match w	nole words				
Index	Channel	SSID	MAC Address	Security No Rogue Device	Signal (%)	Туре	Vendor	Action
Known R	Rogue Device	25						
Search			Match w	nole words				

X-4-6 Information

X-4-6-1 All Events/Activities

Displays a log of time-stamped events for each access point in the Array – use the drop down menu to select an access point and view the log.

Select AP:	74:DA:38:1D:26:4E	٦
	74:DA:38:1D:26:4E	
All Events/A	74:DA:38:1D:26:5A	

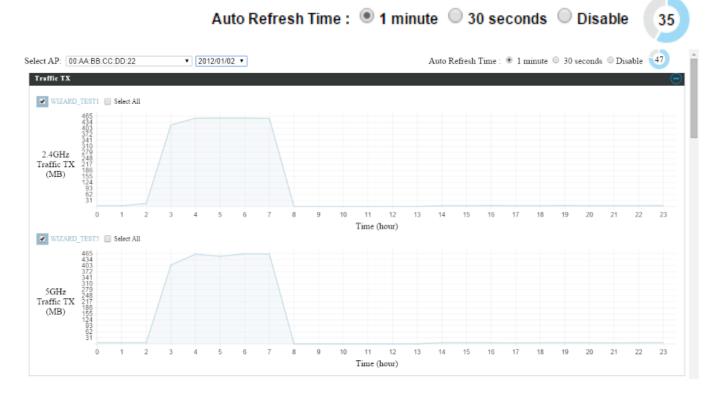
ll Even	ts/Activities			
Search				Match whole words
ID 🔻	Date and Time	Severity 🔺	Users 🔺	Events/Activities
15	2012/01/01 00:01:10	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected
14	2012/01/01 00:07:01	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully
13	2012/01/01 00:00:21	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
12	2012/01/01 00:00:55	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
11	2012/01/01 00:01:05	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
10	2012/01/01 00:07:40	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected
9	2012/01/01 00:09:57	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully
8	2012/01/01 00:00:24	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
7	2012/01/01 00:10:31	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected
6	2012/01/01 00:12:15	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully
5	2012/01/01 00:13:58	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected
4	2012/01/01 00:14:31	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully
3	2012/01/01 00:00:22	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
2	2012/01/01 00:00:55	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
1	2012/01/01 00:00:23	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully

AP Monitoring X-4-6-2

Displays graphical monitoring information about access points in the Array for 2.4GHz & 5GHz: Traffic Tx (data transmitted in MB), Traffic Rx (data received in MB), No. of Clients, Wireless Channel, Tx Power (wireless radio power), CPU Usage and Memory Usage.

Use the drop down menus to select an access point and date.

You can set or disable the auto-refresh time for the data:



Select AP: 74:DA:3		
		vill analysis the system every hour. When the statistics information is ready, AP Controller will retrieve and display. Please wait for a moment.
Managed AP Info		Traffic Tx
Model Name	WAP1200	
Model Image		
Host Name MAC Address	AP74DA381D264E 74:DA:38:1D:26:4E	Client Number
IP Address	192.168.2.101	
Firmware Version	1.8.1	Channel
WLAN Informatio	эп (
	2.4G	Tx Power
	ard WLAN 2.4G Group	
WLAN member list	wap1750	CPU Usage
	5G	
WLAN Groups Wiz	zard WLAN 5G Group 2	Memory / Cache Usage
list	wap1750	
Managed A	P Informatio	on 💽 Traffic 1
		Evpand
WLAN Info	rmation	Expand
Select AP: 74:DA:3	8:1D:26:4E 🔻	
Select Date: NO Da	ta ▼ Managed AP w	vill analysis the system every hour. When the statistics information is ready, AP Controller will retrieve and display. Please wait for a moment.
Managed AP Infor	rmation (Traffic Tx
Model Name	WAP1200	
Model Image	1 de 1	Traffic RX
Host Name	AP74DA381D264E	
MAC Address IP Address	74:DA:38:1D:26:4E 192.168.2.101	Client Number
Firmware Version	1.8.1	
		Channel
WLAN Informatio		
	2.4G ard WLAN 2.4G Group	Tx Power
WLAN member	wap1750	
list		CPU Usage
	5G zard WLAN 5G Group 2	
WLAN member	wap1750	Memory / Cache Usage
list		

X-4-6-3 SSID Overview

Displays graphical monitoring information about access points in the Array for 2.4GHz & 5GHz.

SSID Overview	N Contraction of the second second second second second second second second second second second second second
Manual Refresh	h Refresh
2.4GHz & 5GI	Hz Traffic
2.4GHz Tra	affic Tx 🔄 2.4GHz Traffic RX 🔄 5GHz Traffic Tx 🚺 5GHz Traffic RX
	15 14
	13 12
	11 10
	9 - 8 -
Traffic (KBps)	6
	5 - 4 -
	3 2 1
	wap1750
	SSID
611 . X X	
Client Number	
2.4GHz	
	15 14 13
	12
	10 9
Client Number	8 -
	6 5
	4 - 3 -
	2
	0
	SSID



X-5-1 Access Point

Displays information about each access point and access point group in the local network and allows you to edit access points and edit or add access point groups.

The **search** function can be used to locate an access point or access point group. Type in the search box and the list will update:

		Search	1					Match w	hole words		
Access	Point										
Search				M	atch whole word	ds					
	Index 🔺	MAC Address 🔺	Device Name 🔺	Model 🔺	AP Group	2.4G Channel	5G Channel 🔺	2.4G Tx Power 🔺	5G Tx Power 🔺	Status 🔺 Actio	on
	1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	Wizard AP Grou 2	up 11	36	Full (14dbm)	Full (16dbm)	00)
	2	74:DA:38:1D:26:5A	AP74DA381D265A	WAP1200	System Defaul	lt N/A	N/A	N/A	N/A	0 0)
Search		Group Name	AP Mem	2.40 bers WLA	N WLAN 2.40	ds 3 Guest Network Profile	5G Guest Network	Profile RADIUS F	Profile Access	Control Profile	
		System Default	1		le Profile led Disabled	Disabled	Disabled	Disabl	ed l	Disabled	
	Wizard AP Group 2		1	WLA 2.40		Disabled	Disabled	Disabl	Disabled		
Add	Edit	Clone Delete S	Selected Delete	e All							
Access	Point Sett	ings									
Auto A	pprove	• E	nable Oisable								
Apply											

The **Status** icon displays *grey* (disconnected), *red* (authentication failed/incompatible NMS version), *orange* (upgrading firmware), *yellow* (connecting), *green* (connected) or *blue* (waiting for approval) for each

individual Managed AP. Refer to the *Status Icons in* x-2-3 *Managed AP* for full descriptions.

The "Action" icons enable you to allow or disallow an access point:

Select an access point or access point group using the check-boxes and click "**Edit**" to make configurations, or click "**Add**" to add a new access point group:

The Access Point Settings panel can enable or disable Auto

Approve for all Managed APs. When enabled, Managed APs will automatically join the AP Array with the Controller AP. When disabled, Managed APs must be manually approved to join the AP Array with the Controller AP.

Add

Access Point Settings					
Auto Approve	Enable Disable				
Apply					

Access Point Settings				
Auto Approve	Enable or disable Auto Approve for all Managed APs.			

To manually approve a Managed AP, use the *allow* "Action" icon for the specified access point:

X-5-1-1 Edit Access Point

Configure your selected access point on your LAN. You can set the access point as a DHCP client or specify a static IP address for your access point, and assign the access point to an AP group, as well as edit 2.4GHz & 5GHz wireless radio settings. Event log is displayed at the bottom of the page.

You can also use **Profile Settings** to assign the access point to WLAN, Guest Network, RADIUS and Access Control groups independently from Access Point Group settings.

Click "Save" to save the settings. Click "Cancel" to forfeit the changes. Click "Save and Apply" to save and apply the settings.

Save Cancel Save & Apply

X-5-1-1-1 Edit Basic Settings

When "Override Group Setting" is checked, options/fields will turn white to allow adjustments.

me	AP74DA381D264E	
scription		
AC Address	74:DA:38:1D:26:4E	
Group	Wizard AP Group 2 ▼	
Address Assignment	Override Group Setting	DHCP Client V
Address	192.168.2.101	
bnet Mask	255.255.255.0	
fault Gateway	From DHCP v 0.0.0	
imary DNS	User-Defined T	
condary DNS	User-Defined v	
MP Snooping	Override Group Setti	Disable V
cation Type	Indoor v	
IP Address A	ssignment	✓ Override Group Setting DHCP Client ▼
IP Address	1	192.168.2.101
Subnet Mask	2	255.255.255.0
Default Gate	way	From DHCP v 0.0.0.0
Primary DNS		User-Defined v
Secondary D	NS	User-Defined ▼
IGMP Snoopi	ng	✓ Override Group Setting Disable ▼
Location Typ		Indoor 🔻

Basic Settings	
Name	Edit the access point name. The default name is AP + MAC
	address.
Description	Enter a description of the access point for reference e.g. 2 nd
	Floor Office.
MAC Address	Displays MAC address.
AP Group	Use the drop down menu to assign the AP to an AP Group.

	You can edit AP Groups from the NMS Settings → Access
	Point page.
IP Address	Select "DHCP Client" for your access point to be assigned a
Assignment	dynamic IP address from your router's DHCP server, or select
Assignment	· · ·
	"Static IP" to manually specify a static/fixed IP address for
	your access point (below). Check the box "Override Group
	Setting" if the AP is a member of an AP Group and you wish to
	use a different setting than the AP Group setting.
IP Address	Specify the IP address here. This IP address will be assigned to
	your access point and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default	For DHCP users, select "From DHCP" to get default gateway
Gateway	from your DHCP server or "User-Defined" to enter a gateway
	manually. For static IP users, the default value is blank.
Primary DNS	DHCP users can select "From DHCP" to get primary DNS
	server's IP address from DHCP or "User-Defined" to manually
	enter a value. For static IP users, the default value is blank.
Secondary	DHCP users can select "From DHCP" to get secondary DNS
DNS	server's IP address from DHCP or "User-Defined" to manually
	enter a value. For static IP users, the default value is blank.
IGMP	Enable / Disable the IGMP Snooping function.
Snooping	IGMP snooping is the process of listening to Internet Group
	Management Protocol (IGMP) network traffic.
Location Type	Select the location of the AP (indoor or outdoor).

X-5-1-1-2 Edit Web Account Settings

Web Account Settings			
Override Group Setting			
Administrator Name	admin		
Administrator Password	1234	(6-32Characters)	

When "Override Group Setting" is checked, options/fields will turn white to allow adjustments.

X-5-1-1-3 Edit VLAN Settings

VLAN Settings		
Wired LAN Port	VLAN Mode	VLAN ID
Wired Port(#1)	Override Group Setting Untagged Port 🔻	Override Group Setting 1
Wired Port(#2)	Override Group Setting Untagged Port	Override Group Setting 1
Management VLAN ID	Override Group Setting 1	

When "Override Group Setting" is checked, options/fields will turn white to allow adjustments.

X-5-1-1-4 Edit Radio Settings

Radio Settings			
	Radio B/G/N (2.4 GHz)		Radio A/N/AC (5.0 GHz)
Wireless	Override Group Setting Enable		Override Group Setting Enable T
Band	Override Group Setting 11b/g/n 🔻		□ Override Group Setting 11a/n/ac ▼
Auto Pilot	Override Group Setting Disable V Plea	se set AP position on the Zone Plan first.	Override Group Setting Disable V Please set AP position on the Zone Plan first.
Auto Pilot Sensitivity	Override Group Setting		Override Group Setting
Auto Pilot Range	Override Group Setting Ch 1 - 11 🔻		Override Group Setting Band 1
Auto Pilot Interval	Override Group Setting Half day 🔻		Override Group Setting Half day
Auto Pilot interval	Change channel even if clients are conne	cted	Change channel even if clients are connected
Channel	Override Group Setting Ch 11, 2462MH	Z	Override Group Setting Ch 36, 5.18GHz 🔻
Channel Bandwidth	Override Group Setting 20 MHz	▼	Override Group Setting 20 MHz T
BSS BasicRateSet	Override Group Setting all	▼	Override Group Setting all
Advanced Settings	Radio B/G/N (2.4 GHz)		Radio A/N/AC (5.0 GHz)
Contention Slot	Override Group Setting Short	7	
Preamble Type	Override Group Setting Short	7	
Guard Interval	Override Group Setting Short G		Override Group Setting Short GI V
802.11n Protection	Override Group Setting Enable	V	Override Group Setting Enable V
CE Adaptive	Override Group Setting Disable	•	
DTIM Period	Override Group Setting 1	(1-255)	Override Group Setting 1 (1-255)
RTS Threshold	Override Group Setting 2347	(1-2347)	Override Group Setting 2347 (1-2347)
Fragment Threshold	Override Group Setting 2346	(256-2346)	Override Group Setting 2346 (256–2346)
Multicast Rate	Override Group Setting Auto	V	Override Group Setting Auto
Tx Power	Override Group Setting 100%	T	Override Group Setting 100% V
Beacon Interval	Override Group Setting 100	(40-1000 ms)	Override Group Setting 100 (40-1000 ms)
Station idle timeout	Override Group Setting 60	(30-65535 seconds)	Override Group Setting 60 (30-65535 seconds)
OWDS Settings	Radio B/G/N (2.4 GHz)		Radio A/N (5.0 GHz)
WDS Functionality	None		None
VD\$ #1	AP Device Name User-Defined V	AC Address	AP Device Name User-Defined V MAC Address
VDS #2	AP Device Name User-Defined V	AC Address	AP Device Name User-Defined V MAC Address
VD S #3	AP Device Name User-Defined V	AC Address	AP Device Name User-Defined V MAC Address
NDS #4	AP Device Name User-Defined V	AC Address	AP Device Name User-Defined V MAC Address
WDS VLAN Mode	Untagged Port V (Enter at least one MAC	address.)	Untagged Port V (Enter at least one MAC address.)
WDS VLAN ID	1		1
WDS Encryption	None V (Enter at least one MAC address.)		None V (Enter at least one MAC address.)

Radio Settings	
Wireless	Enable or disable the access point's 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g, 802.11n & 802.11ac can be selected.
Auto Pilot	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 2.4GHz or 5GHz frequency based on availability and potential interference. When disabled, select a channel manually.
Auto Pilot	Select sensitivity of Auto Pilot.
Sensitivity	
Auto Pilot	Select a range from which the auto channel setting (above)

Range	will choose a channel.
Auto Pilot	Specify a frequency for how often the auto channel setting
Interval	will check/reassign the wireless channel. Check/uncheck the
	"Change channel even if clients are connected" box according
	to your preference.
Channel	When Auto Pilot is disabled, select a channel (1-11) manually.
Channel	Set the channel bandwidth or use Auto (automatically select
Bandwidth	based on interference level).
BSS	Set a Basic Service Set (BSS) rate: this is a series of rates to
BasicRateSet	control communication frames for wireless clients.

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.



Changing these settings can adversely affect the performance of your access point.

Advanced Setti	ngs
Contention	Select "Short" or "Long" – this value is used for contention
Slot	windows in WMM (see x-6-7 WMM).
Preamble	Set the wireless radio preamble type. The preamble type in
Туре	802.11 based wireless communication defines the length of
	the CRC (Cyclic Redundancy Check) block for communication
	between the access point and roaming wireless adapters. The
	default value is "Short Preamble".
Guard	Set the guard interval. A shorter interval can improve
Interval	performance.
802.11n	Enable/disable 802.11n protection, which increases reliability
Protection	but reduces bandwidth (clients will send Request to Send
	(RTS) to access point, and access point will broadcast Clear to
	Send (CTS), before a packet is sent from client.)
CE Adaptive	The measurement procedure follows clause 5.3.11.2.2 of the
	ETSI EN 300 328 V1.8.1
DTIM Period	Set the DTIM (delivery traffic indication message) period value
	of the wireless radio. The default value is 1.
RTS	Set the RTS threshold of the wireless radio. The default value
Threshold	is 2347.

Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast	Set the transfer rate for multicast packets or use the "Auto"
Rate	setting.
Tx Power	Set the power output of the wireless radio. You may not
	require 100% output power. Setting a lower power output can
	enhance security since potentially malicious/unknown users
	in distant areas will not be able to access your signal.
Beacon	Set the beacon interval of the wireless radio. The default
Interval	value is 100.
Station idle	Set the interval for keepalive messages from the access point
timeout	to a wireless client to verify if the station is still alive/active.

WDS Settings	
WDS	A wireless distribution system (WDS) is a system enabling the
Functionality	wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them.
AP Device	Set AP Device Name.
Name	
MAC Address	Set MAC Address of AP.
WDS VLAN	Enable / Disable VLAN function.
Mode	
WDS VLAN ID	Set VLAN ID of WDS.
WDS	Set WDS Encryption.
Encryption	

X-5-1-1-5 Edit WMM-EDCA Settings

	W/MM Daram	eters of Access Po	sint	
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	6	3	0
Video	3	4	1	94
Voice	2	3	1	47
	CWMin	eters of Station CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	10	3	0
Video	3	4	2	94
Voice	2	3	2	47

When "Override Group Setting" is checked, options/fields will turn white to allow adjustments.

Override Group Setting

WMM-EDCA Settings:		
Back Ground Access Category (AC) is Back Ground		
Best Effort	Access Category (AC) is Best Effort	
Video	Access Category (AC) is video	
Voice	Access Category (AC) is voice	

X-5-1-1-6 Edit BandSteering Settings

BandSteering Settings		
Bandsteering	Override Group Setting	Off 5G First Balanced User Define

When "Override Group Setting" is checked, options/fields will turn white to allow adjustments.

X-5-1-1-7 Edit Profile Settings

Profile Settings				
	Radio B/G/N (2.4 GHz)		Radio A/N/AC (5.0 GHz)	
WLAN Group	Override Group Setting	Wizard WLAN 2.4G Group 1 V	Override Group Setting	Wizard WLAN 5G Group 2 🔻
Guest Network Group	Override Group Setting	Disable V	Override Group Setting	Disable 🔻
RADIUS Group	Override Group Setting	Disable 🔻		
MAC Access Control Group	Override Group Setting	Disable v		

When "Override Group Setting" is checked, options/fields will turn white to allow adjustments.

Profile Settings	
WLAN Group	Assign the access point's 2.4GHz or 5GHz SSID(s) to a WLAN
	Group. You can edit WLAN groups in NMS Settings → WLAN .
Guest	Assign the access point's 2.4GHz or 5GHz SSID(s) to a Guest
Network	Network Group. You can edit Guest Network groups in NMS
Group	Settings → Guest Network.
RADIUS	Assign the access point's 2.4GHz SSID(s) to a RADIUS group.
Group	You can edit RADIUS groups in NMS Settings → RADIUS .
MAC Access	Assign the access point's 2.4GHz SSID(s) to a RADIUS group.
Control	You can edit RADIUS groups in NMS Settings -> Access
Group	Control

X-5-1-1-8 Events

Press "Refresh" to refresh the event log Press "Save" to save the event log as .log file.

Events	ents				
Search				Match whole words	
ID 🔻	Date and Time	Severity 🔺	Users 🔺	Events/Activities	
15	2012/01/01 00:01:10	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected	
14	2012/01/01 00:07:01	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully	
13	2012/01/01 00:00:21	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully	
12	2012/01/01 00:00:55	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully	
11	2012/01/01 00:01:05	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully	
10	2012/01/01 00:07:40	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected	
9	2012/01/01 00:09:57	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully	
8	2012/01/01 00:00:24	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully	
7	2012/01/01 00:10:31	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected	
6	2012/01/01 00:12:15	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully	
5	2012/01/01 00:13:58	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected	
4	2012/01/01 00:14:31	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully	
3	2012/01/01 00:00:22	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully	
2	2012/01/01 00:00:55	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully	
1	2012/01/01 00:00:23	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully	
Save	Refresh				

X-5-1-2 Add/Edit Access Point Group

Configure your selected access point group. Access point group settings apply to all access points in the group, unless individually set to override group settings.

You can use **Profile Group Settings** to assign the access point group to WLAN, Guest Network, RADIUS and Access Control groups.

Click "Save" to save the settings. Click "Cancel" to forfeit the changes. Click "Save and Apply" to save and apply the settings.

X-5-1-2-1 Edit Basic Group Settings

The **Group Settings** panel can be used to quickly move access points between existing groups: select an access point and use the drop down menu or search

to select access point groups and use << and >> arrows to move APs between groups.

Basic Group Settings		
Name	System Default	
Description	System default group for APs	
IGMP Snooping	Disable •	

Basic Group Se	ttings
Name	Edit the access point group name.
Description	Enter a description of the access point group for reference
	e.g. 2 nd Floor Office Group.
IGMP	Enable / Disable the IGMP Snooping function.
Snooping	IGMP snooping is the process of listening to Internet Group
	Management Protocol (IGMP) network traffic.

X-5-1-2-2 Edit Web Account Group Settings

	gs	
	admin	
Administrator Name	aumm	

X-5-1-2-3 Edit VLAN Group Settings

VLAN Group Settings		
Wired LAN Port	VLAN Mode	VLAN ID
Wired Port(#1)	Untagged Port <	1
Wired Port(#2)	Untagged Port <	1
wirea Port(#2)		1
Management VLAN ID	1	

X-5-1-2-4 Edit Radio Group Settings

adio Group Settings				
auto Group Settings				
	Radio B/G/N (2.4	GHz)	Radio A/N/AC ((5.0 GHz)
Wireless	Enable •		Enable •	
Band	11b/g/n ▼		11a/n/ac ▼	
Auto Pilot	Disable •		Disable •	
Auto Pilot Sensitivity	Low •		Low 🔻	
Auto Pilot Range	Ch 1 - 11 🔻		Band 1	Ŧ
Auto Dilat Interval	Half day 🔻		Half day	7
Auto Pilot Interval	Change channel even if clients are connected		Change channel even if clients are connected	
Channel	Ch 11, 2462M	Hz ▼	Ch 36, 5.180	GHz 🔻
Channel Bandwidth	20 MHz	T	20 MHz	▼
		T	all	¥
BSS BasicRateSet	all		un	
0	js			
0			Radio A/N/AC	
Advanced Setting	Radio B/G/N (2.4			
Advanced Setting	IS Radio B/G/N (2.4 Short ▼			
Advanced Setting Contention Slot Preamble Type	Radio B/G/N (2. Short ▼ Short ▼		Radio A/N/AC	
Advanced Setting Contention Slot Preamble Type Guard Interval	Radio B/G/N (2. Short ▼ Short ▼ Short GI ▼		Radio A/N/AC	
Advanced Setting Contention Slot Preamble Type Guard Interval 802.11n Protection	Radio B/G/N (2.4 Short • Short • Short GI • Enable •		Radio A/N/AC	
Advanced Setting Contention Slot Preamble Type Guard Interval 802.11n Protection CE Adaptive	Radio B/G/N (2.4 Short V Short V Short GI V Enable V Disable V	4 GHz)	Radio A/N/AC	(5.0 GHz)
Advanced Setting Contention Slot Preamble Type Guard Interval 802.11n Protection CE Adaptive DTIM Period	Radio B/G/N (2.4 Short V Short V Short GI V Enable V Disable V 1	4 GHz) (1-255)	Radio A/N/AC Short GI ▼ Enable ▼ 1	(5.0 GHz) (1-255)
Advanced Setting Contention Slot Preamble Type Guard Interval 802.11n Protection CE Adaptive DTIM Period RTS Threshold	Radio B/G/N (2. Short Short Short Charlet Short Short Short GI Charlet Short GI Short	4 GHz) (1-255) (1-2347)	Radio A/N/AC	(5.0 GHz) (1-255) (1-2347)
Advanced Setting Contention Slot Preamble Type Guard Interval 802.11n Protection CE Adaptive DTIM Period RTS Threshold Fragment Threshold	Radio B/G/N (2.4 Short V Short V Short GI V Enable V Disable V 1 2347 2346	4 GHz) (1-255) (1-2347)	Radio A/N/AC (Short GI • Enable • 1 2347 2346	(5.0 GHz) (1-255) (1-2347)
Advanced Setting Contention Slot Preamble Type Guard Interval 802.11n Protection CE Adaptive DTIM Period RTS Threshold Fragment Threshold Multicast Rate	Radio B/G/N (2.4 Short V Short Short GI V Enable V Disable V 1 2347 2346 Auto V	4 GHz) (1-255) (1-2347)	Radio A/N/AC Short GI • Enable • 1 2347 2346 Auto •	(5.0 GHz) (1-255) (1-2347)

Radio Group Se	ettings
Wireless	Enable or disable the access point group's 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Band	Select the wireless standard used for the access point group. Combinations of 802.11b, 802.11g, 802.11n & 802.11ac can be selected.
Auto Pilot	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point group's 2.4GHz or 5GHz frequency based on availability and potential interference. When disabled, select a channel manually.
Auto Pilot Sensitivity	Select sensitivity of Auto Pilot.
Auto Pilot Range	Select a range from which the auto channel setting (above) will choose a channel.

Auto Pilot	Specify a frequency for how often the auto channel setting
Interval	will check/reassign the wireless channel. Check/uncheck the
	"Change channel even if clients are connected" box according
	to your preference.
Channel	When Auto Pilot is disabled, select a channel (1-11) manually.
Channel	Set the channel bandwidth or use Auto (automatically select
Bandwidth	based on interference level).
BSS	Set a Basic Service Set (BSS) rate: this is a series of rates to
BasicRateSet	control communication frames for wireless clients.

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.



Changing these settings can adversely affect the performance of your access points.

Advanced Setti	ngs
Contention	Select "Short" or "Long" – this value is used for contention
Slot	windows in WMM (see x-6-7 WMM).
Preamble	Set the wireless radio preamble type. The preamble type in
Туре	802.11 based wireless communication defines the length of
	the CRC (Cyclic Redundancy Check) block for communication
	between the access point and roaming wireless adapters. The
	default value is "Short Preamble".
Guard	Set the guard interval. A shorter interval can improve
Interval	performance.
802.11n	Enable/disable 802.11n protection, which increases reliability
Protection	but reduces bandwidth (clients will send Request to Send
	(RTS) to access point, and access point will broadcast Clear to
	Send (CTS), before a packet is sent from client.)
CE Adaptive	The measurement procedure follows clause 5.3.11.2.2 of the
	ETSI EN 300 328 V1.8.1
DTIM Period	Set the DTIM (delivery traffic indication message) period value
	of the wireless radio. The default value is 1.
RTS	Set the RTS threshold of the wireless radio. The default value
Threshold	is 2347.

Fragment	Set the fragment threshold of the wireless radio. The default
Threshold	value is 2346.
Multicast	Set the transfer rate for multicast packets or use the "Auto"
Rate	setting.
Tx Power	Set the power output of the wireless radio. You may not
	require 100% output power. Setting a lower power output can
	enhance security since potentially malicious/unknown users
	in distant areas will not be able to access your signal.
Beacon	Set the beacon interval of the wireless radio. The default
Interval	value is 100.
Station idle	Set the interval for keepalive messages from the access point
timeout	to a wireless client to verify if the station is still alive/active.

X-5-1-2-5 Edit WMM-EDCA Settings

	WMM Parameters of Access Point				
	CWMin	CWMax	AIFSN	TxOP	
Back Ground	4	10	7	0	
Best Effort	4	6	3	0	
Video	3	4	1	94	
Voice	2	3	1	47	
	WMM Parameters of Station CWMin CWMax AIFSN TxOP				
Back Ground	4	10	7	0	
Best Effort	4	10	3	0	
Video	3	4	2	94	
Voice	2	3	2	47	

X-5-1-2-6 Edit BandSteering Settings



X-5-1-2-7 Edit Profile Settings

Profile Group Settings			
	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)	
WLAN Group	Disable •	Disable v	
Guest Network Group	Disable •	Disable •	
RADIUS Group	Disable •		
MAC Access Control Group	Disable •		

Profile Group S	ettings
WLAN Group	Assign the access point group's 2.4GHz or 5GHz SSIDs to a
	WLAN Group. You can edit WLAN groups in NMS Settings ->
	WLAN.
Guest	Assign the access point group's 2.4GHz or 5GHz SSIDs to a
Network	Guest Network Group. You can edit Guest Network groups in
Group	NMS Settings -> Guest Network.
RADIUS	Assign the access point group's 2.4GHz SSIDs to a RADIUS
Group	group. You can edit RADIUS groups in NMS Settings ->
	RADIUS.
MAC Access	Assign the access point's 2.4GHz SSIDs to a RADIUS group. You
Control	can edit RADIUS groups in NMS Settings → Access Control.
Group	

X-5-1-2-8 Edit Group Settings



Displays information about each WLAN and WLAN group in the local network and allows you to add or edit WLANs & WLAN Groups. When you add a WLAN Group, it will be available for selection in **NMS Settings** \rightarrow **Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (X-5-1).

