



MANUAL NWAC7000

Wireless Management Platform

V.1.2

Contents

Chapter 1 Manual Introduction 3
Chapter 2:Product Introduction
2.1 Products description
2.2 Products Properties
2.2.1Hardware Property3
2.2.2 Software Property 3
2.3 Product Layout
2.3.2 Rear Panel6
Chapter 3 Configuration Guide7
3.1 Login Web Interface7
Chapter 4 Function Setting
4.1 Device List
4.2 Device Group
4.3 Device Log
4.4 Address Server
4.5 Gateway19
4.5.1 LAN Setting
4.5.2 WAN Setting 20
4.5.3 Cloud Setting
4.5.4 Authentication
4.6 Firewall
4.6.1 IP/Port Filtering
4.6.2 MAC Filtering
4.6.3 URL Filtering
4.6.4 Port Forwarding27
4.6.5 DMZ Settings
4.8 Management
4.8.1 System management
4.8.2 DNS
4.8.3QoS
4.8.4 User management 32
4.8.5 Device Log
4.8.6 Upgrade Firmware
4.8.7 System Time
4.9 Device Status

4.9.1 Basic Status	35
4.9.2 LAN Status	35
4.9.3 WAN Status	36
4.10 Help	36
Appendix A Product SPEC	37

Chapter 1 Manual Introduction

This manual is subject to tell users how to use this WLAN management platform properly for those familiar with basic networking knowledge and terminology.

This user manual including the connection of AC controller, description of this platform's properties, and how to configure this platform; Pre-reading this manual before operation is highly recommended.

Chapter 2: Product Introduction

2.1 Products description

NWAC7000 is a high performance WLAN controller, especially for Indoor and Outdoor wireless access points which set up in hotel or small-medium sized enterprise;

It's capable for managing all Access point, support AP auto-detection, AP status preview, AP configuration, MAC filtering, simultaneous AP software upgrade to provide high quality & performance & reliability. Easy installation & maintenance WIFI service to different clients

2.2 Products Properties

2.2.1Hardware Property

- Deploy dual core CPU, 880Mhz frequency
- Deploy high capacity&speed memory, up to 516M DDR3 SDRAM;
- 5 * 10/100/1000Mbps Gigabit Ethernet ports

2.2.2 Software Property

- The NWAC7000 detects and connects automatically to Wireless Access points. There is no need to configure each AP individually: complete centralized AP management utility
- Monitor remotely the real time , auto inspection of APs, automatic reboot functionality.
- Simultaneous reconfiguration of SSID, Security type and connection type
- Remote adjustment of AP RF power output for maximum Ap coverage
- Remote control of LED lights
- AP address server for automatic assighnment of IP address, in preferred address range.
- Remote management of Channel selection and location remarks.
- MAC filtering for segmentation and securing users.

• Full management by easy WEB interface

2.3 Product Layout

NWAC7000 front panel is like following:



LED indicator:

LED Light	Name	Indication
Power	Power Light	Power is on, means status is up;
1 Ower	Towor Light	Power is off, mean status is down;
Pup	System Light	flashing,means system status is normal
Run		off or stable steady, means status is abnormal

Reset button:

If need to restore the NWAC7000 into factory default, pls do following procedure:

Power on NWAC7000, use a pin to press and hold the reset button until all LED start flashing quickly from flashing slowly. Then release the button and wait for NWAC7000 to reboot to its factory default settings. After that, the default IP address of NWAC7000 is still 192.168.10.1, default user name and password are unchanged : **admin/admin**

Notice:

LAN/WAN port is LAN port only on the default mode, only when WAN setting is enabled then LAN/WAN port will change to WAN port;

2.3.2 Rear Panel

Rear panel of NWAC7000



DC Jacket

DC Jacket located on the right side of NWAC7000's rear panel, input power should be ac power 100-240V~ 50/60Hz 0.3A

Anti-thunder ground connection:



Please deploy ground connection to avoid lightening stroke, by copper core cable in yellow and green jacket;

For detailed installations please refer to related manuals, like <<Anti-thunder installation guide in devices>>

Attention:

Please use original power cord for installation;

Set locate power outlet near the devices, to make safer and easier installation and operation.

The usage of an UPS system is advised.

Chapter 3 Configuration Guide

3.1 Login Web Interface

Pls confirm the following points before login NWAC7000:

1) Connect the management host(PC) to LAN port of AC controller or UP-link port of switch in the network

2) The management host(PC) has been properly installed IE 7.0 or higher browser version

3) The management host's IP address has been into set the same network segment with NWAC7000, namely 192.168.10.X (X is between 2-254 arbitrary integer Number), a subnet mask of 255.255.255.0.

4) In order to ensure a better effect of Web interface displays, it is recommended to adjust the display resolution to 1024×768 or more pixels.

