COMMANDO AIR-AP3000AX Indoor Access Points Configuration Guide

Web Manual

This Guide is intended for network managers familiar with IT concepts and network terminologies. No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of COMMANDO Networks Ltd.

Trademarks and Permissions

COMMANDO Networks trademarks are trademarks of COMMANDO Networks Ltd. The COMMANDO trademarks, service marks ("Marks") and other COMMANDO trademarks are the property of COMMANDO Networks. COMMANDO AIR-AP3000AX products are trademarks or registered trademarks of COMMANDO Networks Ltd. You are not permitted to use these Marks without the prior written consent of COMMANDO Networks. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between COMMANDO Networks and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

TABLE OF CONTENTS

6. COMMANDO Cloud

Overview

COMMANDO AirX Wireless AIR-AP3000AX is Cloud based, enterprise-class wall/ceiling indoor (802.11ax) Wi-Fi 6 wireless access point which works in standalone, FAT mode as well as Controller based FIT mode of operation and provides wireless users with speed up to 2976Mbps with advanced Wi-Fi 6 Technology. It comes with dual band, equipped with separate 1Gbps WAN port & 1Gbps LAN port. It supports 2x2 MU-MIMO and provides data rate up to 2976Mbps for wireless users and supports concurrent 70 wireless clients with simultaneous upload or download of multiple packets at same time which enhances the sharing of files, photo, audio, video, and gaming experience over wireless network.

It supports Seamless Roaming, OFDMA, 1024-QAM, narrower sub-carrier spacing and longer symbol time which improves the stability and data processing efficiency. It can provide powerful wireless coverage to enterprise environments such as small, medium, and large enterprises, university campuses, concert venues, gymnasium, etc.It is powerful, long range & advance Wi-Fi 6 wall/ceiling indoor Access Point supports range of 20meters and above in all direction depending on surrounding conditions with up to 20dBm transmit power for 2.4G, 19dBm transmit Power for 5G.

It is industrial grade Ceiling IEEE 802.3af/at 48V PoE/PoE+ standard, install at every place to work as an stable base station for access users. It is equipped with separate backward compatible 10/100/1000Mbps Ethernet WAN and 10/100/1000Mbps LAN port. It supports (IEEE 802.3af/at) PoE/PoE+, which helps in easy installation by eliminating the need of a dedicated power source and need of a power adapter. It can identify and determine the correct transmission speed and half/full duplex mode of the attached devices. It also supports standard Auto-MDI/MDI-X that can detect the type of connection to any Ethernet device without requiring special straight or crossover cables, Store-and-Forward forwarding scheme to ensure low latency and high data integrity.

It can install at every place to work as a stable base station for wireless users.

Fig 1. Physical port & Description on AIR-AP3000AX

Table 1. Physical port on AIR-AP3000AX Description.

Physical Port	Description
Reset	Reset Button, makes AP revert to default settings after pressing for 15sec.
WAN/PoE	WAN Port, connect with PoE+.
LAN	Dedicated LAN Port
DC	DC input power 12V, 1.5 A.

Lightning-Fast AX3000 WiFi 6 Speeds

New-era business WiFi 6 with speeds up to 2976 Mbps brings more than twice the speed of WiFi 5. Every application feels more fluid with drastically improved WiFi speeds with 1024 QAM with 25%

more data encoded at one time. Long OFDM Symbol able to achieve 11% faster speed with 160MHz Channel Width. It also supports double the data at peak transmission times on a single stream.

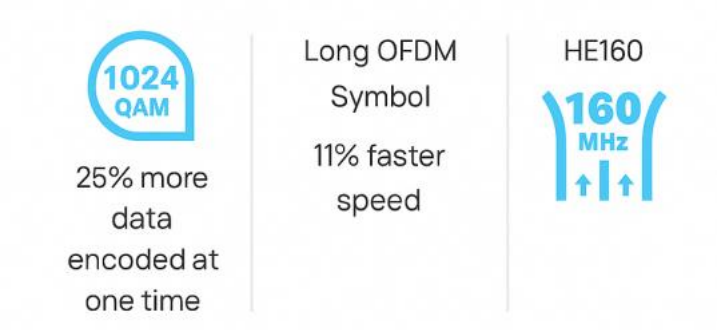


Fig 2. AIR-AP3000AX advantage

Important Note: Access IP for AIR-AP3000AX is 192.168.188.251 and default password is commando.

Recommended: It is required to delete browser history before taking access of device as it can give catch pages error for access of device.

It supports three operational modes FIT, FAT & FAT Routing operation mode. In FIT mode, AP works with the RouteX Controller and all configuration is centrally managed by controller. In FAT mode, AP can use WEBGUI and configure standalone AP. In FAT routing mode can also work as gateway alone with standalone AP operation (Default mode is FIT-AP mode). It supports up to 80 wireless users/clients & supports distance of 20 meters and above from AP in all directions for wireless clients. It is industrial grade Wall/Ceiling Outdoor Access Point with speed up to 3000Mbps which enhances the sharing of files, photo, audio, video and gaming experience over wireless network. It can also be used as DHCP server and works as layer 3 device when configured in FAT-Routing mode. It supports (IEEE 803.3af/802.3at) PoE/PoE+, which helps in easy installation by eliminating the need of a dedicated power source and need of a power adapter. It can identify and determine the correct transmission speed and half/full duplex mode of the attached devices. It also supports standard Auto-MDI/MDI-X that can detect the type of connection to any Ethernet device without requiring special straight or crossover cables,

You can access and manage AIR-AP3000AX using the Web based GUI (Graphical User Interface) , also called WEB-GUI interface.

Introduction

It supports FIT/FAT operation mode. In FIT mode, AP works with the RouteX Series controller and all configuration is centrally managed by controller. In FAT mode, AP can use WEBGUI and configure AP and routing mode. Default mode is FIT mode. COMMANDO AirX AIR-AP3000AX is dual radio Wi-Fi 6 Cloud Indoor Access Point. It works in standalone as well as Controller-based mode. RouteX Series Controller enables communication between wireless users with speed up to 3000Mbps with advanced Wi-Fi 6, OFDMA technology with built-in 2dBi FPC dual band MIMO Antenna. It is standalone device, comes with dual band with 2.4GHz (600Mbps 11ax 2x2) + 5GHz (2400Mbps 3x3), equipped with separate 1G WAN ports and LAN ports. The supports MU-MIMO and DL/UL-OFDMA modulation with 80 end users. These multiple users can upload or download multiple packets at the same time.

It is powerful, long range & advance Wi-Fi 6 wall/ceiling indoor Access Point supports range of 20meters and above in all direction depending on surrounding conditions with up to 20dBm transmit power for 2.4G, 19dBm transmit Power for 5G. It is industrial grade Ceiling IEEE 802.3af/at 48V PoE/PoE+ standard, install at every place to work as an stable base station for access users.It is equipped with separate backward compatible 10/100/1000Mbps Ethernet WAN and 10/100/1000Mbps LAN port.

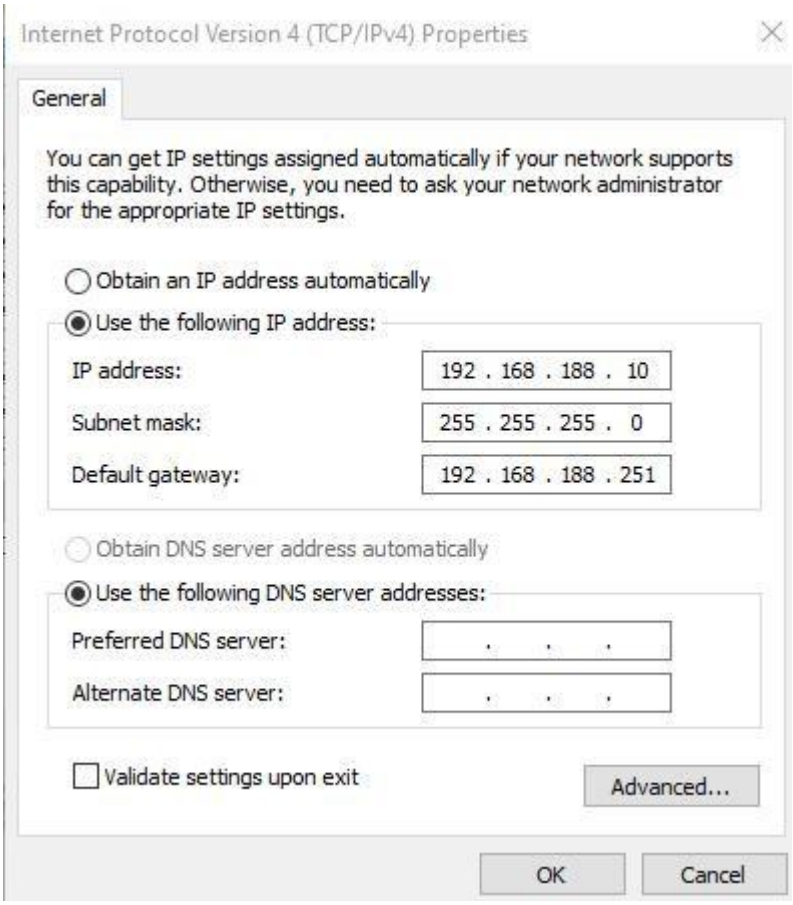
It can install at every place to work as a stable base station for wireless users. Its ceiling-mounted design, integrated Ethernet interface, and sleek appearance make it easy to deploy, and it can be seamlessly integrated into the ceiling or wall without disrupting the overall interior design layout. It is an ideal choice for wireless access in large-scale, low-density, high-bandwidth environments. It supports (IEEE 802.3af/at) PoE/PoE+, which helps in easy installation by eliminating the need of a dedicated power source and need of a power adapter. It can identify and determine the correct transmission speed and half/full duplex mode of the attached devices. It also supports standard Auto-MDI/MDI-X that can detect the type of connection to any Ethernet device without requiring special straight or crossover cables, Store-and-Forward forwarding scheme to ensure low latency and high data integrity.

1. COMMANDO AIR-AP3000AX FAT mode works as autonomous / standalone

How to take access of COMMANDO AIR-AP3000AX?

1) Wired access Via LAN port connected to PC. (Method-1)

Power ON AIR-AP3000AX either by PoE/PoE+ switch or 12V, 1.5A adapter. Connect LAN port of AIR-AP3000AX to PC via RJ-45 cable.
Open Network and sharing enter. Go to Change adapter settings .



Double click on Local Area Connection. Go to Properties. Double click on Internet Protocol Version 4 (TCP/IPv4) option and set any IP address form 192.168.188.1 to 250 and Gateway of PC to be set as 192.168.188.251 to as shown below.

Fig 1. IP setting in PC connected to AIR-AP3000AX

Important Note: Clear browser history to mitigate cache web pages issue.

Open Browser and give IP address 192.168.188.251.

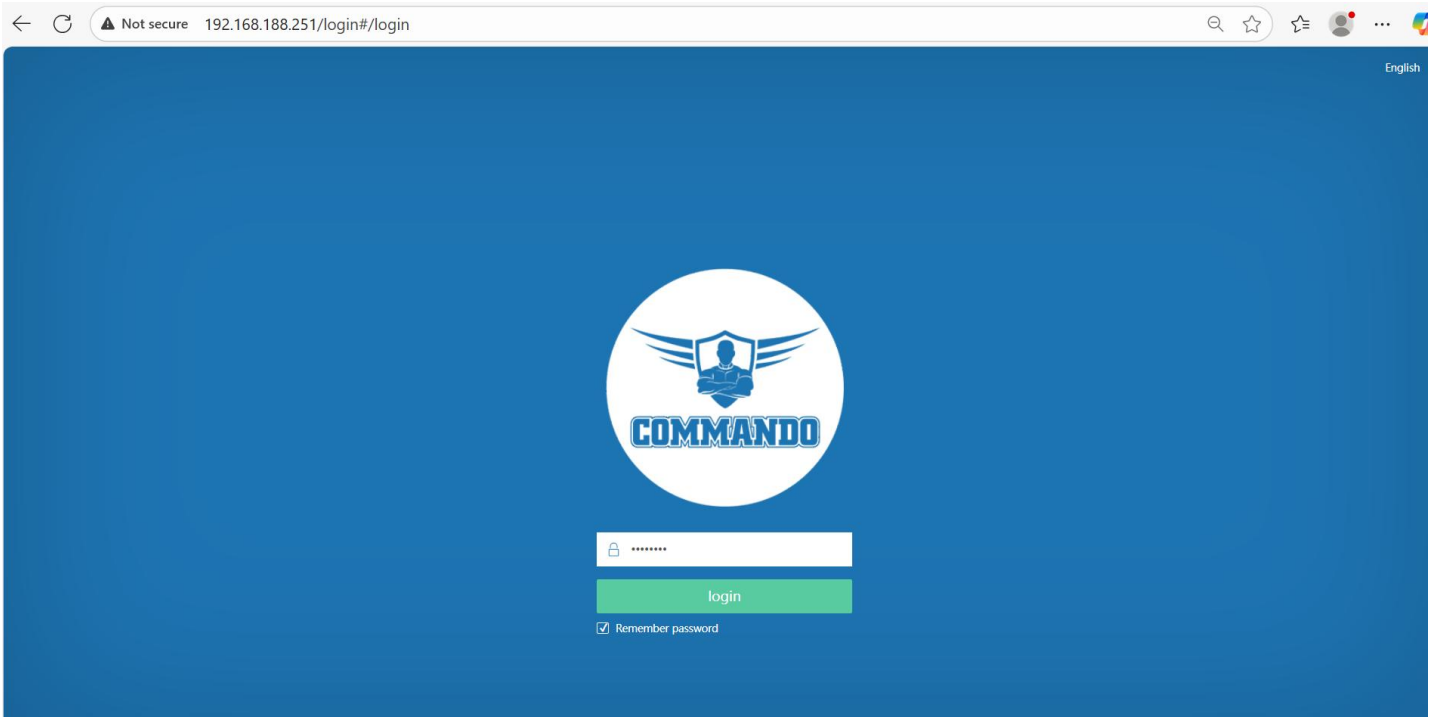


Fig 2. Access page of AIR-AP3000AX

Note: By default password is commando. Please password changed as per user requirement.

2) **Wireless access Via SSID connected to PC.**

Power ON AIR-AP3000AX.
Connect Default SSID named “2.4G_default” or “5G_default” with no default WiFi Password required. It is open to all by default.

Click on properties of connected SSID “2.4G_default” or “5G_default”.

Edit IP setting from DHCP to Manual and set any IP address form 192.168.188.1 to 250 and Gateway of PC to be set as 192.168.188.251 to as shown below.
Note:All Default SSID and password can be changed as per user requirement.