The **search** function can be used to locate a WLAN or WLAN Group. Type in the search box and the list will update:

	Search [↓ Match whole words		
WLAN						
Search			Match whole words			
	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication	
	wap1750	1	WPA2PSK	AES	No additional authentication	
Add Ed	lit Clone Delete Selected	Delete All				
VLAN Grou	ıps					
earch			Match whole words			
	Group Name	WLAN members	WLAN m	ember list	Used AP	Used AP Group
		1	wap	1750	AP74DA381D264E	Wizard AP Group 2
	Wizard WLAN 2.4G Group 1					

Select a WLAN or WLAN Group using the check-boxes and click "**Edit**" or click "**Add**" to add a new WLAN or WLAN Group:



X-5-2-1 Add/Edit WLAN

WLAN Settings		
Name/ESSID		
Description		
VLAN ID	1	
Broadcast SSID	Enable •	
Wireless Client Isolation	Disable	T
802.11k	Disable •	
Load Balancing	50 /10	0
Authentication Method	No Authent	
Additional Authentication	n No addition	al authentication
WLAN Access Policy		
WEAN Access Foney		
Traffic Shaping Settings		
Traffic Shaping	Disable •	
Downlink	50 Mbps	
Uplink	50 Mbps	
WLAN Advanced Se	tings	
Smart Handover Settin	igs	
Smart Handover	Enable	Disable
RSSI Threshold	-80 ▼ dB	
Active WLAN Schedul	Soffings *Place	e enable (NMS Settings
>Advanced->Date and Tir		
work.		
Schedule Group	Disable •	
Save Cancel Sa	ave & Apply	

WLAN Settings	
Name/ESSID	Edit the WLAN name (SSID).
Description	Enter a description of the SSID for reference e.g. 2 nd Floor
	Office HR.
VLAN ID	Specify the VLAN ID.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID
	will be visible to clients as an available Wi-Fi network. When
	disabled, the SSID will not be visible as an available Wi-Fi

	network to clients – clients must manually enter the SSID in
	order to connect. A hidden (disabled) SSID is typically more
	secure than a visible (enabled) SSID.
Wireless Client	Enable or disable wireless client isolation. Wireless client
Isolation	isolation prevents clients connected to the access point from
	communicating with each other and improves security.
	Typically, this function is useful for corporate environments
	or public hot spots and can prevent brute force attacks on
	clients' usernames and passwords.
802.11k	Enable / Disable to define and expose radio and network
	information (helps facilitate the management and
	maintenance of a mobile wireless LAN).
Load Balancing	Load balancing limits the number of wireless clients
	connected to an SSID. Set a load balancing value (maximum
	100).
Authentication	Select an authentication method from the drop down menu.
Method	
WPA Type	It can select WPA only or WPA2 only or WPA/WPA2 Mixed
	Mode-PSK
Encryption	It can select TKIP/AES Mixed Mode or AES
Туре	
Key Renewal	It can set renewal internal time
Interval	
Pre-Shared	It can set Passphrase or Hex (64 characters)
Кеу Туре	
Pre-Shared	It can set 8-64 characters
Кеу	
Additional	Select an additional authentication method from the drop
Authentication	down menu.

Various security options (wireless data encryption) are available. When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.



It is essential to configure wireless security in order to prevent unauthorised access to your network.



Select hard-to-guess passwords which include combinations of numbers, letters and symbols, and change your password regularly.

WLAN Access P	WLAN Access Policy				
Traffic	Enable / Disable traffic shaping.				
Shaping					
Downlink	Set downlink between 1-200Mbps				
Uplink	Set uplink between 1-200Mbps				

WLAN Advance	ed Settings
Smart	Enable or disable Smart Handover.
Handover	
RSSI	Set a RSSI Threshold level.
Threshold	

X-5-2-2 Add/Edit WLAN Group

When you add a WLAN Group, it will be available for selection in NMS Settings \rightarrow Access Point access point Profile Settings & access point group Profile Group Settings (x-5-1).

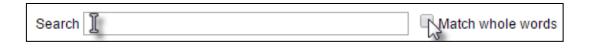
Name	Wizard W	Wizard WLAN 2.4G Group 1				
Description	Created b	Created by Wizard				
	Search Match whole words					
Members		Name/ESSID wap1750	Override	/LAN ID 1	Schedule Group	
	*Schedule Group function will not work until (<u>NMS Settings->Advanced->Date and Time->NTP</u> Time Server) are enabled.					

WLAN Group S	Settings			
Name	Edit the WLAN Group name.			
Description	Enter a description of the WLAN Group for reference e.g. 2 nd			
	Floor Office HR Group.			
Members	Select SSIDs to include in the group using the checkboxes and			
	assign VLAN IDs.			

X-5-3 RADIUS

Displays information about External & Internal RADIUS Servers, Accounts and Groups and allows you to add or edit RADIUS Servers, Accounts & Groups. When you add a RADIUS Group, it will be available for selection in NMS Settings → Access Point access point Profile Settings & access point group Profile Group Settings (X-5-1).

The **search** function can be used to locate a RADIUS Server, Account or Group. Type in the search box and the list will update:



Edit

Add

Make a selection using the check-boxes and click "**Edit**" or click "**Add**" to add a new WLAN or WLAN Group:

Externa	al RADIUS Server					
-						
Search		Match	whole words			
	Name	R	ADIUS Server	Authentication Port Se	ession Timeout (sec)	Accounting
		Plea	ase add External RADIUS Server setting			
Add	Edit Clone Delete Selected D	Delete All				
Add						
Internal	l RADIUS Server					
Interna	i KADIUS Server					
Search		Match	whole words			
	Name	EAP Authentication	Session Timeout (sec)	Termination-Action		
		Please add Internal RADI	IUS Server setting			
Add	Edit Clone Delete Selected D	Delete All				
/100						
RADIU	S Accounts (Max: 256 users)					
	· · ·					
Search		Match	whole words			
Search	Name	Password	whole words Description			
		Password se add User Account				
	Plea	Password				
Add	Plea	Password se add User Account				
Add	Plea Edit Delete Selected Delete All	Password se add User Account Import Export	Description			
Add	Plea Edit Delete Selected Delete All	Password se add User Account Import Export				
Add	Plea Edit Delete Selected Delete All	Password se add User Account Import Export	Description Whole words 5GHz RADIUS Accounts	Used AP	Us	ed AP Group
Add RADIUS Search	Plea Edit Delete Selected Delete All S Group	Password se add User Account Import Export	Description whole words	: Used AP	Us	ed AP Group

X-5-3-1 Add/Edit External RADIUS Server

lame		
escription		
ADIUS Server		
uthentication Port	1812	
hared Secret		
ession Timeout	3600	Seconds
ccounting	Enable	Disable
ccounting Port	1813	

Name	Enter a name for the RADIUS Server.
Description	Enter a description of the RADIUS Server for reference.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication	Set the UDP port used in the authentication protocol of the
Port	RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in
	length. This should match the "MAC-RADIUS" password used
	in x-6-2-3 or x-6-3-3.
Session	Set a duration of session timeout in seconds between 0 –
Timeout	86400.
Accounting	Enable or disable RADIUS accounting.
Accounting	When accounting is enabled (above), set the UDP port used
Port	in the accounting protocol of the RADIUS server. Value must
	be between 1 – 65535.

X-5-3-2 Add/Edit Internal RADIUS Server

P Certificate File Format PKCS#12(*.pfx/*.p12)				
Upload EAP Certificate File	Choose File	No file chosen		
Password of EAP Certificate File				
Upload ternal RADIUS Server				
ternal KADIUS Server				
Name				
Name Description				
	PEAP(MS-P	EAP) v		
Description	PEAP(MS-P	EAP) V		
Description EAP Internal Authentication	PEAP(MS-P	EAP) ▼ Seconds		
Description EAP Internal Authentication Shared Secret	3600			
Description EAP Internal Authentication Shared Secret	3600 Reauthenic	Seconds		

Upload EAP Cert	ificate File
EAP Certificate	Displays the EAP certificate file format: PKCS#12(*.pfx/*.p12)
File Format	
EAP Certificate	Click "Upload" to open a new window and select the location
File	of an EAP certificate file to use. If no certificate file is
	uploaded, the internal RADIUS server will use a self-made
	certificate.

Internal RADIUS	I RADIUS Server	
Name	Enter a name for the Internal RADIUS Server.	
Description	Enter a description of the Internal RADIUS Server for	
	reference.	
EAP Certificate	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)	
File Format		
EAP Certificate	Click "Upload" to open a new window and select the location	
File	of an EAP certificate file to use. If no certificate file is	
	uploaded, the internal RADIUS server will use a self-made	

	certificate.
EAP Internal	Select EAP internal authentication type from the drop down
Authentication	menu.
Shared Secret	Enter a shared secret/password for use between the internal
	RADIUS server and RADIUS client. The shared secret should
	be 1 – 99 characters in length.
Session	Set a duration of session timeout in seconds between 0 –
Timeout	86400.
Termination	Select a termination-action attribute: "Reauthentication"
Action	sends a RADIUS request to the access point,
	"Not-Reauthentication" sends a default termination-action
	attribute to the access point, "Not-Send" no
	termination-action attribute is sent to the access point.

X-5-3-3 Add/Edit/Import/Export RADIUS Accounts

The internal RADIUS server can authenticate up to 256 user accounts. The "RADIUS Accounts" page allows you to configure and manage users.

RADIUS Accounts			
User Name			
Example: USER1, USER2, USER3			
		1	
Add Reset			
User Registration List			
User Name	Password	Description	Action
	Please add Acco	unt(s)	
Save Cancel Save & Apply			

<u>Auu</u>

RADIUS	Accounts	
User Nam		
	= JSER1, USER2, USER3	
EdimaxN	lew	
Add	Reset	
User Registration List		
User Registration List		
User Name	Password	Description
EdimaxNew	••••	
Edimax1	Configured	Edimax1

RADIUS Accounts		
User Name Enter the user names here, separated by commas.		
Add Click "Add" to add the user to the user registration list.		
Reset	Clear text from the user name box.	

User Registration List		
User Name	Displays the user name.	
Password	Enter a password.	
Description	Enter a description of the user.	
Delete	Delete the user.	

<u>Edit</u>

User Registration List		
User Name	Password	Description
Edimax1	····	Edimax1
Save Cancel Save & Apply		

Edit User Registration List		
User Name	Existing user name is displayed here and can be edited	
	according to your preference.	
Password	assword Enter or edit a password for the specified user.	
Description	Displays current description of the user and can be edited.	

Delete	Delete selected user from the user registration list.	
Selected		
Delete All	Delete all users from the user registration list.	

<u>Import</u>

If you wish to import RADIUS accounts, press "Import". The following page is displayed below. Choose a file from a file and press "Upload" to import RADIUS accounts.

upload RADI	US Accounts file	Choose File	No file chosen	
Upload	Cancel			

<u>Export</u>

If you wish to export your current list of RADIUS accounts, press "Export". Your list will be saved in a format similar to the one below:

🗟 local_radius_users.csv

X-5-3-4 Add/Edit RADIUS Group

When you add a RADIUS Group, it will be available for selection in NMS Settings \rightarrow Access Point access point Profile Settings & access point group Profile Group Settings (x-5-1).

Group Name			
Description			
2.4GHz RADIUS	Primary : Disabled	Secondary : Disabled V	
5GHz RADIUS	Primary : Disabled	Secondary : Disabled V	
	Search	Match whole	words
Members		Username	Password
		Edimax1	Configured
	Add	•	•••

RADIUS Group Settings			
Group Name Edit the RADIUS Group name.			
Description	Enter a description of the RADIUS Group for reference.		
2.4GHz	Enable/Disable primary & secondary RADIUS servers for		
RADIUS 2.4GHz.			
5GHz Enable/Disable primary & secondary RADIUS servers for 5GHz			
RADIUS			
Members	nbers Add RADIUS user accounts to the RADIUS group.		

X-5-4 Access Control

MAC Access Control is a security feature that can help to prevent unauthorized users from connecting to your access point.

This function allows you to define a list of network devices permitted to connect to the access point. Devices are each identified by their unique MAC address. If a device not on the list of permitted MAC addresses attempts to connect to the access point, it will be denied.

The Access Control panel displays information about MAC Access Control & MAC Access Control Groups and Groups and allows you to add or edit MAC Access Control & MAC Access Control Group settings. When you add an Access Control Group, it will be available for selection in **NMS Settings** \rightarrow **Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (x-5-1).

The **search** function can be used to locate a MAC address or MAC Access Control Group. Type in the search box and the list will update:



Make a selection using the check-boxes and click "**Edit**" or click "**Add**" to add a new MAC Address or MAC Access Control Group:

MAC Acc	MAC Access Control (Max: 256 items)						
Search			Match whole wor	ds			
	MAC Address		De	scription			
		Please add MAC Acce	ess Control setting				
Add	Add Delete Selected Delete All						
MAC Acc	MAC Access Control Group						
Search	Search Match whole words						
	Group Name	Policy	Members	Used AP	Used AP Group		
			No MAC Access Cor	trol Group			
Add	Edit Clone Delete Selecte	Delete All					

Delete the selected entry(s) from the list.	
Selected	
Delete All	Delete all entries from the table.

X-5-4-1 Add/Edit MAC Access Control

Click "Add" to enter the page shown below:

MAC Access Control		
Add MAC Address		
Example: MAC1, MAC2, MAC3		
Remain entries(256)		
Add Reset	#	
MAC Access Control List		
MAC Address	Description	Delete
Ple	ease add MAC Addresses.	
Save Cancel Save & Apply		

Add MAC	Enter a MAC address of computer or network device manually	
Address	e.g. 'aa-bb-cc-dd-ee-ff' or enter multiple MAC addresses	
	separated with commas, e.g.	
	'aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg'	
Add	Click "Add" to add the MAC address to the MAC address filtering	
	table.	
Reset	Clear all fields.	

MAC address entries will be listed in the "MAC Address Filtering Table". Select an entry using the "Select" checkbox.

X-5-4-2 Add/Edit/Clone MAC Access Control Group

When you add an Access Control Group, it will be available for selection in **NMS Settings** \rightarrow **Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (x-5-1).

Click "Add" to enter the page shown below:

MAC Filter Group Setting	s			
Group Name	Please enter a new grou	up name		
Description	Please enter a new grou	Please enter a new group description		
Action	Blacklist 🔻		_	
	Search	Match whole words		
Members		MAC Address	Description	
		AA:BB:CC:DD:EE:FF		
Save Cancel Save &	Apply			

MAC Filter G	MAC Filter Group Settings			
Group	Edit the MAC Access Control Group name.			
Name				
Description	tion Enter a description of the MAC Access Control Group for			
	reference.			
Action Select "Blacklist" to deny access to specified MAC addresses				
	the group, and select "Whitelist" to permit access to specified			
	MAC address in the group.			
Members	Check the checkbox to add MAC addresses to the group.			

X-5-5 Guest Network

You can setup an additional "Guest" Wi-Fi network so guest users can enjoy Wi-Fi connectivity without accessing your primary networks. The "Guest" screen displays settings for your guest Wi-Fi network.

The Guest Network panel displays information about Guest Networks and Guest Network Groups and allows you to add or edit Guest Network and Guest Network Group settings. When you add a Guest Network Group, it will be available for selection in NMS Settings \rightarrow Access Point access point Profile Settings & access point group Profile Group Settings (x-5-1).

The **search** function can be used to locate a Guest Network or Guest Network Group. Type in the search box and the list will update:

Search	ole words
--------	-----------

Make a selection using the check-boxes and click "**Edit**" or click "**Add**" to add a new Guest Network or Guest Network Group.



Guest N	letwork				
Search		Match wh	ole words		
	Name/ESSID	VLAN ID Authe	ntication Encryption	Additional Authentication	
		Please add Guest Ne	twork setting		
Add	Edit Clone Delete Selected	Delete All			
Guest N	letwork Group				
Search		Match where the second seco	ole words		
	Group Name	Guest Network members	Guest Network member	er list Used AP	Used AP Group
		Ple	ase add Guest Network Group s	etting	
Add	Edit Clone Delete Selected	Delete All			

Delete	lete Delete the selected entry(s) from the list.	
Selected		
Delete All	Delete all entries from the table.	

X-5-5-1 Add/Edit Guest Network

Click "Add" to enter the page shown below:

Guest Netwo	rk Settings			
Name/ESSID				
Description				
VLAN ID		1		
Broadcast S		Enable <		
Wireless Clie	ent Isolation	STA Separator V		
802.11k		Disable ▼		
Load Balanci	ing	50 /100		
Authenticatio	on Method	No Authentication	1	
Additional A				•
Guest Access	s Policy			
Guest Portal	Settings			
Guest Portal		Disable 🔻		
Traffic Shapir	ng Settings			
Traffic Shapi		Disable •		
Downlink	Ę	50 Mbps		
Uplink	Ę	50 Mbps		
Layer 3-Filter	ing Settings			
Rules	Disable	•		
	Туре	IP Address	Sub	net Mask
	Disable •	0.0.0.0	0.0.0.0	
	Disable •	0.0.0.0	0.0.0.0	
	Disable •	0.0.0.0	0.0.0.0	
	Disable •	0.0.0.0	0.0.0.0	
Exceptions	Disable •	0.0.0.0	0.0.0.0	
	Disable •	0.0.0.0	0.0.0.0	
	Disable 1	0.0.0.0	0.0.0.0	
	Disable •	0.0.0.0	0.0.0.0	
	Disable •		0.0.0.0	
	Disable 1		0.0.0.0	
Guest Netwo	rk Advance	ed Settings		
		*This function will not v		
Settings->Advanced->Date and Time->NTP Time Server) are enabled. Schedule Group Disable ▼				
Save Can		0.0.1		
	cel Save	& Apply		

Cuest Network Cettings				
Guest Network S				
Name/ESSID	Edit the Guest Network name (SSID).			
Description	Enter a description of the Guest Network for reference e.g.			
	2 nd Floor Office HR.			
VLAN ID	Specify the VLAN ID.			
Broadcast SSID Enable or disable SSID broadcast. When enabled, the				
	will be visible to clients as an available Wi-Fi network. When			
	disabled, the SSID will not be visible as an available Wi-Fi			
	network to clients – clients must manually enter the SSID in			
	order to connect. A hidden (disabled) SSID is typically more			
	secure than a visible (enabled) SSID.			
Wireless Client	Enable or disable wireless client isolation. Wireless client			
Isolation	isolation prevents clients connected to the access point from			
	communicating with each other and improves security.			
	Typically, this function is useful for corporate environments			
	or public hot spots and can prevent brute force attacks on			
	clients' usernames and passwords.			
802.11k	Enable / Disable to define and expose radio and network			
	information (helps facilitate the management and			
	maintenance of a mobile wireless LAN).			
Load Balancing	Load balancing limits the number of wireless clients			
	connected to an SSID. Set a load balancing value (maximum			
	100).			
Authentication	Select an authentication method from the drop down menu.			
Method				
Additional	Select an additional authentication method from the drop			
Authentication	down menu.			
Authentitation				

Various security options (wireless data encryption) are available. When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.



It is essential to configure wireless security in order to prevent unauthorised access to your network.



Select hard-to-guess passwords which may include combinations of numbers, letters and symbols, and change your passwords regularly. Please refer to x-6-2-3 or x-6-3-3 for more information on authentication and additional authentication types.

Guest Access Po	licy
Guest Portal	Enable or disable guest portal for the guest network.
Traffic Shaping	Enable or disable traffic shaping for the guest network.
Downlink	Enter a downlink limit in MB.
Uplink	Enter an uplink limit in MB.
Rules	Enter IP addresses to be filtered according to the drop down
	menu: "Allow all by Default", "Deny all by Default", "Internet
	Only" and "Disable"
Exceptions	After selecting the rule above, exceptions can be setup to
	allow / deny guest access.

Guest Network Advanced Settings			
Schedule	Select a schedule group.		
Group			

Clone	Select an entry and clone its settings. You will be taken to the
	add guest network settings page shown above. Enter / edit
	the fields and save your selection.

X-5-5-2 Add/Edit Guest Network Group

When you add a Guest Network Group, it will be available for selection in **NMS Settings** \rightarrow **Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (x-5-1).

Name				
Description				
Members	Search		Match whole words	
		Name/ESSID	VLAN ID	Schedule Group
		EdimaxGuest	Override 1	Override Disable 🔻
	*Schedule Gro enabled.	up function will not	work until (<u>NMS Settings->Advanced->C</u>	Date and Time->NTP Time Server) are

Guest Network Group Settings			
Group Name	Edit the Guest Network Group name.		
Description	Enter a description of the Guest Network for reference.		
Members	Add SSIDs to the Guest Network group.		

earch			• N	atch whole words					
	Name	Create Time	Valid Pe	iod Expiration Date	Description	Traffic Usage	Traffic Limitation	Status	Action
	aaa	2012/01/01 02:40:	05 Alway	;		0%	Disabled	0	06
	test1	2017/08/28 18:47:	20 Alway	;		0%	Disabled	0	06
	t2	2017/08/30 14:17:	26 Alway	;	t2	0%	Disabled	0	06
Jser Gro	Edit Clone	Delete Selected	Delete All Expire	d Users Delete All	Upload List Dow	nload List			
Jser Gro Search	oup			atch whole words					
Jser Gro	Gro	Delete Selected	· ·			Description		Role Ty Defau	pe
Jser Gro	Gro	up Name	User members	atch whole words				Role Ty	pe It
fser Gro	Gro	up Name Default	User members 0	atch whole words User member				Role Ty Defau	pe It nanager

User Panel

Press "Add" to add a new user, or "Edit" to edit an existing user, or "Clone" to clone an existing user's settings. For the 3 options specified above, enter the fields below:

User Settings	
Name	
Description	
Password	
Confirm Password	
User Group	Default T
Usage Traffic Managemer	ıt
Maximum Usage Traffic	■ Enable 100 MB ▼ (Max: 1 TB)
Apply Cancel	

Press "Save" to save the above actions, or "Cancel" to forfeit the changes. Check the checkbox of the user(s) you wish to delete and press "Delete Selected" to delete (multiple selections possible).

Press "Delete All Expired Users" to delete the expired users.

Press "Delete All" to delete all users.

Use "Upload List" to upload a user list.

Use "Download List" to download existing list for possible future reference.

User Group Panel

Click "Add" to add a new user group, or "Edit" to edit an existing user group, or "Clone" to clone an existing user group's settings. For the 3 options specified above, enter the fields below:

User Group Se	ettings		
Name			
Description			
Role Type	Default	T	
	Search	Match whole	words
Members	Name	User Group	Description
		Please add User setting	g
Apply Car	ncel		

Press "Save" to save the above actions, or "Cancel" to forfeit the changes. Check the checkbox of the user group(s) you wish to delete and press "Delete Selected" to delete (multiple selections possible).

Press "Delete All" to delete all user groups.

X-5-7 Guest Portal

A guest portal is a web page which is displayed to newly connected users before they are granted broader access to network resources.

Guest Portal					
Search		Match whole words			
Name		Guest Portal Type	Used Guest Network		
		Please add Guest Portal setting			
Add Edit Delete Se	Delete All				
Guest Portal Settings					
Idle Timeout	5 • minutes				
Login Password Retry Lockout	5 (1-30 times)				
Save Save & Apply					

Check the checkbox of the portal(s) you wish to delete and press "Delete Selected" to delete (multiple selections possible). Press "Delete All" to delete all portals.

Guest Portal Settings			
Idle Timeout	Idle Timeout Select an idle timeout time from the drop down menu.		
Login	Enter a number (between 1 and 30) for the number of login		
Password	password retry. If login password has been entered		
Retry Lockout	incorrectly for the number entered here, it will be locked.		

Add / Edit

Enter the fields according to the selected "Guest Portal Type" below:

Dynamic Users	•
Free	
Service Level Agreement	
Static Users	
Dynamic Users	
External Captive Portal	

Press "Save & Apply" to save the above actions, or "Cancel" to forfeit the changes.

X-5-7-1 Free Guest Portal Type

Guest Portal Settings	
Name	portal1
Description	portl1
Guest Portal Type	Free •
Landing Page	● Promotion URL http:// ▼
Save & Apply Cancel	

Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Landing Page	Enter a "Promotion URL".

X-5-7-2 User Level Agreement Guest Portal Type

Guest Portal Settings		
Name	portal1	
Description	porti1	
Guest Portal Type	Service Level Agreement	
Landing Page	Redirect to the original URL	
	Promotion URL http://	
Default Language	Global (English)	
Guest Portal Customization		
Levin Portel		
<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>		

Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Landing Page	Select between "Redirect to the original URL" or "Promotion
	URL" (enter the promotion URL).
Default	Choose a default language.
Language	

For Login Portal, click "Edit" and see below to edit the login portal.

X-5-7-3 Static Users Guest Portal Type

Guest Portal Settings		
Name	portal1	
Description	portl1	
Guest Portal Type	Static Users	
Authentication Server	Local Database	
Authentication User Group	111 •	
Landing Page	 Redirect to the original URL Promotion URL http:// 	
Default Language	Global (English)	
Login Portal Edit		
	Captive Portal Login	
Login page preview	Global (English) • User Name	
	Password	
	Login Remember Me	
	Accept <u>Terms of use</u>	

Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Authentication	Select an authentication server.
Server	
Authentication	Select an authentication user group.
User Group	

Landing Page	Select between "Redirect to the original URL" or "Promotion
	URL" (enter the promotion URL).
Default	Choose a default language.
Language	

For Login Portal, click "Edit" and see below to edit the login portal.