Operation Steps:

A. Open IE browser, Input http://192.168.10.1/ in the address bar to login NWAC7000 Web management interface.

🕘 http:// 192.168.10.1 💌

B. Now please enter username and password. Factory default is:

Username: admin

Password: admin

Click: "OK"

C. After a successful login, then see NWAC7000 Web interface page:

	V (O O))											
Memory Usage:	۳	III De	vice List				Search by IP		×		٩	Function
	3%	□ Select □ ♀	SN Location Name	Device IP 192.168.200.49	Device MAC 70:B3:D5:8D:C1:6F	Users 0	Version V2.0	Channel 11/36	Online Time	Group N/A	Config	Batch Set
			2	192.168.200.148	70:B3:D5:8D:C1:09	0	V2.0	7/36	0:00:37	N/A	2	
CPU Usage:	۲	□ 💡	3	192.168.200.169	70:B3:D5:8D:C1:1E	0	V2.0	11/44	0:01:09	N/A	ď	Refresh
ОСРС) J: Dual 880MHz											Delete
Device List	OK Zero Config											Clear all devices
												Reboot
Device Group	Device Log											Reset
												upgrade

In the above Web Interface Page, there are three parts.

The main menu area on the left, to show this WLAN controller's main function.

It is the AP List on the middle part, to show the Wireless AP info which can be accessed by this WLAN controller.

Function list are on the right part. For example, click Device List, then all functions of Device List are displayed.

Chapter 4 Function Setting

4.1 Device List

Device list show the current wireless AP accessed by the NWAC7000, display the total quantity/Online/Offline Wireless AP connected to NWAC7000,

Then Wireless AP's name, IP address, MAC address, QTY of end users, Firmware version, Channel as showed in following picture:

Mennory Usage: III Device List Search by JP IIII P IIII Device List Search by JP IIIII P Select: SN Location Name Device IP IIIII Device List Search by JP IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	<u>nı</u>	V @ O I I											
138/b 18elect Select Select Select N Location Name Device IP Device MAC Users Version Chunnel Online Time Group Cru Usage: Image: Image	Memory Usage:	٣	III De	vice List				Search by IP		~		٩	Function 🛛 😔
Memory:2048M I 192168.200.49 7083:D5:8D:C1:6F 0 V2.0 11/36 0.01:00 N/A Image: Control of the state		3%	Select	SN Location Name	Device IP	Device MAC	Users	Version	Channel	Online Time	Group	Config	
CPU Usage: 3 192.168.200.169 0 V2.0 1/36 0.000.37 N/A V2 CPU Usage: 0 3 192.168.200.169 70:83.D5:8D:C1:1E 0 V2.0 11/44 © 0.01:09 N/A V2 Device List Image: Comparison of the second secon	Me	mory:2048M		1	192.168.200.49	70:B3:D5:8D:C1:6F	0	V2.0	11/36	0:01:00	N/A		Batch Set
Refresh	CDITILisade			2	192.168.200.148	70:B3:D5:8D:C1:09	0	V2.0	7/36	0:00:37	N/A		
CPU: Dual 880MHz Delete Delete Delete Clear all devices Clear all devices Reboot Device Group Device Log	CFU Usage.			5	192.100.200.109	70.83.05.80.01.11	0	¥2.0	11/44	0.01.09	N/A		Refresh
Clear all devices Device List Device Config Device Group Device Log	Ср	J: Dual 880MHz											Delete
Reboot Device Group Device Log	Device List	CK♥ Zero Config											Clear all devices
Device Group Device Log													Reboot
	Device Group	Device Log											Reset

Let's introduce following button one by one:

Select: click the white box to make hook, to select this AP

Blue balloon: Click it to set the AP's Location and Device name, fill in the right info if needed, will be showed in Device list when Apply.

Picture showed as follow:



SN: Show how many AP access by this AC controller

Location: show where the AP physical location is.

Name: what's the name of this AP.

Device IP: AP's IP address, click this IP address, can access into AP's GUI when you set an static IP address for your PC in same IP segment.

When there are multiple APs in the device list and you want to find out one AP, you can input this AP's IP address for quick search.

Device MAC: AP's MAC address, if you want to find out one AP quickly by MAC address, just input the MAC address in top of this GUI, then search.

Users: How many end users access into this AP

Version: The firmware version of this AP

Channel: the channel of this wireless AP

Online Time: How long this wireless AP online and access into this AC controller.

Group: you can set some AP in one group, then this part will show group name mainly.



This picture, will show each AP's status, Basic info, and advanced setting.

After change settings, press "Apply" to finish.

Device Status: show AP's Model number, online time, MAC address, IP address, firmware info, channel, RF Power showed in above picture.

Device Network: Show the Wireless AP's WAN network info and IP address

w	an Device Config			\times
	Device Status	IP Setting	DHCP V	
		IP Address	192 . 168 . 188 . 3	
	Device Network	Subnet Mask	255 . 255 . 254 . 0	
	Wireless Basic			
	Wireless Advanced			
	Apply			
	Close			

Wireless Basic: Mainly to setup the AP's SSID, VLAN, Security.

For the VLAN, the top networking should be with VLAN switch, and input the switch's VLAN ID in the blank part. The VLAN ID range is $0\sim4094$.



Since this is a DUAL band AP, both bands need to be configurated.

Wireless Advanced: user can configure the AP's mode, channel, Fragment Threshold, coverage threshold, Max Station



Remark: For Fragment Threshold, RTS Threshold, Beacon Interval, Aggregation, ShortGI, Rev Option, we recommand to keed in default.

Max Station, mean QTY of end users. 0 mean no limited.