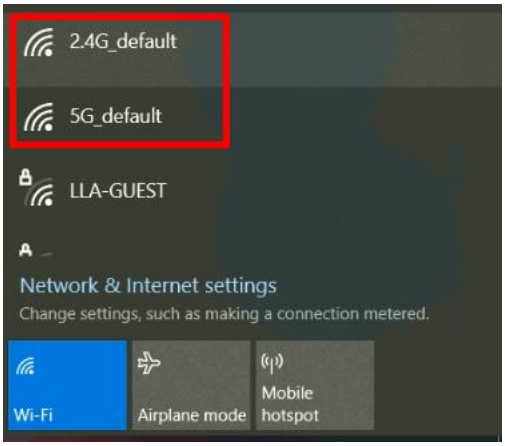


Fig 3. Default Open SSID of AIR-AP3000AX

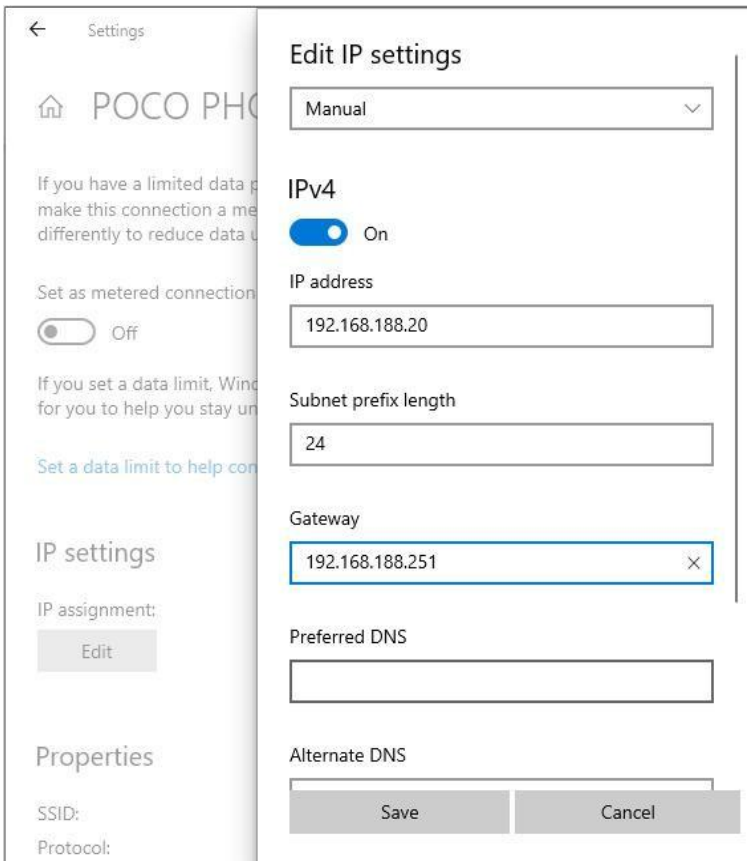


Fig 4. Edit IP setting from DHCP to Manual as shown for 2.4G_default

Open any web browser like Chrome/Firefox/Internet Explorer/Opera etc and enter default IP address 192.168.188.251 in address field.

Caution: If you have already taken any Other COMMANDO wireless device access. Then before

taking access of this device, you are required to clean the browser history to avoid catch pages issue.

Important Note: If you reset it by pressing Reset button to factory reset then access page will come in Chinese language.

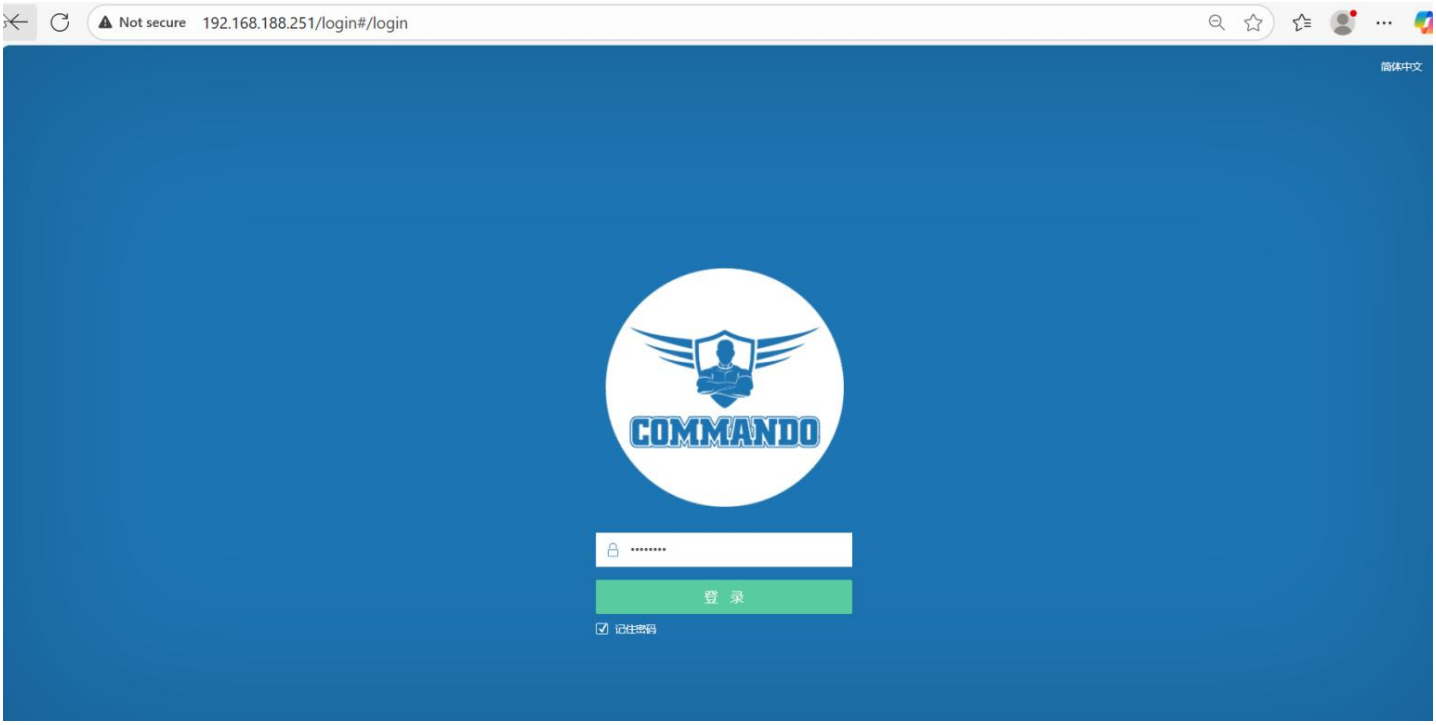


Fig 5. Login page for AIR-AP3000AX Page

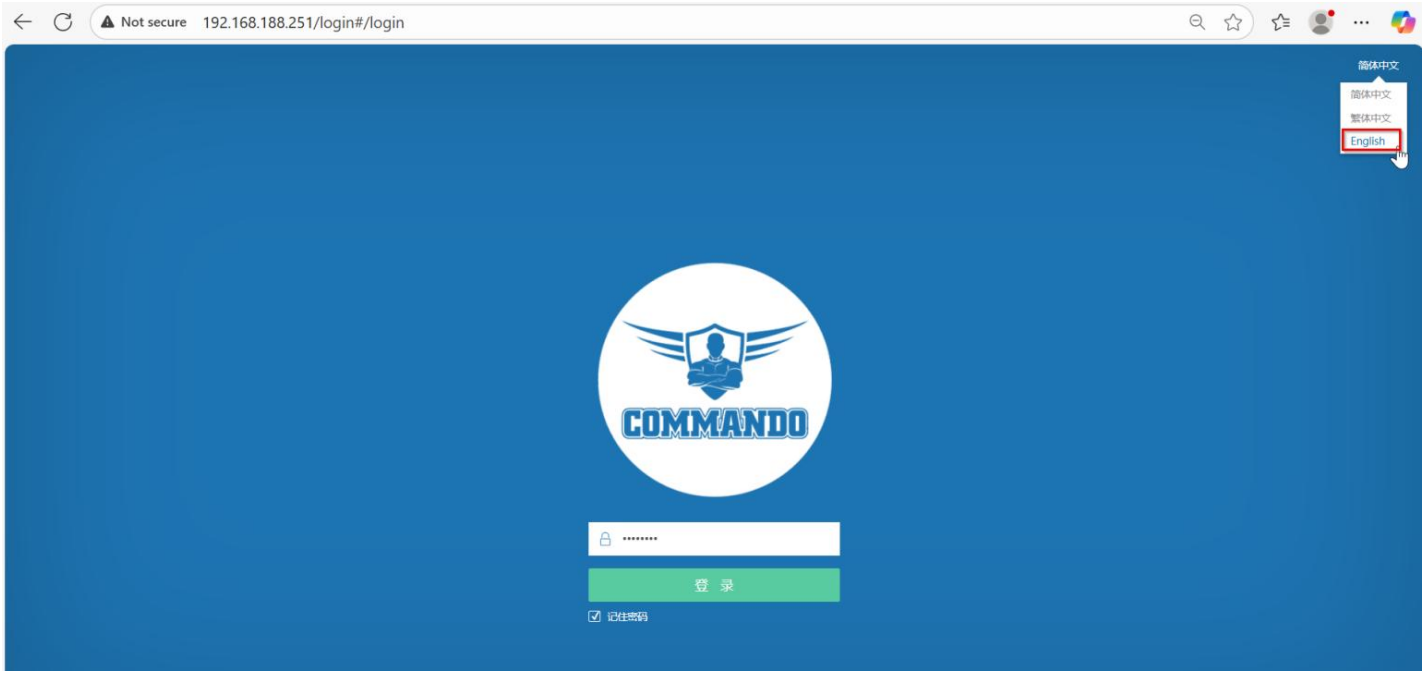


Fig 6. To change Login Language to English for AIR-AP3000AX Page

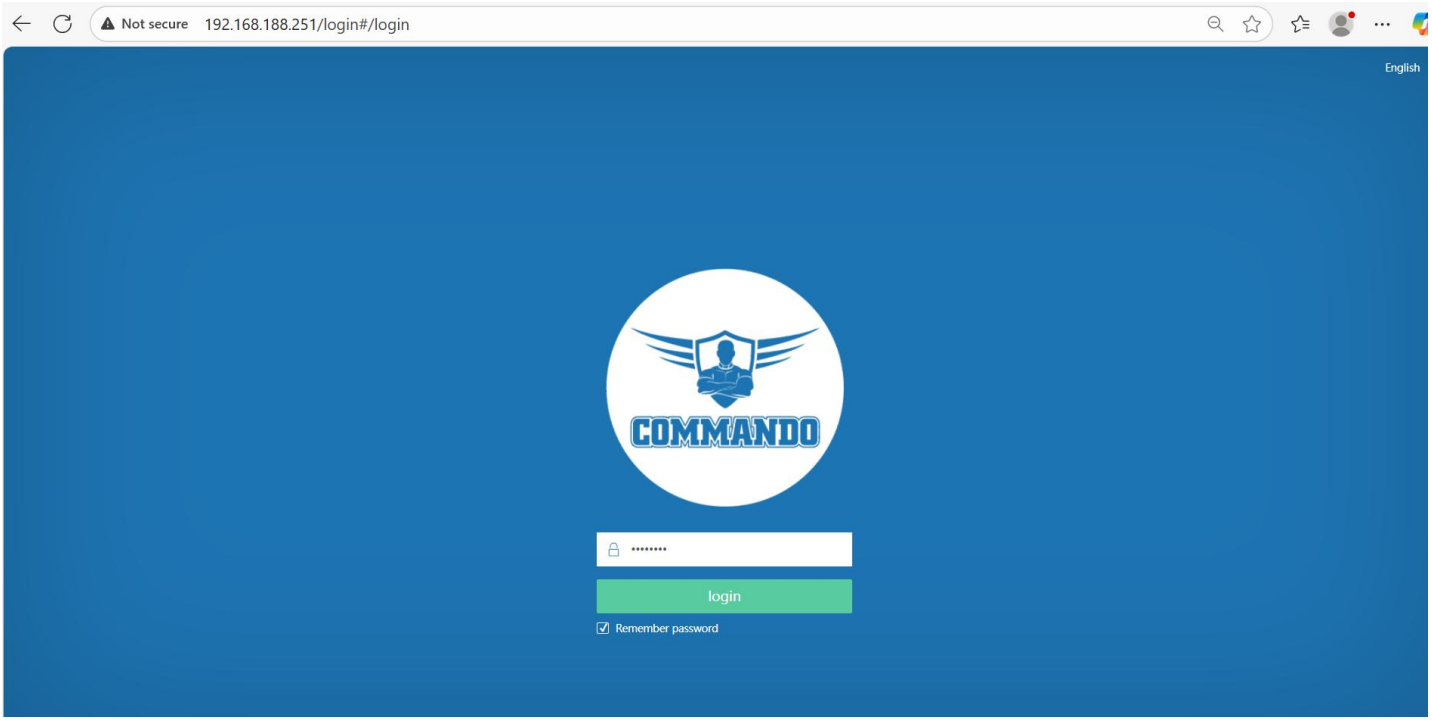


Fig 7. Login for AIR-AP3000AX Page

Note: By default password is commando.
This password can be changed as per user requirement.

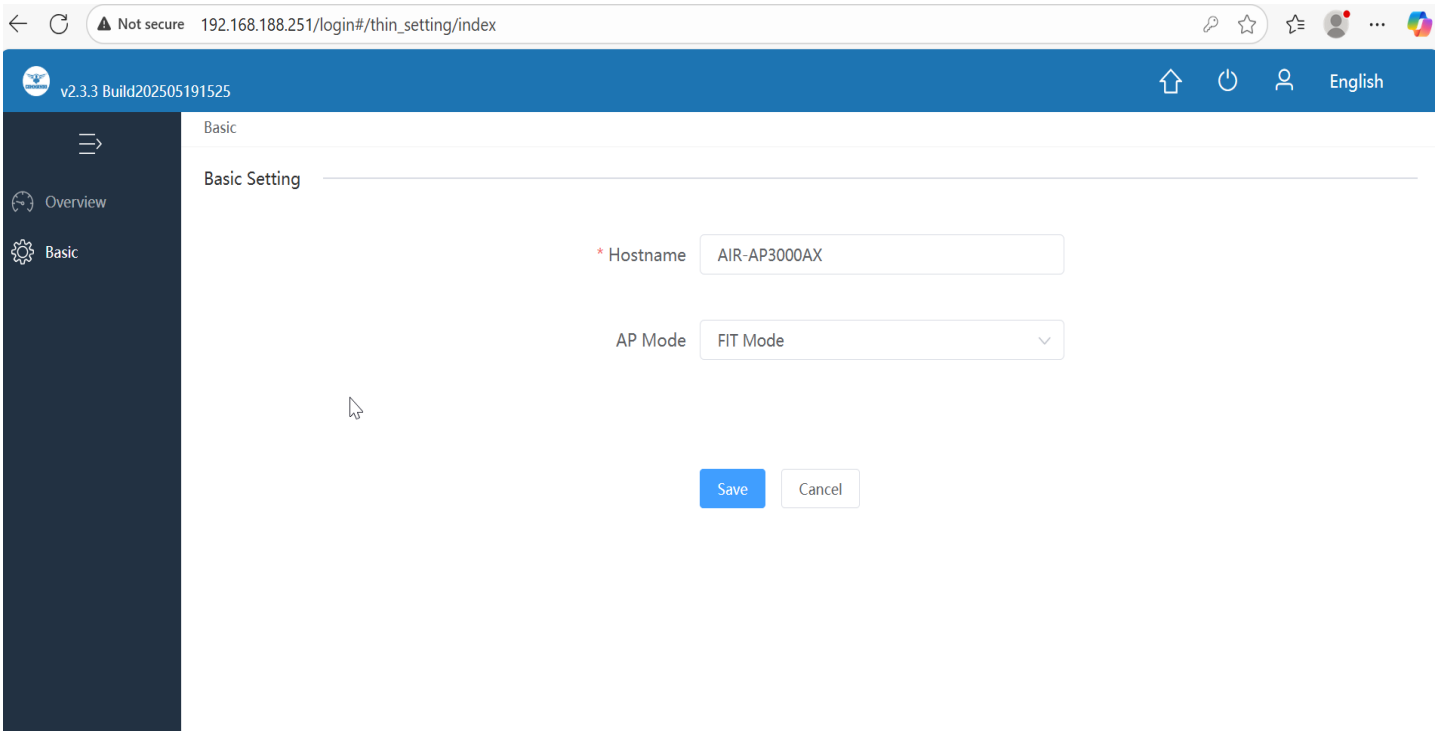


Fig 8. Login page for AIR-AP3000AX Page

After getting this page select mode for operation for AIR-AP3000AX

1. **FIT Mode:** Default mode of operation and works with RouteX Controller.