X-5-7-4 Dynamic Users Guest Portal Type

Name portal1 Description port11 Quest Fortal Type Dynamic Users Authentication User Group 111 Landing Page Promotion URL Promotion URL Promotion URL Default Language Ciclobal (English) Fortal Cettors Buser Group Test Generation URL Map/192.168.2.3/fondidesk.html Guest Account Creation Preplace expined user, when user table is full Printour Message Edit Login Portal Edit Captive Portal Login Login page preview Captive Portal Login Login page preview Captive Portal Login Login page preview Login	Guest Portal Settings	
Description portI1 Guest Forcial Type Dynamic Users Authentication Server Local Database • Authentication User Group 111 anding Page Promotion URL http:// • Default Language Global (English) • Fond Desk Settings User Group 1651 • Generation URL http:// 162 168 2.3/montides. html Guest Acount Creation Replace expired user, when user table is full Printout Message Edit Notification Method Pinntout Capital Castomization Capital Castomization Capitre Portal Login User Around Castomization Capitre Portal Login User Name Capitre Portal Login User Name Capitre Portal Login User Name Resember Me	News	portal1
Guest Portal Type Dynamic Users Authentication Sever Local Database • Authentication User Group I11 Landing Page		
Authentication Server Local Database Authentication User Group III1 Promotion URL [http:// Promotio		
Authentication User Group 111 Redirect to the original URL Promotion URL http:// Promotion USE Settings Front Desk Settings User Group Itest Redirece or produce or prod		
Landing Page Promotion URL http:/// Promotion URL http:/// Default Language Global (English) Generation URL http:/// Generation URL Http://// Generation URL Http:/// Generation URL Http://// Generation URL Http:/// Gen		
Landing Page Promotion URL http:// Default Language Global (English) Front Desk Setting: User Group Itest Generation URL Generation URL Generation URL Court Action Propose expired user, when user table is full Printout Message Edit Notification Method Printout Court Portal Edit Login Portal Edit Login page preview User Name Password Egin Password	Authentication User Group	
Default Language		
Froat Desk Settings User Group Generation URL Generation Webod Printout Message Edit Notification Method Colspan="2">Generation Method Colspan="2">Generation Customization Generation Customization Colspan="2">Generation Customization Colspan="2">Colspan="2">Generation Customization Colspan="2">Generation Customization Colspan="2">Generation Customization Colspan="2">Generation Customization Colspan="2">Customization Colspan="2">Customization Customization Customization Customization Customization Customization Customization Customization	Landing Page	Promotion URL http:// *
Froat Desk Settings User Group Generation URL Generation Webod Printout Message Edit Notification Method Colspan="2">Generation Method Colspan="2">Generation Customization Generation Customization Colspan="2">Generation Customization Colspan="2">Colspan="2">Generation Customization Colspan="2">Generation Customization Colspan="2">Generation Customization Colspan="2">Generation Customization Colspan="2">Customization Colspan="2">Customization Customization Customization Customization Customization Customization Customization Customization	Default Learning	Clabal (English)
User Group Lest Generation URL http://192.188.2.3/fonddesk.html Guest Account Creation	Default Language	
User Group Test Generation URL http://192.188.2.3/fonddesk.html Guest Account Creation Replace expired user, when user table is full Printout Message Edit Notification Method Printout		
Generation URL http://192.168.2.3/fontdesk.html Guest Account Creation Replace expired user, when user table is full Printout Message Edit Notification Method Printout	Front Desk Settings	
Generation URL http://192.168.2.3/fontdesk.html Guest Account Creation Replace expired user, when user table is full Printout Message Edit Notification Method Printout	User Group	tect V
Guest Account Creation Replace expired user, when user table is full Printout Message Edit Notification Method Printout Gest Portal Customization Login Portal Edit User Name Password User Name Password		
Printout Message Edit Notification Method Printout Cest Portal Castomization Login Portal Edit User Name Password Password Login Password Password Login		
Guest Portal Customization Login Portal Edit Login page preview Captive Portal Login User Name Password Password Capin Login Remember Me	Printout Message	
Guest Portal Customization Login Portal Edit Login page preview Captive Portal Login User Name Password Password Capin Login Remember Me	Notification Method	Printout
Login Portal Edit Login page preview Image: Captive Portal Login User Name Image: Captive Portal Password Image: Captive Portal Image: Captive Portal Login Image: Captive Portal Image: Captive Portal Login Image: Captive Portal Image: Captive Portal Login Image: Captive Portal Login Image: Captive Portal L		
Login page preview Login value Login page preview Login value Login Login Login Remember Me	Guest Portal Customization	
Login page preview Circle Portal Login Circle (English) User Name Password Login • Remember Me	Login Portal Edit	
Login page preview User Name Password Login VRemember Me		
User Name Password Login Remember Me	Login page preview	NETWORKING PEOPLE TOGETHER
Login		User Name
Login		Password
⊮ Remember Me		
⊮ Remember Me		
Accept <u>lerms of use</u>		
		Accept <u>lerms of use</u>

Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Authentication	Select an authentication server.
Server	
Authentication	Select an authentication user group.
User Group	
Landing Page	Select between "Redirect to the original URL" or "Promotion
	URL" (enter the promotion URL).
Default	Choose a default language.
Language	

Front Desk Settings	
User Group	Select a user group.
Generation	Go to this URL to create dynamic account (and password) for
URL	a user.
Guest Account	Check / uncheck to enable / disable "Replace expired user
Creation	when user table is full".
Printout	Click "Edit" to edit printout message, please see below.
Message	
Notification	Check / uncheck to enable / disable notification by printout.
Method	

Е

Definition Table	
Symbol	Description
{SSID}	The SSID for Guest Portal user
{USERNAME}	The Name of Guest Portal user
{PASSWORD}	The Password of Guest Portal user
{EXPIRETIME}	The expire time of user account
{CREATETIME}	The create time of user account
(SN)	The Serial number of user account
* While printing the user data in Front Desk page, the "Symbol" will b	se replaced by the value in Users database.
Printout Content	
Welcome!	
EDIMAX Technology Co,. Ltd	
Guest Internet Service	
SSID: {SSID}	
Username: {USERNAME}	
Password: {PASSWORD}	
Expire Time: {EXPIRETIME}	
Create Time: {CREATETIME}	
S/N: {SN}	
Thank you very much !	
Preview Confirm Cancel	

Click "Preview" to preview the printout, "Confirm" to confirm the message, or "Cancel" to cancel the changes.

For **Login Portal**, click "Edit" and see below to edit the login portal.

X-5-7-5 External Captive Portal Guest Portal Type

Guest Portal Settings		
Name		
Description		
Guest Portal Type	External Captive Portal The second sec	
Landing Page	 Use external redirect URL Promotion URL http:// 	
External Settings	Autheritication Tout T	
External Type	Authentication Text	
Login URL	http:// 172.217.27.132 Resolve	
		(16-
Authentication Text	32Characters) To know how to use Authentication Text. Please, <u>Click me</u> .	(10-

Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Landing Page	Select between "Use external redirect URL" or "Promotion
	URL" (enter the promotion URL).

External Settings	5
Login URL	Enter / edit a login URL.
Authentication	Enter an authentication text.
Text	Click "Click me" for help.

X-5-7-6 Editing "Login Portal"

Login Portal Customization	
Header Image	Choose File No file chosen
	Size: 800x200 pixels
Logo Image	Choose File No file chosen
Title Message	Captive Portal Login
Background Color	FFFFF
Terms of use	Accept by Default Terms and Conditions of Use Please read these terms and conditions of use ("Terms and Conditions") carefully before accessing and browsing this web site ("Web Site"). You can use this web site only if you agree to and accept the Terms and Conditions without limitation or reservation. We may at our sole and exclusive discretion, change, alter, modify, add, and/or remove portions of the Terms and Conditions at any time by updating the contents of this page. You are requested to visit this page and check the then effective Terms and Conditions periodically.
Preview Confirm Cancel	

Header Image	Click "Choose File" to select a file as the header image.
Logo Image	Click "Choose File" to select a file as the logo image.
	(Only for Static and Dynamic users guest portal type)
Title Message	Enter / edit a title message.
	(Only for Static and Dynamic users guest portal type)
Background	Click on the field where color selection will be available.
Color	Select a desired color.

	FFFFF
Terms of use	Enter / edit the terms of use message

Click "Preview" to preview the printout, "Confirm" to confirm the message, or "Cancel" to cancel the changes.

X-5-8 Zone Edit

Zone Edit displays information about zones for use with the Zone Plan feature and allows you to add or edit zones.

The **search** function can be used to find existing zones. Type in the search box and the list will update:

Search	Match whole words

Add

Make a selection using the check-boxes and click "Edit" or click "Add" to add a new zone.

Zone Edit	t i i i i i i i i i i i i i i i i i i i			
Search		Mate	h whole words	
			655360 bytes Available (655360 bytes Total)
	Name/Location	Мар	Map Size	Number of APs
	F	Please add Zone Edit setting		
Add	Edit Clone Delete Selected D	elete All		

Add/Edit Zone

Map Image File	Choo	se File No file chosen			
Upload	*				
iember(s) Settings					
	-J				
ember(s) Settings					
ember(s) Settings	Search		Match whole words		
ember(s) Settings	Search	MAC Address	Match whole words Device Name	Model	Status
iember(s) Settings	Search	MAC Address System Default		Model	Status
ember(s) Settings				Model WAP1200	Status
ember(s) Settings		System Default	Device Name		

Upload Zone Ima	age
Choose File	Click to locate an image file to be displayed as a map in the
	Zone Plan feature. Typically a floor plan image is useful.

Member(s) Setti	ng
Name/Location	Name the location or simply enter the name of the location.
Description	Enter a description of the zone/location for reference.
Members	Assign access points to the specified zone/location for use
	with the Zone Plan feature.

X-5-9 Schedule

Setup schedule start time/end time in Active WLAN Schedule Settings or Guest Network Advanced Settings.

Schedul	e				
Search		Match v	whole words		
	Name	Description	Day of week	Time	
		Please add Schedu	Ile setting		
Add	Add Edit Delete Selected Delete All				
Schedul	e Groups				
Search		Match v	whole words		
	Group Name	Schedule members	Schedule member list		
Please add Schedule group setting					
Add	Edit Delete Selected Delete	All			

Check the checkbox of the schedules(s) you wish to delete and press "Delete Selected" to delete (multiple selections possible).

Press "Delete All" to delete all schedules.

Add / Edit

Name	Office Schedule					
Description						
Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.

X-5-10 Smart Roaming

Smart roaming permits continuous connectivity on wireless devices that are moving. The handoffs from one station to another are fast and secure, and are managed seamlessly.

Roaming Groups						
	Group Name	Used WLAN/GUEST SSID	Used WLAN/GUEST Group	Used AP Number		
		Please add Roaming Gr	oup setting			
Add Edi	t Delete Selected Delete A	П				
Add / E	dit					

Roaming Group Settings		
Name		
Description		
Mobility Domain		
Encryption Key		
Over the DS	Enable Disable	
SSID Type	• WLAN GUEST	
GUEST SSID	GUEST Group: 1234 ▼ GUEST: None ▼	
WLAN SSID	WLAN Group: group1 ▼ WLAN: None ▼	
Save Cancel Save &	Apply	

Roaming Group Settings		
Name	Enter / edit the name of roaming group.	
Description	Enter / edit a description for reference.	
Mobility	Enter / edit a mobility domain.	
Domain		
Encryption Key	Enter / edit an encryption key.	
Over the DS	Check to enable / disable this function.	
SSID Type	Select the SSID type.	
Guest SSID	Select the Guest Group from the drop down menu. Select a	
	Guest from the drop down menu.	
WLAN SSID	Select the WLAN Group from the down down menu. Select a	
	WLAN from the drop down menu.	

X-5-11 Device Monitoring

This page monitors the device's status (alive or not alive) after you set the Device IP.

Device Monitoring						
Search			Match whole words			
	Device IP		Description	Status		
Please add devices						
Add Edit Delete Selected Delete All Email Setting						

Add / Edit

Device Monitoring						
Add IP Address						
Add Reset						
Devices List						
Device IP	Description	Delete				
192.168.2.100	cap300					
Apply Cancel						

Enter an IP Address(es) and click "Add" to add the device(s). Click "Reset" to clear the field.

Press "Apply" to apply the above action or "Cancel" to forfeit the addition.

X-5-12 Firmware Upgrade

Firmware Upgrade allows you to upgrade firmware to Access Point Groups. First, upload the firmware file from a local disk or external FTP server: locate the file and click "Upload" or "Check". The table below will display the *Firmware Name, Firmware Version, NMS Version, Model and Size*.

Then click "Upgrade All" to upgrade all access points in the Array or select Access Point groups from the list using check-boxes and click "Upgrade Selected" to upgrade only selected access points.

	re Upgrade									
Updat	te firmware from		🖲 Local 🛛 🔍 External	FTP Server						
Firmw	vare File	(Choose File No file	chosen						
Timeo	out	1	150 Seconds							
Uplo	ad Firmware Name	F	irmware Version	NMS Version	Model	Size (bytes)				
Access	Point Group									
	Group Name	Index	MAC Address	Device Name	Model	IP Address	Status	Firmware Version	NMS Version	Progress
	System Default (1)									
		1	74:DA:38:1D:26:5A	AP74DA381D265A	WAP1200	192.168.2.102	0	1.8.1	1.3.2.0	0%
	Wizard AP Group 2 (1)				1					
		1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	0	1.8.1	1.3.2.0	0%
Upgra	de Selected Upg	rade All	Refresh							

X-5-13 Advanced

X-5-13-1 System Security

Configure the NMS system login name and password.

NMS Security Name	administrator	
NMS Security Key	1234567890123456	(8~16 Characters)
Sync NMS Security with Active Managed APs		curity Name and Key, please make sure all ed; all other configuration update is complete, and

Press "Apply" to apply the settings.

X-5-13-2 Date & Time

Configure the date & time settings of the AP Array. The date and time of the access points can be configured manually or can be synchronized with a time server.

Date and Time Settings	
Local Time	2012 ▼ Year Jan ▼ Month 1 ▼ Day 0 ▼ Hours 00 ▼ Minutes 00 ▼ Seconds
Acquire Current Time from Your PC	
NTP Time Server	
Use NTP	Enable
Auto Daylight Saving	C Enable
Server Name	User-Defined T
Update Interval	24 (Hours)
Time Zone	
Time Zone	(GMT+08:00) Taipei, Taiwan ▼
Save Cancel Save & Apply	

Date and Time Settings	
Local Time	Set the access point's date and time manually using the drop
	down menus.
Acquire	Click "Acquire Current Time from Your PC" to enter the
Current Time	required values automatically according to your computer's
from your PC	current time and date.

NTP Time Server	
Use NTP	The access point also supports NTP (Network Time Protocol)
	for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you
	wish.
Update	Specify a frequency (in hours) for the access point to
Interval	update/synchronize with the NTP server.

Time Zone	
Time Zone	Select the time zone of your country/ region. If your
	country/region is not listed, please select another
	country/region whose time zone is the same as yours.

Press "Save" to save the above actions, "Cancel" to forfeit the changes, or "Save & Apply" to save and apply the above actions.

X-5-13-3 Google Maps

Click on the link below the entry field and follow Google's instructions to obtain an API key. Enter the key into the entry field.

Google Maps		
АРІ Кеу	(Please go to <u>https://console.developers.google.com/flows/enableapi?</u> apiid=maps_backend&keyType=CLIENT_SIDE&reusekey=true to apply for an API key.)	
Apply Cancel		

Press "Apply" to apply the setting or "Cancel" to forfeit the change.



X-6-1 Network Settings

X-6-1-1 LAN-Side IP Address

The "LAN-side IP address" page allows you to configure your AP Controller on your Local Area Network (LAN). You can enable the access point to dynamically receive an IP address from your router's DHCP server or you can specify a static IP address for your access point, as well as configure DNS servers. You can also set your AP Controller as a DHCP server to assign IP addresses to other devices on your LAN.

The access point's default IP address is 192.168.2.2

Disable other DHCP servers on the LAN if using AP Controllers DHCP Server.

P Address Assignment	Static IP Address V	
Address	192.168.2.2	
Subnet Mask	255.255.255.0	
Default Gateway		
Primary DNS Address	0.0.0.0	
Secondary DNS Address	0.0.0.0	

LAN-side IP Ac	ldress
IP Address	Select "Static IP" to manually specify a static/fixed IP address
Assignment	for your access point. Select "DHCP Client" for your access
	point to be assigned a dynamic IP address from your router's
	DHCP server, or select "DHCP Server" for your access point to

act as a DHCP server and assign IP addresse	es on your LAN.
---	-----------------

Static IP Addre	ess
IP Address	Specify the IP address here. This IP address will be assigned to
	your access point and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default For DHCP users, select "From DHCP" to get default gatewa	
Gateway	from your DHCP server or "User-Defined" to enter a gateway
	manually. For static IP users, the default value is blank.
Primary DNS For static IP users, the default value is blank.	
Address	
Secondary	For static IP users, the default value is blank.
DNS Address	

PAddress Assignment	DHCP Client •
Address	192.168.2.2
ubnet Mask	255.255.255.0
efault Gateway	From DHCP V
rimary DNS Address	From DHCP • 0.0.0.0
econdary DNS Address	From DHCP • 0.0.0.0

DHCP Client	
IP Address	When "DHCP Client" is selected this value cannot be modified.
Subnet Mask	When "DHCP Client" is selected this value cannot be modified.
Default	Select "From DHCP" or select "User-Defined" and enter a
Gateway	default gateway.
Primary DNS	Select "From DHCP" or select "User-Defined" and enter a
Address	primary DNS address.
Secondary	Select "From DHCP" or select "User-Defined" and enter a
DNS Address	secondary DNS address.

LAN-side IP A			
LAN-SIDE IP A	udress		
IP Address Assi	ignment	DHCP Server	T
IP Address		192.168.2.2	
Subnet Mask		255.255.255.0	
IP Address Ran	ge	192.168.2.120	~ 192.168.2.140
Domain Name		setup.edimax.com	
Lease Time	Lease Time		
Default Gateway	/		
Primary DNS Ac	ldress	0.0.0.0	
Secondary DNS Address		0.0.0.0	
DHCP Server S	static IP Address		
Index	MAC Address	IP Address	Action
1			Add
DHCP Client L	ist		
Index	MAC Address IP	Address Lease Time	
	No DHCP Clier		
			Apply
			Apply

DHCP Server	
IP Address	Specify the IP address here. This IP address will be assigned to
	your access point and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
IP Address	Enter the start and end IP address of the IP address range
Range	which your access point's DHCP server will assign to devices on
	the network.
Domain	Enter a domain name.
Name	
Lease Time	Select a lease time from the drop down menu. IP addresses will
	be assigned for this period of time.
Default	Enter a default gateway.
Gateway	
Primary DNS	Enter a primary DNS address.
Address	
Secondary	Enter a secondary DNS address.
DNS Address	

Your access point's DHCP server can be configured to assign static (fixed) IP addresses to specified network devices, identified by their unique MAC address:

DHCP Server S	Static IP Address
MAC	Enter the MAC address of the network device to be assigned a
Address	static IP address.
IP Address	Specify the IP address to assign the device.
Add	Click to assign the IP address to the device.

X-6-1-2 LAN Port Settings

The "LAN Port" page allows you to configure the settings for your AP Controllers wired LAN (Ethernet) ports.

Wired LAN Port	Enable	Speed & Duplex	Flow Control	802.3az
LAN1	Enabled •	Auto 🔻	Enabled •	Enabled •
LAN2	Enabled T	Auto 🔻	Enabled ▼	Enabled •

Wired LAN	Identifies LAN port 1 or 2.
Port	
Enable	Enable/disable specified LAN port.
Speed &	Select a speed & duplex type for specified LAN port, or use the
Duplex	"Auto" value. LAN ports can operate up to 1000Mbps and
	full-duplex enables simultaneous data packets
	transfer/receive.
Flow Control	Enable/disable flow control. Flow control can pause new
	session request until current data processing is complete, in
	order to avoid device overloads under heavy traffic.
802.3az	Enable/disable 802.3az. 802.3az is an Energy Efficient Ethernet
	feature which disables unused interfaces to reduce power
	usage.

"VLAN" (Virtual Local Area Network) enables you to configure VLAN settings. A VLAN is a local area network which maps workstations virtually instead of physically and allows you to group together or isolate users from each other. VLAN IDs in the range 1 – 4095 are supported.

VLAN Interface		
Wired LAN Port	VLAN Mode	VLAN ID
LAN1	Untagged Port V	1
LAN2	Untagged Port	1
Wireless 2.4GHz	VLAN Mode	VLAN ID
SSID [WALL 1963 - 108.4_1]	Untagged Port	
SSID (WAP 255-106CA, C, 2	Untagged Port	1
2210 [mill] - 2004 [Million] of [d	Unlagged Port	1
Wireless 5GHz	VLAN Mode	VLAN ID
SSID [WAP1700 F1006A_A]	Untagged Port	1
Management VLAN		
VLAN ID	1	
		Apply

VLAN Interface	VLAN Interface		
Wired LAN	Identifies LAN port 1 or 2 and wireless SSIDs.		
Port/Wireless			
VLAN Mode	Select "Tagged Port" or "Untagged Port" for specified LAN		
	interface.		
VLAN ID	Set a VLAN ID for specified interface, if "Untagged Port" is		
	selected.		

Management V	'LAN
VLAN ID	Specify the VLAN ID of the management VLAN. Only the hosts
	belonging to the same VLAN can manage the device.

Press "Apply" to confirm the settings.

X-6-2 2.4GHz 11bgn

The "2.4GHz 11bgn" menu allows you to view and configure information for your access point's 2.4GHz wireless network across five categories: Basic, Advanced, Security, WDS & Guest Network.

X-6-2-1 Basic

The "Basic" screen displays basic settings for your access point's 2.4GHz Wi-Fi network (s).

2.4GHz Basic Settings	
Wireless	Enable 🖲 Disable
Band	11b/g/n ▼
Enable SSID number	2 🔻
SSID1	VLAN ID 1
SSID2	VLAN ID 1
Auto Channel	Enable Disable
Auto Channel Range	Ch 1 - 11 🔻
Auto Channel Interval	One day 🔻
Auto channel interval	Change channel even if clients are connected
Channel Bandwidth	Auto 🔻
BSS BasicRateSet	all
1	
	Apply Cancel

Wireless	Enable or disable the a	ccess point's 2.4GHz	wireless radio.
	When disabled, no 2.40	GHz SSIDs will be acti	ve.
Band	Wireless standard used	I for the access point	
	Combinations of 802.1	1b, 802.11g & 802.11	In can be selected.
Enable SSID	Select how many SSIDs	to enable for the 2.4	IGHz frequency
Number	from the drop down m	enu. A maximum of 2	16 can be enabled.
	Enable SSID number	1 🔻	
	SSID1	40 YO 10 YO 10 YO 10	VLAN ID 1
	Enable SSID number	3 🔻	
	SSID1	an se an suite	VLAN ID 1
	SSID2	2	VLAN ID 1
	SSID3	1 1 1 1 1 1 1 1 1 1	VLAN ID 1
SSID#	Enter the SSID name fo	r the specified SSID (up to 16). The SSID
	can consist of any com	bination of up to 32 a	alphanumeric
	characters.		•
VLAN ID	Specify a VLAN ID for e	ach SSID.	
Auto	Enable/disable auto ch	annel selection.	
Channel	Enable: Auto channel s	election will automat	tically set the
	wireless channel for th		,
		•	112 Inequency based
	on availability and pote		
	Disable: Select a chann	el manually as showi	n in the next table.

Auto	Soloct a range to which auto channel selection can choose
	Select a range to which auto channel selection can choose
Channel	from.
Range	
Auto	Select a time interval for how often the auto channel setting
Channel	will check/reassign the wireless channel.
Interval	Check/uncheck the "Change channel even if clients are
	connected" box according to your preference.
Channel	Select the channel bandwidth:
Bandwidth	20MHz (lower performance but less interference); or
	40MHz (higher performance but potentially higher
	interference); or
	Auto (automatically select based on interference level).
BSS	Set a Basic Service Set (BSS) rate: this is a series of rates to
BasicRateSet	control communication frames for wireless clients.

When auto channel is disabled, configurable fields will change. Select a wireless channel manually:

Auto Channel	Enable Disable	
Auto Channel Range	Ch 1 - 11 🔻	
Auto Channel Interval	One day 🔻	
Auto Chaimer Interval	Change channel even if clients are connected	
Channel Bandwidth	Auto 🔻	
BSS BasicRateSet	all 🔹 🔻	
Auto Channel	Enable Disable	
Channel	Ch 11, 2462MHz 🔻	
Channel Bandwidth	Auto, +Ch 7 🔹	
BSS BasicRateSet	all 🔹	

Channel	Select a wireless channel from 1 – 11.
Channel	Set the channel bandwidth:
Bandwidth	20MHz (lower performance but less interference); or
	40MHz (higher performance but potentially higher
	interference); or
	Auto (automatically select based on interference level).

BSS	Set a Basic Service Set (BSS) rate: this is a series of rates to
BasicRateSet	control communication frames for wireless clients.

Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

X-6-2-2 Advanced

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

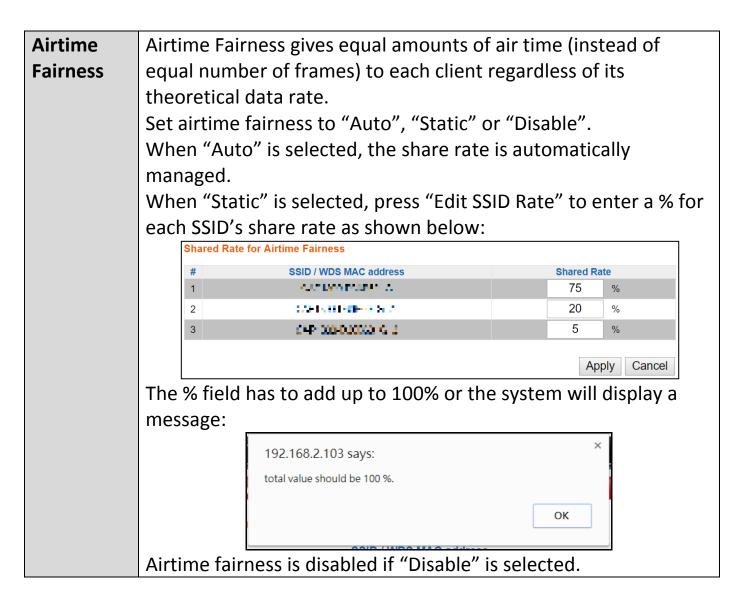
.4GHz Advanced Settings		
Contention Slot	Short ▼	
Preamble Type	Short V	
Guard Interval	Short GI V	
802.11g Protection	Enable	Disable
802.11n Protection	Enable	Disable
DTIM Period	1	(1-255)
RTS Threshold	2347	(1-2347)
Fragment Threshold	2346	(256–2346)
Multicast Rate	Auto 🔻	
Tx Power	100% 21dbm	•
Beacon Interval	100	(40-1000 ms)
Station Idle Timeout	60	(30-65535 seconds)
Airtime Fairness	Disabled •	Edit SSID Rate

Contention	Select "Short" or "Long" – this value is used for contention
Slot	windows in WMM (see x-6-7 WMM).
Preamble	Set the wireless radio preamble type. The preamble type in
Туре	802.11 based wireless communications defines the length of the
	CRC (Cyclic Redundancy Check) block for communication
	between the access point and roaming wireless adapters. The
	default value is "Short Preamble".
Guard	Set the guard interval. A shorter interval can improve
Interval	performance.

Apply

Cancel

802.11gEnable/disable 802.11g protection, which increases reliabilitProtectionreduces bandwidth (clients will send Request to Send (RTS) t	.0
	CTS),
access point, and access point will broadcast Clear to Send (
before a packet is sent from client).	
802.11n Enable/disable 802.11n protection, which increases reliabilit	;y
Protection but reduces bandwidth (clients will send Request to Send (R ⁻	TS)
to access point, and access point will broadcast Clear to Sene	d
(CTS), before a packet is sent from client).	
DTIM Set the DTIM (delivery traffic indication message) period val	ue of
Period the wireless radio. The default value is 1.	
RTS Set the RTS threshold of the wireless radio. The default value	e is
Threshold 2347.	
Fragment Set the fragment threshold of the wireless radio. The default	t
Threshold value is 2346.	
MulticastSet the transfer rate for multicast packets or use the "Auto"	
Rate setting. The range of the transfer rate is between 1Mbps to	
54Mbps	
Tx Power Set the power output of the wireless radio. You may not req	uire
100% output power. Setting a lower power output may enha	ance
security since access to your signal can be potentially prever	nted
from malicious/unknown users in distant areas.	
Beacon Set the beacon interval of the wireless radio. The default val	ue is
Interval 100.	
Station Set the interval for the access point to send keepalive messa	ges
idle to a wireless client to check if the station is still alive/active.	
timeout	



Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

The access point provides various security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

It is essential to configure wireless security in order to prevent unauthorised access to your network.

SSID	CHT 2004C00CC0 CX
Broadcast SSID	Enable V
Wireless Client Isolation	Disable •
802.11k	Disable ▼
Load Balancing	100 /100
Authentication Method	No Authentication v
Authentication Method Additional Authentication	No Authentication No additional authentication
	No additional authentication • ettings
Additional Authentication	No additional authentication

SSID Selection	Select a SSID to configure its security settings.
Broadcast SSID	Enable or disable SSID broadcast.
	Enable: the SSID will be visible to clients as an available Wi-Fi
	network.
	Disable: the SSID will not be visible as an available Wi-Fi
	network to clients – clients must manually enter the SSID in
	order to connect. A hidden (disabled) SSID is typically more
	secure than a visible (enabled) SSID.
Wireless Client	Enable or disable wireless client isolation.
Isolation	Wireless client isolation prevents clients connected to the
	access point from communicating with each other and
	improves security. Typically, this function is useful for
	corporate environments or public hot spots and can prevent
	brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients
	connected to an SSID. Set a load balancing value (maximum
	100).
Authentication	Select an authentication method from the drop down menu
Method	and refer to the appropriate information below for your
	method.

X-6-2-3-1 No Authentication / Additional Authentication

When "No Authentication" is selected in "Authentication Method", extra options are made available in the next line:

Additional	Select an additional authentication method from the drop
Authentication	down menu or select "No additional authentication" for no
	authentication, where no password/key is required to
	connect to the access point.
	For other options, refer to the information below.



"No additional authentication" is not recommended as anyone can connect to your device's SSID. Additional wireless authentication methods can be applied to all authentication methods:



WPS must be disabled to use additional authentication. See X-6-4 WPS for WPS settings.

MAC Address Filter

Restrict wireless clients access based on MAC address specified in the MAC filter table.



See X-6-6 MAC Filter to configure MAC filtering.

MAC-RADIUS Authentication

Restrict wireless clients access based on MAC address via a RADIUS server, or password authentication via a RADIUS server.



See X-6-5 RADIUS to configure RADIUS servers.



WPS must be disabled to use MAC-RADIUS authentication. See X-6-4 WPS for WPS settings.