Coverage Threshold: Applicated in Roaming mainly, the working status showed as follow:

Set AP1's Coverage Threshold is -75dBm Set AP2's Coverage Threshold is -90dBm AP1 and AP2, with same SSID and password End user move from A to B to C, then will connect with AP1 in place A, connect with AP2 in place B and C, even AP1's signal strength stronger than AP2; Just because in place B, AP2's Coverage Threshold less than AP1



Connected AP: Show how many pieces AP connected into this AC controller, and how many AP can access into this AC controller.

Online AP: QTY of AP which online in this AC controller

Offline AP: QTY of AP which offline in this AC controller

Users: Mean how many end users access into this AC controller.

ALL AP: Mean now show all the online AP, offline AP. Can select online AP or offline AP.

Refresh Interval: mean how long this AC controller will refresh the AP QTY.

Bearch by IP	
Search by MAC	-

Search by IP: mean search the wireless AP by IP address, make hook in the white box, input IP address, then search.

Search by MAC: mean search the wireless AP by MAC address, make hook in the white box, input MAC address, then search



Batch Set: mean can configure the wireless AP's data in batch.Refresh: Scan the AP list again.Delete: Select some AP, then delete from this AC controller.Clear all devices: Will delte all settings in APsReboot: Select some AP, then restart this APReset: Select some AP, revert to factory default.

Upgrade: can upgrade firmware for wireless AP

4.2 Device Group

Click Device Group at first, then will show New/Delete,

Cick New, then configure the data in Wireless Basic and Wireless Advanced part;

Pls note, this data will be applied for all the APs in this group. After finish all, set a group name, then Apply to finish.

For detail procedure, pls refer to following picture:



Add /Remove AP into group:

Pls follow the steps showed in following picture:

Memory Usage:	۲	Dev	vice Group											Function 🛛 📀
	2%	Select	SN		Wlan	Group N	Name				Contains AP		Config	
Ме	mory:2048M		1	-		TEST				📫 Ti	he group consists of A	AP [0]	Z	New
				Wlan G	roup D	evice Li	ist						\times	
CPU Usage:	۲			Select	SN Add	Locat a dovice	tion	Name	Device	ID Device	MAC Online Ti	mo	Group	Delete
	0/				🗆 Sel	ect SN	N	Location	Name	Device IP	Device MAC	Group		
СР	J: Dual 880MHz					1		TEST	Hello	192.168.188.2	70:B3:D5:8D:C1:09	N/A		
						2				192.168.188.3	70:B3:D5:8D:C1:6F	N/A		
Device List	CK Zero Config			1	U	3				192.108.188.4	70.03.09.80.C1.1E	N/A		
Device Group	Device Log													
9	10			Add AP	Add A	Р								
Address Server	Gateway													

The group consists of AP [0] Please click :

Then add APP to Wlan group device List

Select APs and add these APs

4.3 Device Log

Device Log show AP's record, such as on line recording, offline recording, device configuration record.