2. **FAT-Routing mode:** Select this mode to be managed AP to be connected to the AP LAN for management. When using the whole network management function, the AP mode should be switched to FAT-routing mode or FAT-AP mode, and the superior equipment should turn off the AC management function.

3. **FAT-AP mode:** There is no limit to selecting the AP connection interface in this mode. The managed device is set wireless in Wi-Fi settings, and separate SSID setting is not supported.

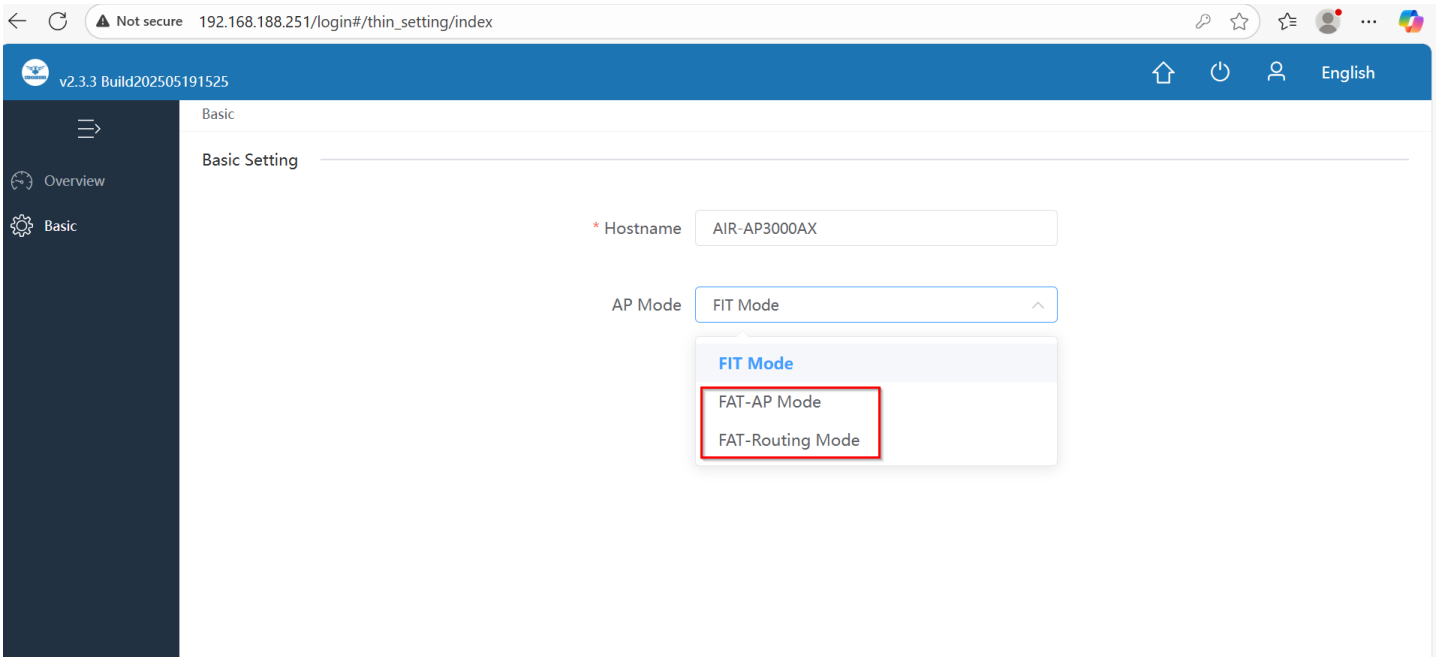


Fig 9. Selection of FAT mode of operation for AIR-AP3000AX Page

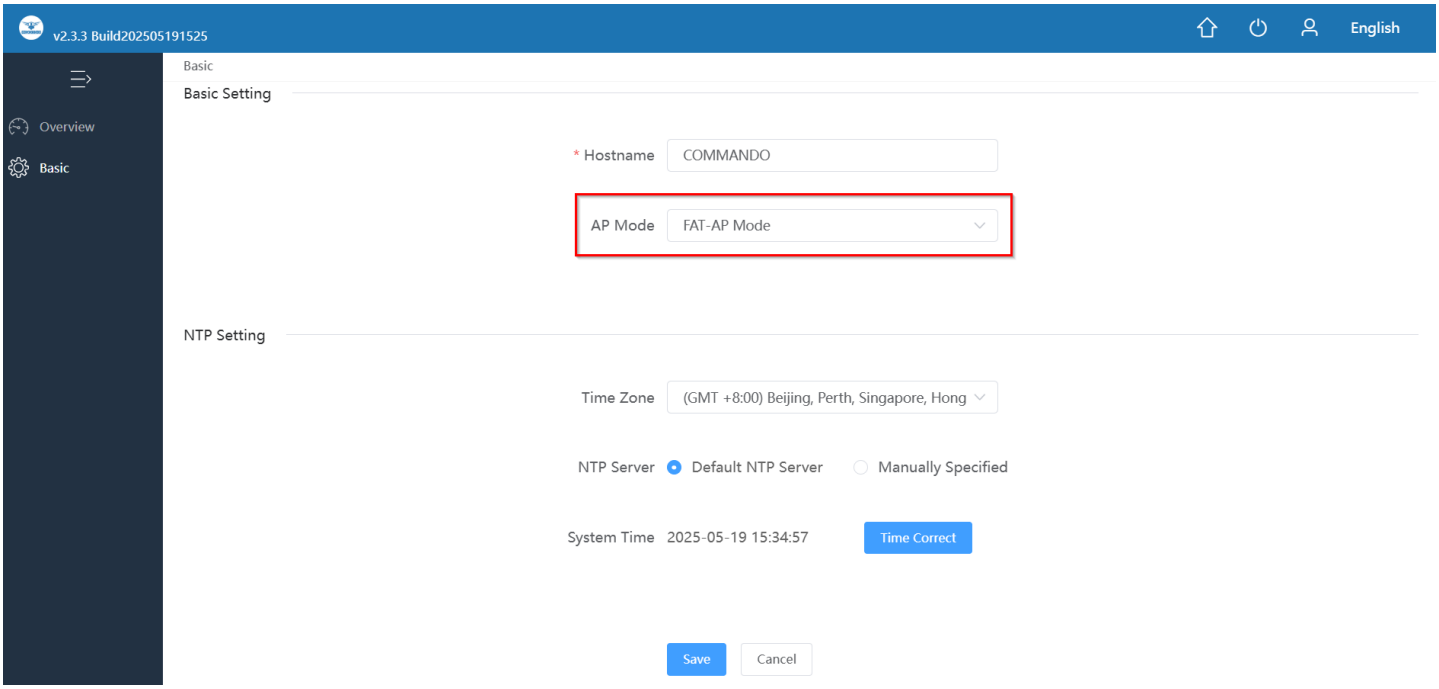


Fig 10. Selected of FAT-AP mode of operation for AIR-AP3000AX Page

After selecting mode save and confirm.

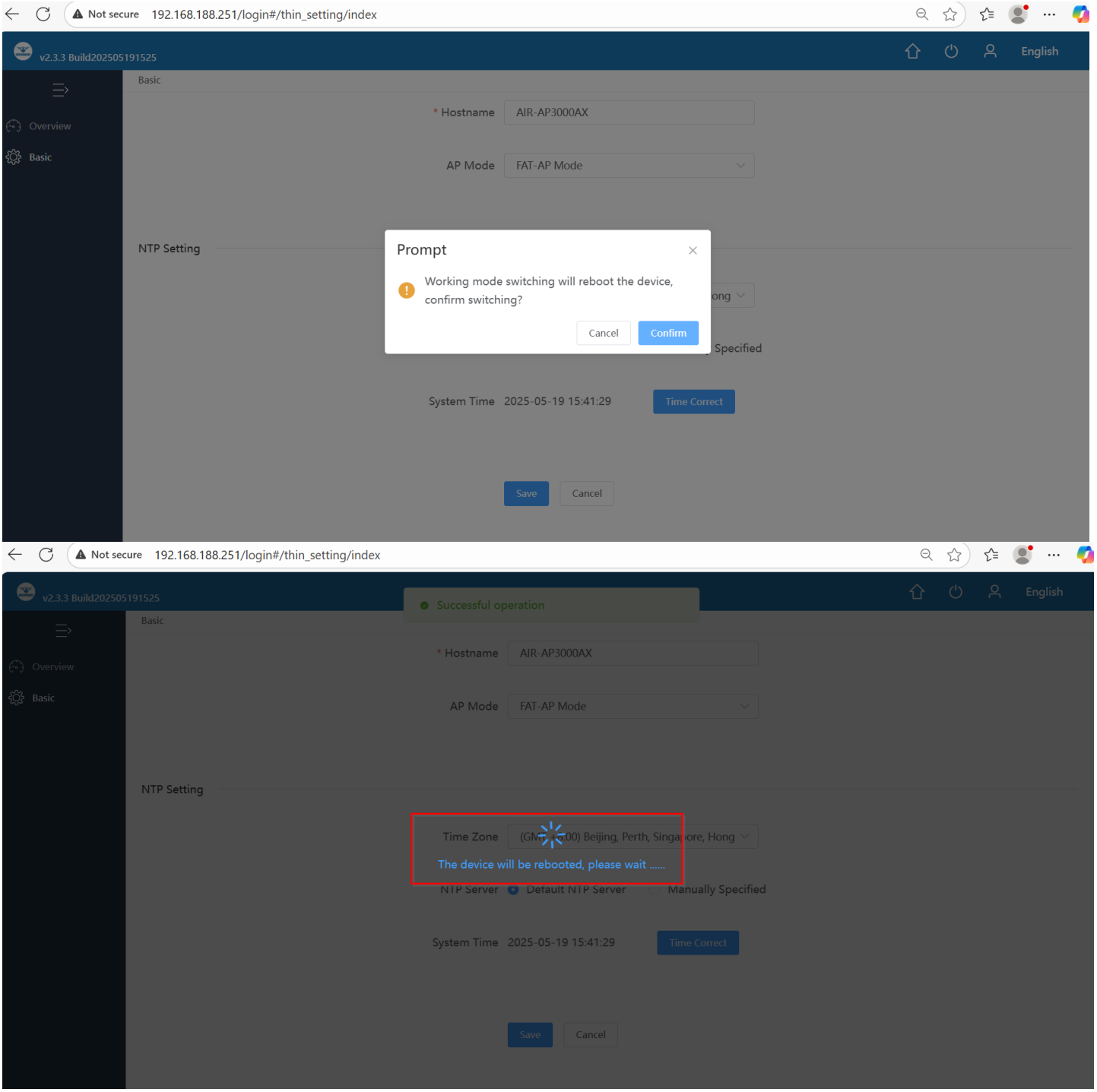


Fig 11. Switching FAT-AP mode of operation for AIR-AP3000AX Page

Note: Enter the Password commando

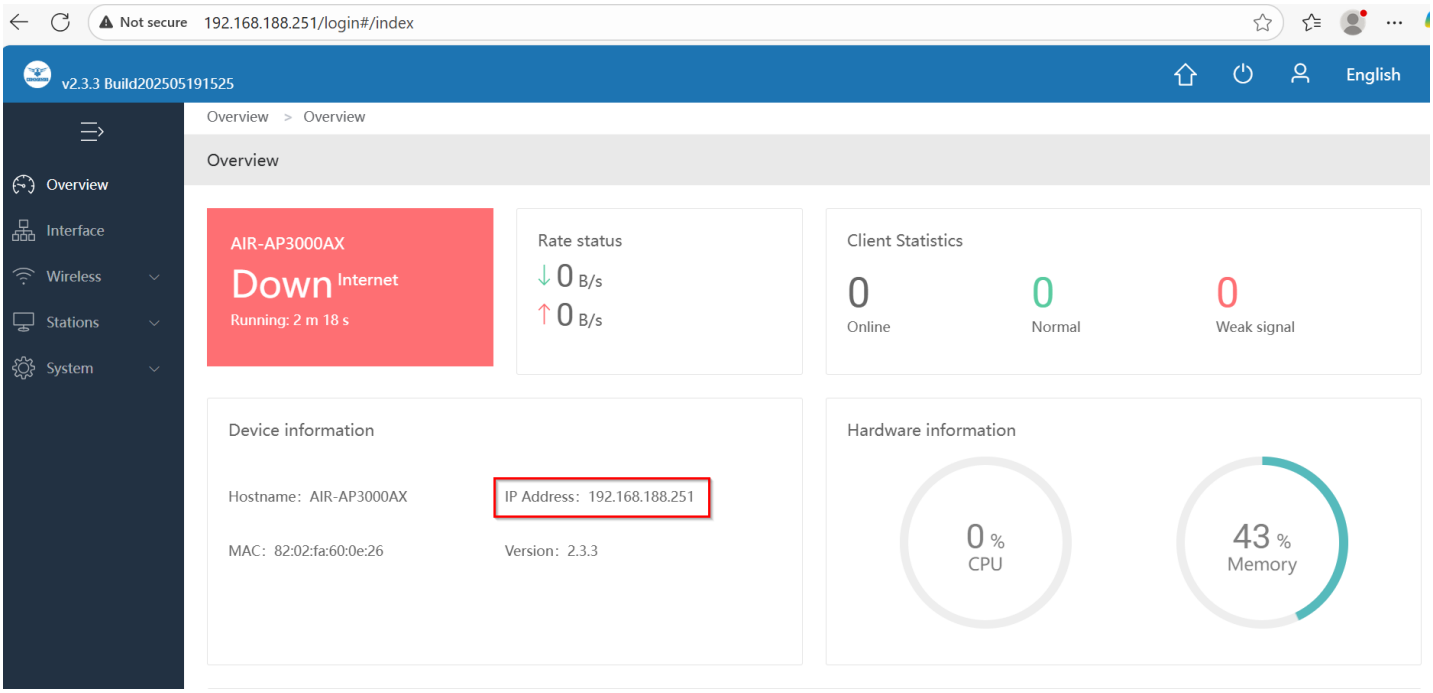


Fig 12. Switching FAT-AP mode of operation for AIR-AP3000AX Page

Very important to understand that if you are connecting WAN with DHCP setting on other router/gateway/ device then the default IP 192.168.188.251 will be changed to IP got from DHCP server due to following default setting in COMMANDO AP.