Additional Authentication	MAC RADIUS authentication		
MAC RADIUS Password	 Use MAC address Use the following password 		

MAC Filter & MAC-RADIUS Authentication

Restrict wireless clients access using both of the above MAC filtering & **RADIUS** authentication methods.

Additional Authentication	MAC filter & MAC RADIUS authentication ▼	
MAC RADIUS Password	 Use MAC address Use the following password 	

MAC RADIUS	Select whether to use MAC address or password
Password	authentication via RADIUS server. If you select "Use the
	following password", enter the password in the field below.
	The password should match the "Shared Secret" used in x-6-5
	RADIUS.

WEP (Wired Equivalent Privacy) is a basic encryption type. When selected, a notice will pop-up as exemplified below:

WPS 2.0 will be disabled if WEP is used.

Below is a figure showing the configurable fields:

Authentication Method	WEP 🔻
Key Length	64-bit 🔻
Кеу Туре	ASCII (5Characters) ▼
Default Key	Key 1 🔻
Encryption Key 1	
Encryption Key 2	
Encryption Key 3	
Encryption Key 4	

Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit
	and is recommended.
Кеу Туре	Choose from "ASCII" (any alphanumerical character 0-9, a-z
	and A-Z) or "Hex" (any characters from 0-9, a-f and A-F).
Default Key	Select which encryption key $(1 - 4 below)$ is the default key.
	For security purposes, you can set up to four keys (below)
	and change which is the default key.
Encryption Key	Enter your encryption key/password according to the format
1-4	you selected above.

For a higher level of security, please consider using WPA encryption.

X-6-2-3-3 IEEE802.1x/EAP

Below is a figure showing the configurable fields:

Authentication Method	IEEE802.1x/EAP ▼
Key Length	64-bit 🔻

X-6-2-3-4 WPA-PSK

WPA-PSK is a secure wireless encryption type with strong data protection and user authentication, utilizing 128-bit encryption keys.

Below is a figure showing the configurable fields:

Authentication Method	WPA-PSK V
802.11r Fast Roaming	Enable Disable
WPA Туре	WPA/WPA2 Mixed Mode-PSK <
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)
Pre-shared Key Type	Passphrase •
Pre-shared Key	

Fast Roaming Settings will also be shown:

802.11r Fast Transition Roaming Settings	
mobility_domain	
Encryption Key	
Over the DS	Enable Disable

802.11r Fast	When your device roams from one AP to another on the
Roaming	same network, 802.11r uses a feature called Fast Basic
	Service Set Transition (FT) to authenticate more quickly. FT
	works with both preshared key (PSK) and 802.1X
	authentication methods.
WPA Type	Select from WPA/WPA2 Mixed Mode-PSK, WPA2 or WPA
	only. WPA2 is safer than WPA, but is not supported by all
	wireless clients. Please make sure your wireless client
	supports your selection.
Encryption	Select "TKIP/AES Mixed Mode" or "AES" encryption type.
Key Renewal	Specify a frequency for key renewal in minutes.
Interval	
Pre-Shared	Choose from "Passphrase" (8 – 63 alphanumeric characters)

Кеу Туре	or "Hex" (up to 64 characters from 0-9, a-f and A-F).
Pre-Shared	Please enter a security key/password according to the
Кеу	format you selected above.

802.11r Fast Transition Roaming Settings		
Mobility_dom	Specify the mobility domain (2.4GHz or 5GHz)	
ain		
Encryption Key	Specify the encryption key	
Over the DS	Enable or disable this function.	
X-6-2-3-5	WPA-EAP	

Authentication Method	WPA-EAP 🔻
802.11r Fast Roaming	Enable Disable
WPA Туре	WPA/WPA2 mixed mode-EAP <
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)

Fast Roaming Settings will also be shown:

802.11r Fast Transition Roaming Settings		
mobility_domain		
Encryption Key		
Over the DS	Enable Disable	

WPA Туре	Select from WPA/WPA2 Mixed Mode-EAP, WPA2-EAP or WPA-EAP.
Encryption Type	Select "TKIP/AES Mixed Mode" or "AES" encryption type.
Key Renewal Interval	Specify a frequency for key renewal in minutes.

WPA-EAP must be disabled to use MAC-RADIUS authentication.

802.11r Fast Transition Roaming Settings		
Mobility_dom	Specify the mobility domain (2.4GHz or 5GHz)	
ain		
Encryption Key	Specify the encryption key	
Over the DS	Enable or disable this function.	

Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

Wireless Distribution System (WDS) can bridge/repeat access points together in an extended network. WDS settings can be configured as shown below.

When using WDS, configure the IP address of each access point to be in the same subnet and ensure there is only one active DHCP server among connected access points, preferably on the WAN side.

WDS must be configured on each access point, using correct MAC addresses. All access points should use the same wireless channel and encryption method.

2.4GHz	
WDS Functionality	Disabled v
Local MAC Address	80:1F:02:F1:96:8A
WDS Peer Settings	
WDS #1	MAC Address
WDS #2	MAC Address
WDS #3	MAC Address
WDS #4	MAC Address
WDS VLAN	
VLAN Mode	Untagged Port v (Enter at least one MAC address.)
VLAN ID	1
WDS Encryption method	
Encryption	None (Enter at least one MAC address.)
	Apply Reset

2.4GHz	2.4GHz		
WDS	Select "WDS with AP" to use WDS with access point or "WDS		
Functionality	Dedicated Mode" to use WDS and also block communication		
	with regular wireless clients. When WDS is used, each access		
	point should be configured with corresponding MAC addresses,		
	wireless channel and wireless encryption method.		
Local MAC	Displays the MAC address of your access point.		
Address			

WDS Peer Settings	
WDS #	Enter the MAC address for up to four other WDS devices you
	wish to connect.

WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to "Untagged Port" or "Tagged Port".
VLAN ID	Specify the WDS VLAN ID when "Untagged Port" is selected above.

WDS Encryption method		
Encryption	Select whether to use "None" or "AES" encryption and enter a	
	pre-shared key for AES consisting of 8-63 alphanumeric	
	characters.	

Press "Apply" to apply the configuration, or "Reset" to forfeit the changes.

X-6-2-5 Guest Network

Enable / disable guest network to allow clients to connect as guests.

Guest Network		
Guest Network	Enable Disable	
		Apply Cancel

X-6-3 5GHz 11ac 11an

The "5GHz 11ac 11an" menu allows you to view and configure information for your access point's 5GHz wireless network across five categories: Basic, Advanced, Security, WDS & Guest Network.

X-6-3-1 Basic

The "Basic" screen displays basic settings for your access point's 5GHz Wi-Fi network (s).

5GHz Basic Settings	
Wireless	Enable Disable
Band	11a/n/ac ▼
Enable SSID number	1 •
SSID1	VLAN ID 1
Auto Channel	Enable Disable
Auto Channel Range	Band 1 T
Auto Channel Interval	One day Change channel even if clients are connected
Channel Bandwidth	Auto 80/40/20 MHz T
BSS BasicRateSet	all 🔹
	Apply Cancel

Wireless	Enable or disable the access point's 5GHz wireless radio. When		
	disabled, no 5GHz SSID	s will be active.	
Band	Wireless standard used for the access point.		
	Combinations of 802.12	1a, 802.11n & 802.1	1ac can be selected.
Enable SSID	Select how many SSIDs to enable for the 2.4GHz frequency		
Number	from the drop down menu. A maximum of 16 can be enabled.		
	Enable SSID number	1 •	
	SSID1	ALC: NO REPORT	VLAN ID 1
	Enable SSID number	3 🔻	
	SSID1	an an an Alfred	VLAN ID 1
	SSID2	1 1 1 1 1 1 1 1 1 1	VLAN ID 1
	SSID3	** ** ** * *	VLAN ID 1
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID		
	can consist of any combination of up to 32 alphanumeric		
	characters.		
VLAN ID	Specify a VLAN ID for each SSID.		
Auto	Enable/disable auto channel selection. Auto channel selection		
Channel	will automatically set the wireless channel for the access		
	point's 5GHz frequency based on availability and potential		
	interference. When disabled, configurable fields will change as		
	shown below:		
Auto	Select a range to which auto channel selection can choose		

Channel	from.	
Range		
Auto	Select a time interval for how often the auto channel setting	
Channel	will check/reassign the wireless channel.	
Interval	Check/uncheck the "Change channel even if clients are	
	connected" box according to your preference.	
Channel	Select the channel bandwidth:	
Bandwidth	vidth 20MHz (lower performance but less interference); or	
	Auto 40/20 MHz; or	
	Auto 80/40/20 MHz (automatically select based on	
	interference level).	
BSS	Set a Basic Service Set (BSS) rate: this is a series of rates to	
BasicRateSet	control communication frames for wireless clients.	

When auto channel is disabled, configurable fields will change. Select a wireless channel manually:

Auto Channel	Enable Disable
Auto Channel Range	Band 1 🔻
Auto Channel Interval	One day 🔻
	Change channel even if clients are connected
Channel Bandwidth	Auto 80/40/20 MHz 🔻
BSS BasicRateSet	all 🔻
Auto Channel	Enable Disable
Channel	Ch 36, 5.18GHz 🔹
Channel Bandwidth	Auto 80/40/20 MHz 🔻
BSS BasicRateSet	all 🔻

Channel	Select a wireless channel.	
Channel	Select the channel bandwidth:	
Bandwidth	20MHz (lower performance but less interference); or	
	Auto 40/20 MHz; or	
	Auto 80/40/20 MHz (automatically select based on	
	interference level).	
BSS	Set a Basic Service Set (BSS) rate: this is a series of rates to	
BasicRateSet	control communication frames for wireless clients.	

Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

X-6-3-2 Advanced

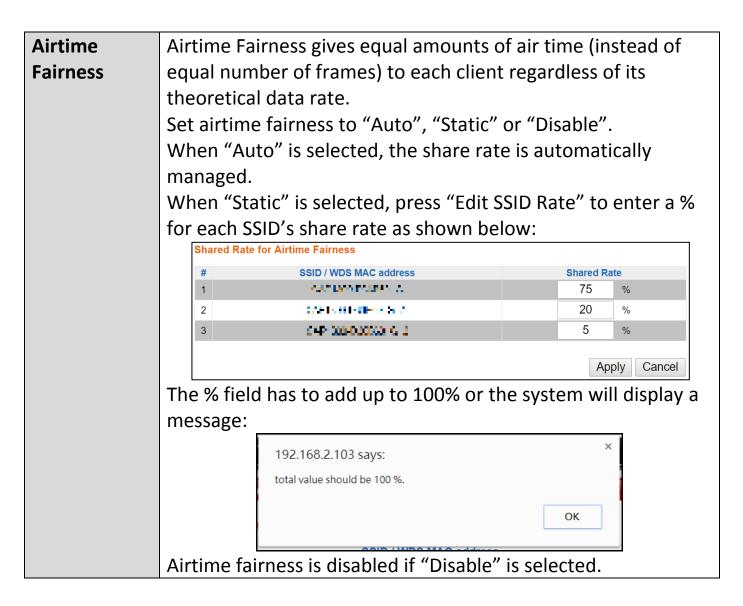
These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

	Changing these settings can adversely affect the performance of your access point.
	access point.

5GHz Advanced Settings			
Guard Interval	Short GI ▼		
802.11n Protection	Enable		
DTIM Period	1	(1-255)	
RTS Threshold	2347	(1-2347)	
Fragment Threshold	2346	(256–2346)	
Multicast Rate	Auto 🔻		
Tx Power	100% 21dbm	100% 21dbm ▼	
Beacon Interval	100	(40-1000 ms)	
Station Idle Timeout	60	(30-65535 seconds)	
Beamforming	Enable Disable		
Airtime Fairness	Disabled Edit SSID Rate		
			Apply Cancel

Guard	Set the guard interval. A shorter interval can improve
Interval	performance.
802.11n	Enable/disable 802.11n protection, which increases reliability
Protection	but reduces bandwidth (clients will send Request to Send
	(RTS) to access point, and access point will broadcast Clear to
	Send (CTS), before a packet is sent from client.)
DTIM Period	Set the DTIM (delivery traffic indication message) period value
	of the wireless radio. The default value is 1.
RTS	Set the RTS threshold of the wireless radio. The default value
Threshold	is 2347.
Fragment	Set the fragment threshold of the wireless radio. The default
Threshold	value is 2346.

Multicast	Set the transfer rate for multicast packets or use the "Auto"
Rate	setting.
Tx Power	Set the power output of the wireless radio. You may not
	require 100% output power. Setting a lower power output can
	enhance security since potentially malicious/unknown users in
	distant areas will not be able to access your signal.
Beacon	Set the beacon interval of the wireless radio. The default value
Interval	is 100.
Station idle	Set the interval for keepalive messages from the access point
timeout	to a wireless client to verify if the station is still alive/active.
Beamforming	Beamforming is a signal processing technique used in sensor
	arrays for directional signal transmission or reception.
	This is achieved by combining elements in an antenna array in
	such a way that signals at particular angles experience
	constructive interference while others experience destructive
	interference. Beamforming can be used at both the
	transmitting and receiving ends in order to achieve spatial
	selectivity. The improvement compared with omnidirectional
	reception / transmission is known as the directivity of the
	array.



Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

The access point provides various security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

It's essential to configure wireless security in order to prevent unauthorised access to your network.

SSID	CA11206-0.05063_4 ×
Broadcast SSID	Enable •
Vireless Client Isolation	Disable v
802.11k	Disable v
_oad Balancing	100 /100
Authentication Method	No Authentication Image: A standard in the
Authentication Method Additional Authentication	No Authentication▼No additional authentication▼
Additional Authentication GHz Wireless Advanced Set mart Handover Settings	No additional authentication
Additional Authentication GHz Wireless Advanced Set	No additional authentication

SSID Selection	Select which SSID to configure security settings for.	
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will	
	be visible to clients as an available Wi-Fi network. When	
	disabled, the SSID will not be visible as an available Wi-Fi	
	network to clients – clients must manually enter the SSID in	
	order to connect. A hidden (disabled) SSID is typically more	
	secure than a visible (enabled) SSID.	

Wireless Client	Enable or disable wireless client isolation. Wireless client	
Isolation	isolation prevents clients connected to the access point from communicating with each other and improves security.	
	Typically, this function is useful for corporate environments or	
	public hot spots and can prevent brute force attacks on clients'	
	usernames and passwords.	
Load Balancing	Load balancing limits the number of wireless clients connected	
	to an SSID. Set a load balancing value (maximum 100).	
Authentication	Select an authentication method from the drop down menu	
Method	and refer to the appropriate information in x-6-2-3 <i>Security</i> for	
	your method.	

Press "Apply" to apply the configuration, or "Cancel" to forfeit the changes.

Please refer back to x-6-2-3 *Security* for more information on authentication and additional authentication types.

Wireless Distribution System (WDS) can bridge/repeat access points together in an extended network. WDS settings can be configured as shown below.

When using WDS, configure the IP address of each access point to be in the same subnet and ensure there is only one active DHCP server among connected access points, preferably on the WAN side.

WDS must be configured on each access point, using correct MAC addresses. All access points should use the same wireless channel and encryption method.

5GHz WDS Mode		
WDS Functionality	Disabled v	
Local MAC Address	80:1F:02:F1:96:8B	
WDS Peer Settings		
WDS #1	MAC Address	
WDS #2	MAC Address	
WDS #3	MAC Address	
WDS #4	MAC Address	
WDS VLAN		
VLAN Mode	Untagged Port v (Enter at least one MAC address.)	
VLAN ID	1	
Encryption method		
Encryption	None (Enter at least one MAC address.)	
	Apply Reset	

5GHz WDS Mod	de	
WDS	Select "WDS with AP" to use WDS with access point or "WDS	
Functionality	Dedicated Mode" to use WDS and also block communication	
	with regular wireless clients. When WDS is used, each access	
	point should be configured with corresponding MAC	
	addresses, wireless channel and wireless encryption method.	
Local MAC	Displays the MAC address of your access point.	
Address		

WDS Peer Settings		
WDS #	Enter the MAC address for up to four other WDA devices you	
	wish to connect.	

WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to "Untagged Port" or "Tagged Port".
VLAN ID	Specify the WDS VLAN ID when "Untagged Port" is selected above.

WDS Encryption		
Encryption	Select whether to use "None" or "AES" encryption and enter a	
	pre-shared key for AES with 8-63 alphanumeric characters.	

Press "Apply" to apply the configuration, or "Reset" to forfeit the changes.

X-6-3-5 Guest Network

Enable / disable guest network to allow clients to connect as guests.

Guest Network		
Guest Network	Enable Disable	
		Apply Cancel

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the compatible device or from within the compatible device's firmware / configuration interface (known as PBC or "Push Button Configuration"). When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. "PIN code WPS" is a variation of PBC which includes the additional use of a PIN code between the two devices for verification.

Please refer to the manufacturer's instructions of your WPS device.

WPS	Enable
Apply	
WPS	
Product PIN	58327142 Generate PIN
Push-button WPS	Start
WPS by PIN	Start
WPS Security	
WPS Status	Not Configured Release

WPS	Check/uncheck this box to enable/disable WPS functionality.
	WPS must be disabled when using MAC-RADIUS
	authentication (see x-6-2-3-1 & x-6-5).

Press "Apply" to apply the configuration.

WPS	
Product PIN	Displays the WPS PIN code of the device, used for PIN code
	WPS. You will be required to enter this PIN code into another
	WPS device for PIN code WPS. Click "Generate PIN" to
	generate a new WPS PIN code.
Push-Button	Click "Start" to activate WPS on the access point for
WPS	approximately 2 minutes.
WPS by PIN	Enter the PIN code of another WPS device and click "Start" to
	attempt to establish a WPS connection. WPS function will last
	for approximately 2 minutes.

WPS Security	
WPS Status	WPS security status is displayed here. Click "Release" to clear
	the existing status.

X-6-5 RADIUS

The RADIUS menu allows you to configure the access point's external RADIUS server settings.

A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

The access point can utilize a primary and a secondary (backup) external RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz).



To use RADIUS servers, go to "Wireless Settings" → "Security" **and select** $\overset{\bullet}{\longrightarrow}$ "MAC RADIUS Authentication" \rightarrow "Additional Authentication" and select "MAC RADIUS Authentication" (see X-6-2-3 & X-6-3-3).

X-6-5-1 RADIUS Settings

Configure the RADIUS server settings for 2.4GHz and 5GHz. Each frequency can use an internal or external RADIUS server.

RADIUS Server (2	.4GHz)				
		Primary RAD	IUS Server		
RADIUS Type	Internal •	-			
RADIUS Server					
Authentication Port	1812				
Shared Secret					
Session Timeout	3600	second(s)			
Accounting	Enable	Disable			
Accounting Port	1813				
		Secondary RA	DIUS Server		
RADIUS Type	Internal •	External			
RADIUS Server					
Authentication Port	1812		٦		
Shared Secret					
Session Timeout	3600	second(s)			
Accounting	Enable	Disable			
Accounting Port	1813				
RADIUS Server (5	CH7)				
Kilbios server (, GIIZ)				
	(GII2)	Priman/ PAF	IIIS Server		1
		Primary RAD	IUS Server		i
RADIUS Type RADIUS Server	Internal		IUS Server		
RADIUS Type			IUS Server		
RADIUS Type RADIUS Server	Internal		IUS Server		
RADIUS Type RADIUS Server Authentication Port	Internal		IUS Server		
RADIUS Type RADIUS Server Authentication Port Shared Secret	Internal I	External	IUS Server		
RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting	Internal Iternal I	External second(s)	IUS Server		
RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout	Internal I I I I I I I I I I I I I I I I I I I	External second(s) Disable			
RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting Accounting Port	 Internal 1812 3600 Enable 1813 	External second(s) Disable Secondary RA			
RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting Accounting Port RADIUS Type	Internal I I I I I I I I I I I I I I I I I I I	External second(s) Disable Secondary RA			
RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting Accounting Port RADIUS Type RADIUS Server	 Internal 1812 3600 Enable 1813 Internal 	External second(s) Disable Secondary RA			
ADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting Accounting Port RADIUS Type RADIUS Server Authentication Port	 Internal 1812 3600 Enable 1813 	External second(s) Disable Secondary RA			
RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting Accounting Port Accounting Port RADIUS Type RADIUS Server Authentication Port Shared Secret	 Internal 1812 3600 Enable 1813 Internal 1812 1812 	External second(s) Disable Secondary RA External			
RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting Accounting Port Accounting Port RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout	 Internal 1812 3600 Enable 1813 Internal 1812 1812 3600 	External second(s) Disable External second(s)			
RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting Accounting Port Accounting Port RADIUS Type RADIUS Server Authentication Port Shared Secret	 Internal 1812 3600 Enable 1813 Internal 1812 3600 Enable 3600 Enable 	External second(s) Disable Secondary RA External			
RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting Accounting Port Accounting Port RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout	 Internal 1812 3600 Enable 1813 Internal 1812 1812 3600 	External second(s) Disable External second(s)			
RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting Accounting Port Accounting Port RADIUS Type RADIUS Server Authentication Port Shared Secret Session Timeout Accounting	 Internal 1812 3600 Enable 1813 Internal 1812 3600 Enable 3600 Enable 	External second(s) Disable External second(s)			

RADIUS Type	Select "Internal" to use the access point's built-in RADIUS
	server or "external" to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication	Set the UDP port used in the authentication protocol of the
Port	RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in
	length. This should match the "MAC-RADIUS" password used
	in x-6-2-3 or x-6-3-3.
Session	Set a duration of session timeout in seconds between 0 –
Timeout	86400.
Accounting	Enable or disable RADIUS accounting.
Accounting	When accounting is enabled (above), set the UDP port used
Port	in the accounting protocol of the RADIUS server. Value must
	be between 1 – 65535.

Internal Server X-6-5-2

The access point features a built-in RADIUS server which can be configured as shown below used when "Internal" is selected for "RADIUS Type" in the "Wireless Settings" \rightarrow "RADIUS" \rightarrow "RADIUS Settings" menu.



To use RADIUS servers, go to "Wireless Settings" → "Security" **and select** $\overset{\bullet}{\longrightarrow}$ "MAC RADIUS Authentication" \rightarrow "Additional Authentication" and select "MAC RADIUS Authentication" (see X-6-2-3 & X-6-3-3).

Internal Server		
Internal Server	Enable	
EAP Internal Authentication	▼	
EAP Certificate File Format	PKCS#12(*.pfx/*.p12)	
EAP Certificate File	Upload	
Shared Secret		
Session-Timeout	3600	second(s)
Termination-Action	 Reauthenication (RADIL Not-Reauthenication (Dell Not-Send 	
		Apply Cancel

Internal Server	Check/uncheck to enable/disable the access point's internal
	RADIUS server.
EAP Internal	Select EAP internal authentication type from the drop down
Authentication	menu.
EAP Certificate	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
File Format	
EAP Certificate	Click "Upload" to open a new window and select the location
File	of an EAP certificate file to use. If no certificate file is
	uploaded, the internal RADIUS server will use a self-made
	certificate.
Shared Secret	Enter a shared secret/password for use between the internal
	RADIUS server and RADIUS client. The shared secret should
	be 1 – 99 characters in length. This should match the

	"MAC-RADIUS" password used in x-6-2-3 or x-6-3-3.	
Session	Set a duration of session timeout in seconds between 0 –	
Timeout	86400.	
Termination	Select a termination-action attribute:	
Action	Reauthentication: sends a RADIUS request to the access	
	point; or,	
	Not-Reauthentication: sends a default termination-action	
	attribute to the access point; or	
	Not-Send: no termination-action attribute is sent to the	
	access point.	

X-6-5-3 RADIUS Accounts

The internal RADIUS server can authenticate up to 256 user accounts. The "RADIUS Accounts" page allows you to configure and manage users.

RADIUS Accounts (Ma	ax: 256 users)			
User Name				
Example: USER1, USER2	, USER3, USER4			
Add Reset				
User Registration List				
Select	User Name	Password		Customize
	No	user entries		
			Delete Selec	cted Delete All

Enter a username in the box below and click "Add" to add the username. The webpage will display the message below:

You may press CONTINUE button to continue configuring other setting or press APPLY button to restart the system for changes to take effect.		
	Apply	Continue

If you choose to apply the settings (by clicking "Apply"), your system will restart the system with a message shown below:

Configuration is complete. Reloading now...

Please wait for 58 seconds.

Press "Continue" see the new user registration list.

User Registrat	tion List		
Select	User Name	Password	Customize
	USER1	Not Configured	Edit
		Delet	e Selected Delete All

Select "Edit" to edit the username and password of the RADIUS account:

Edit User Registration	List	
User Name	USER1	(4-16Characters)
Password		(6-32Characters)
Password		(6-32Characters)
		Apply Cance

User Name	me Enter the user names here, separated by commas.		
Add	Click "Add" to add the user to the user registration list.		
Reset	Clear text from the user name box.		

Select	Check the box to select a user.
User Name	Displays the user name.
Password	Displays if specified user name has a password (configured) or
	not (not configured).
Customize	Click "Edit" to open a new field to set/edit a password for the
	specified user name (below).

Delete	Delete selected user from the user registration list.
Selected	
Delete All	Delete all users from the user registration list.

X-6-6 MAC Filter

MAC filtering is a security feature that can help to prevent unauthorized users from connecting to your access point.

This function allows you to define a list of network devices permitted to connect to the access point. Devices are each identified by their unique MAC address. If a device which is not on the list of permitted MAC addresses attempts to connect to the access point, it will be denied.



To enable MAC filtering, go to "Wireless Settings" → "2.4G Hz 11bgn" → "Security" → "Additional Authentication" **and select** "MAC Filter" **(see** X-6-2-3 **Security).**

The MAC address filtering table is displayed below:

Add MAC Addresses	
Enable Wireless Access Control	Enable Disable
Wireless Access Control Mode	Blacklist V
Apply	
Add MAC Addresses	
Add Reset	

Add MAC	Enter a MAC address of computer or network device manually			
Address	e.g. 'aa-bb-cc-dd-ee-ff' or enter multiple MAC addresses			
	separated with commas, e.g.			
	'aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg'			
Add	Click "Add" to add the MAC address to the MAC address			
	filtering table.			
Reset	Clear all fields.			

MAC address entries will be listed in the "MAC Address Filtering Table". Select an entry using the "Select" checkbox.

MAC Address Filtering Table	
Select	MAC Address
	AND AN AVEN
	Delete Selected Delete All Export

Select	Delete selected or all entries from the table.		
MAC Address	ess The MAC address is listed here.		
Delete	Delete the selected MAC address from the list.		
Selected			
Delete All	Delete all entries from the MAC address filtering table.		
Export	Click "Export" to save a copy of the MAC filtering table. A new		
	window will pop up for you to select a location to save the file.		

X-6-7 WMM

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard, which provides Quality of Service (QoS) features to IEE 802.11 networks. WMM prioritizes traffic according to four categories: background, best effort, video and voice.

		ameters of Access F				
CWMin CWMax AIFSN TxC						
Back Ground	4	10	7	0		
Best Effort	4	6	3	0		
Video	3	4	1	94		
Voice	2	3	1	47		
	CWMin	CWMax	AIFSN	TxOP		
Back Ground	4	10	7	0		
Best Effort	4	10	3	0		
Video	3	4	2	94		
	2	3	2	47		

Configuring WMM consists of adjusting parameters on queues for different categories of wireless traffic. Traffic is sent to the following queues:

Background	Low Priority	High throughput, non time sensitive bulk data e.g. FTP
	Medium Priority	Traditional IP data, medium throughput and delay.
Video	High Priority	Time sensitive video data with minimum time delay.
Voice	High Priority	Time sensitive data such as VoIP and streaming media with minimum time delay.

Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can be adjusted further manually:

CWMin	Minimum Contention Window (milliseconds): This value is input
	to the initial random backoff wait time algorithm for retry of a
	data frame transmission. The backoff wait time will be generated
	between 0 and this value. If the frame is not sent, the random
	backoff value is doubled until the value reaches the number
	defined by CWMax (below). The CWMin value must be lower
	than the CWMax value. The contention window scheme helps to
	avoid frame collisions and determine priority of frame
	transmission. A shorter window has a higher probability
	(priority) of transmission.
CWMax	Maximum Contention Window (milliseconds): This value is the
	upper limit to random backoff value doubling (see above).
AIFSN	Arbitration Inter-Frame Space (milliseconds): Specifies additional
	time between when a channel goes idle and the AP/client sends
	data frames. Traffic with a lower AIFSN value has a higher
	priority.
ТхОР	Transmission Opportunity (milliseconds): The maximum interval
	of time an AP/client can transmit. This makes channel access
	more efficiently prioritized. A value of 0 means only one frame
	per transmission. A greater value means higher priority.