N						
Memory Usage:	۲	🛃 Device Log				Function 🛛 📀
	12% Iemory:2048M	1970/01/01 05:21:39 1970/01/01 05:21:43 1970/01/01 05:21:47 1970/01/01 07:48:39 1970/01/01 07:48:41 1970/01/01 07:48:48	Device192.168.188.2 Device192.168.188.4 Device192.168.188.3 Device192.168.188.3 Device192.168.188.3 Device192.168.188.2	MAC[70:83:D5:8D:C1:09] MAC[70:83:D5:8D:C1:1E] MAC[70:83:D5:8D:C1:6F] MAC[70:83:D5:8D:C1:6F] MAC[70:83:D5:8D:C1:6F] MAC[70:83:D5:8D:C1:6F]	offline offline offline offline online Downloading configuration online	Clear
CPU Usage:	ت ۵۵۷	1970/01/01 07:48:49 1970/01/01 07:48:56 1970/01/01 07:48:57 1970/01/01 07:48:58	Device192.168.188.2 Device192.168.188.4 Device192.168.188.4 Device192.168.188.3	MAC[70:B3:D5:8D:C1:09] MAC[70:B3:D5:8D:C1:1E] MAC[70:B3:D5:8D:C1:1E] MAC[70:B3:D5:8D:C1:1E] MAC[70:B3:D5:8D:C1:6F]	Downloading configuration online Downloading configuration Wireless transmission power change	
	JYO PU: Dual 880MHz	1970/01/01 07:48:58 1970/01/01 07:48:58 1970/01/01 07:48:58 1970/01/01 07:49:01 1970/01/01 07:49:01 1970/01/01 07:49:02 1970/01/01 07:49:02	Device192.168.188.3 Device192.168.188.3 Device192.168.188.3 Device192.168.188.2 Device192.168.188.2 Device192.168.188.2 Device192.168.188.2	MAC[70:B3:D5:8D:C1:6F] MAC[70:B3:D5:8D:C1:6F] MAC[70:B3:D5:8D:C1:6F] MAC[70:B3:D5:8D:C1:09] MAC[70:B3:D5:8D:C1:09] MAC[70:B3:D5:8D:C1:09] MAC[70:B3:D5:8D:C1:09]	Wireless transmission power change Configuring wireless network parameters Complete the configuration wireless network parameters. Wireless transmission power change Wireless transmission power change Configuring wireless network parameters Complete the configuration wireless network parameters.	
Device List	CK Zero Config	1970/01/01 07:49:09 1970/01/01 07:49:09 1970/01/01 07:49:10 1970/01/01 07:49:10 1970/01/01 09:23:50 1970/01/01 09:23:54 1970/01/01 09:23:54	Device192.168.188.4 Device192.168.188.4 Device192.168.188.4 Device192.168.188.4 Device192.168.188.4 Device192.168.188.4 Device192.168.188.4	MAC[70:B3:D5:8D:C1:1E] MAC[70:B3:D5:8D:C1:1E] MAC[70:B3:D5:8D:C1:1E] MAC[70:B3:D5:8D:C1:1E] MAC[70:B3:D5:8D:C1:1E] MAC[70:B3:D5:8D:C1:09] MAC[70:B3:D5:8D:C1:05]	Wireless transmission power change Wireless transmission power change Configuring wireless network parameters Complete the configuration wireless network parameters. offline offline	
		1970/01/01 19:53:25 1970/01/01 19:53:27 1970/01/01 19:53:33 1970/01/01 19:53:35 1970/01/01 19:53:41	Device192.168.188.3 Device192.168.188.3 Device192.168.188.2 Device192.168.188.2 Device192.168.188.4	MAC[70:B3:D5:8D:C1:6F] MAC[70:B3:D5:8D:C1:6F] MAC[70:B3:D5:8D:C1:09] MAC[70:B3:D5:8D:C1:09] MAC[70:B3:D5:8D:C1:1E]	online Downloading configuration online Downloading configuration online	
Device Group	Device Log	1970/01/01 19:53:43 1970/01/01 19:53:43 1970/01/01 19:53:43 1970/01/01 19:53:43 1970/01/01 19:53:43 1970/01/01 19:53:53	Device192.168.188.4 Device192.168.188.3 Device192.168.188.3 Device192.168.188.3 Device192.168.188.3 Device192.168.188.4	MAC[70:B3:D5:8D:C1:1E] MAC[70:B3:D5:8D:C1:6F] MAC[70:B3:D5:8D:C1:6F] MAC[70:B3:D5:8D:C1:6F] MAC[70:B3:D5:8D:C1:6F] MAC[70:B3:D5:8D:C1:1E]	Downloading configuration Wireless transmission power change Wireless transmission power change Configuring wireless network parameters Complete the configuration wireless network parameters. Wireless transmission power change	

4.4 Address Server

Through Address Server, to set server IP address, subnet mask; Server address Pool, main to assign IP address to the connected wireless AP, no need to specify the IP address for wireless AP manually when operation.

Ме	mory:2048M		Server IP Address 192	. 168 . 188 . 1		Refresh
CPU Usage:	۳	Ser	ver Address Count 100	(1-300)		Apply
	0/		Effective Time(s) 86400	Range:(300-864000)s		
СР	J: Dual 880MHz	All	ocated AP number 3			
		AP address information list				
	1	AP Device Name	IP Address	MAC Address	Lease Time	
Device List	Zero Config	NWA300 NWA300 NWA300	192.168.188.2 192.168.188.3 192.168.188.4	70:b3:d5:8d:c1:09 70:b3:d5:8d:c1:6f 70:b3:d5:8d:c1:1e	0 D 22:30:16 0 D 22:30:15 0 D 22:30:14	
Device Group	Device Log					
Q Address Server	Gateway					
System uptim	e0Day 21:23:8	So	ftware VersionNWAC7000-S	PI-V2.0-B20160519145948		

Please use the correct IP address range.

Server IP Address: modify the default AP address server's IP address; (default is 192.168.188.1)

Server Subnet: Modify AC controller's subnet; 255.255.255.0 in default

Server Address Pool: When wireless AP connected with this address server, then address server will assign IP address for wireless AP. (The default IP address pool is 192.168.188.2-192.168.188.254)

4.5 Gateway

4.5.1 LAN Setting

🔶 AP Management	LAN Settings	Function
Help	LAN IP Setting	LAN Settings
Z Status	Subnet Mask 255 - 255 - 252 - 0	WAN Settings
	DHCP Server • Enable Disable DHCP IP Count 192 . 168 . 10 . 101	Cloud Settings
Network Firewall	DHCP Lease Time 86400 Range:(300-864000)s	Authentication
Management	Static Bind IP-MAC List Add Refresh 192 168 10 192 192.168 10 192	Local Auth

LAN IP Setting:

Set IP address for LAN

Subnet mask

Set Subnet mask for LAN

DHCP Server

DHCP server enable mean it will assign IP address for users.

DHCP IP Count

DHCP Client IP mean the IP address range assigned by DHCP Server.

DHCP Lease Time

The networking device get IP lease time from DHCP server.

Static Bind IP-MAC List

Can delete it the IP/MAC address from this list if no need to bind.

Local IP-MAC List

Can add/refresh the IP/MAC list connected into this AC controller.