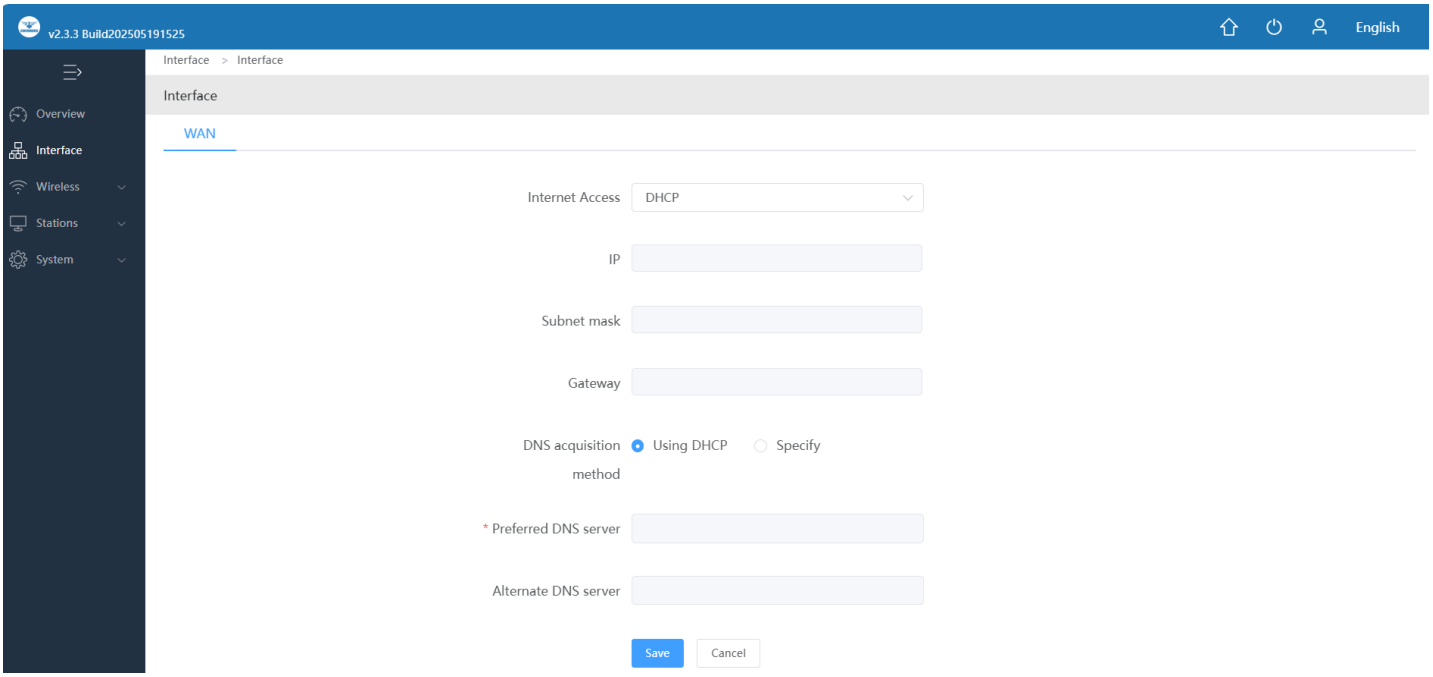


Fig 13. WAN setting in FAT-AP mode of operation for AIR-AP3000AX Page

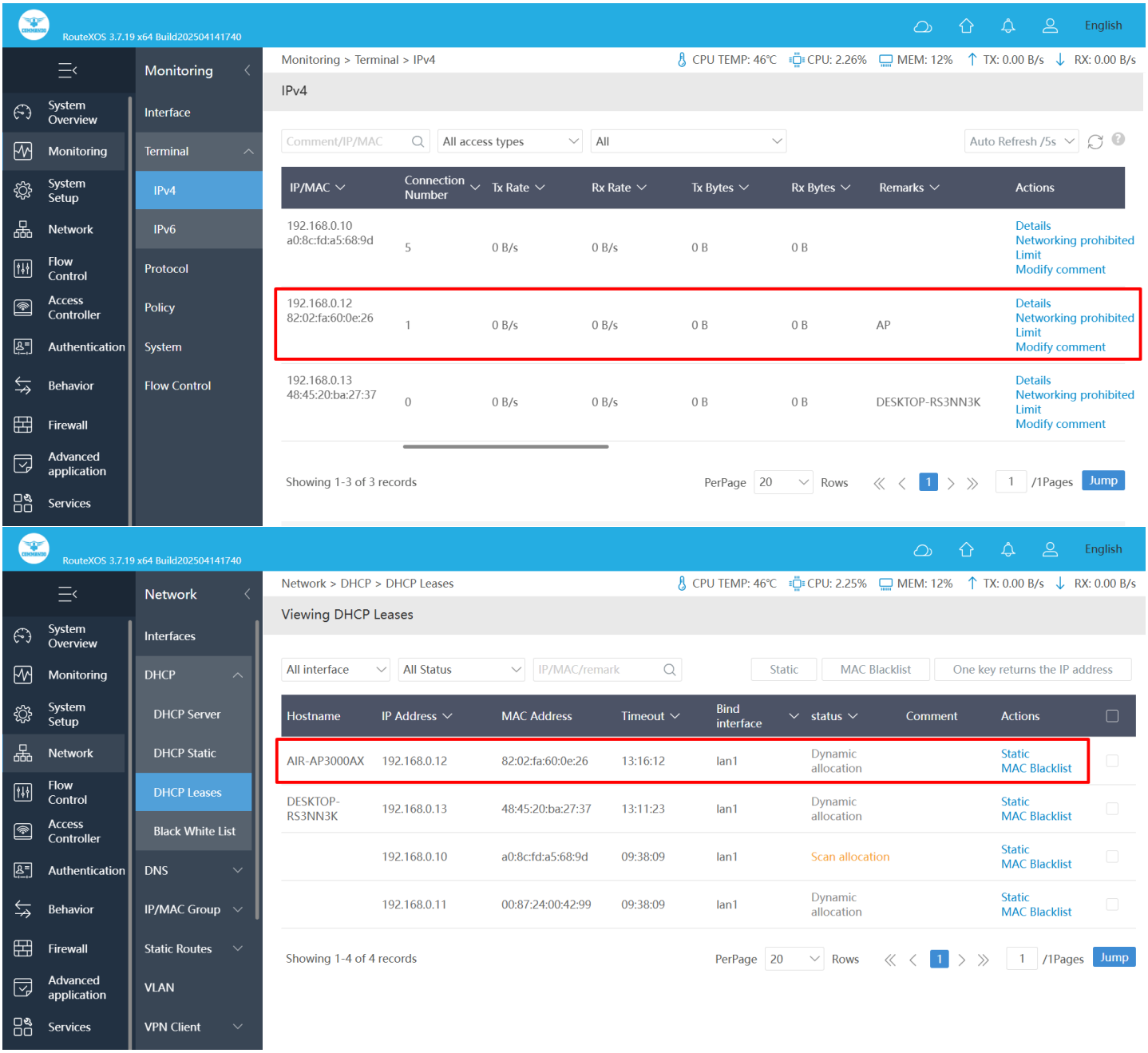


Fig 14. New IP for WAN from DHCP Page

Now this default IP 192.168.188.251 will not work and taken over by new IP 192.168.0.12 provided by DHCP server providing internet.

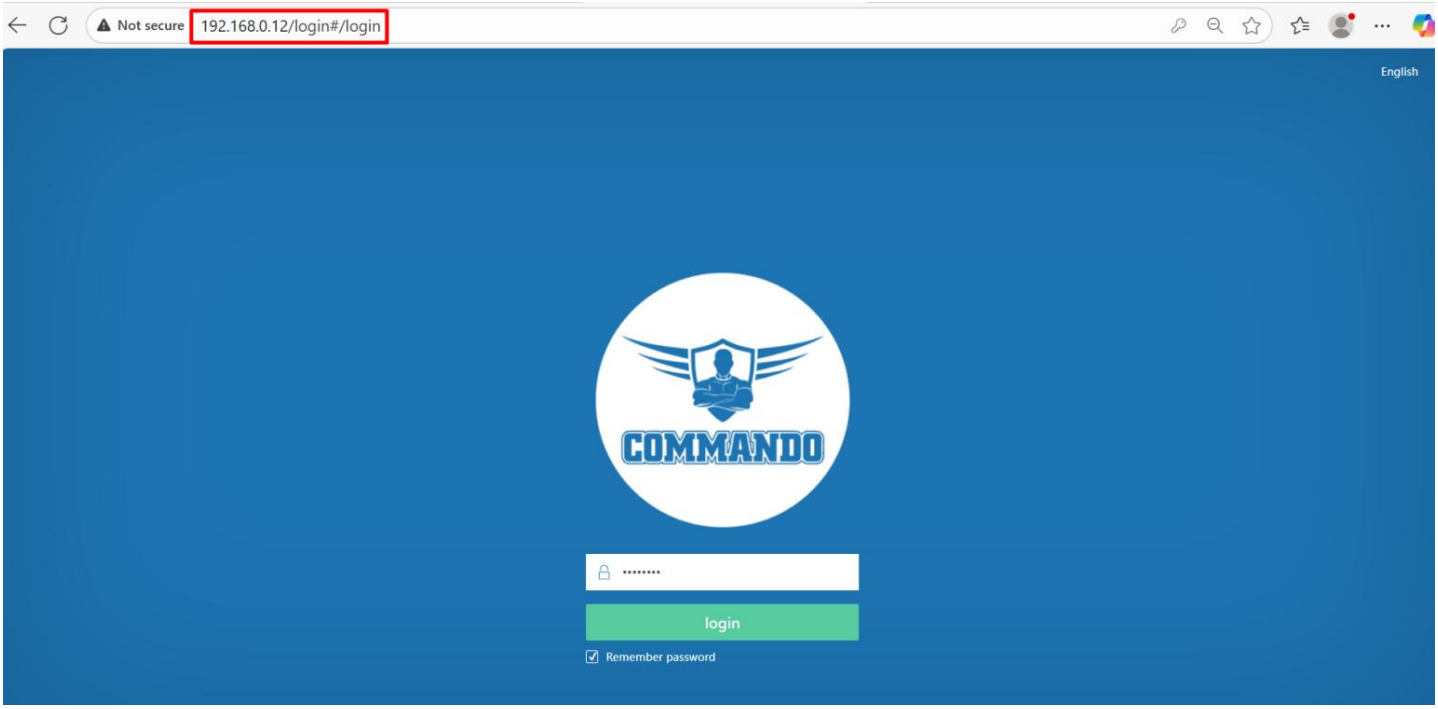


Fig 15. New DHCP IP on WAN port access page AIR-AP3000AX Page

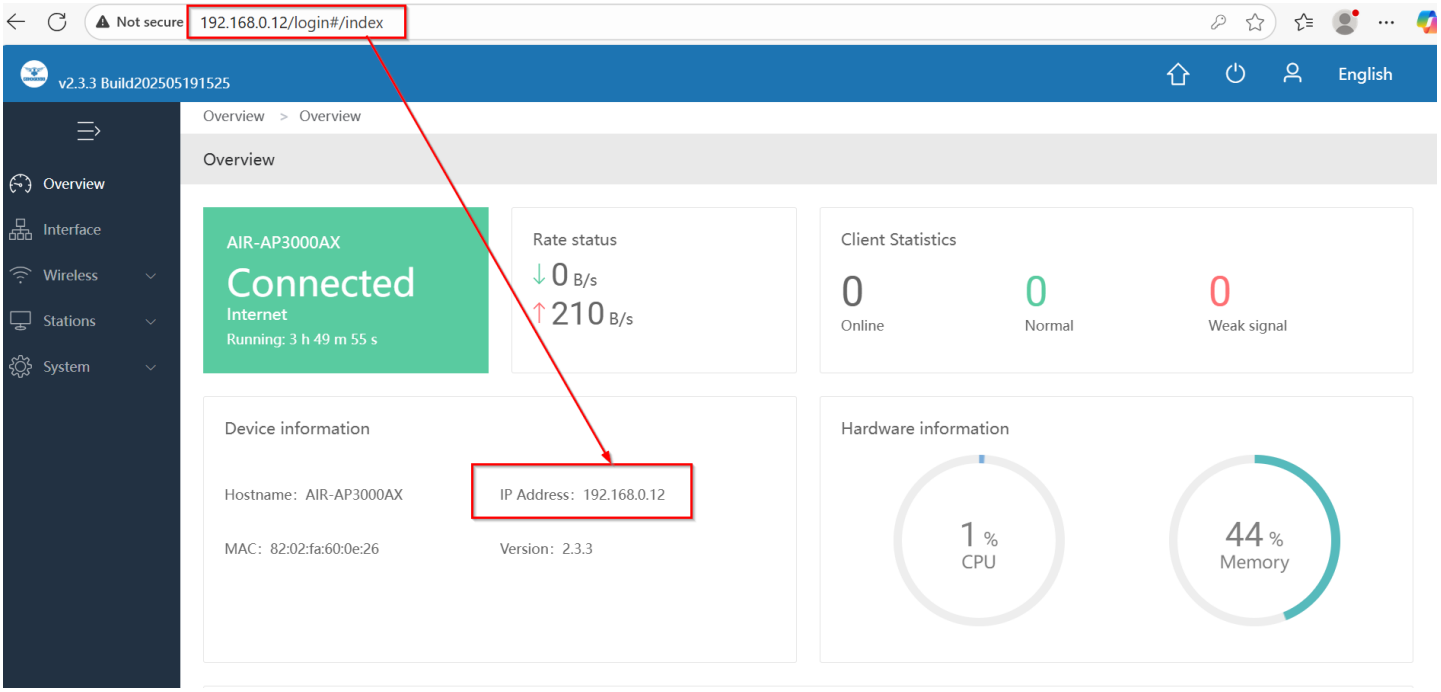


Fig 16. Access of AIR-AP3000AX Page

Common issues faced While access of AP3000AX access of device. This is due to Web page Browsing history issue.

Problem faced Ex-1: After changing the mode to FAT AP menu not shown.