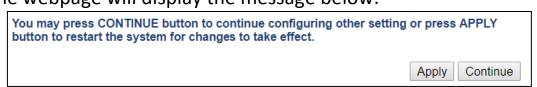
X-6-8 Schedule

The schedule feature allows you to automate the wireless network for the specified time ranges. Wireless scheduling can save energy and increase the security of your network.

Check/uncheck the box "Enable" and select "Apply" to enable/disable the wireless scheduling function.

Enable the wireless network during the following schedules.					
This function	will not work until	date and time are set.	Settings		
Schedule		Enable			
Apply Schedule Lis	s f				
#	SSID	Day of Week	Time	Select	
		No schedule entries			
		Add E	dit Delete Selected	Delete All	

1. Select "Add" to add a schedule. The webpage will display the message below:



If you choose to apply the settings (by clicking "Apply"), your system will restart the system with a message shown below:

Configuration is complete. Reloading now				
Please wait for 5	seconds.			

2. Settings page will be shown if "Continue" is selected: Check/uncheck the box of the desired SSID network, day of schedule and select the Start Time and End Time (using the dropdown menu). Select "Apply" to apply the settings, or "Cancel" to forfeit the schedule.

Settings						
		-				
	2.4GHz SS	D				
		10 M PAR			5GHz SSID	
					100 YO 100 YO	E.c.
	- 100 March 100	an ta ta ta ta ta ta ta ta ta ta ta ta ta				
Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
Start Time 00	▼ : 00 ▼ End T	ime 00 ▼ : 00 ▼			[Apply Cancel

Schedules will be shown in the Schedule List as exemplified below:

Sched	ule List			
#	SSID	Day of Week	Time	Select
	2012/00/2015	buy of Hook	11110	Cicce
1	2010 00 OV 15	Mon.	07:00-16:00	
			Add Edit Delete Selected	Delete All
			Add Edit Delete Selected	Delete All

3. Select "Add" to add more schedules; or Check the box of currently available schedule, select "Edit" to edit, or select "Delete Selected" to delete; or Select "Delete All" to delete all schedules.

X-7 Local Settings

X-7-1 Operation Mode

The access point can function in five different modes. Set the operation mode of the access point here.

- 1. AP Mode: The device acts as a standalone access point
- 2. Repeater Mode: The device acts as a wireless repeater (also called wireless range extender) that takes an existing signal from a wireless router or wireless access point and rebroadcasts it to create a second network.
- 3. AP controller Mode: The device acts as the designated master of the AP array
- 4. Managed AP Mode: The device acts as a slave AP within the AP array.
- 5. Client Bridge Mode: The device is now a client bridge. The client bridge receives wireless signal and provides it to devices connected to the bridge (via Ethernet cable).

Operation Mode		
Operation Mode	AP Controller Mode •	
Wireless Mode		
2.4GHz Mode	Access Point	
5GHz Mode	Access Point V	
Management		
Self AP Management Mode	Disable •	
		Apply Cancel
	AP Mode	

AP Mode	▼
AP Mode	
Repeater Mode	
Repeater Mode AP Controller Mode	;
Managed AP mode Client Bridge Mode	
Client Bridge Mode	



In Managed AP mode some functions of the access point will be disabled in this user interface and must be set using Edimax Pro NMS on the AP Controller.



In AP Controller Mode the access point will switch to the Edimax Pro NMS user interface.

X-7-2 Network Settings

X-7-2-1 System Information

"System Information" page displays basic system information.

System						
Model			6 W.			
Product Name			AP801F02F1968A			
Uptime			1 day 23:51:09			
System Time			/01/02 23:53:07			
Boot from			Internal memory			
Firmware Version			1.8.1			
MAC Address			80:1F:02:F1:96:8A			
Management VLAN IE	D		1			
IP Address			192.168.2.103 Refresh			
Default Gateway			192.168.2.70			
DNS			192.168.2.70			
DHCP Server			192.168.2.70			
Wired LAN Port Set	ttings					
Win	ed LAN Port		Status		VLAN Mode	חוי
	LAN1		Connected (100 Mbps Full-Duplex)		Untagged Port	
	LAN2		Disconnected ()		Untagged Port	/ 1
Wireless 2.4GHz						
Status			Enabled			
MAC Address			80:1F:02:F1:96:8A			
Channel			Ch 7 (Auto)			
Transmit Power			100% 28dbm			
RSSI			-63/-79/-80			
an oraș. An oraș	II.		No Authentication No Encryption 1 No Authentication No Encryption 1		I authentication I authentication	Disabled Disabled
Wireless 2.4GHz /W	DS Disabled					
	MAC Address		Encryption Type No WDS entries.		VLAN Mode/ID	
Wireless 5GHz						
0						
Status			Enabled			
MAC Address			80:1F:02:F1:96:8B			
Channel			Ch 36 + 40 + 44 + 48 (Auto)			
Transmit Power			100% 24dbm			
RSSI			0/0			
Wireless 5GHz /SSI	D					
		Auth	entication Encryption VLAN ID			Wireless Client
	SSID	N	lethod Type VLAN ID	Additional Aut	hentication	Isolation
AND DOUBLE		No Au	thentication No Encryption 1	No additional a	uthentication	Disabled
Wireless 5GHz /WD	S Disabled					
wireless SGHZ /WD	5 Disableu					
	MAC Address		Encryption Type		VLAN Mode/ID	
			No WDS entries.			
			no troc onatos.			
Refresh						

System	
Model	Displays the model number of the access point.
Product	Displays the product name for reference, which consists of
Name	"AP" plus the MAC address.
Uptime	Displays the total time since the device was turned on.
System Time	Displays the system time.
Boot From	Displays information for the booted hardware, booted from
	internal memory.
Firmware	Displays the firmware version.
Version	
MAC Address	Displays the access point's MAC address.
Management	Displays the management VLAN ID.
VLAN ID	
IP Address	Displays the IP address of this device. Click "Refresh" to
	update this value.
Default	Displays the IP address of the default gateway.
Gateway	
DNS	IP address of DNS (Domain Name Server)
DHCP Server	IP address of DHCP Server.

Wired LAN Port	Wired LAN Port Settings			
Wired LAN	AN Specifies which LAN port (1 or 2).			
Port				
Status Displays the status of the specified LAN port (connected or				
	disconnected).			
VLAN	Displays the VLAN mode (tagged or untagged) and VLAN ID			
Mode/ID	for the specified LAN port. See X-6-1-3 VLAN.			

Wireless 2.4GH	z (5GHz)	
Status	Displays the status of the 2.4GHz or 5GHz wireless (enabled or	
	disabled).	
MAC Address	Displays the access point's MAC address.	
Channel	Displays the channel number the specified wireless frequency	
	is using for broadcast.	
Transmit	Displays the wireless radio transmit power level as a	
Power	percentage.	
RSSI	Received signal strength indicator (RSSI) is a measurement of	

the	power	present in	а	received	radio	signal.
		present m	С	1 CCCIVCO	iaaio	SiBrian

Wireless 2.4GHZ	2 (5GHz) / SSID		
SSID	Displays the SSID name(s) for the specified frequency.		
Authentication	Displays the authentication method for the specified SSID.		
Method	See x-6-1 <i>Network Settings</i> .		
Encryption	Displays the encryption type for the specified SSID. See x-6-1		
Туре	Network Settings.		
VLAN ID	Displays the VLAN ID for the specified SSID. See X-6-1-3 VLAN.		
Additional	Displays the additional authentication type for the specified		
Authentication	SSID. See x-6-1 <i>Network Settings</i> .		
Wireless Client	Displays whether wireless client isolation is in use for the		
Isolation	specified SSID. See x-6-1-3 VLAN.		

Wireless 2.4GHZ (5GHz) / WDS Status			
MAC Address	isplays the peer access point's MAC address.		
Encryption	Displays the encryption type for the specified WDS.		
Туре	See x-6-2-4 WDS .		
VLAN Mode/ID	Displays the VLAN ID for the specified WDS. See X-6-2-4 WDS.		

Select "Refresh" to refresh all information.

X-7-2-2 Wireless Clients

"Wireless Clients" page displays information about all wireless clients connected to the access point on the 2.4GHz or 5GHz frequency.

Refresh Time										
Auto Refresh	Time	• 5 seconds • 1 second • Disable	● 5 seconds ○ 1 second ○ Disable							
Manual Refres	sh	Refresh	Refresh							
2.4GHz WLAI	N Client Table									
#	SSID	IP Address MAC Address Tx Rx Signal (%) RSSI (dbm) Connected Time Idle Time Vendor	r Kick							
		No wireless client								
5GHz WLAN	Client Table									
#	SSID	IP Address MAC Address Tx Rx Signal (%) RSSI (dbm) Connected Time Idle Time Vendor	r Kick							
		No wireless client								

Refresh time						
Auto Refresh	Select a time interval for the client table list to automatically					
Time	refresh.					
Manual	Click refresh to manually refresh the client table.					
Refresh						

2.4GHz (5GHz) V	2.4GHz (5GHz) WLAN Client Table					
SSID	Displays the SSID which the client is connected to.					
MAC Address Displays the MAC address of the client.						
TxDisplays the total data packets transmitted by the specified client.						
Rx	Displays the total data packets received by the specified client.					
Signal (%)	Displays the wireless signal strength for the specified client.					
Connected Displays the total time the wireless client has been						
Time	connected to the access point.					
Idle Time	Client idle time is the time for which the client has not					
	transmitted any data packets i.e. is idle.					
Vendor	The vendor of the client's wireless adapter is displayed here.					

X-7-2-3 Wireless Monitor

"Wireless Monitor" is a tool built into the access point to scan and monitor the surrounding wireless environment. Select a frequency and click "Scan" to display a list of all SSIDs within range along with relevant details for each SSID.

Site Survey ● Wireless 2.4G / 5G ● 2.4G ● 5G Scan								
Channel Survey result			Export					
Wireless 2.	4GHz							
Ch	SSID	MAC Address	Security	Signal (%)	Туре	Vendor		
			You can click Scan button to start.					
Wireless 50	Hz							
Ch	SSID	MAC Address	Security	Signal (%)	Туре	Vendor		
			You can click Scan button to start.					

Wireless Monitor						
Site Survey Select which frequency (or both) to scan, and click "Scan" to						
	begin.					
Channel After a scan is complete, click "Export" to save the results						
Survey Result	local storage.					

Site Survey Res	ults			
Ch	Displays the channel number used by the specified SSID.			
SSID	Displays the SSID identified by the scan.			
MAC Address Displays the MAC address of the wireless router/access point				
	for the specified SSID.			
Security Displays the authentication/encryption type of the speci				
	SSID.			
Signal (%)	Displays the current signal strength of the SSID.			
Туре	Displays the 802.11 wireless networking standard(s) of the			
specified SSID.				
Vendor Displays the vendor of the wireless router/access point				
	specified SSID.			

"System log" displays system operation information such as up time and connection processes. This information is useful for network administrators. Older entries will be overwritten when the log is full

earch				🗆 Ma	tch whole words	
ID 🔻	Date and Time	Category 🔺	Severity 🔺	Users 🔺	Events/Activities	
186	/01/03 01:00:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
185	/01/03 00:30:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
184	/01/03 00:00:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
183	/01/02 23:30:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
182	/01/02 23:00:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
181	/01/02 22:30:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
180	/01/02 22:00:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
179	/01/02 21:30:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
178	/01/02 21:00:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600	
177	/01/02 20:36:40	SYSTEM	Low	admin	WLAN[5G], Best channel selection start, switch to channel 36 + 40 + 44 + 48	
176	/01/02 20:36:29	SYSTEM	Low	admin	Bandsteering, Stopping	
175	/01/02 20:36:18	SYSTEM	Low	admin	Bandsteering, Stopping	
174	/01/02 20:36:18	SYSTEM	Low	admin	Traffic Shaping ssid, Stopping	
173	/01/02 20:36:18	SYSTEM	Low	admin	SNMP, start SNMP server	
172	/01/02 20:36:18	SYSTEM	Low	admin	SNMP, stop SNMP server	
171	/01/02 20:36:18	SYSTEM	Low	admin	LAN, Firewall Disabled	
170	/01/02 20:36:18	SYSTEM	Low	admin	LAN, NAT Disabled	
169	/01/02 20:36:18	SYSTEM	Low	admin	LAN, stop Firewall	
168	/01/02 20:36:18	SYSTEM	Low	admin	LAN, stop NAT	
167	/01/02 20:36:18	SYSTEM	Low	admin	SCHEDULE, Schedule Stopping	

Save	Click to save the log as a file on your local computer.
Clear	Clear all log entries.
Refresh	Refresh the current log.

The following information/events are recorded by the log:



Mount & unmount

Wireless Client

Connected & disconnected Key exchange success & fail

Authentication
 Authentication fail or successful.

```
    Association
    Success or fail
```

WPS M1 - M8 messages WPS success Change Settings ♦ System Boot Displays current model name NTP Client Wired Link LAN Port link status and speed status Proxy ARP Proxy ARP module start & stop ♦ Bridge Bridge start & stop. ♦ SNMP SNMP server start & stop. ♦ HTTP HTTP start & stop. HTTPS HTTPS start & stop. ♦ SSH SSH-client server start & stop. Telnet Telnet-client server start or stop. ◆ WLAN (2.4G) WLAN (2.4G] channel status and country/region status

WLAN (5G)

WLAN (5G) channel status and country/region status

X-7-3 Management

X-7-3-1 Admin

You can change the password used to login to the browser-based configuration interface here. It is advised to do so for security purposes.

If you change the administrator password, please make a note of the new password. In the event that you forget this password and are unable to login to the browser based configuration interface, see 1-5 Reset for how to reset the access point.

Account to Manage This Device							
Administrator Name	admin						
Administrator Password	•••••			(4-32Characters)			
	•••••			(Confirm)			
Apply	Apply						
Advanced Settings							
Product Name	AP801F02	2F1968A					
HTTP Port	80						
HTTPS Port	443	(443, 1024 - 6553	5)				
Management Protocol	 ✓ HTTP ✓ HTTPS ✓ TELNET SSH 						
Login Timeout	5 v (mins)						
Apply							

Account to Manage This Device						
Administrator	Set the access point's administrator name. This is used to log					
Name in to the browser based configuration interface and must k						
between 4-16 alphanumeric characters (case sensitive).						
Administrator	Set the access point's administrator password. This is used to					
Password	log in to the browser based configuration interface and must					
	be between 4-32 alphanumeric characters (case sensitive).					

Press "Apply" to apply the configuration.

Advanced Settin	gs				
Product Name	Edit the product name according to your preference				
	consisting of 1-32 alphanumeric characters. This name is used				
	for reference purposes.				
Management Check/uncheck the boxes to enable/disable specified					
Protocol	management interfaces (see below). When SNMP is enabled,				
	complete the SNMP fields below.				
SNMP Version	Select SNMP version appropriate for your SNMP manager.				
SNMP Get Enter an SNMP Get Community name for verification with					
Community	SNMP manager for SNMP-GET requests.				
SNMP Set	Enter an SNMP Set Community name for verification with the				
Community	SNMP manager for SNMP-SET requests.				
SNMP Trap	Enable or disable SNMP Trap to notify SNMP manager of				
	network errors.				
SNMP Trap	Enter an SNMP Trap Community name for verification with				
Community the SNMP manager for SNMP-TRAP requests.					
SNMP Trap	Specify the IP address or sever name (2-128 alphanumeric				
Manager	characters) of the SNMP manager.				
Manager	characters) of the SNMP manager.				

HTTP

Internet browser HTTP protocol management interface

TELNET

Client terminal with telnet protocol management interface

SNMP

Simple Network Management Protocol. SNMPv1, v2 & v3 protocol supported. SNMPv2 can be used with community based authentication. SNMPv3 uses user-based security model (USM) architecture.

Press "Apply" to apply the configuration.

X-7-3-2 Date and Time

Configure the date and time settings of the access point here. The date and time of the device can be configured manually or can be synchronized with a time server.

Date and Time Settings								
Local Time	2012	▼ Year	Jan	¥	Month	1	▼	Day
	0	▼ Hours	00	V	Minutes	00	T	Seconds
Acquire Current Time from Your PC								
NTP Time Server								
Use NTP	Enable							
Auto Daylight Saving	Enable							
Server Name	User-Defir	ned 🔻						
Update Interval	24	(Hours)						
Time Zone								
Time Zone (GMT+08:00) Taipei, Taiwan ▼								T
								Apply Cancel

Date and Time Settings		
Local Time	Set the access point's date and time manually using the drop	
	down menus.	
Acquire	Click "Acquire Current Time from Your PC" to enter the	
Current Time	required values automatically according to your computer's	
from your PC	current time and date.	

NTP Time Server		
Use NTP	The access point also supports NTP (Network Time Protocol)	
	for automatic time and date setup.	
Server Name	Enter the host name or IP address of the time server if you	
	wish.	
Update	Specify a frequency (in hours) for the access point to	
Interval	update/synchronize with the NTP server.	

Time Zone	
Time ZoneSelect the time zone of your country/region. If your	
	country/region is not listed, please select another
	country/region whose time zone is the same as yours.

X-7-3-3 Syslog Server Settings

The system log can be sent to a server.

Syslog Server Settings		
Transfer Logs	Enable Syslog Server	
		Apply Cancel

Syslog Server Settings		
Transfer Logs	Check the box to enable the use of a syslog server.	
	Enter a host name, domain or IP address for the server,	
	consisting of up to 128 alphanumeric characters.	

X-7-3-4 Syslog E-mail Settings

Syslog E-mail Settings		
E-mail Logs		
E-mail Subject		
SMTP Server Address		
SMTP Server Port		
Sender E-mail		
Receiver E-mail		
Authentication	Disable •	
		Apply Cancel

Syslog E-mail Settings		
E-mail Logs	Check the box to enable/disable e-mail logs.	
E-mail Subject	Specify the subject line of log emails.	
SMTP Server	Specify the SMTP server address used to send log emails.	
Address		
SMTP Server	Specify the SMTP server port used to send log emails.	
Port		
Sender E-mail	Specify the sender email address.	
Receiver	Specify the email to receive log emails.	
E-mail		
Authentication	Disable or select authentication type: SSL or TLS. When using	
	SSL or TLS, enter the username and password.	

X-7-3-5 I'm Here

The access point features a built-in buzzer which can sound on command using the "I'm Here" page. This is useful for network administrators and engineers working in complex network environments to locate the access point.

Duration of Sound			
Duration of Sound	10	(1-300 seconds)	
			Sound Buzzer



A The buzzer is loud!

Duration of	Set the duration for which the buzzer will sound when the	
Sound	"Sound Buzzer" button is clicked.	
Sound Buzzer	Activate the buzzer sound for the above specified duration of	
	time.	

X-7-4 Advanced

X-7-4-1 LED Settings

The access point's LEDs can be manually enabled or disabled according to your preference.

LED Settings		
Power LED	● On ● Off	
Diag LED	● On ○ Off	

Power LED	Select on or off.
Diag LED	Select on or off.

X-7-4-2 Update Firmware

The "Firmware" page allows you to update the firmware of the system. Updated firmware versions often offer increased performance and security, as well as bug fixes. Download the latest firmware from the Edimax website.

Firmware Location		
Update firmware from	a file on your PC	
II-late Pierrene form DC		
Update Firmware from PC		
Firmware Update File	Choose File No file chosen	
Update		



Do not switch off or disconnect the access point during a firmware upgrade, as this could damage the device.

Firmware	Click "Choose File" to upload firmware from your local computer.
Location	

X-7-4-3 Save/Restore Settings

The device's "Save / Restore Settings" page enables you to save / backup the device's current settings as a file to your local computer, and restore the access point to previously saved settings.

Save/Restore Method	
Using Device	Using your PC
Save Settings to PC	
Save Settings	Encrypt the configuration file with a password.
Save	
Restore Settings from PC	
Restore Settings	Choose File No file chosen Open file with password.
Restore	

Save Settings to PC		
Save Settings	Encryption: If you wish to encrypt the configuration file with	
	a password, check the "Encrypt the configuration file with a	
	password" box and enter a password.	
	Click "Save" to save current settings. A new window will	
	open to allow you to specify a location to save to.	

Restore Settings from PC		
Restore	Click the "Choose File" button to find a previously saved	
Settings	settings file on your computer. If your settings file is	
	encrypted with a password, check the "Open file with	
	password" box and enter the password in the following field.	
	Click "Restore" to replace your current settings.	

X-7-4-4 Factory Default

If the access point malfunctions or is not responding, rebooting the device (VI-5-5 **Reboot**) maybe an option to consider. If rebooting does not work, try resetting the device back to its factory default settings. You can reset the access point back to its default settings using this feature if the reset button is not accessible.

This will restore all settings to factory defaults.	
	Factory Default

FactoryClick "Factory Default" to restore settings to the factoryDefaultdefault. A pop-up window will appear and ask you to confirm.



After resetting to factory defaults, please wait for the access point to reset and restart.

If the access point malfunctions or is not responding, rebooting the device may be an option to consider. You can reboot the access point remotely using this feature.

This will reboot the product. Your settings will not be changed. Click "Reboot" to reboot the product now.

Reboot

Reboot	Click "Reboot" to reboot the device. A countdown will	
	indicate the progress of the reboot.	

X-8 Toolbox

The Toolbox panel provides network diagnostic tools: *Ping, Traceroute,* and *IP Scan*.

X-8-1 Network Connectivity

X-8-1-1 Ping

Ping is a computer network administration utility used to test whether a particular host is reachable across an IP network and to measure the round-trip time for sent messages.

Ping Test		
Destination Address	Exe	ecute
Result		

Destination Address	Enter the address of the host.
Execute	Click "Execute" to ping the host.

X-8-1-2 Trace Route

Traceroute is a diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network.

Traceroute Test	
Destination Address	Execute
Result	

Destination Address	Enter the address of the host.
Execute	Click "Execute" to execute the traceroute command.

X-8-1-3 IP Scan

	in										. *	SC	an																		
Result																															
G	Graphi	c Illus	tratio	n: 🗆	un-u	sed	dis	stribut	ed	non	-distri	butab	le	scani	ning																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
0-31																															
32-63																															
64-95																															
96-127																															
128-159																															
128-159 160-191																															

Appendix XI

Configuring your IP address XI-1

The access point uses the default IP address 192.168.2.2. In order to access the browser based configuration interface, you need to modify the IP address of your computer to be in the same IP address subnet e.g. 192.168.2.x (x = 3 -254).

The procedure for modifying your IP address varies across different operating systems; please follow the guide appropriate for your operating system.

In the following examples we use the IP address 192.168.2.10 though you can use any IP address in the range 192.168.2.x (x = 3 - 254).



If you've changed the AP Controller's IP address, or if your ateway/router uses a DHCP server, make sure you enter the correct IP address. Refer to your gateway/router's settings. Your computer's IP address must be in the same subnet as the AP Controller.



If using a DHCP server on the network, it is advised to use your DHCP server's settings to assign the AP Controller a static IP address.

1. Click the "Start" button (it should be located in the lower-left corner of your computer) → "Control Panel" → "Network and Internet Connections" → "Network Connections" → "Local Area Connection". The "Local Area Connection Properties" window will appear, select "Internet Protocol (TCP / IP)", and click "Properties".

🕹 Local Area Connection Properties 🛛 🔹 💽
General Authentication Advanced
Connect using:
AMD PCNET Family PCI Ethernet Ad
This connection uses the following items:
 Client for Microsoft Networks File and Printer Sharing for Microsoft Networks QoS Packet Scheduler Internet Protocol (TCP/IP)
□ <u>In</u> stall Uninstall Properties
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
 Sho<u>w</u> icon in notification area when connected ✓ Notify <u>m</u>e when this connection has limited or no connectivity
OK Cancel

2. Select "Use the following IP address", then input the following values:

IP address: 192.168.2.10 Subnet Mask: 255.255.255.0

Click 'OK' when finished.

Internet Protocol (TCP/IP) Prop	erties 🛛 🛛 🛛 🛛
General	
You can get IP settings assigned aut this capability. Otherwise, you need to the appropriate IP settings.	
O Obtain an IP address automatic O Use the following IP address:	ally
<u>I</u> P address:	192.168.2.10
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
Default gateway:	
○ O <u>b</u> tain DNS server address auto	·
Preferred DNS server:	
<u>A</u> lternate DNS server:	
	Ad <u>v</u> anced
	OK Cancel

1. Click the "Start" button (it should be located in the lower-left corner of your computer) → "Control Panel" → "View Network Status and Tasks" → "Manage Network Connections" → "Local Area Network" → "Properties". The "Local Area Connection Properties" window will appear, select "Internet Protocol Version 4 (TCP / IPv4)", and then click "Properties".

Intel(R) PRO/1	000 MT Network Conne	ection
		Configure
his connection uses	the following items:	
Client for Mic		
🗹 📙 QoS Packet	Scheduler	
	er Sharing for Microsoft	
🗹 🔺 Internet Prote	ocol Version 6 (TCP/IP)	v6)
 Internet Proto Internet Proto 	col Version 6 (TCP/IP) col Version 4 (TCP/IP)	v6) v4)
Internet Proto Internet Proto Internet Proto Internet Proto Internet Proto Internet Proto	ocol Version 6 (TCP/IP) ocol Version 4 (TCP/IP) opology Discovery Map	v6) v4) per I/O Driver
Internet Proto Internet Proto Internet Proto Internet Proto Internet Proto Internet Proto	col Version 6 (TCP/IP) col Version 4 (TCP/IP)	v6) v4) per I/O Driver
✓ Internet Prote ✓ Internet Prote ✓ Internet Prote ✓ ✓ Internet Prote ✓ ✓ Internet Prote ✓ ✓ ✓ Internet Prote ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	ocol Version 6 (TCP/IP) ocol Version 4 (TCP/IP) opology Discovery Map opology Discovery Resp	v6) v4) per I/O Driver ponder
Internet Proto Internet Proto Internet Proto Internet Proto Internet Proto Internet Proto	ocol Version 6 (TCP/IP) ocol Version 4 (TCP/IP) opology Discovery Map	v6) v4) per I/O Driver
 ✓ Internet Proto ✓ Internet Proto ✓ Ink-Layer To ✓ Link-Layer To Install Description 	Decol Version 6 (TCP/IP) Decol Version 4 (TCP/IP) Decology Discovery Map Depology Discovery Resp Uninstall	v6) per I/O Driver ponder Properties
 ✓ Internet Prote ✓ Internet Prote ✓ Internet Prote ✓ Ink-Layer Transmission Contra 	ocol Version 6 (TCP/IP) ocol Version 4 (TCP/IP) opology Discovery Map opology Discovery Resp	v6) per I/O Driver ponder Properties toccol. The default

2. Select "Use the following IP address", then input the following values:

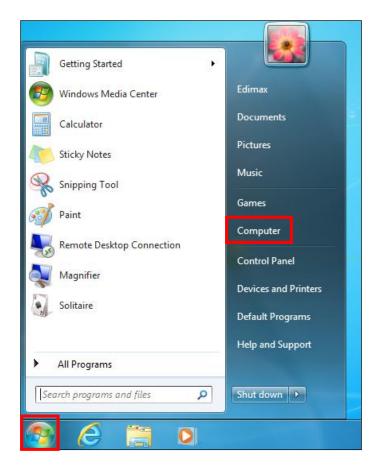
IP address: 192.168.2.10 Subnet Mask: 255.255.255.0

Click 'OK' when finished.

u can get IP settings assigned auto is capability. Otherwise, you need t	
r the appropriate IP settings.	-
Obtain an IP address automatication of the second secon	ally
IP address:	192.168.2.10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	i kon an i
🔿 Obtain DNS server address auto	matically
Ouse the following DNS server ad	dresses:
Preferred DNS server:	
Alternate DNS server:	Grab selected Region
	Advanced

XI-1-3 Windows 7

1. Click the "Start" button (it should be located in the lower-left corner of your computer), then click "Control Panel".