4.5.2 WAN Setting

🔶 AP Manageme	WAN Settings	Function 🛛 📀
Help	WAN Setting	LAN Settings
Status	Dynamic IP Static IP pPTP Disable	WAN Settings
	Primary DNS 8 8 8 8 Secondary DNS 4 4 4 4	Cloud Settings
Network Firewa	Advanced Settings	Authentication
Storage/Server Managerr	MAC Clone Scan MAC Enable uPNP Enable IGMP proxy Enable Ping Access on WAN Enable Web Server Access on WAN Port: Enable Web Server Access on WAN Port: 0000 (Port Range 1-65535) Enable IPsec pass through on VPN connection Enable PPTP pass through on VPN connection Enable L2TP pass through on VPN connection Apply	Local Authentication

Click Gateway will automatically jump to the WAN settings as below;

When select to intelligent gateway, NWAC7000 will have a router function, can work as a main router with Gigabit WAN/LAN port. It support Dynamic IP, Static IP; PPPOE; PPTP.

Dynamic IP: WAN interface obtains IP and DNS information through DHCP mode.

PPPOE(ADSL): WAN interface obtains IP and DNS information via PPPOE dial-up mode.

Static IP: Set IP and DNS information for WAN interface manual

PPTP: WAN interface obtains IP and DNS information via PPTP mode

MAC Clone: Specifies the WAN interface MAC, by clicking [Search MAC Address] button, and then will pop up a connected device's MAC, select the MAC desired to clone. You can manually specify the MAC

Enable IGMP Proxy: Enables IGMP proxy, this feature can be forwarded IGMP data from WAN to the LAN

Enable Ping Address on WAN: This feature allows outer net to ping WAN

Enable Web Server Address on WAN port: Enable this feature, allows to manage NWAC7000 from outer net via a specified remote management port

4.5.3 Cloud Setting

AP Management	Cloud Settings	Function 🛛 😔
Help		
	Cloud server settings Cloud Server Settings Enable	LAN Settings
Status	Cloud Server	WAN Settings
• •	Contact Information	Cloud Settings
Network Firewall		Authentication
🔅 Management		Local Auth

Cloud Server Setting: Enable or Disable.

Cloud Server: Input the cloud server's IP address or domain name.

Login Name: mean the account name in this cloud server.

Contact information: input if you have.

4.5.4 Authentication

A. Remote Authentication:

Remote Authentication: work with cloud server to do the advertisement or portal authentication.

Pls note: the cloud server should support wifidog.

🔶 AP	Management	Authentication			Function 🛛 📀
He	lp	Authentication Authentication	Disable Remote Authentication Local Authentication		LAN Settings
<u>~</u>	Status	Gateway ID Web server name Port	yowifi 2060	Default:2060 Range[1-65535]	WAN Settings
	V	Maximum users Client Timeout	500 20	Default:500 Range[1-500] Default:20 min Range[1-65535min]	Cloud Settings
Network	Firewall	Authentication server Authentication server SSL Enable	95.110.169.204		Authentication
	0	Authentication server Port Authentication server path	80	Default:80 Range[1-65535]	Local Authentication
Storage/Server	Management	External domain white list			

How to make NWAC7000 work with your authentication server:

Gateway ID: Mean Gateway's MAC address.

In this part, our NWAC7000 should work in Intelligent Gateway, mean this ID is the MAC of NWAC7000.

Web server name: this name is from server supplier, can fill or not fill. Take our cloud Platform for example: input wifidog in this part.

Port: this part should match with the server's port, the default is 2060, the range is 1~65535

Maximum users: mean the end user will comply with this authentication; Default is 500, range is 1~500.

Client Timeout: the authentication time, default is 20 mins, the range is 1~65535 min.

Authentication Server: mean the server name which support wifidog for authentication, it is an important data.

Authentication server SSL enable: disable or enable, based on server.

Authentication server port: matched with server data, default is 80, the range is 1~65535.

Authentication server path: the patch of authentication server. If no data, pls use default.

External domain white list: User can visit this domain directly, no need any authentication.

Add external domain white list: Just input the domain in yellow part, then click add domain.

Delete external domain white list: click ²³ this button to delete it

MAC white list: User with MAC address in MAC white list can access into Internet directly, no need authentication.

Add white MAC: Input the MAC address in blue part, or scan the MAC address, then click add MAC.

Delete White MAC: click ¹⁰⁰ this button to delete it.

After finished this settings, then Apply to complete the Remote authentication setting and make it work with authentication server.

B. Local Authentication:

For Local Authentication, just do advertisement in AC controller part, no need to access into cloud server.

Maximum users: max user QTY will do the authentication.

External domain white list: User can visit this domain directly, no need any authentication

MAC white list: the MAC address will not do the authentication.

← AP Management	Authentication	Function 🛛 👁
Help	Authentication	LAN Settings
Katus	Maximum users 500 Default:500 Range[1-500]	WAN Settings
	External domain white list	Cloud Settings
Network Firewall	Add MAC	Authentication
Storage/Server Management	MAC white list	Local Authentication
	Apply	
← AP Management	Authentication	Function 🛛 😒
Help	Authentication Local Authentication	LAN Settings
🛩 Status	Maximum users 500 Default:500 Range[1-500] Add domain iteols info	WAN Settings
	External domain white list ibook.info captive.apple.com	Cloud Settings
Network Firewall	appleiphonecell.com Scan MAC	Authentication
Storage/Server Management	MAC white MAC IP Address d8:d1:cb:bb:88:40 192.168.10.2 00:22:68:18:29:87 192.168.10.100	Local Authentication
	Apply	

When choose Local Authentication in Authentication part, then Apply; please upload the pictures should show to end users.