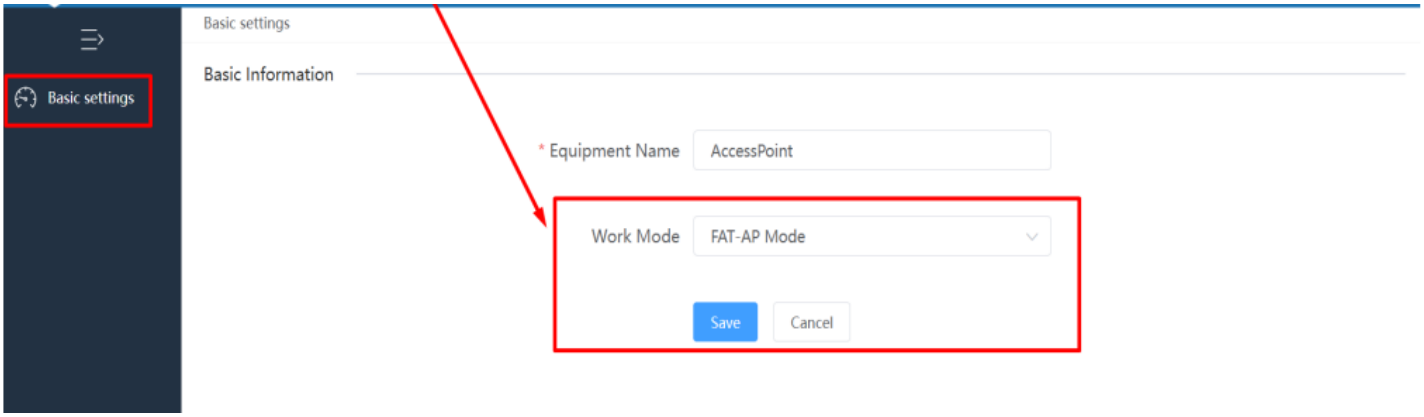


Fig 17. Access of AIR-AP3000AX in FAT AP mode browsing history error Page

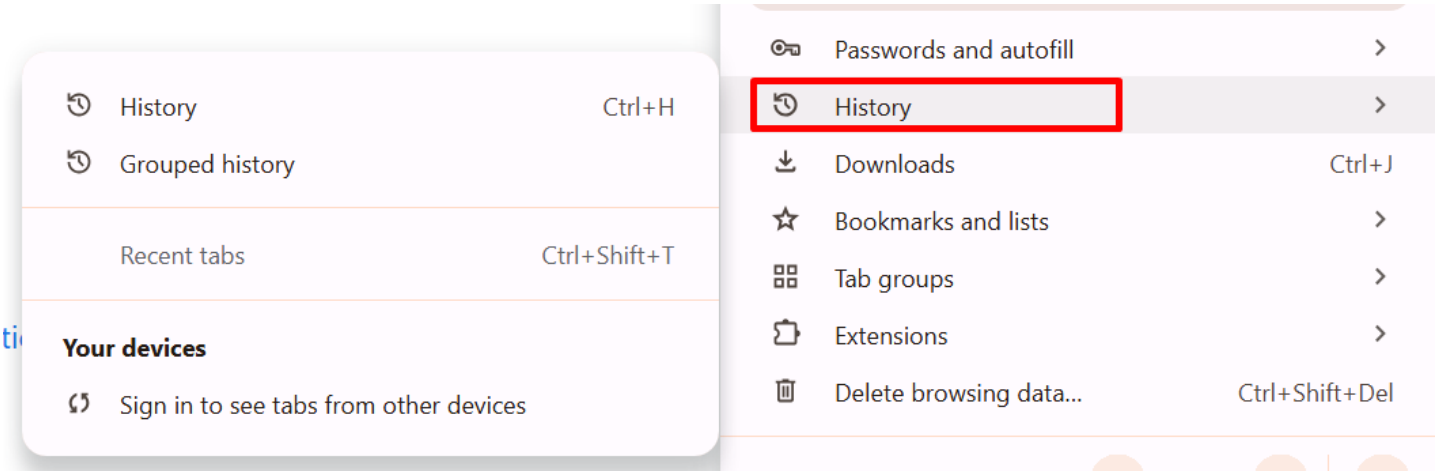


Fig 18. History of Web pages error Page

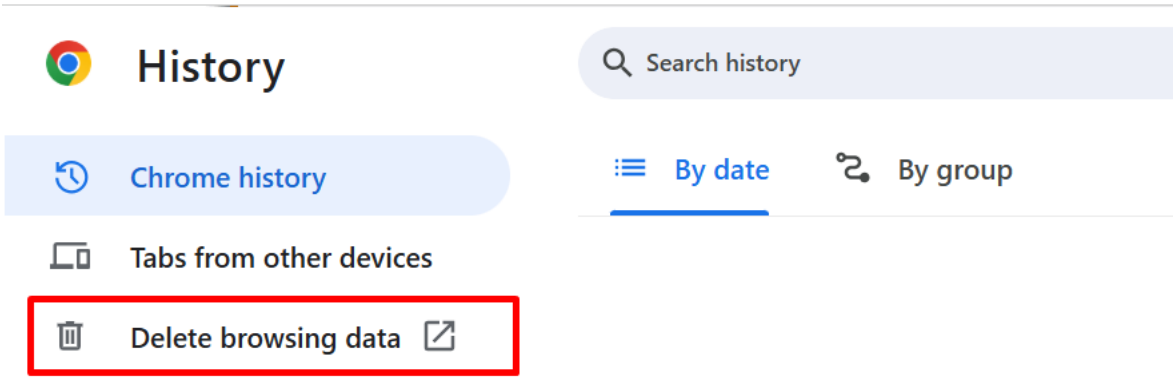


Fig 19. Delete History of Web pages for all times Page

1. System overview

After login, System overview page will be showed. This page will show Information like WAN connection status, number of user connected, Device name, IP address to access, firmware, hardware like CPU and memory status, RF channel and bandwidth in 2G/5G Wi-Fi along with interface information can help to troubleshoot network issue, if any very easily.

For System overview page click on System overview to display page information.

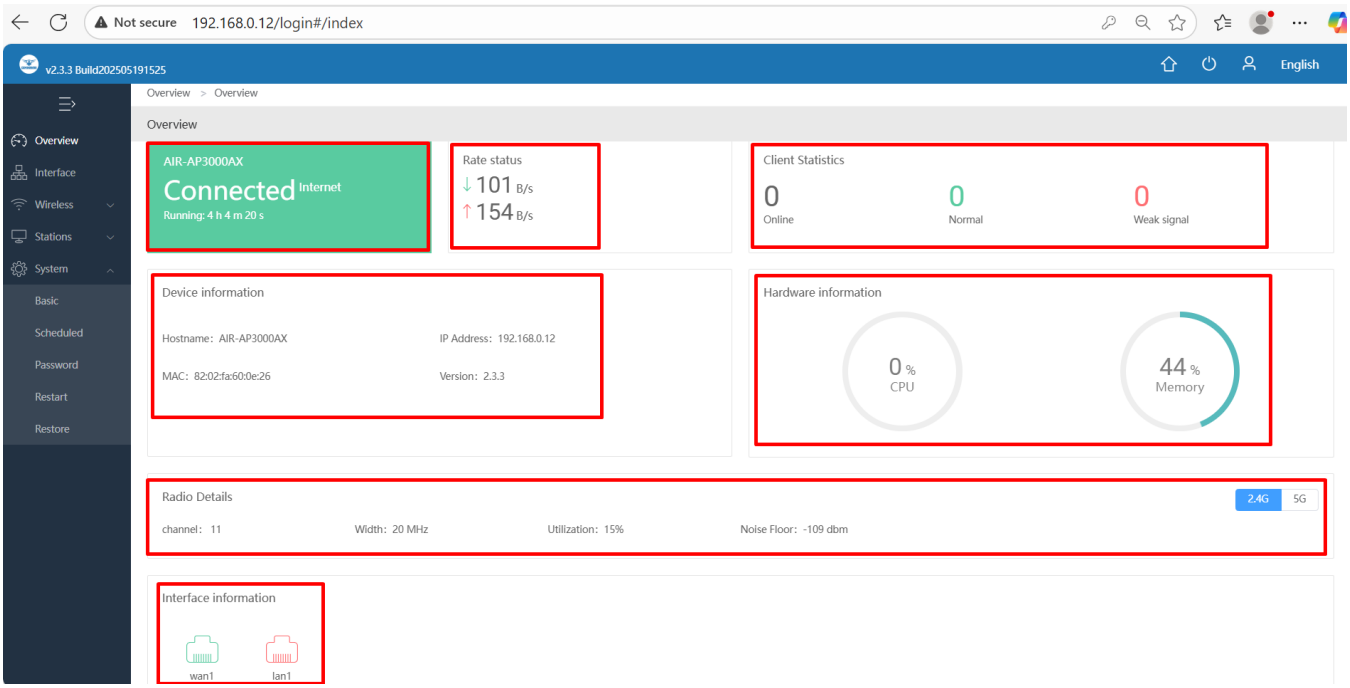


Fig 1.1 Home page Components of AIR-AP3000AX Page

Configuration with icons

On right corner there are easy to configure icons which allows to upgrade, device reboot, Reset to factory default, passwords and sign out along with Language setting for display pages.

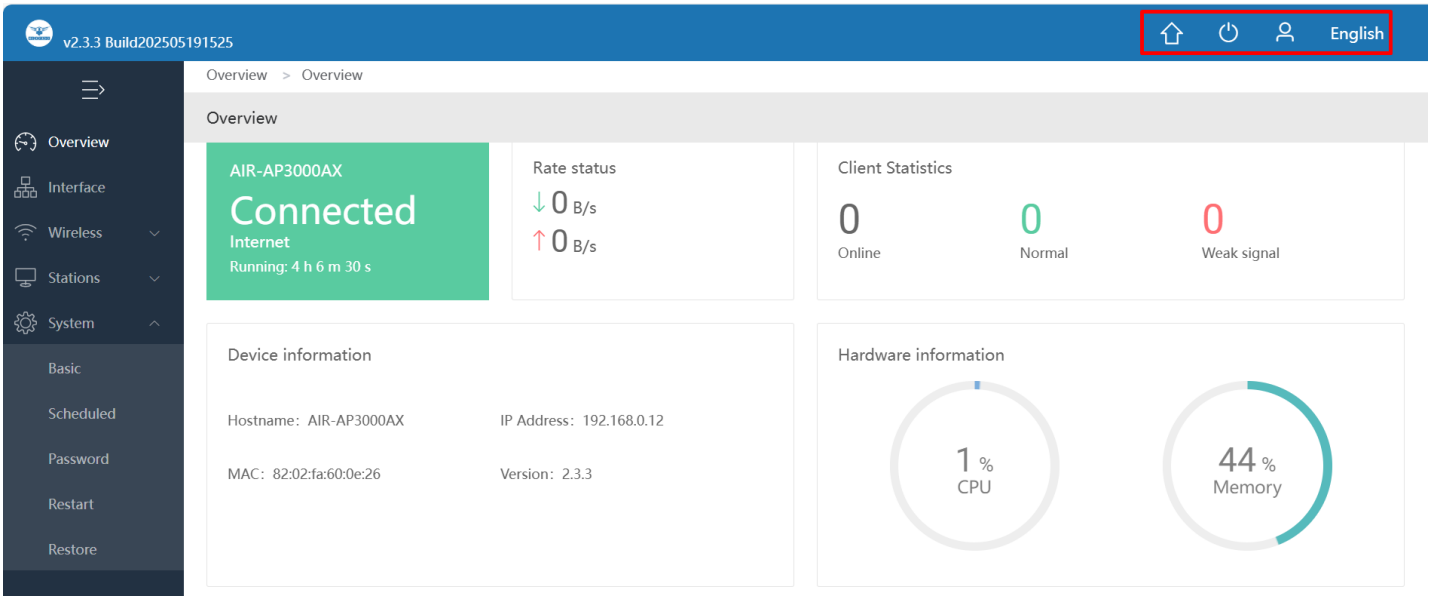


Fig 1.2 Configuration with icons in AIR-AP3000AX Page

Version Upgrade:

Displays the current configuration version of the AP and allows Automatic Updates.

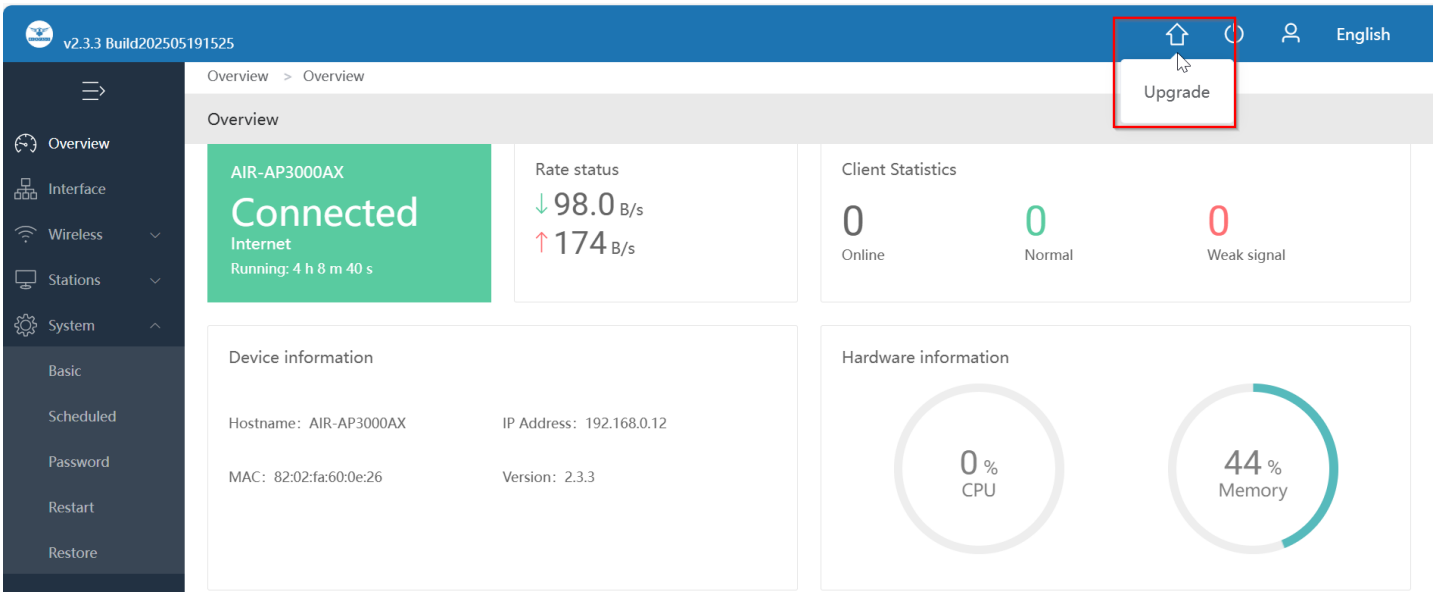


Fig 1.3 Upgrade icons in AIR-AP3000AX Page

Upgrade Version: Displays the current Configuration version is latest or not and Auto Upgrade option you can upgrade firmware to get more functions and better performance.

Note:

1. After upgrading, the device will reboot automatically.
2. To avoid damage to device, please don't turn off the device while upgrading.
3. It is advised to backup the configuration before upgrading.

For Version upgrade click on upgrade icons.