2. Under "Network and Internet" click "View network status and tasks".



3. Click "Local Area Connection".

View your basic network inf	ormation and se	et up connect	ions	
M		 ×	Ö	See full map
TS-WIN7 (This computer)	Home network		Internet	
View your active networks			C	Connect or disconnect
Home network Home network		Access type: HomeGroup: Connections:	No Internet Ready to cr	

4. Click "Properties".

🃮 Local Area Conne	ction Status		×
General	/ Ship		
Connection			_
IPv4 Connectivit	y:	No Internet acce	ess
IPv6 Connectivit	y:	No network acce	ess
Media State:		Enab	led
Duration:		02:08:	52
Speed:		100.0 Mb	ps
Details			
Activity			_
	Sent —	Receiv	ed
Bytes:	951,332	4,398,1	.84
Properties	Oisable	Diagnose	
		C	ose

5. Select "Internet Protocol Version 4 (TCP/IPv4) and then click "Properties".

Local Area Connection Properties	23							
Networking								
Connect using:								
Broadcom 440x 10/100 Integrated Controller								
Configure								
This connection uses the following items:								
Gient for Microsoft Networks GoS Packet Scheduler								
Image of a construction of the constructio								
Internet Protocol Version 6 (TCP/IPv6)								
Internet Protocol Version 4 (TCP/IPv4)								
Install Uninstall Properties								
Description								
TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.								
ОК Са	ncel							

6. Select "Use the following IP address", then input the following values:

IP address: 192.168.2.10 Subnet Mask: 255.255.255.0

Click 'OK' when finished.

ou can get IP settings assigned auto is capability. Otherwise, you need t r the appropriate IP settings.	o ask your network administrator
Obtain an IP address actionatics	an y
IP address:	192.168.2.10
Subnet mask:	255.255.255.0
Default gateway:	i e se a
💿 Obtain DNS server address auto	matically
Ose the following DNS server ad	dresses:
Preferred DNS server:	
Alternate DNS server:	Grab selected Region
	Advanced

1. From the Windows 8 Start screen, switch to desktop mode by clicking the "Desktop" box.



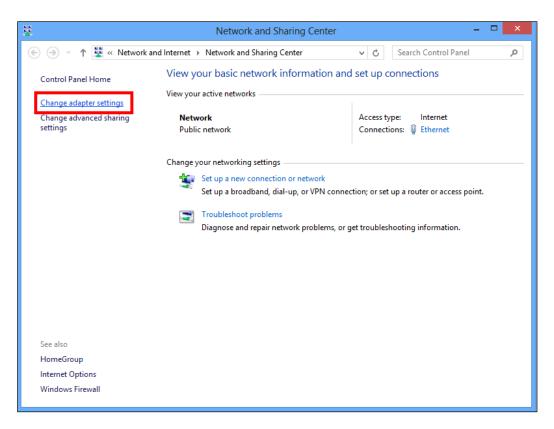
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



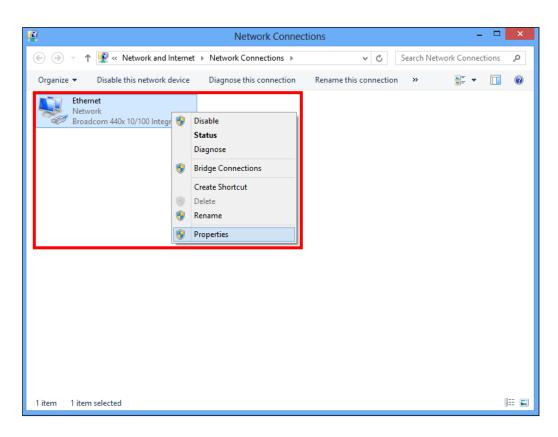
3. Right click "Network" and select "Properties".

🖗 l 🔁 👔 = l	Network	- 0 ×
File Network View		v (?
	✓ C Search Network	م,
Network discovery and file sharing are turne	d off. Network computers and devices are not visible. Click to change	х
 * Favorites Desktop Downloads Recent places * Libraries Documents Documents Music Pictures Videos * Computer Expand Open in new window Pin to Start Map network drive Disconnect network driv Picete 	This folder is empty.	
0 items		811 🔳
6	- No 🔁 🛛	2:53 PM 12/3/2012

4. In the window that opens, select "Change adapter settings" from the left side.



5. Right click the connection and select "Properties".



6. Select "Internet Protocol Version 4 (TCP/IPv4) and then click "Properties".

Ethernet Properties		x	
Networking			
Connect using:			
Broadcom 440x 10/100 Integrated Control	ller		
	Configure	1	
This connection uses the following items:		-	
	File and Printer Sharing for Microsoft Networks Microsoft Network Adapter Multiplexor Protocol		
Microsoft LLDP Protocol Driver	L/O D:		
 Link-Layer Topology Discovery Mapper Link-Layer Topology Discovery Respon 			
Internet Protocol Version 6 (TCP/IPv6)			
Internet Protocol Version 4 (TCP/IPv4)	· · ·	-	
<	>		
Install Uninstall	Properties		
Description			
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.			
ОК	Cance	<u>+</u>	

7. Select "Use the following IP address", then input the following values:

IP address: 192.168.2.10 Subnet Mask: 255.255.255.0

Click 'OK' when finished.

Internet Protocol Version 4 (TCP/IPv4) Properties		
General		
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.		
Obtain an IP address automatic	ally	
Use the following IP address:		
IP address:	192 . 168 . 128 . 10	
Subnet mask:	255 . 255 . 255 . 0	
Default gateway:		
O Obtain DNS server address auto	omatically	
• Use the following DNS server ad	Idresses:	
Preferred DNS server:		
Alternate DNS server:	· · ·	
Ualidate settings upon exit	Advanced	
	OK Cancel	

XI-1-5 Mac

1. Have your Macintosh computer operate as usual, and click on "System Preferences"



2. In System Preferences, click on "Network".



3. Click on "Ethernet" in the left panel.

0 0	Network	
▲ ▶ Show All		Q
	Location: Location (5/2/13	2:54 PM) 🗘
Ethernet Connected FireWire Not Connected	Status:	Connected Ethernet is currently active and has the IP address 169.254.75.4.
● Wi-Fi Off	Configure IPv4:	Using DHCP \$
	Subnet Mask: Router:	255.255.0.0
	DNS Server: Search Domains:	
	Search Bonnains.	
+ - * -		Advanced ?
Click the lock to	prevent further changes.	Assist me Revert Apply

4. Open the drop-down menu labeled "Configure IPv4" and select "Manually".

0 0	Network	
◄ ► Show All		٩
Locat	ion: Location (5/2/13 2:54 PM)	\$
Ethernet Connected Image: Connected FireWire Not Connected Image: Connected Wi-Fi Off Image: Connected	Configure IPv4 Using DF Using DF Using DF Using Po Subnet Mask Router	currently active and has the IP 9.254.75.4. HCP HCP with manual address otP
+ - * -		Advanced ?
Click the lock to prevent fu	rther changes. Assist 1	me Revert Apply

5. Enter the IP address 192.168.2.10 and subnet mask 255.255.255.0. Click on "Apply" to save the changes.

● ○ ○		Network		
Show All]			Q
	Location:	Location (5/2/13	2:54 PM)	•
Ethernet Connected FireWire Not Connected	*** ***	Status:	Connected Ethernet is currently act address 169.254.75.4.	tive and has the IP
● Wi-Fi Off	(1)	Configure IPu4 IP Address: Subnet Mask:	192.168.2.10	÷
		Router: DNS Server:		
		Search Domains:		
+ - * -				Advanced ?
Click the lock to	prevent furthe	r changes.	Assist me	Revert Apply

XI-2 Command Line Interface

Settings can also be configured using the Command Line Interface using the steps and commands shown below:

Edit Mode

- **1.** Log on this product.
- Enter the "edit start" command. man\$ edit start
- The change of prompt from "man \$" to "man [edit] \$" indicates that Edit Mode is initiated. man[edit]\$

In Edit Mode, if more than one command is entered, you can reflect the settings using the following:

man[edit]\$ wlan 5g band 11a11n brs 24m channel 40 bandwidth 40m+ex_lower_ch

man[edit]\$ config timezone 50 man[edit]\$ edit end

When you run the "edit end" command exit Edit Mode, the setting will be achieved.

XI-2-1 Config

config apname

Name / rename this product. <Syntax of the command> config apname (apname)

- <Parameter>

 (apname) name of the product
 (Default configuration)
- <Default configuration>
 AP (MAC address LAN side of this product)
- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # config apname enterprise-network

config basic_info show status

Show the configuration information setup.

<The syntax of the command>

config basic_info show status { admin|buzzer|date&time | led_settings | syslog_server }

- <Parameter>
 NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples>
 # config basic_info show status date&time
 # config basic_info show status led_settings

config buzzer time

Set the sound time. <The syntax of the command> config buzzer time (time)

- <Parameter>
 (time) Buzzer Time. (1~300 sec)
- <Default configuration> 10
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # config buzzer time 50

config date

Set the internal clock function of this product. <The syntax of the command>

config date (yy) | (yyyy)/(mm)/(dd) [(HH):(MM):(SS) | (HH):(MM)]

- <Parameter>
 - (yy) | (yyyy) Enter the two-digit or four-digit year setting.
 - (mm) Enter the two-digit month setting.
 - (dd) Enter the two-digit day setting.
 - (HH) Entered in 24-hour time display setting.
 - (MM) Enter the minute to set.
 - (SS) Enter the second to set.
- <Default configuration>
 - Jan 1st 2012 00:00:00
- <Command mode> Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- **<Examples>** # config date 2012/10/10 12:34:56

config firmware

Update the firmware of this product. <The syntax of the command>

config firmware target tftp server (tftp-server) file (filename)

- <Parameter>

 (tftp-server) Update the firmware from the TFTP server.
 (filename) Set the name of the firmware file.
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples>
 # config firmware target tftp server 192.168.2.100 file CAP1300.bin

config init

Return to the initial value all the parameters that are set in this product.

<The syntax of the command>

config init [force]

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode> Immediate Mode
- <Compatible Products> CAP1300
- <Examples>
 # config init
 # config init force

config led_setting

Set the LED of this product. <The syntax of the command>

config led_setting {led} {on | off}

- <Parameter>
 {led} Enter power or diag to set either the power or diag LED
- <Default configuration>
 On
- **<Command mode>** Immediate Mode

- <Compatible Products> CAP1300
- <Examples> # config led_setting power on # config led_setting diag off

config management

Settings for the management interface of this product. <The syntax of the command> config management {protocol} {disable | enable}

config management snmp version v1/v2 rcom (rcom) rwcom (rwcom)

config management snmp version v3

config management snmp trap {disable | enable} trapcom (trapcom) ip (ipaddress)

- <parameter< th=""><th>:></th></parameter<>	:>
---	----

{**protocol**} **http** Set http protocol

- Ssh Set ssh protocol.
- snmp Set snmp protocol.
- telnet Set telnet protocol.
- https Set https protocol.
- (rcom) Set the community name specified when the SNMP manager sends a "GET Request" for this product. (6~32 characters)
- (rwcom) Set the community name specified when the SNMP manager to send a "SET Request" for this product. (6~32 characters)
- (v3_name) Set the name of SNMP v3.
- (v3_passwd) Set the password of SNMP v3.
- (trapcom) Set the trap community name specified.
- (ipaddress) Set the trap community name specified.
- <Default configuration>
 - enable : http enable : https
 - enable: telnet
 - disable : ssh
 - disable : snmp
 - rcom : public
 - rwcom : private
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products>
 - CAP1300
- <Examples>
 - # config management http disable
 - # config management snmp enable

 - # config management snmp version v3 v3_name edimax v3_passwd edimax3047
 - # config management snmp trap enable trapcom public ip 192.168.2.100

config ntp client

Set the NTP client function of this product. <The syntax of the command>

config ntp client disable

config ntp client enable server (ntp-server) interval (ntp-interval)

- <Parameter>

 (ntp-server) Set the host name or IP address of the NTP server.
 (ntp-interval) Set the interval time to query the NTP server. (1~24)

 <Default configuration>

 Invalid
- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # config ntp client enable server clock.stdtime.gov.tw interval 24
 # config ntp client disable

config password

Set the password to log in to the setup screen of this product. <The syntax of the command>

config password (username) (oldpassword) (newpassword)

- <Parameter>

 (username)
 Specifies the user name.
 (oldpassword)
 Enter the password that is currently set.
 (newpassword)
 Enter the password to the new one.
- <Default configuration>
 Administrator Name: admin
 Administrator Password: admin
- <Command mode> Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples> # config password admin 1234 abc789

config reboot

Reboot of this product. <The syntax of the command>

config reboot [force]

- <Parameter>
 NA
- <Default configuration> NA
- <Command mode>

Immediate Mode

- <Compatible Products> CAP1300
- <Examples> # config reboot
 # config reboot force

config restore

Restore the settings from the configuration file of this product. <The syntax of the command>

config restore target tftp server (tftp-server) file (filename) [pass (password)] [force]

- <Parameter>

tftpRestore configuration from the TFTP server.(tftp-server)Set the host name or IP address of the TFTP server.(filename)Set the name of the configuration file.(password)Set a password to protect the configuration file.

- <Default configuration>
- NA
- <Command mode> Immediate Mode
- <Compatible Products> CAP1300

<Examples>
 # config restore target tftp server 192.168.3.66 file edimax-cap1300.bin pass 123456

config save

Save the file to the current settings of this product.

<The syntax of the command>

config save target tftp server (tftp-server) file (filename) [pass (password)] [force]

- <Parameter>
 tftp Save the settings to TFTP server.
 (tftp-server) Set the host name or IP address of the TFTP server.
 (filename) Set the name of the configuration file.
 (password) Set a password to protect the configuration file.
- <Default configuration> NA
- <Command mode>

Immediate Mode

- <Compatible Products> CAP1300
- <Examples>
 # config save target tftp server 192.168.11.66 file edimax-cap1300.bin

config syslog clinet

Set the transfer function by the syslog protocol log information. <The syntax of the command>

config syslog client enable server (servername) config syslog client disable

- <Parameter>
 (servername) Set the host name or IP address of the syslog server.
- <Default configuration> Invalid
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # config syslog client enable server 192.168.3.202
 # config syslog client disable

config timezone

Set time zone of the internal clock of this product. <The syntax of the command>

config timezone {zone-name}

<Parameter>

{zone-name} Specify a time zone.

The values that can be set are as follows:

- 0 | (GMT-12:00) Eniwetok, Kwajalein, International Date Line West
- 1 | (GMT-11:00) Midway Island, Samoa
- 2 | (GMT-10:00) Hawaii
- 3 | (GMT-09:00) Alaska
- 4 | (GMT-08:00) Pacific Time (US & Canada); Tijuana
- 5 | (GMT-07:00) Arizona
- 6 | (GMT-07:00) Chihuahua, La Paz, Mazatian
- 7 | (GMT-07:00) Mountain Time (US & Canada)
- 8 | (GMT-06:00) Central America
- **9** | (GMT-06:00) Central Time (US & Canada)
- 10 | (GMT-06:00) Guadalajara, Mexico City, Monterrey
- 11 | (GMT-06:00) Saskatchewan
- 12 | (GMT-05:00) Bogota, Lima, Quito
- 13 | (GMT-05:00) Eastern Time (US & Canada)
- 14 | (GMT-05:00) Indiana (East)
- 15 | (GMT-04:00) Atlantic Time (Canada)
- 16 | (GMT-04:00) Caracas, La Paz
- 17 | (GMT-04:00) Santiago
- 18 | (GMT-03:00) Newfoundland

- 19 | (GMT-03:00) Brasilia
- 20 | (GMT-03:00) Buenos Aires, Georgetown
- 21 | (GMT-03:00) Greenland
- 22 | (GMT-02:00) Mid-Atlantic
- **23** | (GMT-01:00) Azores
- 24 | (GMT-01:00) Cape Verde Is.
- 25 | (GMT) Casablanca, Monrovia
- 26 | (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
- 27 | (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
- 28 | (GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
- 29 | (GMT+01:00) Brussels, Copenhagen, Madrid, Paris
- 30 | (GMT+01:00) Sarajevo, Sofija, Warsaw, Zagreb, Skopje, Vilnius
- 31 | (GMT+01:00) West Central Africa
- 32 | (GMT+02:00) Athens, Istanbul, Minsk
- **33** | (GMT+02:00) Bucharest
- 34 | (GMT+02:00) Cairo
- 35 | (GMT+02:00) Harare, Pretoria
- 36 | (GMT+02:00) Helsinki, Riga, Tallinn
- **37** | (GMT+02:00) Jerusalem
- 38 | (GMT+03:00) Baghdad
- **39** | (GMT+03:00) Kuwait, Riyadh
- 40 | (GMT+03:00) Moscow, St. Petersburg, Volgograd
- 41 | (GMT+03:00) Nairobi
- 42 | (GMT+03:30) Tehran
- 43 | (GMT+04:00) Abu Dhabi, Muscat
- 44 | (GMT+04:00) Baku, Tbilisi, Yerevan
- 45 | (GMT+04:30) Kabul
- 46 | (GMT+05:00) Ekaterinburg
- 47 | (GMT+05:00) Islamabad, Karachi, Tashkent
- 48 | (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi
- 49 | (GMT+05:45) Kathmandu
- 50 | (GMT+06:00) Almaty, Novosibirsk
- 51 | (GMT+06:00) Astana, Dhaka
- **52** | (GMT+06:00) Sri, Jayawardenepura
- **53** | (GMT+06:30) Rangoon
- 54 | (GMT+07:00) Bangkok, Hanoi, Jakarta
- 55 | (GMT+07:00) Krasnoyarsk
- 56 | (GMT+08:00) Beijing, Hong Kong
- 57 | (GMT+08:00) Irkutsk, Ulaan Bataar
- 58 | (GMT+08:00) Kuala Lumpur, Singapore
- **59** | (GMT+08:00) Perth

- **60** | (GMT+08:00) Taipei, Taiwan
- 61 | (GMT+09:00) Osaka, Sapporo, Tokyo
- 62 | (GMT+09:00) Seoul
- **63** | (GMT+09:00) Yakutsk
- 64 | (GMT+09:00) Adelaide
- 65 | (GMT+09:30) Darwin
- 66 | (GMT+10:00) Brisbane
- 67 | (GMT+10:00) Canberra, Melbourne, Sydney
- 68 | (GMT+10:00) Guam, Port Moresby
- 69 | (GMT+10:00) Hobart
- 70 | (GMT+10:00) Vladivostok
- 71 | (GMT+11:00) Magadan, Solamon, New Caledonia
- 72 | (GMT+12:00) Auckland, Wllington
- 73 | (GMT+12:00) Fiji, Kamchatka, Marshall Is.

<Default configuration> (GMT+09:00)Osaka, Sapporo,Tokyo

- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples> # config timezone 60

config username

Set the user name and password that is used to authenticate users of this product. <The syntax of the command>

config username admin (username) (oldpassword) (newpassword)

- <Parameter>

 (username)
 Specifies the user name or administrator name.
 (oldpassword)
 Enter the password that is currently set.
 (newpassword)
 Enter the password to the new one.
- <Default configuration>
 Administrator Name: admin
 Administrator Password: admin
- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # config username admin administrator 1234 1234

XI-2-2 LAN

lan ether port {pd / pse} 8023az

Enable or disable 802.3az for wired ports. <The syntax of the command> lan ether port {pd | pse} 8023az {state}

<Parameter>

_

_

pdSet one of wired ports.pseSet two of wired ports.{state}disableDisable the ether port of 802.3az.enableEnable the ether port of 802.3az.Configuration>

- All valid
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # lan ether port pse 8023az disable

lan ether port {pd / pse} link

Enable or disable the wired port. <The syntax of the command>

lan ether port {pd pse} link {disable	e enable}
---	-------------

<Parameter>

pd Set one of wired ports.pse Set two of wired ports.

- **<Default configuration>** All valid
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # lan ether port pse link disable

lan ether port {pd / pse} speed

Set the wired ports of PHY. <The syntax of the command>

lan ether port {pd	pse} speed speed auto flowctl {state}
lan ether port {pd	<pre>pse} speed speed {speed} duplex {duplex} flowctl {state}</pre>
lan ether port {pd	<pre>pse} speed speed 1000 duplex full flowctl {state}</pre>

- <Parameter>

pd Set the one of wired ports.

pse Set the two of wired ports.

- {speed} 10 Set to 10Mbps. 100 Set to 100Mbps.
- {duplex} full Set to full duplex half Set to half duplex.
- {state}disableDisable the flow control.enableEnable the flow control.
- <Default configuration> speed:auto, flowctl:enable (The same configuration on all ports)
- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>

lan ether port pd speed speed auto flowctl enable# lan ether port pse speed speed 100 duplex full flowctl disable# lan ether port pse speed speed 1000 duplex full flowctl enable

lan ether port {pd / pse} vlan mode

Set the wired ports of VLAN.

<The syntax of the command>

lan ether port {pd | pse} vlan mode {tagged | untagged} vlan (vlanid)

- <Parameter>
 pd Set the one of wired ports.

 pse Set the two of wired ports.
 (vlanid) Set the VLAN ID. (1~4094)

 <Default configuration>
- Vlanid : 1, untagged (The same configuration on all ports)
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # lan ether port pd vlan mode untagged vlan 404
 # lan ether port pse vlan mode tagged vlan 403

lan ether show status

Show the status of the VLAN wired ports. <The syntax of the command>

lan ether show status

- <Parameter>

NA

- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples># lan ether show status

lan ip defaultgw

Set the default route, or manual setting of the default gateway that has the management subnet. (If you want to remove the default gateway address set, you enter the clear.)

<The syntax of the command>

lan ip defaultgw {clear | (gateway)}

- <Parameter>
 (gateway) Enter the default gateway address.
- <Default configuration> NA
- <Command mode> Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # lan ip defaultgw clear
 # lan ip defaultgw 192.168.0.250

lan ip dhcp

Set the static ip to dhcp. <The syntax of the command>

lan ip dhcp

- **<Parameter>** NA
- <Default configuration>
 DHCP
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # lan ip dhcp

lan ip dns

Set the address of the DNS server for the subnet management. <The syntax of the command> lan ip dns {primary | secondary} { (dnsserver) | clear }

- <Parameter>

 (dnsserver)
 Enter the IP address of the DNS server.
- <Default configuration> DHCP
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # lan ip dns primary 10.10.1.127
 # lan ip dns secondary clear

lan ip static

Set the DHCP to static IP. <The syntax of the command> lan ip static (ipaddress) subnet_mask (maskip)

- <Parameter>

 (ipaddress)
 (maskip)
 Set the subnet-mask of the lan.
- <Default configuration>
 DHCP
- <Command mode> Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # lan ip static 192.168.10.100 subnet_mask 255.255.255.0

lan ip show status
Show the status of IP settings.
<The syntax of the command>

lan ip show status

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # lan ip show status

lan ip vlan

Set the VLAN ID of this product. <The syntax of the command>

lan ip vlan (vlanid)

- <Parameter>
 (vlanid) Set the VLAN ID. (1-4094)
- <Default configuration>
 - 1
- **Command mode>**Immediate Mode, Edit Mode
- **<Compatible Products>** CAP1300
- <Examples> # lan ip vlan 1

XI-2-3 Show

show status config admin

Show the username and advanced settings. <The syntax of the command> show status config admin

- <Parameter>
 NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples>
 # show status config admin

show status config buzzer

Show the sound time status. <The syntax of the command> show status config buzzer

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products>

CAP1300

 <Examples> # show status config buzzer

show status config date&time

Show the date and time. <The syntax of the command> show status config date&time.

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status config date&time

show status config led_settings

Show the LED settings.

<The syntax of the command>

show status config led_settings

- **<Parameter>** NA
- <Default configuration> NA
- **<Command mode>** Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status config led_settings

show status config syslog_server

Show the status of syslog server. <The syntax of the command> show status config syslog_server

- <Parameter>
 NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode

- <Compatible Products> CAP1300
- <Examples> # show status config syslog_server

show status maclist
Show the maclist information.
<The syntax of the command>
show status maclist

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status maclist

show status lan ether

Show the VLAN information. <The syntax of the command>

show status lan ether

- <Parameter>
 NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status lan ether

show status lan ip

Show the IP information. <The syntax of the command>

show status lan ip

- <Parameter>
 NA
- <Default configuration> NA
- **<Command mode>** Immediate Mode, Edit Mode, Reference Mode

- <Compatible Products> CAP1300
- <Examples>
 # show status lan ip

show status radius
Show the radius information.
<The syntax of the command>
show status radius

- <Parameter>
 NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status radius

show status system_info

Show the system information. <The syntax of the command>

show status system_info

- <Parameter>
 NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status system_info

show status log
Show the system log information.
<The syntax of the command>

show status log

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode>

Immediate Mode, Edit Mode, Reference Mode

- <Compatible Products> CAP1300
- <Examples> # show status system_info

show status wlan {2.4g | 5g} advanced

Show the wireless advanced information. <The syntax of the command> show status wlan {2.4g | 5g} advanced

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples># show status wlan 2.4g advanced

show status wlan {2.4g / 5g} basic

Show the wireless information. <The syntax of the command> show status wlan {2.4g | 5g} basic

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status wlan 2.4g basic

show status wlan {2.4g | 5g} clients

Show the status of wireless clients information. <The syntax of the command>

show status wlan {2.4g | 5g} clients

- <Parameter>
 - NA
- <Default configuration>

NA

- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status wlan 2.4g clients

show status wlan {2.4g | 5g} security

Show the wireless security information. <The syntax of the command> show status wlan {2.4g | 5g} security

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status wlan 2.4g security

show status wlan {2.4g | 5g} wds

Show the wireless wds information. <The syntax of the command> show status wlan {2.4g | 5g} wds

- <Parameter>
 NA
- <Default configuration> NA
- **<Command mode>** Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples>
 # show status wlan 2.4g wds

show status wlan monitor

Show the status of wireless monitor. <The syntax of the command>

show status wlan monitor

<Parameter>
 NA

- <Default configuration> NA
- **<Command mode>** Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status wlan monitor

show status wlan wmm

Show the status of wireless QoS configuration. <The syntax of the command> show status wlan wmm

- <Parameter>
 NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status wlan wmm

show status wlan wps

Show the status of wireless security WPS. <The syntax of the command> show status wlan wps

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # show status wlan wps

XI-2-4 Wlan

wlan {2.4g | 5g} 80211n_protect

Set the 802.11n protection.

udan En 00211n musto at (stato)
wlan 5g 80211n_protect {state}

wlan 2.4g {protect} {state}	

<parameter< th=""><th>`></th><th></th></parameter<>	`>	
{protect}	80211n_protect	Set the 802.11n protection.
	80211g_protect	Set the 802.11g protection.
{state}	disable	Disable the 802.11n or 802.11g protection.
	enable	Enable the 802.11n or 802.11g protection.
<default co<="" td=""><th>nfiguration></th><td></td></default>	nfiguration>	
Enable		
<command mode=""/>		
Immediate	Mode, Edit Mode	
<compatibl< td=""><th>e Products></th><td></td></compatibl<>	e Products>	
CAP1300		
<examples></examples>	>	
# wlan 5g 8	0211n_protect enabl	e
#	80211g protect disa	hlo

wlan {2.4g | 5g} basic_info show status

Show the wireless information. <The syntax of the command>

wlan {media} basic_info show status { advanced | basic | clients | security | wds }

{media}	2.4g	Show the wireless 802.11g information.
	5g	Show the wireless 802.11a information.
<default co<="" td=""><th>onfiguratio</th><td>on></td></default>	onfiguratio	on>
NA		
<command< td=""><th>l mode></th><td></td></command<>	l mode>	
Immediate	Mode, Edi	it Mode, Reference Mode
		-
Immediate <compatib< b=""> CAP1300</compatib<>		-
< Compatib CAP1300	le Product	-
< Compatib CAP1300 < Examples	le Product	-

wlan {2.4g | 5g} beacon dtim

Configure the transmission interval of the DTIM.

<The syntax of the command>

wlan {media} beacon dtim (num)

<Parameter>

{media} 2.4g Set the interval between transmission of 802.11g.

Set the interval between transmission of 802.11a.

(num) Set the transmission interval. (1~255)

- <Default configuration>
 - 1

5g

- **<Command mode>** Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples># wlan 5g beacon dtim 100

wlan {2.4g | 5g} beacon interval

Configure the transmission interval of the beacon. <The syntax of the command>

wlan {media} beacon interval (num)	

- <Parameter>

{media}2.4gConfigure the interval between transmission of 802.11g.5gConfigure the interval between transmission of 802.11a.