The step showed as following picture.

Local Auth	Function 🛛 👁
Local Auth Advertising Picture Upload first pictures Bestand kiezen Geen bestand gef ozen Update Pictures	LAN Settings
First pictures button name Auth Buttorn	WAN Settings
Second pictures button name Auth Button2 Second pictures redirect url	Cloud Settings
Third pictures button name Auth Button3	Authentication
Third pictures redirect url Save Preview	Local Auth
	Local Auth Local Auth Advertising Picture Upload first pictures Bestand kiezen Geen bestand gelozen Update Pictures First pictures button name Auth Button2 Second pictures redirect url Third pictures button name Auth Button3 Third pictures redirect url Update Pictures



4.6 Firewall

4.6.1 IP/Port Filtering

	V@01)		
🗲 АР	Management	IP/Port Filtering	Function 📀
н	elp	IP/Port Filtering IP/Port Filtering Close	IP/Port Filtering
~	Status	IP Range 192 . 168 . 10 192 . 168 . 10 . Protocol TCP+UDP V	MAC Filtering
•		Port Range - (Range 1-65535) Mark	URL Filtering
Network	Firewall	Max rule counts : 200 Add Delete Cancel Apply	Port Forwarding
Constant Con		IP Range Port Range Protocol Mark	DMZ Settings



IP/Port Filtering

IP/Port forwarding enabled, router will limited the data forwarding according to the filtering rule. If the filtering rule is [refuse], then the router will refuse to forward the data in accordance with filtering rule.; If the filtering rule is [allow], the router will forward the data in accordance with filtering rule.

IP Range

Set IP address range

Protocol

Set filtering rule protocol

Port Range

Set filtering port range

Mask

A simple description of the entry rules, for user's easy management;

4.6.2 MAC Filtering

	CO)			
🔶 AP Mana	agement	MAC Filtering		Function
Help		MAC Filtering	MAC Filtering Close	IP/Port Filtering
Zar Star	tus		MAC Scan MAC Mark	MAC Filtering
(Detwork	Firewall	MAC	Max rule counts : 200 Add Delete Cancel Apply Mark	URL Filtering Port Forwarding

MAC Filtering

Enabling Mac filtering, router will restrict data forwarding based on the selected filtering rules; When selected **Close**, router will decline the pointed incoming data; When selected as **Open**, then router will allow the pointed incoming rules;

Mac address

Set up rules in mac address, users can click **Searching Mac Address** from the clients in routers, or can set up the mac address manually;

Mask

A simple description of the entry rules, for user's easier management;

4.6.3 URL Filtering

🔶 AP Mana	agement	URL Filtering	Function 🛛 😔
Help		URL Filtering URL Filtering Close	IP/Port Filtering
Z Sta	tus	URL Max rule counts : 200 Add Delete Cancel Apply	MAC Filtering
	•	URL	URL Filtering
Network	Firewall		Port Forwarding

URL Filtering

Enabling URL filtering, router will restrict access to the pointed URL;

URL address

Set up the declined URL address

4.6.4 Port Forwarding

<u>.</u>			
÷ ,	AP Management	Port Forwarding	Function 🛛 오
	Help	Port Forwarding Rule Type User-defined	IP/Port Filtering
<u>~</u>	Status	Bule Name Lan IP 192 168 10	MAC Filtering
Network	Firewall	Exemal Port - (Range 1-65535) Internal Port - (Range 1-65535) Protocol TCP V	URL Filtering Port Forwarding
C Management		Max rule counts : 200 Add Delete Cancel Rule Name Forward IP Protocol External Port Internal Port	DMZ Settings

Port forwarding

Port forwarding is to forward data from one port to another port, enabling external users have access to an internal private IP in LAN, from an external triggered NAT router ;

Rule Type

Set up rule type, which have specific port number;

Rule name

Port forwarding rule name

LAN IP

IP of the port forwarding

External port

External port number of port forwarding

Internal port

Internal port number of port forwarding

Protocol

Protocol used for port forwarding

4.6.5 DMZ Settings

UIVG	0)) × × ×		
👉 AP Manage	ement	DMZ Settings	Function 🛛 😔
Help		DMZ Setting	IP/Port Filtering
Zatu Statu	JS	Apply	MAC Filtering
	•		URL Filtering
Network Fire	rewall		Port Forwarding
C Management			DMZ Settings

DMZ

DMZ is short for demilitarized zone; It's a compartment between security zone and nonsecurity zone, in order to solve the problem of external network cannot access into internal server after firewall installation; This DMZ zone is a small network zone between external and internal network; While in this small zone, users usually place some open server, like web server, FTP server, or forum; DMZ will protect internal network more efficiently, because this network allocation is another obstacle for hackers, compared to normal firewall;