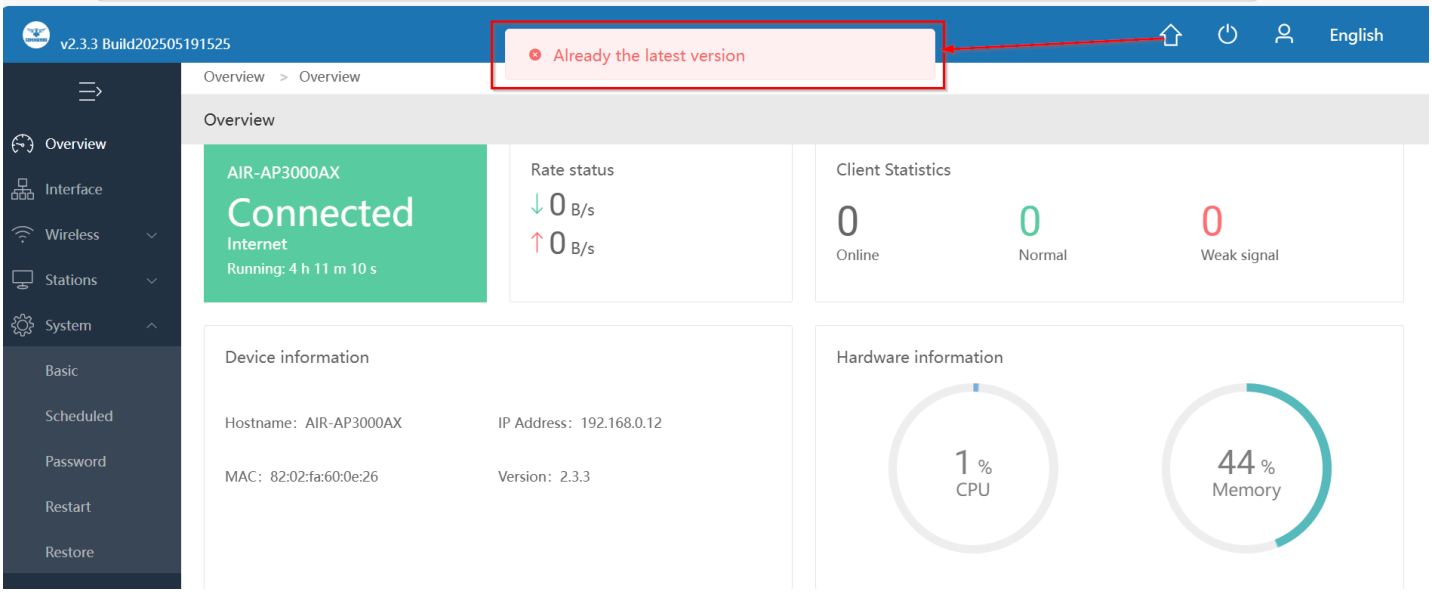


Fig 1.4 Version Checking in AIR-AP3000AX Page

Reboot / Reset to factory default Icon:

The configuration will not be lost after rebooting. The Internet connection will be temporarily interrupted while rebooting.

For Reboot, Click on Device reboot

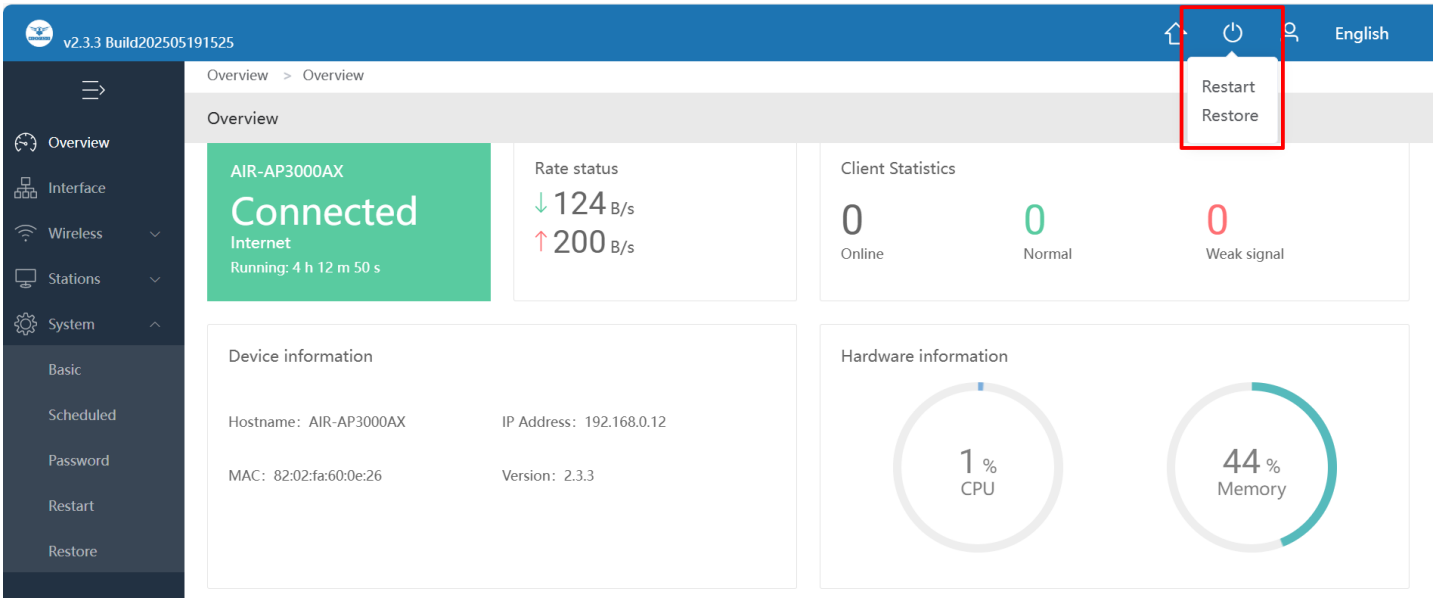


Fig 1.5 Device restart and Restore option in AIR-AP3000AX Page

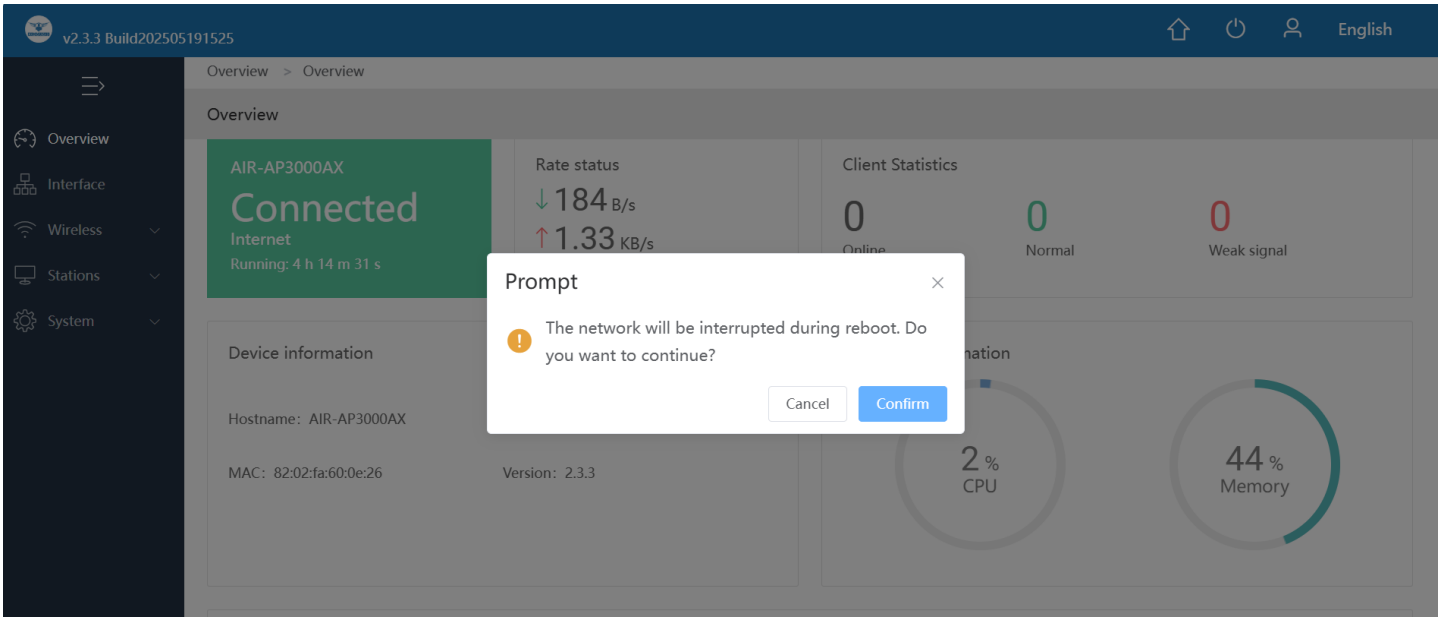


Fig 1.6 Restart option in AIR-AP3000AX Page

Restore Factory

Restore configuration feature allow end users to reset the AP to factory default settings, You can restore the AP to its factory default settings by the Reset button or by factory reset option in this page. It must be noted that once the AP is reset, all the current configuration settings will be lost.

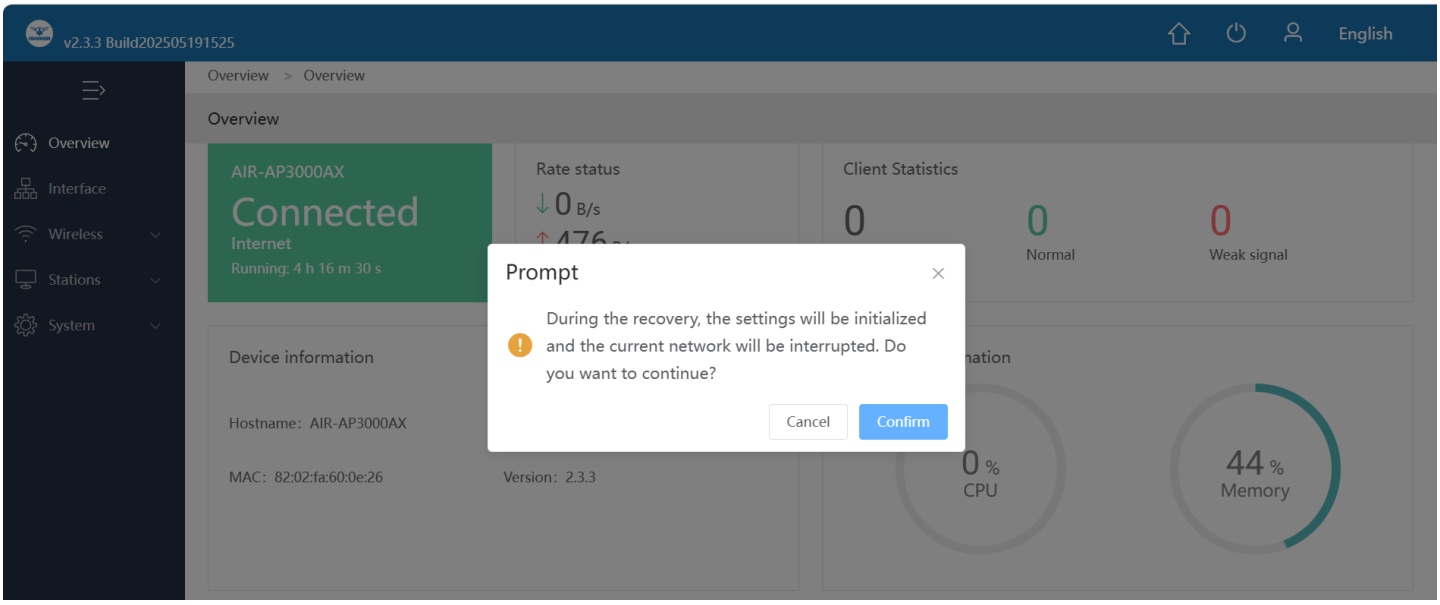


Fig 1.7 Reset option in AIR-AP3000AX Page

Password Setting:

On this page, you can modify the factory default username of the AP and create multiple new password

Note:

The factory default password is commando.

You can modify default password. The Password length minimum 8 and maximum 64 characters, and can contain letters, numbers, special symbols as per user. All the fields are case-sensitive.