(num) Set the transmission interval. (20~1000 ms)

- <Default configuration> 100
- <Command mode>
 Immediate Mode, Edit Mode
 <Compatible Products>
- CAP1300
- <Examples>
 # wlan 5g beacon interval 200

wlan {2.4g | 5g} channel change_ch_if_STA_connected

Set the change channel function of this product. (The station is connected status.) <The syntax of the command>

wlan {media} channel change_ch_if_STA_connect {disable enable}
--

<Parameter>

{media}

Set the function enable or disable on 802.11g.

Set the function enable or disable on 802.11a.

- <Default configuration>
 Disable
- **<Command mode>** Immediate Mode, Edit Mode

2.4g

5g

- <Compatible Products> CAP1300
- <Examples>
 # wlan 2.4g channel change_ch_if_STA_connect enable

wlan {2.4g | 5g} channel checktime

Set the channel check time.

<The syntax of the command>

wlan {media} channel checktime {per	riod}
-------------------------------------	-------

- <Parameter>

{med	ia}	2.4g	Set the channel check time on 802.11g.
		5g	Set the channel check time on 802.11a.
{perio	od}	half_hr	Set the half hour time to check channel.
		one_hr	Set the one hour time to check channel.
		two_hr	Set the two hours time to check channel.
		half_day	Set the half day time to check channel.
		one_day	Set the one day time to check channel.
		two_day	Set the two days time to check channel.
		• •••••	

- <Default configuration> half hour
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples> # wlan 5g channel checktime one_hr

wlan {2.4g | 5g} {disable | enable}

Set the radio to enable or disable the wlan. <The syntax of the command>

wlan {media} {state}

- <Parameter>

{media}	2.4g	Enable or disable the wlan of the 802.11g.
	5g	Enable or disable the wlan of the 802.11a.
{state}	disable	Disable the wlan.
	enable	Enable the wlan.

- <Default configuration>

2.4g: disable

5g: disable

- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples> # wlan 5g enable # wlan 2.4g enable

wlan **{2.4g | 5g}** *fragmentthreshold* Set the fragment threshold.

<the command="" of="" syntax="" the=""></the>						
wlan {media} fragmentthreshold (num)						
-	- <parameter></parameter>					
	{media}	2.4g	Enable or disable the wlan of the 802.11g.			
		5g	Enable or disable the wlan of the 802.11a.			
	(num)	Set the threshold for the frame size of frame transmission to perform fragmentatio				
	(256~2346)					
-	<default configuration=""></default>					
	2.4g: 2346					
	5g: 2346					
_	<command n<="" th=""/> <th>node></th> <th></th>	node>				
	Immediate M		Mode			
-	<compatible< th=""><th></th><th></th></compatible<>					
	CAP1300					
-	<examples></examples>					
	# wlan 5g frag	-				
	# wlan 2.4g fr	agmentth	reshold 2344			
Set	<i>wlan {2.4g 5g} keepalive</i> Set the keepalive interval terminal.					
	he syntax of th					
WI	an {media} kee	epalive (ni	um)			
-	<parameter></parameter>					
	{media}	2.4g	Set the keepalive interval function of 802.11g terminal.			
	(5g	Set the keepalive interval function of 802.11a terminal.			
	(num)	-				
-	 (num) Set the interval between sending keepalive. (0~65535 seconds) <default configuration=""></default> 60 					
-	- <command mode=""/>					
	Immediate Mode, Edit Mode					
-	- <compatible products=""></compatible>					
_	CAP1300 - <examples></examples>					
	# wlan 5g kee	palive 120)			
			·			
wl	an {2.4g 5g}	gi				
Set the guard interval.						
	he syntax of th		nd>			
	an (madia) ai l					

wlan {media} gi {mode}

<Parameter> _

{media}	2.4g	Set the guard interval of 802.11g.
	5g	Set the guard interval of 802.11a.

{mode}	short	Set the guard interval to short.
· · ·		0

Set the guard interval to long.

- <Default configuration> short
- <Command mode>
 Immediate Mode, Edit Mode

long

- <Compatible Products> CAP1300
- <Examples>
 # wlan 2.4g gi long

wlan {2.4g | 5g} mrate

Configure the multicast or broadcast rate. <The syntax of the command>

wlan {media} mrate {rate}

<paramete< th=""><th>r></th><th></th></paramete<>	r>	
{media}	2.4g	Set the multicast / broadcast rate of 802.11g
	5g	Set the multicast / broadcast rate of 802.11a
{rate}	Set one	e of the following rates.
(1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, auto)		
<default co<="" td=""><td>onfiguratio</td><td>on></td></default>	onfiguratio	on>
auto		
<command mode=""/>		
Immediate	Mode, Ed	it Mode

- <Compatible Products> CAP1300
- <Examples>
 # wlan 5g mrate auto

wlan {2.4g | 5g} rtsthreshold

Set the RTS Threshold. <The syntax of the command> wlan {media} rtsthreshold (num)

- <Parameter>

{media}2.4gSet the RTS threshold of 802.11g

Set the RTS threshold of 802.11a

(num) Set the threshold on the frame size you begin sending RTS / CTS. (1~2347)

- <Default configuration>

5g

- 2347
- <Command mode> Immediate Mode, Edit Mode
- <Compatible Products> CAP1300

 <Examples> # wlan 5g rtsthreshold 1800

wlan {2.4g | 5g} ssid addsecurity

Configure additional authentication SSID.

<The syntax of the command>

<No additional authentication>

wlan {media} ssid addsecurity { ssidname (ssid) | ssidnum (ssidnum) } mode none

<Limited by the MAC address list>

wlan {media} ssid addsecurity { ssidname (ssid) | ssidnum (ssidnum) } mode macfilter

<MAC-RADIUS authentication>

wlan {media} ssid addsecurity { ssidname (ssid) | ssidnum (ssidnum) } mode macradius
{ authmac | authpass (authpass) }

<MAC address list + MAC-RADIUS authentication>

wlan {media} ssid addsecurity { ssidname (ssid) | ssidnum (ssidnum) } mode macradius+macfilter { authmac | authpass (authpass) }

<Parameter>

{media}	2.4g	Set the addsecurity of the SSID on 802.11g.	
	5g	Set the addsecurity of the SSID on 802.11a.	
(ssid)	Specify tl	he SSID to be set.	
(ssidnum)	Specify tl	he number of the SSID to be set.	
authmac	The MAC	address as the password authentication MAC RADIUS.	
authpass	Set the p	assword in the password authentication MAC RADIUS.	
(authpass)	Enter a s	hared secret.	
<default con<="" th=""><th colspan="3">ifiguration></th></default>	ifiguration>		
NA			
<command n<="" th=""/> <th colspan="3">mode></th>	mode>		
Immediate M	Immediate Mode, Edit Mode		
<compatible products=""></compatible>			
CAP1300			
<examples></examples>			
# wlan 5g ssid addsecurity ssidname edimax5g01-168801 mode none			
# wlan 2.4g ssid addsecurity ssidnum 1 mode macfilter			
# wlan 5g ssio	# wlan 5g ssid addsecurity ssidname edimax5g01-168801 mode macradius authmac		
# wlan 2.4g s	an 2.4g ssid addsecurity ssidnum 2 mode macradius+macfilter authpass 12345678		

wlan {2.4g | 5g} ssid create

Create the number of the SSID. <The syntax of the command> wlan {media} ssid create (num)

- <Parameter>
 {media}
 2.4g
 Create the multi-SSID on 802.11g.

5g Create the multi-SSID on 802.11a.

(num) Create the number of the SSID.(1~5)

- <Default configuration>
 5g ssid number: 1
 2.4g ssid number: 1
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples> # wlan 2.4g ssid create 5

wlan {2.4g | 5g} ssid {disable | enable}

Enable or disable the SSID.

<The syntax of the command>

wlan {media} ssid {disable | enable} { ssidname (ssid) | ssidnum (ssidnum)}

- <Parameter>
 {media}
 2.4g
 To enable or disable the SSID on 802.11g.
 5g
 To enable or disable the SSID on 802.11a.
 (ssid)
 Specify the SSID to be set.
 (ssidnum)
 Specify the number of the SSID to be set.
- <Default configuration>
 Enable
- <Command mode>
 Immediate Mode, Edit Mode
 Commatible Products
- <Compatible Products> CAP1300
- <Examples>
 # wlan 2.4g ssid disable ssidnum 2
 # wlan 5g ssid enable ssidname edimax5g01-168801

wlan {2.4g | 5g} ssid loadbalance

Set the loadbalance of the SSID. <The syntax of the command> wlan {media} ssid loadbalance { ssidname (ssid) | ssidnum (ssidnum)} limit (num)

- <Parameter>
 - {media}2.4gSet the loadbalance of the SSID on 802.11g.5gSet the loadbalance of the SSID on 802.11a.(ssid)Specify t⊢ SSID to be set.(ssidnum)Specify t⊢ number of the SSID to be set.(num)Set the number of the loadbalance<Default configuration>
 - 50

- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # wlan 2.4g ssid loadbalance ssidnum 2 limit 20
 # wlan 5g ssid loadbalance ssidname edimax5g01-168801 limit 30

wlan {2.4g | 5g} ssid privacy

Set the privacy separator feature.

<The syntax of the command>

wlan {media} ssid privacy { ssidname (ssid) | ssidnum (ssidnum) } { station | ssid | disable }

- <parameter></parameter>

{media}	2.4g	Set the privacy separator feature on 802.11g.	
	5g	Set the privacy separator feature on 802.11a.	
(ssid)	Specify th	ne SSID to be set.	
(ssidnum)	Specify th	ne number of the SSID to be set.	
station	To prohib	it communication between all wireless cordless handset in the device.	
	(Between devices)		
ssid	Prohibit communication between different networks SSID.		
disable	Do not us	se the privacy separator feature.	
<default cont<="" th=""><th colspan="3">It configuration></th></default>	It configuration>		
Disable	able		
<command mode=""/>			
Immediate Mode, Edit Mode			
<compatible products=""></compatible>			
CAP1300			
<examples></examples>			
# wlan 2.4g ssid privacy ssidname edimax2g01-168800 station			
# wlan 5g ssid privacy ssidnum 2 ssid			

wlan {2.4g | 5g} ssid rename

Change the name of the SSID. <The syntax of the command>

wight (modia) said ronama	(ccidnama (ccid) ccidnum (ccidnum)) (nouvecid)
widh filleuid? Ssiù rendille	{ssidname (ssid) ssidnum (ssidnum)} (newssid)

- <Parameter>

{media}	2.4g	Change the name of the SSID on 802.11g.
	5g	Change the name of the SSID on 802.11a.
(ssid)	Specify the SSID to be changed.	
(ssidnum)	Specify the number of the SSID to change.	
(newssid)	Specify the SSID to set a new.	

wlan 2.4g ssid rename ssidname CAP1300-D6D5A0_G air_station_2.4g_2
wlan 5g ssid rename ssidnum 2 air_station_5g_2

wlan {2.4g | 5g} ssid security

<Default configuration>

Immediate Mode, Edit Mode <Compatible Products>

<Command mode>

_

Set the security of the SSID.

<The syntax of the command>

<No authenticate>

CAP1300

wlan {media} ssid security {ssidname (ssid) | ssidnum (ssidnum)} mode no_auth

<WEP authentication>

wlan {media} ssid security {ssidname (ssid) | ssidnum (ssidnum)} mode wep length { 64 | 128 } keytype {ascii | hex} defaultkey (num_1-4) key (wepkey)

<EAP authentication>

wlan {media} ssid security {ssidname (ssid) | ssidnum (ssidnum)} mode eap length { 64 | 128 }

<WPA-PSK authentication>

wlan {media} ssid security {ssidname (ssid) | ssidnum (ssidnum)} mode

{ wpapsk|wpa2psk|wpa2mixedpsk } type {cipher} period (num) keytype {passpharse | hex} key (psk)

<WPA-EAP EAP authentication>

wlan {media} ssid security {ssidname (ssid) | ssidnum (ssidnum)} mode

{ wpaeap | wpa2eap | wpa2mixedeap } type {cipher} period (num)

- <Parameter>

{media}	2.4g	Set the security of the SSID on 802.11g.		
	5g	Set the security of the SSID on 802.11a.		
(ssid)	Specify t	he SSID to be set.		
(ssidnum)	Specify t	he number of the SSID to be set.		
(num_1-4)	Specify t	he encryption key number to be default key.(1~4)		
(wepkey)	Enter the	he WEP encryption key.		
	ascii	(key length of 64-bit for ascii are 5 characters)		
		(key length of 128-bit for ascii are 13 characters)		
	hex	(key length of 64-bit for hex are 10 characters)		
		(key length of 128-bit for hex are 26 characters)		
{cipher}	Specify one of the following encryption method.			
	aes	When security mode choose wpaeap/wpa2eap/wpamixedwap or		
		wpapsk/pa2psk/wpamixedpsk, specify the AES encryption method.		

		tkip	When security mode choose wpaeap or wpapsk, specify the TKIP encryption	
			method.	
		mixed	When security mode choose wpaeap/ wpamixedeap or	
			wpapsk/wpamixedpsk, specify the TKIP and AES encryption method.	
	(num)	Specify th	ne period to key renewal. (0~9999 minutes)	
	(psk)	Enter the	pre-shared key.	
		passphra	se (Enter 8 characters)	
		hex (Ente	er 64 characters)	
•	<default conf<="" th=""><th>figuration</th><th>></th></default>	figuration	>	
	No authentica	ate		
-	<command mode=""/>			
	Immediate Mode, Edit Mode			
-	<compatible products=""></compatible>			
	CAP1300			
•	<examples></examples>			
	# wlan 2.4g ssid security ssidname CAP1300-D6D5A0_G mode wep length 64 keytype ascii			
	defaultkey 2 key 12345			
	# wlan 5g ssid security ssidname CAP1300-D6D5A0_G mode no_auth			
	# wlan 5g ssid security ssidnum 1 mode wpa2psk type aes period 60 keytype passphrase key			
	12345678			
	# wlan 2.4g ss	sid security	y ssidnum 2 mode wpaeap type mixed period 100	

wlan {2.4g | 5g} ssid vlan

Set the VLAN ID. <The syntax of the command> wlan {media} ssid vlan {ssidname (ssid) | ssidnum (ssidnum)} vlanid (vlanid)

- <Parameter>

_

{media}	2.4g	Set the VLAN ID on 802.11g.
	5g	Set the VLAN ID on 802.11a.
(ssid)	Specify the SSID to be set.	
(ssidnum)	Specify the number of the SSID to be set.	
(vlanid)	Set the VLAN ID. (1~4094)	

- <Default configuration>

1

- **<Command mode>** Immediate Mode, Edit Mode

 - <Compatible Products> CAP1300

<Examples> # wlan 2.4g ssid vlan ssidname edimax2g03-168800 vlanid 4000 # wlan 5g ssid vlan ssidnum 2 vlanid 2000

wlan {2.4g | 5g} txpower

Configure the wireless transmit power.

<The syntax of the command>

wlan {media} txpower {power}

_	<parameter></parameter>			
	{media}	2.4g	Set the 802.11g radio transmit power.	
		5g	Set the 802.11a radio transmit power.	
	{power}	In the range of 10-100%, and set the transmission power in 10%, 25%, 50%, 75%, 90%,		
		100%.		
		(10, 25, 5	50, 75, 90, 100)	
-	<default cont<="" th=""><th>figuration</th><th>></th></default>	figuration	>	
	100			
-	<command mode=""/>			
	Immediate M	ode, Edit	Mode	
-	- <compatible products=""></compatible>			
	CAP1300			
-	- <examples></examples>			
	# wlan 2.4g t>	power 50		

wlan {2.4g | 5g} wds delete

Remove the connection destination of the WDS.

<The syntax of the command>

wlan {media} wds delete all

wlan {media} wds delete num (peernum)

5g

wlan {media} wds delete address (peeraddress)

- <parameter></parameter>

{media} 2.4g Delete a destination on 802.11g WDS.

Delete a destination on 802.11a WDS.

(peernum) Specify the peer number of the MAC address to be deleted.

(peeraddress) Specify the MAC address to be deleted from the peer.

- <Default configuration>
- NA
- <Default configuration> 100
- <Command mode> Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples> wlan 5g wds delete all wlan 2.4g wds delete address 12:22:33:44:55:66 wlan 5g wds delete num 1

<The syntax of the command>

wlan {media} wds mode {mode)}

<Parameter>

Set the WDS function on 802.11g. {media} 2.4g Set the WDS function on 802.11a. 5g {mode} disable Disable the WDS dedicated_wds Set the WDS with WDS. wds_with_ap Set the WDS with AP. <Default configuration> disable <Command mode> Immediate Mode, Edit Mode <Compatible Products> CAP1300 <Examples> # wlan 5g wds mode disable

wlan 2.4g wds mode wds_with_ap

wlan {2.4g | 5g} wds num

Add a connection destination of the WDS.

<The syntax of the command>

wlan {media} wds num (1-4) add (peeraddress) vlan_mode untagged vlan (vlanid) {none|aes} key (psk) wlan {media} wds num (1-4) add (peeraddress) vlan_mode tagged {none|aes} key (psk)

- <Parameter>

{media}	2.4g	Add a destination on 802.11g WDS.	
	5g	Add a destination on 802.11a WDS.	
(vlanid)	Set the \	/LAN ID. (1~4094)	
(peeraddress) Set the MAC address of the destination.			
(psk)	encrypti	on key of WDS.	

- <Default configuration>
 NA
- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- **<Examples>** # wlan 5g wds num 1 add 22:22:33:

wlan 5g wds num 1 add 22:22:33:44:55:66 vlan_mode untagged vlan 1 none # wlan 2.4g wds num 2 add 12:22:33:44:55:66 vlan_mode tagged aes key 12345678

wlan 2.4g band

Set the operating mode of the radio and BasicRateSet on 802.11g, and configure the wireless channel. <The syntax of the command>

wlan 2.4g band 11b brs { 2m | all } channel {ch} bandwidth 20m
wlan 2.4g band 11b brs { 2m | all } channel {auto-ch} bandwidth 20m
wlan 2.4g band { 11g | 11b11g} brs {brs} channel {ch} bandwidth 20m
wlan 2.4g band { 11g | 11b11g} brs {brs} channel {auto-ch} bandwidth 20m
wlan 2.4g band { 11g | 11b11g} brs {brs} channel {auto-ch} bandwidth 20m
wlan 2.4g band { 11g11n|11b11g11n} brs {brs} channel {ch} bandwidth {width}
wlan 2.4g band { 11g11n|11b11g11n} brs {brs} channel {auto-ch} bandwidth {width}

<parameter></parameter>					
{brs}	Select from the following basic rate set				
	2m	Set to 1/2	Mbps		
	11m	Set to 1/2	Set to 1/2/5.5/11 Mbps		
	24m	Set to 1/2	Set to 1/2/5.5/6/11/12/24Mbps		
	All	Set all rate	e supported by current band		
{ch}	Set the w	vireless chai	nnel of 802.11g		
	Available	channel nu	ımber: 1-13		
{autoch}	Set the w	vireless auto	o channel of 802.11g		
	Available	/ailable channel number: auto_1-11ch, auto_1-13ch			
{width}	Set the wireless bandwidth of 802.11g				
	20m		Set to 20MHz normal mode		
	40m+ex_	_upper_ch	Set to 40MHz normal mode plus extra upper channel		
			Available values: 1-9		
	40m+ex_	lower_ch	Set to 40MHz normal mode plus extra lower channel		
			Available values: 5-13		
	auto+ex_	_upper_ch	Set to auto mode plus extra upper channel		
			Available values: 1-9		
	auto+ex_	_lower_ch	Set to auto mode plus extra lower channel		
			Available values: 5-13		
{autowidth}					
	20m	Set to 20N	/Hz normal mode		
	40m Set to 40MHz normal mode				

auto Set to auto mode

- <Default configuration>

Mode: 11b11g11n BasicRateSet: 11m Channel: auto_1-11ch Bandwidth: 20m

- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # wlan 2.4g band 11b brs 2m channel 6 bandwidth 20m

wlan 2.4g band 11b11g brs 24m channel 13 bandwidth 20m
wlan 2.4g band 11b11g brs 11m channel auto_1-11ch bandwidth 20m
wlan 2.4g band 11b11g11n brs all channel 10 bandwidth 40m+ex_lower_ch

wlan 2.4g conslot

Set the contention slot of 802.11g. <The syntax of the command> wlan 2.4g conslot {mode}

-	<parameter></parameter>		
	{mode}	short	Set the contention slot to short.
		long	Set the contention slot to long.

- <Default configuration> short
- <Command mode> Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # wlan 2.4g conslot long

wlan 2.4g preamble

Set the preamble of 802.11g <The syntax of the command> wlan 2.4g preamble {mode}

	(Deve ve et ev)		
-	<parameter:< th=""><th>></th><th></th></parameter:<>	>	
	{mode}	short	Set the preamble to short.
		long	Set the preamble to long.

- <Default configuration> short
- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples> # wlan 2.4g preamble long

wlan 5g band

Set the operating mode of the radio and BasicRateSet on 802.11a, and configure the wireless channel. <The syntax of the command>

wlan 5g band 11a brs {brs} channel {ch} bandwidth 20m wlan 5g band 11a brs {brs} channel {auto-ch} bandwidth 20m wlan 5g band { 11a11n | 11a11n11ac } brs {brs} channel {ch} bandwidth {width} wlan 5g band { 11a11n | 11a11n11ac } brs {brs} channel {auto-ch} bandwidth

{autowidth}

 <parameter> <pre>{brs}</pre> Select from the following basic rate set 24m Set to 6/12/24 Mbps All Set all rate supported by current band {ch} Set the wireless channel of 802.11a Available channel number: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 12 124, 128, 132, 136, 140 {autoch} Set the wireless auto channel of 802.11a Available channel number: w52, w52+w53, w52+w53+w56 {width} Set the wireless bandwidth of 802.11a 20m Set to 20MHz normal mode</parameter> 			
24mSet to 6/12/24 MbpsAllSet all rate supported by current band{ch}Set the wireless channel of 802.11aAvailable channel number: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 12124, 128, 132, 136, 140{autoch}Set the wireless auto channel of 802.11aAvailable channel number: w52, w52+w53, w52+w53+w56{width}Set the wireless bandwidth of 802.11a			
AllSet all rate supported by current band{ch}Set the wireless channel of 802.11a Available channel number: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 12 124, 128, 132, 136, 140{autoch}Set the wireless auto channel of 802.11a Available channel number: w52, w52+w53, w52+w53+w56 Set the wireless bandwidth of 802.11a			
{ch} Set the wireless channel of 802.11a Available channel number: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 12 124, 128, 132, 136, 140 {autoch} Set the wireless auto channel of 802.11a Available channel number: w52, w52+w53, w52+w53+w56 {width} Set the wireless bandwidth of 802.11a			
Available channel number: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 12 124, 128, 132, 136, 140 {autoch} Set the wireless auto channel of 802.11a Available channel number: w52, w52+w53, w52+w53+w56 {width} Set the wireless bandwidth of 802.11a			
124, 128, 132, 136, 140 {autoch} Set the wireless auto channel of 802.11a Available channel number: w52, w52+w53, w52+w53+w56 {width} Set the wireless bandwidth of 802.11a			
 {autoch} Set the wireless auto channel of 802.11a Available channel number: w52, w52+w53, w52+w53+w56 {width} Set the wireless bandwidth of 802.11a 	20,		
Available channel number: w52, w52+w53, w52+w53+w56{width}Set the wireless bandwidth of 802.11a			
{width} Set the wireless bandwidth of 802.11a			
20m Sat to 20MHz normal made			
2011 Set to 2001/12 normal mode			
40m+ex_upper_ch Set to 40MHz normal mode plus extra upper channel			
Available values: 36, 44, 52, 60, 100, 108, 116, 124, 132			
40m+ex_lower_ch Set to 40MHz normal mode plus extra lower channel			
Available values: 40, 48, 56, 64, 104, 112, 120, 128, 136			
80m Set to 80/40/20 MHz normal mode			
{autowidth} Set the wireless auto bandwidth of 802.11a			
20m Set to 20MHz normal mode			
40m Set to 40/20MHz normal mode			
80m Set to 80/40/20MHz normal mode			
- <default configuration=""></default>			
Mode: 5g11n			
BasicRateSet: 24m			
Channel: w52(auto)			
Bandwidth: 40m	40m		
- <command mode=""/>			
Immediate Mode, Edit Mode			
<compatible products=""> CAP1300</compatible>			
- <examples></examples>			
# wlan 5g band 11a brs all channel 40 bandwidth 20m			
# wlan 5g band 11a brs all channel w52+w53 bandwidth 20m			
# wlan 5g band 11a11n brs 24m channel 36 bandwidth 40m+ex_upper_ch			
# wlan 5g band 11a11n brs 24m channel 140 bandwidth 20m			
# wlan 5g band 11a11n brs 24m channel w52+w53+w56 bandwidth 40m			
# wlan 5g band 11a11n11ac brs 24m channel 44 bandwidth 80m			

wlan maclist add

Add the registration of MAC address restriction list. <The syntax of the command>

wlan maclist add (macaddress)

- <Parameter>

(macaddress) Enter the MAC address to be registered in the list.

- <Default configuration>
 - NA
- <Command mode> Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # wlan maclist add 12:22:33:44:55:66

wlan maclist delete

Remove the registration of MAC address restriction list. <The syntax of the command>

wlan maclist delete { all | address (macaddress) | num (list-number) } [force]

<Parameter>

(macaddress) Specify the MAC address to be deleted from the list.

(list-number) Specify the list number of the MAC address to be deleted.

- <Default configuration>
 NA
- <Command mode> Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # wlan maclist delete all force
 # wlan maclist delete address 12:22:33:44:55:66 force
 # wlan maclist delete num 1 force

wlan maclist show status

Show the registration of MAC address restriction list. <The syntax of the command>

wlan maclist show status

- <Parameter>
 - NA
- <Default configuration>
 NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # wlan maclist show status

wlan wmm {ap | sta}

Set the WMM parameters.

<The syntax of the command>

wlan wmm {ap | sta} {parameter} bk (value) be (value) vi (value) vo (value)

- <Parameter>

(parameter) aifsn, cwmax, cwmain, txop

(value) Set the parameter values. (according to the rules set input 1 < cwmin < 32767, 1 <

cwmax <32767, 1 < aifsn < 15, 0 < txop <65535)

- <Default configuration>

	CWMin	CWMax	AIFSN	ТхОР
Back Ground	4	10	7	0
Best Effort	4	6	3	0
Video	3	4	1	94
Voice	2	3	1	47
		STA		
	CWMin	CWMax	AIFSN	ТхОР
Back Ground	15	1023	7	0
Best Effort	15	1023	3	0
Video	7	15	2	94
Voice	3	7	2	47

 - <Command mode> Immediate Mode, Edit Mode

- <Compatible Products> CAP1300

<Examples>

wlan wmm ap aifsn bk 10 be 10 vi 10 vo 10 # wlan wmm sta txop bk 65535 be 65535 vi 65535 vo 65535

wlan wmm show status

Show the QoS configuration information. <The syntax of the command> wlan wmm show status

- **<Parameter>** NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # wlan wmm show status

wlan wmm qos

Enable or disable the wmm qos. <The syntax of the command>

wlan wmm qos {disable | enable}

- <Parameter>
 NA
- <Default configuration> disable
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples> # wlan wmm qos enable

wlan wps create pincode

Generate the WPS PIN code.

<The syntax of the command>

wlan wps create pincode

- **<Parameter>** NA
- <Default configuration> NA
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples> # wlan wps create pincode

wlan wps {disable | enable}

Enable or disable the WPS. <The syntax of the command>

wlan wps {state}

-	<parameter></parameter>	•	
	{state}	disable	Disable WPS.
		enable	Enable WPS.
-	<default con<="" th=""><th>figuration</th><th>></th></default>	figuration	>
	enable		
-	<command r<="" th=""/> <th>node></th> <th></th>	node>	
	Immediate N	1ode <i>,</i> Edit I	Vode
-	<compatible< th=""><th>Products></th><th>•</th></compatible<>	Products>	•
	CAP1300		
-	<examples></examples>		
	# wlan wps d	isable	

wlan wps release Release the WPS. <The syntax of the command>

wlan wps release

- <Parameter>
 NA
- <Default configuration> NA
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples> # wlan wps release

wlan wps show status Show the status of wlan security WPS. <The syntax of the command>

wlan wps show status

- <Parameter>
 NA
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # wlan wps show status

wlan wps start enrollee pincode

Enter the PIN code to start WPS. <The syntax of the command> wlan wps start encrollee pincode (pincode)

- <Parameter>
 - (pincode) Enter the pincode (0~99999999).
- <Default configuration>
 NA
- **<Command mode>** Immediate Mode
- <Compatible Products> CAP1300
- <Examples># wlan wps start enrollee pincode 14766084

wlan wps start push_button Start the WPS by push the button. <The syntax of the command>

wlan wps start push_button

- **<Parameter>** NA
- <Default configuration> NA
- **<Command mode>** Immediate Mode
- <Compatible Products> CAP1300
- <Examples># wlan wps start push_button

XI-2-5 Radius

radius {2.4g | 5g} {primary | secondary} enable server

Configure the enable built-in RADIUS server.