IP LAN IP

IP address of DMZ host

4.8 Management

4.8.1 System management

	<u>/ (0))</u>		
<table-cell-rows> АР М</table-cell-rows>	Management	System	Function 😔
Не	lp	Save/Reload Settings	System
<u>~</u>	Status	Backup Save the configuration file to your computer Bladeren Using the saved configuration file recovery configuration	DDNS
•		Reset Default Restore the factory default settings, please press this button	Smart QoS
Network	Firewall	Reboot Reboot	User
🌣 Management			Logs
			Upgrade Firmware

Backup

Save the configuration files to your computer

Restore

Using the saved configuration file recovery configuration

Restore default

Restore the factory default settings, please press this button

Reboot

Reboot the system

4.8.2 DNS

ບເດຍາ		
🔶 AP Management	DDNS	Function 🛛 👁
Help	DDNS Settings Dynamic DNS Disable	System
Z Status	Арріу	DDNS
		Smart QoS
Network Firewall		User
Anagement		Logs
		Upgrade Firmware
		Curture Time

Enable or disable DNS

4.8.3QoS

🔶 AP Management	Smart QoS	Function 🛛 오
Help	Qos Basic Settings Status O Enable © Disable	System
Z Status	Upload 50000 Download 50000	DDNS
	Apply Qos rule setting	Smart QoS
Network Firewall	IP Address Range 192 168 10 ~ 192 168 10 MAC Address Scan MAC	User
O Management	Mode Shared Exclusive	Logs
	Max bandwidth(Decimal point is not allowed) Download 0 Kbps	Upgrade Firmware
	Mark (Double-click the selected items to modify the settings, QoS allows you to add up to 8 rules) Add Delete Modify Cancel	System Time

Status

Enable or Disable QoS function

Upload

Set up total uploading bandwidth

Download

Set up total downloading bandwidth

IP Address Range

Set up IP range of bandwidth

MAC address

Set up bandwidth control by mac address, user can choose it from Scan MAC, or setup by manual.

Mode

QoS mode settings, shared mode means under the QoS rules, the main PC within all IP range can share the specified bandwidth;

Exclusive mode means single main PC can share the specified bandwidth;

Max bandwidth

Max bandwidth under QoS rules

4.8.4 User management

<u>n</u>			
<table-cell-rows> АР</table-cell-rows>	Management	User	Function 🛛 👁
H	elp	User Settings User Name admin	System
<u>~</u>	Status	Password ••••• Confirm Password	DDNS
•		Apply	Smart QoS
Network	Firewall		User
Ö Management			Logs
			Upgrade Firmware

User Name

Reset new log-in user name

Password

Reset new log-in password

Confirm Password

Comparison to new password, to confirm user input password correctly in two times

4.8.5	Device	Log
-------	--------	-----

🔶 AP Management	Logs	Function 🛛 👁
Help	System Logs	System
<mark>∼</mark> Status	Remote Log Service	DDNS
	System Log View	Smart QoS
Network Firewall		User
0		Logs
	5	Upgrade Firmware
	Refresh Clear	System Time

Status

Enable or Disable to show system log

Remote Log Service

To decide whether send System log into some pointed remote server synchronously;

4.8.6 Upgrade Firmware

ΩΙνοοη				
🗲 АР Ма	lanagement	Upgrade Firmware	Function 🛛 😒	
Help	p 🥖	Software Version NWAC7000-SPI-V2.0-B20160519145948	System	
🗠 St	tatus	For software upgrade 1. Click on [Browse] and select the software to be upgraded 2. Click [upgrade] button Bladeren	DDNS	
Network	Firewall	Note Upgrade software may cause the system to interrupt	Smart QoS	
•		In the process of updating the firmware, do not power down, or it may damage the system!	Logs	
Management			Upgrade Firmware	
			System Time	

This feature allows the device firmware upgrade.

Noted:Upgrading software may cause system outage, In the process of upgrading the firmware, do not power off, otherwise it may damage the AC controller!

4.8.7 System Time

<table-cell-rows> AP Management</table-cell-rows>	System Time	Function 🛛 👁
Help	System Time System Time 1970-01-01 01:08:14 Synchronization with the host	System
Z Status	Status () Enable () Disable NTP Server time.nist.gov	DDNS
	Gustom NTP server	Smart QoS
Network Firewall	Vhen device running at 0:00 V Automatic reboot	User
0	Apply	Logs
		Upgrade Firmware
		System Time

Synchronization with the host

Synchronization time with connected $\ensuremath{\mathsf{PC}}$ and router

Status

Enable or Disable NTP

NTP Server

Select the server time synchronization

Custom NTP Server

Setting user-defined synchronization server IP address

Time Zone

Setting the router's time zone

4.9 Device Status

4.9.1 Basic Status

Show NWAC7000's firmware version, hardware version, system uptime.