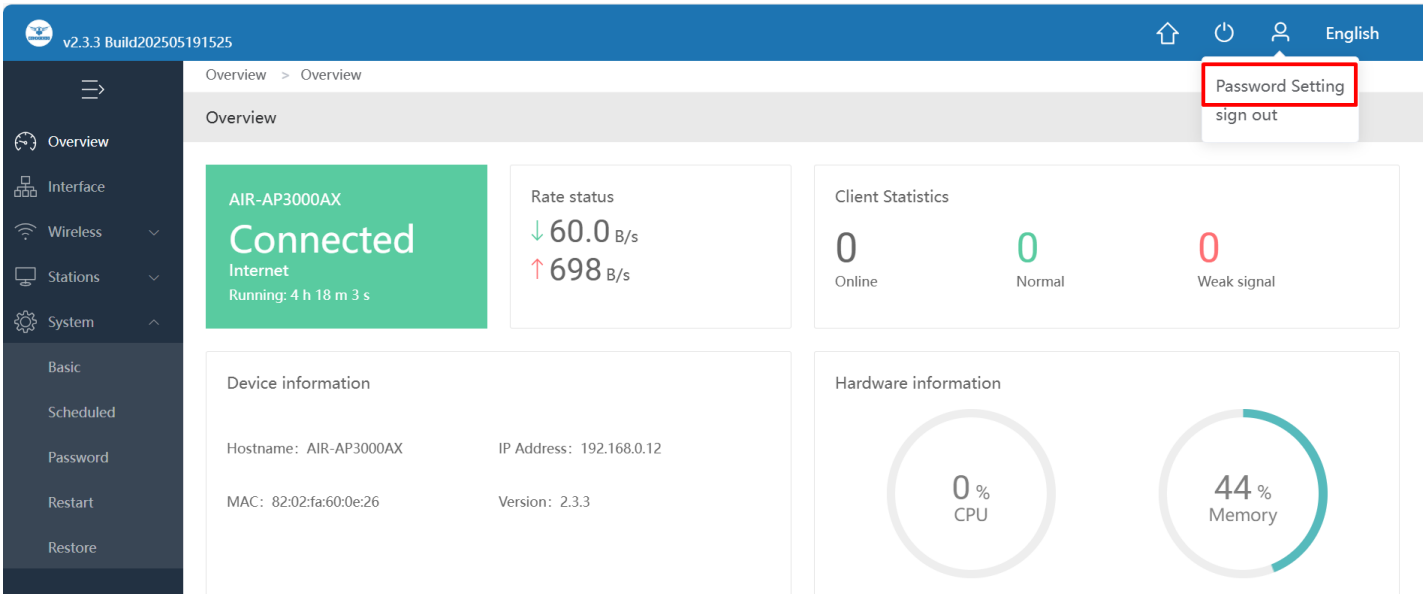


Fig 1.8 Password Setting option in AIR-AP3000AX Page

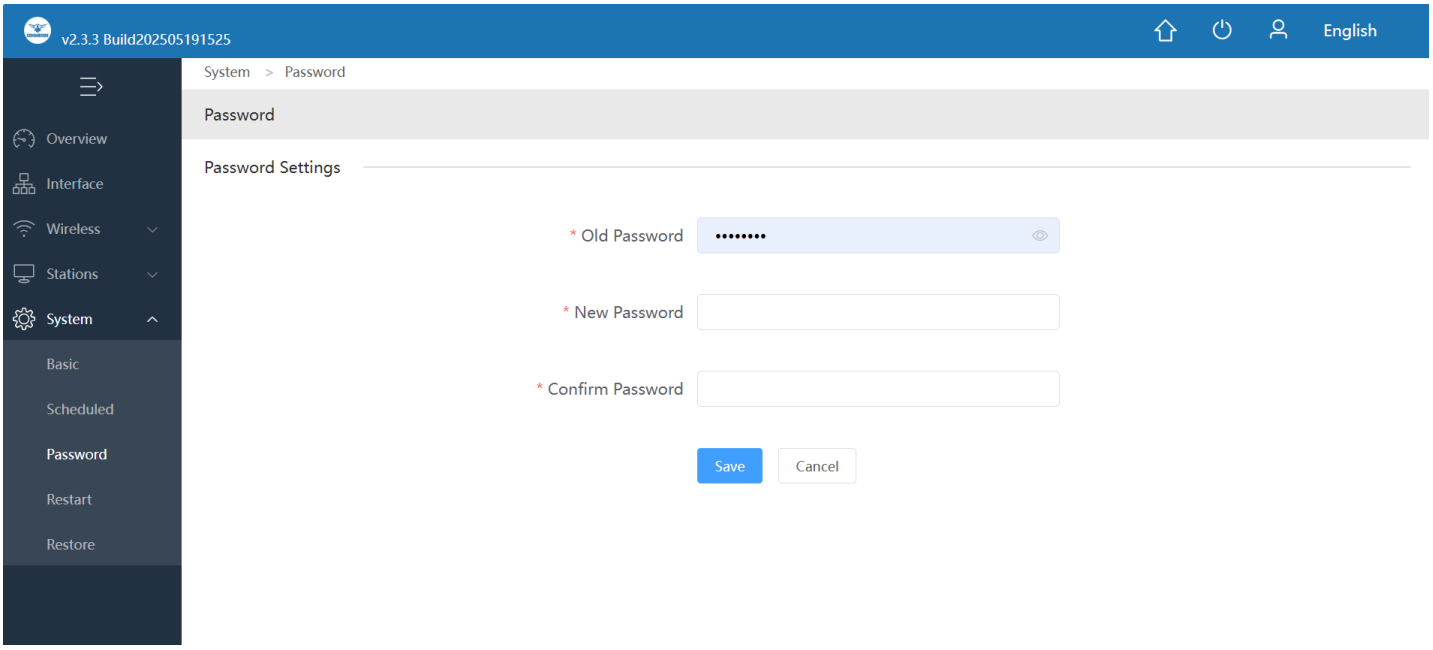


Fig 1.9 Login Setting option in AIR-AP3000AX Page

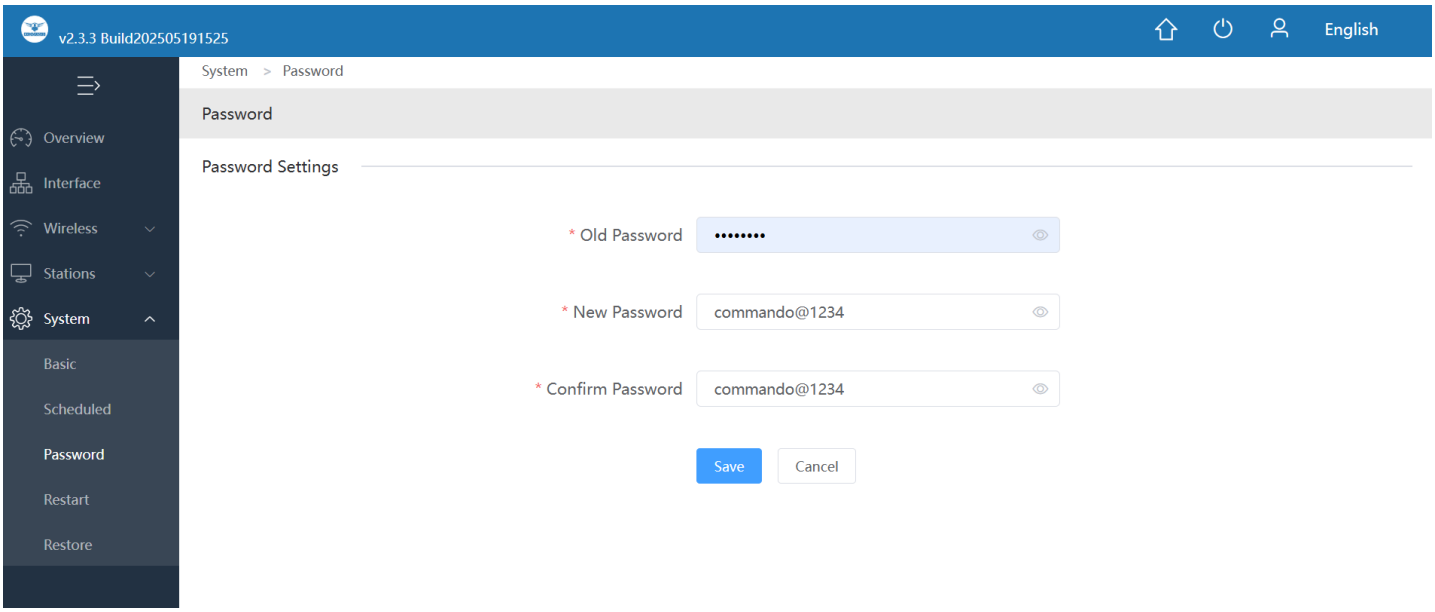


Fig 1.10 Login Setting as per user in AIR-AP3000AX Page

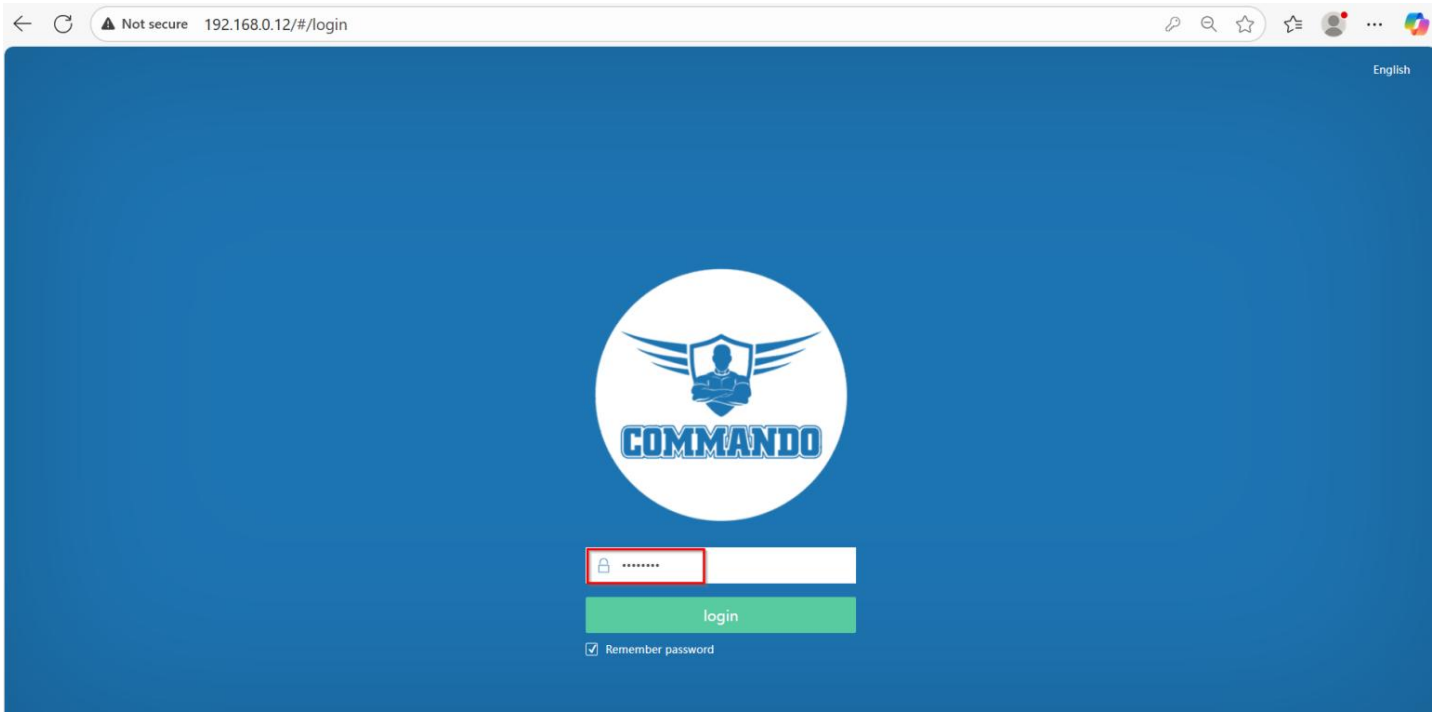


Fig 1.11 Login Setting as per new password in AIR-AP3000AX Page

Sign Out:

Sign out means to end access of device. Sign out informs the device that the current user wishes to end the login session. After Clicking Sign Out, it will be directed to Login page.

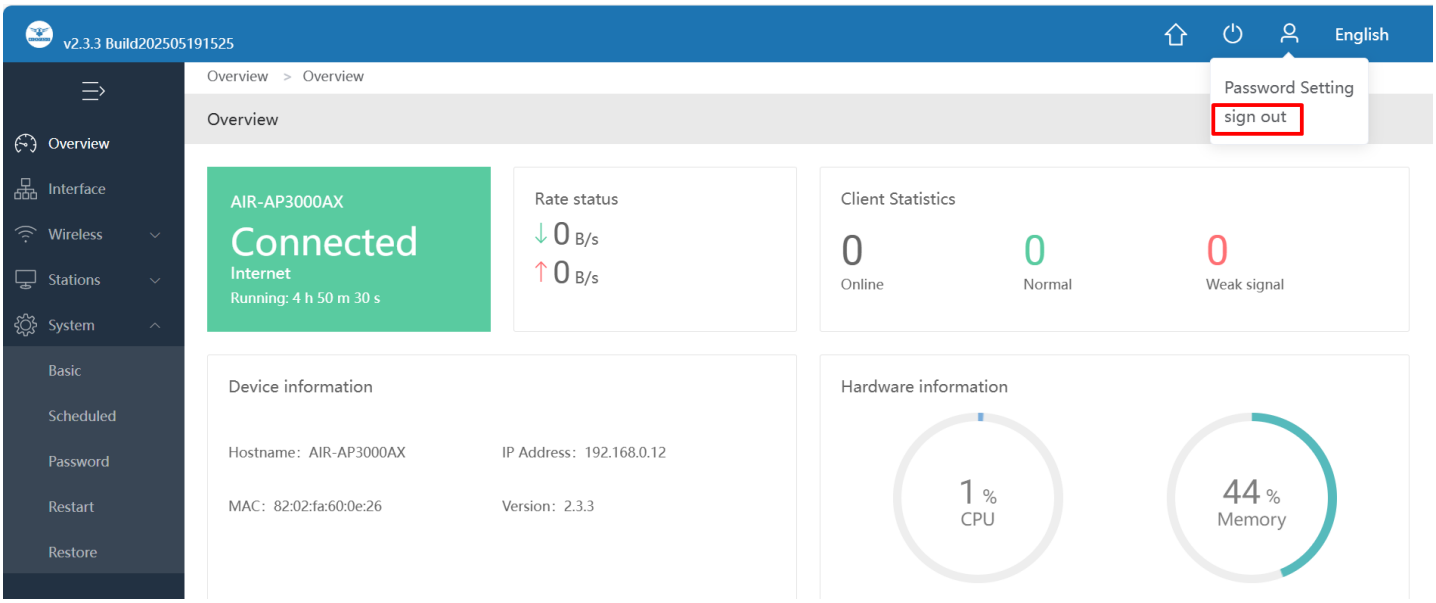


Fig 1.12 Sign Out Setting in AIR-AP3000AX Page

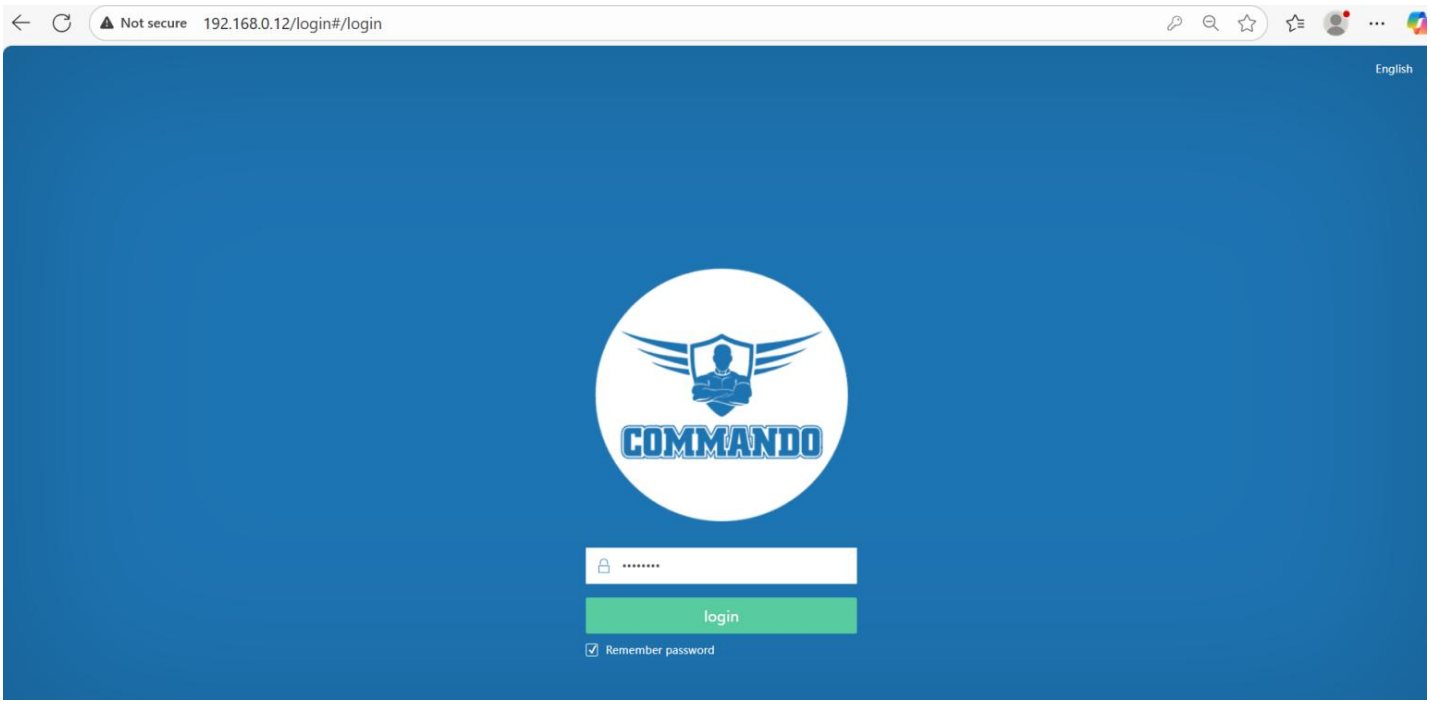


Fig 1.13 After Sign out AIR-AP3000AX Page

Language Options:

Helps to select language as per choice of user.