<The syntax of the command>

radius <media> {primary | secondary} enable server (host) secret (secret) authport (port)

<parameter></parameter>				
<media></media>	2.4g Set the radius server of 802.11g.			
	5g	Set the radius server of 802.11a.		
(host)	Specifies	s the IP address or domain name of the host.		
(secret)	Set the SharedSecret.			
(port)	Set the L	JDP port of the server used in RADIUS authentication protocol. (1~65535)		
<default conf<br="">primary port: secondary po <command n<br=""/>Immediate M <compatible CAP1300 <examples> # radius 2 4g</examples></compatible </default>	1812 rt: 1812 node> ode, Edit Products	Mode		

radius {2.4g | 5g} {primary | secondary} session_time

Set the RADIUS time to server communication will allow wireless devices.

<The syntax of the command>

radius <media> [primary | secondary] session_time (num)

<Parameter>

(num)

<media> 2.4g Set the radius server of 802.11g.

5g Set the radius server of 802.11a.

Set the time of the session-time (0~86400 sec)

- <Default configuration> primary session-timeout: 3600 secondary session-timeout: 3600
- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products>
 CAP1300
- <Examples> # radius 5g secondary session_time 4800

radius {2.4g | 5g} {primary | secondary} accounting

Enable or disable the RADIUS Accounting. <The syntax of the command> radius <media> {primary | secondary} accounting (state)

<Parameter>

<media></media>	2.4g	Set the radius server of 802.11g.
	5g	Set the radius server of 802.11a.
(state) enable		Enable the RADIUS Accounting.
	disable	Disable the RADIUS Accounting.

- <Default configuration> enable
- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # radius 5g secondary accounting disable
 # radius 5g primary accounting disable

radius {2.4g | 5g} {primary | secondary} accounting_port

Set the UDP port of the server used in RADIUS Accounting protocol.
<the command="" of="" syntax="" the=""></the>
radius <media> {primary secondary} accounting_port (port)</media>
< Revenue to r >

<Parameter>
 <media>
 2.4g Set the radius server of 802.11g.
 5g Set the radius server of 802.11a.
 (port)
 Set the UDP port.(0~65535)

 <Default configuration>

primary: 1813

secondary: 1813

- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # radius 5g secondary accounting_port 1814
 # radius 2.4g primary accounting_port 1815

radius {2.4g | 5g} {primary | secondary} accounting_interval

Set the Accounting interval.

<The syntax of the command>

- <Parameter>

<media></media>	2.4g	Set the radius server of 802.11g.
	5g	Set the radius server of 802.11a.
(interval)	Set the	accounting interval (60 ~ 86400)

- <Default configuration>
- <Command mode>
 Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # radius 5g secondary accounting_interval 60

radius 2.4g primary accounting_interval 86400

radius {2.4g | 5g} {primary | secondary} type [internal | external]

Set the radius type. <The syntax of the command> radius <media> {primary | secondary} type [internal|external]

- <Parameter>
 <media> 2.4g Set the radius server of 802.11g.
 5g Set the radius server of 802.11a.
- <Default configuration>
- **<Command mode>** Immediate Mode, Edit Mode
- <Compatible Products> CAP1300
- <Examples>
 # radius 5g primary type external
 # radius 2.4g primary type internal

radius admin add

Add the radius user accounts. <The syntax of the command>

radius admin add (username) (password)

- <Parameter>
 - (username) username of the radius account
 - (password) password of the radius account
- <Default configuration> NA
- **<Command mode>** Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # radius admin add edimax 1234

radius admin delete

delete the radius user accounts. <The syntax of the command>

radius admin delete all radius admin delete num (list_number)

<Parameter>

(list_number) number of the username list

- <Default configuration>
 NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples>
 # radius admin delete all
 # radius admin delete num 2

radius internal {disable | enable}

enable or disable the internal radius. <The syntax of the command>

radius internal enable

- <Parameter>
 NA
- <Default configuration>
 Disable
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode

- <Compatible Products> CAP1300
- <Examples>
 # radius internal disable
 # radius internal enable

radius internal session_timeout

Set the internal RADIUS time to server communication will allow wireless devices. <The syntax of the command>

radius internal session_timeout (sec)

- <Parameter>
 - (sec) Set the time of the session-timeout (**0~86400 sec**)
- <Default configuration> NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples>
 # radius internal session_timeout 86400

radius internal shared_key

Set the shared key of internal RADIUS server. <The syntax of the command> radius internal shared_key (key)

- <Parameter>
 (key)
 Set the shared key
- <Default configuration>
 NA
- <Command mode>
 Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # radius internal shared_key 1234

radius internal termination_action [not_reauth | not_send | reauth]

Set the termination action to internal RADIUS server.

<The syntax of the command>

radius internal termination_action [not_reauth | not_send | reauth]

- **<Parameter>** NA
- <Default configuration>
 Not-Reauthenication

- **<Command mode>** Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # radius internal termination_action not_reauth

radius show status

Show the radius information. <The syntax of the command> radius show status

- <Parameter>

NA

- <Default configuration> NA
- **<Command mode>** Immediate Mode, Edit Mode, Reference Mode
- <Compatible Products> CAP1300
- <Examples> # radius show status

XI-2-6 Exit

exit

Quit the CLI. <The syntax of the command>

exit

- **<Parameter>** NA
- <Default configuration> NA
- **<Command mode>** Immediate Mode
- <Compatible Products> CAP1300
- <Examples> # exit

XI-2-7 Quit

quit
Quit the CLI.
<the command="" of="" syntax="" the=""></the>
quit
- <parameter></parameter>
NA
 - <default configuration=""></default>
NA
- <command mode=""/>
Immediate Mode
- <compatible products=""></compatible>
CAP1300
- <examples></examples>
quit

XI-2-8 Command

Command Upload the cli command from tftp server <The syntax of the command> Command tftp_server (tftp-server) file (filename)

<Parameter>

 (tftp-server) Update the Command from the TFTP server.
 (file server) Catalate server of the Command file

(filename) Set the name of the Command file.

- <Default configuration> NA
- **<Command mode>** Immediate Mode
- <Compatible Products> CAP1300
- <Examples> # Command tftp_server 192.168.2.100 file command.ext

XI-3 Setting AP via ManageEngine MibBrowser with SNMPv3 - Example

XI-3-1 Setting in Web

- 1. The length of the password needs to be equal or greater than 8.
- 2. SNMP Version: V3

ALC: NOT THE OWNER OF THE OWNER OWNER OF THE OWNER OF THE OWNER OF THE OWNER OF THE OWNER OF THE OWNER OF THE OWNER OF THE OWNER	Information Network Settings	Wireless Settin	gs Management A	dvanced Operation Mode
Management	Admin			
> Admin				
> Date and Time	Account to Manage This Dev	vice		
> Syslog Server	Administrator Name	admin		
				(1-32Characters)
Ping Test	Administrator Password			(Confirm)
I'm Here	Apply			
	.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
	Advanced Settings			
	Advanted Strings			
	Product Name	AP74DA3	803B620	
	HTTP Port	80	(80, 1024-65535)	
	HTTPS Port	443		
	Management Protocol	 ✓ HTTP ✓ HTTPS ✓ TELNET ✓ SSH ✓ SNMP 		
	Login Timeout	30 ▼ (min	s <u>)</u>	
	SNMP Version	v3 v]	
	SNMP Get Community	public		
	SNMP Set Community	private		
	SNMP V3 Name	admin		
	SNMP V3 Password	•••••		
	SNMP Trap	Disabled	▼	
	SNMP Trap Community	public		
	SNMP Trap Manager			
	SNMP V3 Name SNMP V3 Password SNMP Trap SNMP Trap Community	admin •••••• Disabled	▼	

XI-3-2 Setting Rule

If you want to set Basic Wireless Setting via SNMP, the related variables need to be set together. Please refer to the file *Edimax-7476HPC_private_MIB_20150715_v1.1*, for setting Radio or SSID.

Example: Basic Wireless Settings	Settings
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.3.3 i 2	Auto Channel Disable
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.2.3 i 3	11b/g/n: band
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.4.3 i 7	7: channel
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.6.3 i 1	20M: Bandwidth
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.7.3 i 5	all: basic rate

STRING: -v3 -l noAuthNoPriv -u admin -a MD5 -x DES

Reference: Radio Related page of *Edimax-7476HPC_private_MIB_20150715_v1.1*

XI-3-3 Setting in ManageEngine MibBrowser

1. Set the version of SNMP

0	ManageEngine	MibBrows	er Free Tool			
File	Edit View Ope	erations H	leip			
20 L	Settings	Alt+S	🏂 🗊 📹 🕹	🔨 🖄 🛅 🐞 🛫 🐵 🧠 🔤 🖬 🖨 🧼 🚺 Dominad		
3 L	Find Node	Ctrl+F	Host	localhost	✓ Port	161
			Community	*****	Write Community	
			Set Value		•	
			Device Type			
			Device Type Ide	ntified Not Available (了 Reload	
			Suggested OID:	None		
			Object ID			
			Loading MIBs .\m Loading MIBs Fai	bs/RFC1213-MIB //mibs/F-MIB ed:		

Figure 1 Step 1:Edit → Settings

Jeneral N	lib Settings	Cemplate Settings			
SNMP Ve	rsion	2.			
	© v1		⊚ v2c		 Image: Image: Ima
General (Options			Get Bulk Optio	ons
Time Out	5		<u>+</u>	Han Danakii	50
Retries	0		*	Max. Repetitio	
Encoding	ISO885	9_1	•	Non Repeate	ers 0
Valid	ate Broadca	ST Address		V3 Options Context Name	
				Context ID	
Save)	/3 Settings t	o File o Database	Se St		Adding V3 entry ettings
Save S	/3 Settings t /3 Settings t	o Database		et EngineID For Database S	A REAL PROPERTY OF
Save Save	/3 Settings t /3 Settings t	o Database		et EngineID For Database S	ettings

Figure 2 Step 2: Check v3 and click Add

General 1	Mib Settings	Template Settings		
SNMP V	ersion			
	⊚ v1	(v2c	v3
General			Get Bulk	Options
Time Out				<u>г</u> 11
SnmpPara				
V3 Parameter	2		1	n
Target Host	192.168.2.2	1	Target Port	161
User Name	admin		Security Level	NoAuth,NoPriv
Auth Protocol	MD5	÷	Auth Password	
Priv Protocol	CBC-DES	÷	Priv Password	
Context Name	Ì		Engine ID	
		ОК	Cancel Ar	oply
User	Secur Au	th Priv Auth.	Priv Targe.	
	Add	M	lodify	Delete

Figure 3 Step 3: Enter AP's IP and Administrator Name (User Name)

Jeneral Mit	Settings	Template Settings]		
SNMP Vers					
(🗇 v1		⊚ v2c		v3
General Op	tions		1	Get Bulk Optio	ns
Time Out	5		*	Max. Repetitio	50
Retries	0	0			
Encoding	ISO88	59_1	•	Non Repeate	rs 0
Net Mask				Context Name	:8802224416317a2ff4e
V3 Settings	Settings	to File to Database	E Se	et EngineID For Database Se	Adding V3 entry
	Seungs				
Save V3	our Au	h Priv A1 A NO_P		Targe Ta 192.16161	
Save V3 User See admin No.	our Au	and the second second second second second second second second second second second second second second second		and the second second	

Figure 4 Step 4: Click OK

2. Load MIB Module

r Free Tool	
lp	
a 🔚 🗊 🔊	📉 🖄 📰 🛛 🛎 🛫 🐵 👒 🔚 🖛 🎒 🧇 🚺
Host	192.168.2.2
Community	•••••
Set Value	
Device Type	
Device Type Iden	ntified Not Available
100 million (100 m	
ouggested oibs	None -
Object ID	
	Host Community Set Value Device Type Device Type Ider Suggested OIDs

Figure 5 <u>Click Load MIB Module</u> and choose the file, *edimax_20150728.txt* (MIB file)

3. Add variables

ManageEngine MibBrowser Free Tool			
File Edit View Operations Help			The second s
🚴 🌲 🗊 🗛 🖣 🗞 🗞 🖓 👘 🎒 😭 🥂			
Configuration of the second seco	Community Step 2-2. Device Type Identified Bit Available Buggested ODs None Object ID iso rag dod internet prove relequient elisasc celsoCethagOrong saleOethagTable h	Port Vitte Community C Robust Step 2-1.	
Construction of the second secon	1.		
	Step 3-1.	2 Step 3-2.	Step 4.
L		(S)	IS-Var Add Edit Delete
lobal View 🛅			

Figure 6 Example of setting the variable

Step 1.: Select the OID.

Step 2-1.: Enter the index of Radio (2.4G).

Step 2-2.: Enter the Set Value.

Step 3-1.: Click MultiVar.

Step 3-2.: Check Multi-Var.

Step 4.: Add this Variable

4. Set SNMP variables

ManageEngine MibBrowser Free Tool				
e Edit View Operations Help				
	🖽 🍓 🖄	🚭 🧠 🖬 🛱 🧭 🚱 🚺 Move Free Doos		
Loaded MibModules	Host	192.168.2.2	- Port 161	
	Community		Write Community	
	Set Value 5	5		
dhcpEnableGroup	Device Type			
(e) macFilterGroup		ified Not Available	C Reload	
configurationGroup	Suggested OIDs	None		
DuzzerGroup	Object ID iso	o org.dod internet private enterprises edimax redioSettingsGroup redioSettingsTable basicRate.3		
💮 🛄 syslogGroup				
iii) rebootGroup iiii) rebootGroup iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii				
radioSettingsGroup				
adioSettingsTable				
band autoChannelEnable				
- autochannelEnable				
* autoChannelRange				
basicRate				
- the power				
- tsThreshold				
- The fragmentThreshold				
ssidNumber				
(i) clientinfoGroup				
ssidSettingsGroup snmpV2				
B Shinby2				
F	Description MultiVes	e		
		invete enterprises educate indicolettinger5 or up indicolettingerTable entoChannelEcable 3 : 2		
32	to org dod internet pr	rivate enterprises edimos: radioSettingsOutrup radioSettingsTable band 3 : 3		
	to org dod internet pr	rivate enterprises edimaas radioSettingsGooup radioSettingsTable runtimeChannel.3 : 7 rivate enterprises edimaas radioSettingsGroup radioSettingsTable bandwidth.3 : 1		
		revel emergence.ecumo: rencorrentgoric op menormage rece entry and 5 - 1 revele enterprises.ecumo: redioSettingsGroup redioSettingsTable basicRate 3 : 5		
				V Multi-Var Add Edit Delete

Figure 7 All the variables have been added. Click SET SNMP Variables

XII-1 How to Create and Link WLAN & Access Point Groups

NMS can be used to create individual SSIDs and group multiple SSIDs together into WLAN groups. You can then assign individual access points to use those WLAN group settings and/or group multiple access points together into access point groups, which you can also assign to use WLAN group settings.

Follow the example below to:

- **A.** Create a WLAN group.
- **B.** Create an access point group.
- **C.** Assign the access point group to use the SSID group settings.

XII-1-1 Create WLAN Group

1. Go to **NMS Settings** → **WLAN** and click **"Add"** in the **WLAN** panel:

Dashboard	Zone Plan N	MS Monitor NMS	Settings Loo	al Network	Local Settings	Toolbox	
> Access Point		_					
Access Forme	WLAN						
> WLAN	Search		(Match who	ole words		
> RADIUS		Name/ESSI	D	LAN ID	Authentication	Encryption	Additional Authentication
Access Control				Please	add WLAN setting		
> Guest Network	Add	Edit Clone De	lete Selected	Delete All			
> Users							
> Guest Portal	WLAN G	roups					
> Zone Edit	Search		(Match who	ble words		
> Schedule		Group Name	WLAN members	WLAN	member list	Used AP	Used AP Group
> Smart Roaming		group1	0				
> Device Monitoring	Add	Edit Clone De	lete Selected	Delete All]		
> Firmware Upgrade							
> Advanced							
System Security							

Enter an SSID name and set authentication/encryption and click "Save & Apply":

ame/ESSID	
escription	
LAN ID	1
roadcast SSID	Enable V
Vireless Client Isolation	Disable v
02.11k	Disable v
.oad Balancing	50 /50
Authentication Method	No Authentication ▼
Additional Authentication	No additional authentication
raffic Shaping Settings	By SSID ▼
/LAN Access Policy raffic Shaping Settings	
raffic Shaping Settings Traffic Shaping	
Traffic Shaping Settings Traffic Shaping Downlink	44 Mbps
raffic Shaping Settings Traffic Shaping	
Traffic Shaping Settings Traffic Shaping Downlink	44 Mbps
Traffic Shaping Settings Traffic Shaping Downlink Jplink	44 Mbps 44 Mbps
raffic Shaping Settings Traffic Shaping Downlink Jplink WLAN Advanced Settin	44 Mbps 44 Mbps
raffic Shaping Settings Fraffic Shaping Downlink Jplink WLAN Advanced Settin Smart Handover Settings	44 Mbps 44 Mbps gs
Traffic Shaping Settings Traffic Shaping Downlink Jplink WLAN Advanced Settin Smart Handover Settings Smart Handover	44 Mbps 44 Mbps gs Enable Disable
raffic Shaping Settings Fraffic Shaping Downlink Jplink WLAN Advanced Settin Smart Handover Settings	44 Mbps 44 Mbps gs
raffic Shaping Settings Fraffic Shaping Downlink Jplink WLAN Advanced Settin Smart Handover Settings Smart Handover	gs Enable ● Disable -80 ▼ dB
Traffic Shaping Settings Traffic Shaping Downlink Jplink WLAN Advanced Settin Smart Handover Settings Smart Handover RSSI Threshold	gs Enable ● Disable -80 ▼ dB

3. The new SSID will be displayed in the **WLAN** panel. **Repeat** to add additional SSIDs according to your preference.

WLAN						
Search		N	Match whole words			
	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication	
	WLAN 1	1	OPEN	NONE	No additional authentication	
	WLAN 2	1	OPEN	NONE	No additional authentication	
	WLAN 3	1	OPEN	NONE	No additional authentication	
	WLAN 4	1	OPEN	NONE	No additional authentication	
WLAN Groups						
WLAN Groups Search		O N	Match whole words			
	Group Name	WLAN members	Natch whole words	ember list	Used AP	Used AP Grou

4. Click "Add" in the WLAN Groups panel:

WLAN Gr Search	roups		Natch whole words			
	Group Name	WLAN members	WLAN member list	Used AP	Used AP Group	
	group1	0				
Add	Edit Clone Delete Selected	Delete All				

5. Enter a name for the SSID group and check the boxes to select which SSIDs to include in the group. Click "Save and Apply" when done.

WLAN Group	Settings				
Name					
Description					
	Search			Match whole words	
		Name/ESSID	١	/LAN ID	Schedule Group
Members		WLAN 1	Override	1	Override Disable •
		WLAN 2	Override	1	Override Disable •
		WLAN 3	Override	1	Override Disable •
		WLAN 4	Override	1	Override Disable •
Save Cance	Save & A	pply			

6. The new WLAN group will be displayed in the WLAN Group panel. Repeat to add additional WLAN groups according to your preference:

arch			Match whole words			
	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication	
	WLAN 1	1	OPEN	NONE	No additional authentication	
	WLAN 2	1	OPEN	NONE	No additional authentication	
	WLAN 3	1	OPEN	NONE	No additional authentication	
Add Ec		1 Delete All	OPEN	NONE	No additional authentication	
Add Ec	dit Clone Delete Selected	Delete All	OPEN Match whole words	NONE	No additional authentication	
dd Ec	dit Clone Delete Selected	Delete All	Natch whole words	NONE	No additional authentication	Used AP Group
dd Ec	dit Clone Delete Selected	Delete All	Natch whole words	ember list AN 1		Used AP Group

XII-1-2 Create Access Point Group

1. Go to NMS Settings → Access Point and click "Add" in the Access Point Group panel:

Access Point	Access Point										
WLAN	Search			Match	whole words						
RADIUS	🗌 Index 🔺	MAC Address 🔺	Device Name 🔺	Model 🔺	AP Group 🔺 2	.4G Channel 🔺 5	G Channel 🔺	2.4G Tx Power	sG Tx Po	wer 🔺 Status	Action
Access Control	1	74:DA:38:1F:46:40	AP74DA381F4640	CAP300 S	System Default	N/A	N/A	N/A	N/A	0	0
Guest Network	Refresh E	dit Delete Selecte	d Delete All								
Users											
Guest Portal	Access Point G	roup									
> Zone Edit	Search			Match	whole words						
Schedule		Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Netwo Profile		est Network R	ADIUS Profile	Access Contr	ol Profile
		System Default	1	Disabled	Disabled	Disabled	D	sabled	Disabled	Disable	d
Smart Roaming											
Smart Roaming Device Monitoring	Add Edit	Clone Delete S	elected Delete	e All							
• Device Monitoring	Add Edit		Delete	e All							
Device Monitoring Firmware Upgrade	Access Point Se	ettings		2 All							
		ettings	nable O Disable	≥ All							

2. Enter a Name and then scroll down to the Group Settings panel and use the << button to add selected access points into your group from the box on the right side. Click "Save & Apply" when done.

Basic Group Settings		_		
Name	Access Point Group 1			
Description	Please enter a new grou	up descriptio	n	
IGMP Snooping	Override Default Setting	Disable 1	7	
p Settings				
Abbers	Device Name V	G	earch roup Name : System Default MAC Address A 74:DA:38:1F:46:40	Device Name AP74DA381F4640

3. The new group will be displayed in the **Access Point Group** panel. **Repeat** to add additional access point groups according to your preference:

Search			Match v	vhole words				
	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
	System Default	0	60 Y 10 Y	10010010	A617278	200 C (200	10010010	- 200 T-2000
	Access Point Group 1	1	10010010	100120-001	- 60 YO R	200 T-010	10012010	- AND 1978

XII-1-3 Assign Access Point Group to use the SSID group settings

1. Go to NMS Settings → Access Point and select an access point group using the checkboxes in the Access Point Group panel. Click "Edit":

Search			Match v	vhole words				
	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
	System Default	0	10010010	10010010	200 Y 200 Y	200 C (200	100000	200 Y 200 Y
	Access Point Group 1	1	100120-001	10012010	A617678	200 T 2010	ALC: NO. 1	- AN 1993

2. Scroll down to the Profile Group Settings panel and check the "Override Group Settings" box for WLAN Group (2.4GHz and/or 5GHz). Select your WLAN group from the drop-down menu and click "Apply":

Profile Group Settings			
	Radio B/G/N (2.4 GHz)		Radio A/N/AC (5.0 GHz)
WLAN Group	Override Default Setting)isable 🔻	Override Default Setting WLAN Group 1 ▼
Guest Network Group	Uverride Detault Settind	Disable	Override Default Setting Disable V
		VLAN Group 1 proup1	
RADIUS Group	Override Default Setting	Noablo	
MAC Access Control Group	Override Default Setting	Disable 🔻	

3. Repeat for other access point groups according to your preference.



COPYRIGHT

Copyright © Edimax Technology Co., Ltd. all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission from Edimax Technology Co., Ltd.

Edimax Technology Co., Ltd. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability, or fitness for any particular purpose. Any software described in this manual is sold or licensed as is. Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Edimax Technology Co., Ltd. reserves the right to revise this publication and to make changes from time to time in the contents hereof without the obligation to notify any person of such revision or changes.

The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. The software and specifications are subject to change without notice. Please visit our website www.edimax.com for updates. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

AT	BE	BG	HR	CY	CZ	DK	
EE	FI	FR	DE	EL	HU	ΙE	
IT	LV	LT	LU	MT	NL	ΡL	
PT	RO	SK	SI	ES	SE	UK	UK(NI)

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1. Reorient or relocate the receiving antenna.
- 2. Increase the separation between the equipment and receiver.
- 3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4. Consult the dealer or an experienced radio technician for help.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate equipment.

This device complies with Part 15 of the FCC Rules. Operation si subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device is restricted to indoor use.

Federal Radiation Exposure Statement

- 1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- 2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body or nearby persons.

RED Compliance Statement

Compliance with 2014/53/EU Radio Equipment Directive (RED)

In accordance with Article 10.8(a) and 10.8(b) of the RED, the following table provides information on the frequency bands used and the maximum RF transmit power of the product for sale in the EU:

Frequency range (MHz)	Max. transmit power (dBm)
2400-2483.5	19.90 dBm
5150-5250	22.93 dBm
5250-5350	22.92 dBm
5470-5725	29.29 dBm

A simplified DoC shall be provided as follows: Article 10(9)

Hereby, Edimax Technology Co., Ltd. declares that the radio equipment type AC1300 DBDC Ceiling-mount AP is in compliance with Directive 2014/53/EU The full text of the EU declaration of conformity is available at the following internet

address: http://www.edimax.com/edimax/global/

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical

equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

EU Declaration of Conformity

English: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU, 2014/35/EU. Français: Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/53/EU, 2014/35/EU. Čeština: Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/53/EU, 2014/35/EU. Polski: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/53/EU, 2014/35/EU. Română: Acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE, 2014/35/UE. Это оборудование соответствует основным требованиям и положениям Директивы Русский: 2014/53/EU, 2014/35/EU. Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek Magyar: (2014/53/EU, 2014/35/EU). Türkçe: Bu cihaz 2014/53/EU, 2014/35/EU direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur. Українська: Обладнання відповідає вимогам і умовам директиви 2014/53/EU, 2014/35/EU. Slovenčina: Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/53/EU, 2014/35/EU. Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/53/EU, 2014/35/EU. Deutsch: El presente equipo cumple los requisitos esenciales de la Directiva 2014/53/EU, **Español:** 2014/35/EU. Italiano: Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/53/EU, 2014/35/UE. **Nederlands:** Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/53/EU, 2014/35/EU. Português: Este equipamento cumpre os requesitos essênciais da Directiva 2014/53/EU, 2014/35/EU. Norsk: Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/53/EU, 2014/35/EU. Svenska: Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/53/EU, 2014/35/EU. Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante Dansk: forordninger i direktiv 2014/53/EU, 2014/35/EU. suomen kieli: Tämä laite täyttää direktiivien 2014/53/EU, 2014/35/EU. oleelliset vaatimukset ja muut asiaankuuluvat määräykset.





WEEE Directive & Product Disposal



At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to the supplier for disposal.

Declaration of Conformity

We, Edimax Technology Co., Ltd., declare under our sole responsibility, that the equipment described below complies with the requirements of the European Radio Equipment Directive.

Equipment: AC1300 DBDC Ceiling-mount AP Model No.: CAP1300

The following European standards for essential requirements have been followed:

Directives 2014/53/EU

CE

Spectrum	: EN 300 328 V2.1.1 (2016-11)
	EN 301 893 V2.1.1 (2017-05)
EMC	: Draft EN 301 489-1 V2.2.1 (2019-03)
	Draft EN 301 489-17 V3.2.0 (2017-03)
EMF	: EN 62311:2008
Safety (LVD)	: IEC 62368-1:2014 (2 nd Edition) and/or EN 62368-1:2014+A11:2017

Edimax Technology Europe B.V.		a company of:
Fijenhof 2,		Edimax Technology Co., Ltd.
5652 AE Eindhoven,		No. 278, Xinhu 1st Rd.,
The Netherlands		Neihu Dist., Taipei City,
Printed Name: Title:	David Huang Director Edimax Technology Europe B.V.	Taiwan

Date of Signature:	Nov., 2020
Signature:	Almo
Printed Name:	Albert Chang
Title:	Director
	Edimax Technology Co., Ltd.

Notice According to GNU General Public License Version 2

This product includes software that is subject to the GNU General Public License version 2. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code.

Das Produkt beinhaltet Software, die den Bedingungen der GNU/GPL-Version 2 unterliegt. Das Programm ist eine sog. "Free Software", der Autor stellt das Programm ohne irgendeine Gewährleistungen zur Verfügung. Wir bieten Ihnen für einen Zeitraum von drei Jahren an, eine vollständige maschinenlesbare Kopie des Quelltextes der Programme zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep

intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.