Image: AP Management Image: Basic Info			
Help Status Image: bit info Image: bit info Basic Info Software Version NWAC7000-SPI-V2.0-B20160519145948 Hardware Version V1.1 System uptime 0Day 1:15:42 WAN	← AP Management	Basic Info	Function 🛛 👁
Status Image: Base of the status Hardware Version V1.1 System uptime 0Day 1:15:42 Image: Base of the status Image: Base of the status </th <th>Help</th> <th>Basic Info Software Version NWAC7000-SPI-V2.0-B20160519145948</th> <th>Basic Info</th>	Help	Basic Info Software Version NWAC7000-SPI-V2.0-B20160519145948	Basic Info
Image: Ward with the second secon	Z Status	Hardware Version V1.1 System uptime 0Day 1:15:42	LAN
Network: Firewall			WAN
C Management	Network Firewall		
	🌣 Management		

4.9.2 LAN Status

LAN Setting

Show NWAC7000's LAN IP, DHCP server status and MAC address

nive	O))	
<table-cell-rows> AP Manag</table-cell-rows>	ment LAN	Function
Help	LAN Configuration	Basic Ir
🛩 Statu	S DHCP Status Enable DHCP Client 192.168.10.1-192.168.10.101	LAN
Detwork Fir	Subnet Mask 255.255.252.0 MAC 70:B3:D5:8D:C1:D0	WAN
	Assigned IP Number 0 Assigned IP DHCP Client	
M anagement		

4.9.3 WAN Status

WAN Setting

It shows NWAC7000's WAN status, Connect Type, WAN IP, Subnet Mask, Gateway IP, DNS and MAC info.

Image: AP Management Image: WAN Help Image: WAN Configuration Image: WAN Configuration Basic Info Image: WAN Configuration Basic Info Image: WAN Configuration Image: WAN Configuration Image: WAN Configuration Image: WAN Co			
Help WAN Configuration Basic Info WAN Status WAN port is disconnected Connect Type DHCP LAN WAN IP Subnet Mask WAN Subnet Mask Deafult Gateway WAN	🔶 AP Management	WAN	Function 🛛 📀
Status Connect Type DHCP LAN WAN IP Subnet Mask WAN Subnet Mask Deafult Gateway WAN	Help	WAN Configuration WAN Status WAN port is disconnected	 Basic Info
Subnet Mask Deafult Gateway Network Firewall	Status	Connect Type DHCP WAN IP	LAN
DNS 0.0.0	Detwork Firewall	Subnet Mask Deafult Gateway DNS 0.0.0	WAN
MAC 70:B3:D5:8D:C1:D1	C Management	MAC 70:B3:D5:8D:C1:D1	

4.10 Help

If you meet with problem in understanding on above info, click help, then will pop up one window for better understanding.

LAN Settings	Help X IP Address • Set up the LAN IP address		Function 🛛 📀
LAN IP Setting	Subnet Mask Set up the LAN subnet mask	. 168 . 10 . 1	LAN Settings
DHCP Server Setting	DHCP Server The DHCP server can automatically manage and allocate internal users required IP settings	255 . 252 . 0	WAN Settings
	DHCP IP Count • The DHCP server can automatically manage and distribute IP address range	ole O Disable	Cloud Settings
	DHCP Lease Time • The internal network equipment IP lease time by the DHCP server	0 Range:(300-864000)s	Authentication
□ Static Bind IP-MAC List	Static Bind IP-MAC List • A list of MAC-IP static binding list has been assigned Local IP-MAC List • List of the equipment connected to the IP and MAC device information	cal IP-MAC List Add Refresh	Local Auth
	LAN Settings LAN IP Setting DHCP Server Setting Static Bind IP-MAC List	LAN Settings IP Address LAN IP Setting Set up the LAN IP address LAN IP Setting Set up the LAN subnet mask DHCP Server Can automatically manage and allocate internal users required IP settings DHCP Server Can automatically manage and allocate internal users DHCP Server Setting The DHCP server can automatically manage and distribute IP address range DHCP Server Setting The DHCP server can automatically manage and distribute IP address range DHCP Server Setting The internal network equipment IP lease time by the DHCP server Static Bind IP-MAC List A list of MAC-IP static binding its has been assigned Local IP-MAC List List of the equipment connected to the IP and MAC device information	LAN Settings IP Address LAN IP Setting Set up the LAN subnet mask Set up the LAN subnet mask Set up the LAN subnet mask DHCP Server Setting The DHCP Server can allocate internal users required IP settings DHCP Server Setting DHCP Server can allocate internal users required IP settings DHCP Server Setting DHCP Server can allocate internal users required IP settings DHCP Server Setting DHCP Server can allocate internal users required IP settings DHCP IP Count The internal network equipment IP lease time by the DHCP server Static Bind IP-MAC List A list of MAC-IP setatic binding list has been assigned Local IP-MAC List A list of the equipment connected to the IP and MAC device information

Appendix A Product SPEC

Item		Parameter
Standa	rd Protocol	IEEE 802.3、IEEE 802.3u
QTY of m	anageable AP	Default: 200pcs, Max: 300pcs
C	PU	MT7621, 880MHz
FL	ASH	128Mb
D	DR3	DDR3 4096Mb
Power Consumption		< 5W
Interface	LAN port	Four 10/100M/1000M RJ45 port (Auto MDI/MDIX)
	LAN/WAN port	1 LAN/WAN port, Default is LAN port, WAN port when open WAN mode
LED	Power	Adapter
Indicator	Run	System status
Demension (L x W x H)		440mm x200 mm x 45mm
Cooling		Nature cooling + Fan cooling
		Working temperature : 0°C~40°C
Working environment		Storage temperature : -40°C~70°C
		Working Humanity : 10%~90%RH (No condensation)
		Storage Humanity : 5%~90%RH (No condensation)
F	ower	100-240V~ 50/60Hz