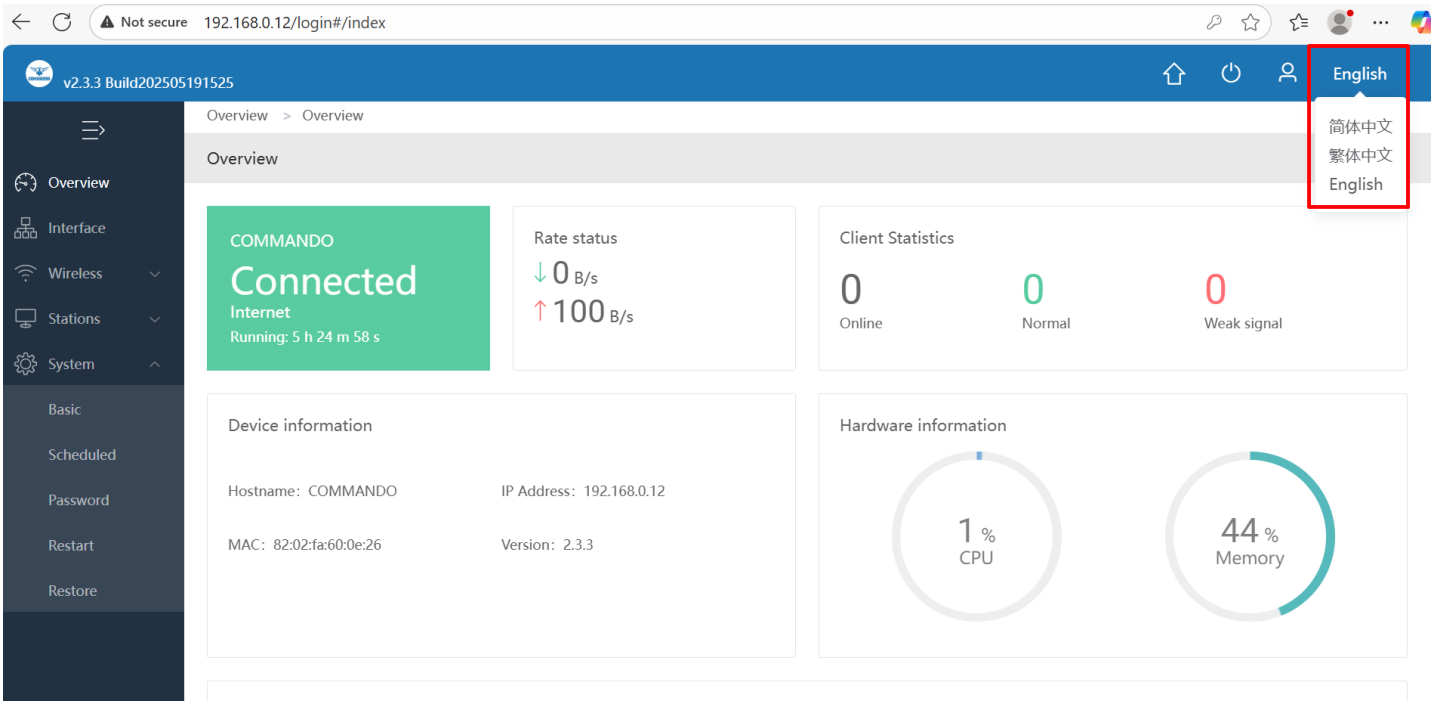


Fig 1.14 Language Option in AIR-AP3000AX Page

Note: Default language setting is English. After Factory reset Default language is Chinese which can be changed to English.

1.1 WAN Information

In WAN Information of AP, Status of WAN connection along with device name, uptime and the Rate status in bits/second is displayed of the AP is shown.

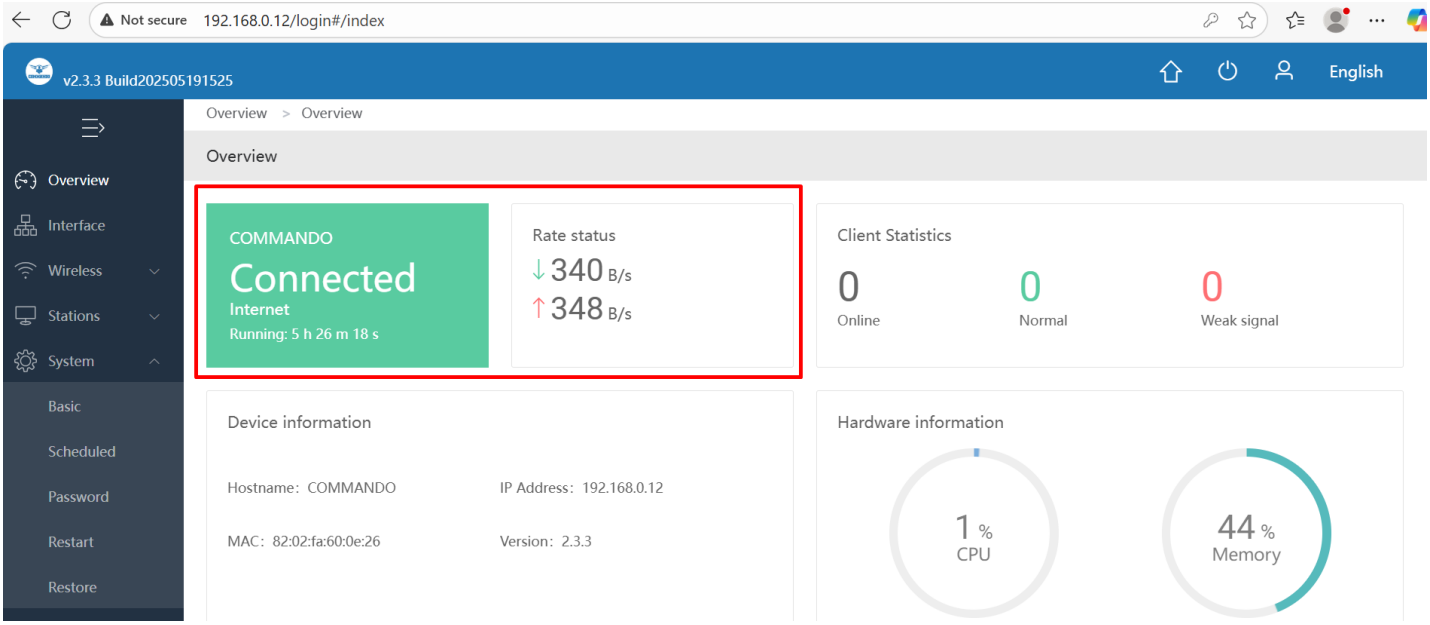


Fig 1.1.1 WAN Status of AIR-AP3000AX

1.2 User Information

You can view User Information like how many wireless clients and their categories like Online user with Normal range or weak signal users which are connected to AP.

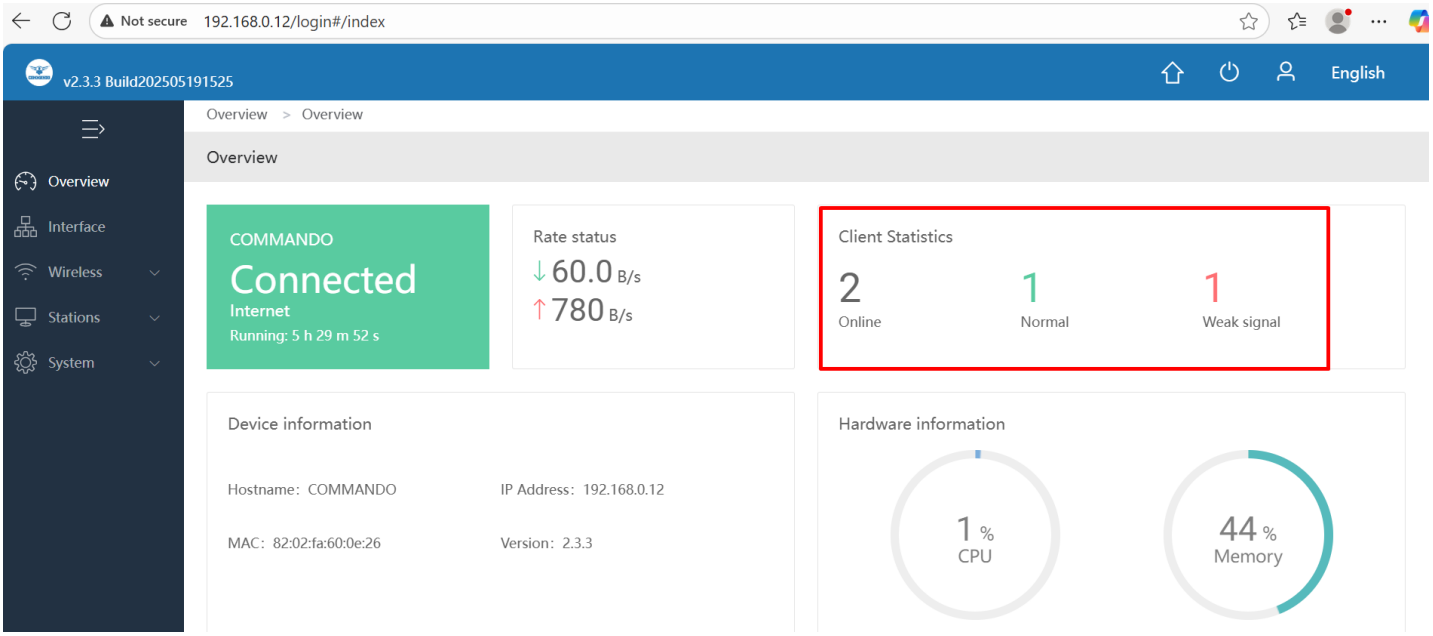


Fig 1.1.2 Device Description of AIR-AP3000AX

1.3 Device Information

Device information show Equipment name default Equipment name is COMMANDO, Device model name AIR-AP3000AX, current IP address by default 192.168.188.251 can change as per user requirement and also device MAC address along with software current firmware version.

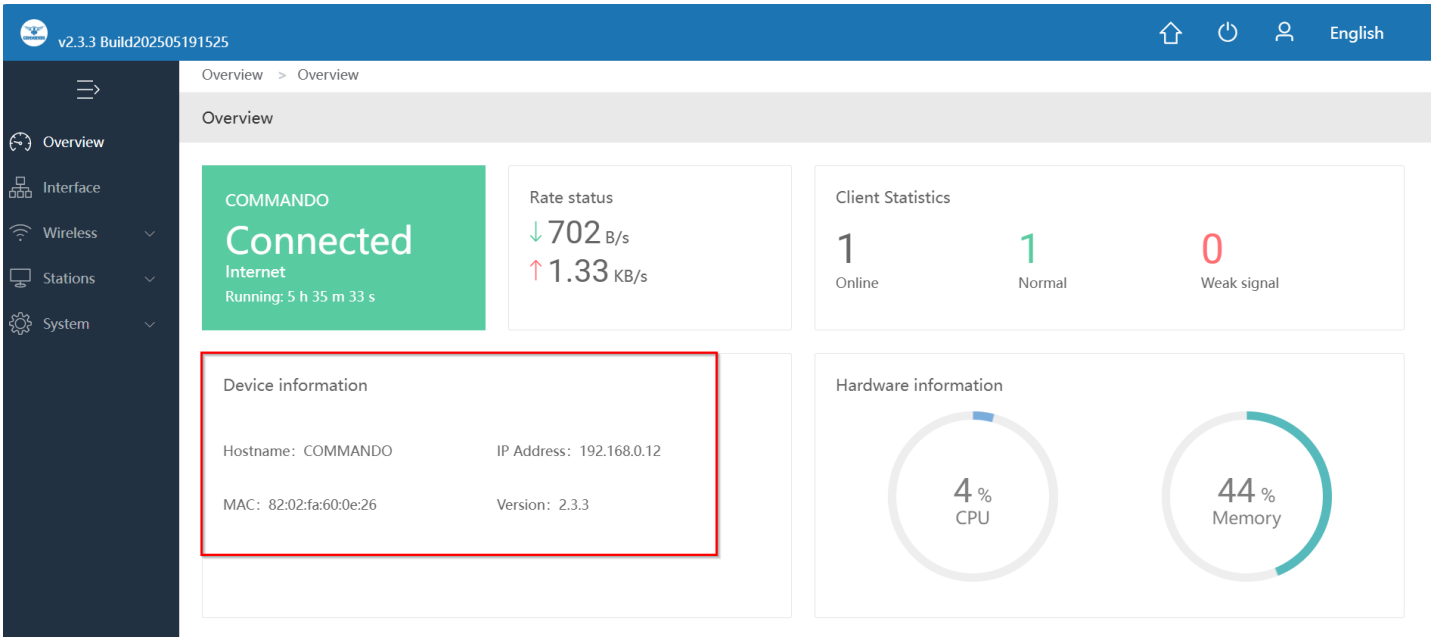


Fig 1.1.3 Device Information of AIR-AP3000AX

1.4 Hardware information:

Hardware information shows CPU and Memory usage percentage.

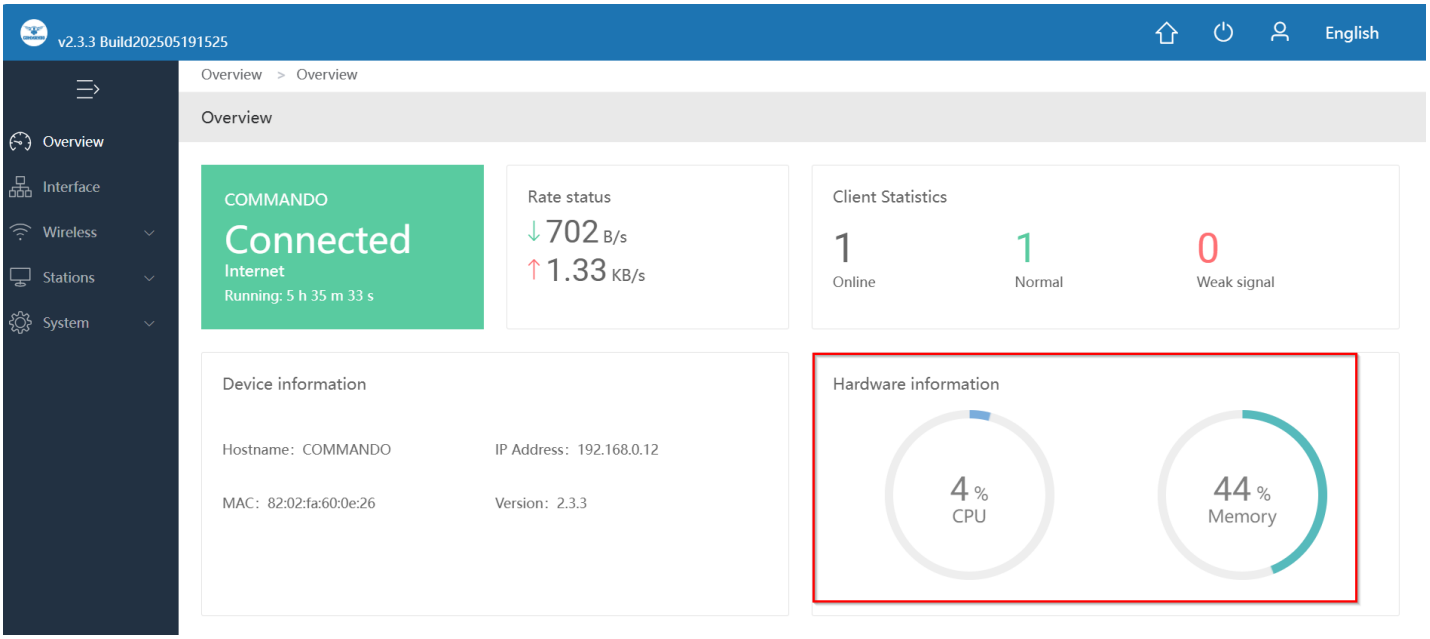


Fig 1.1.4 Hardware information of AIR-AP3000AX

1.5 RF information

In RF Information shows 2.4G and 5G channel used either manual or auto along with channel bandwidth used 20/40/80 MHz with Channel utilization rate, Channel noise floor in dbm with Signal strength.

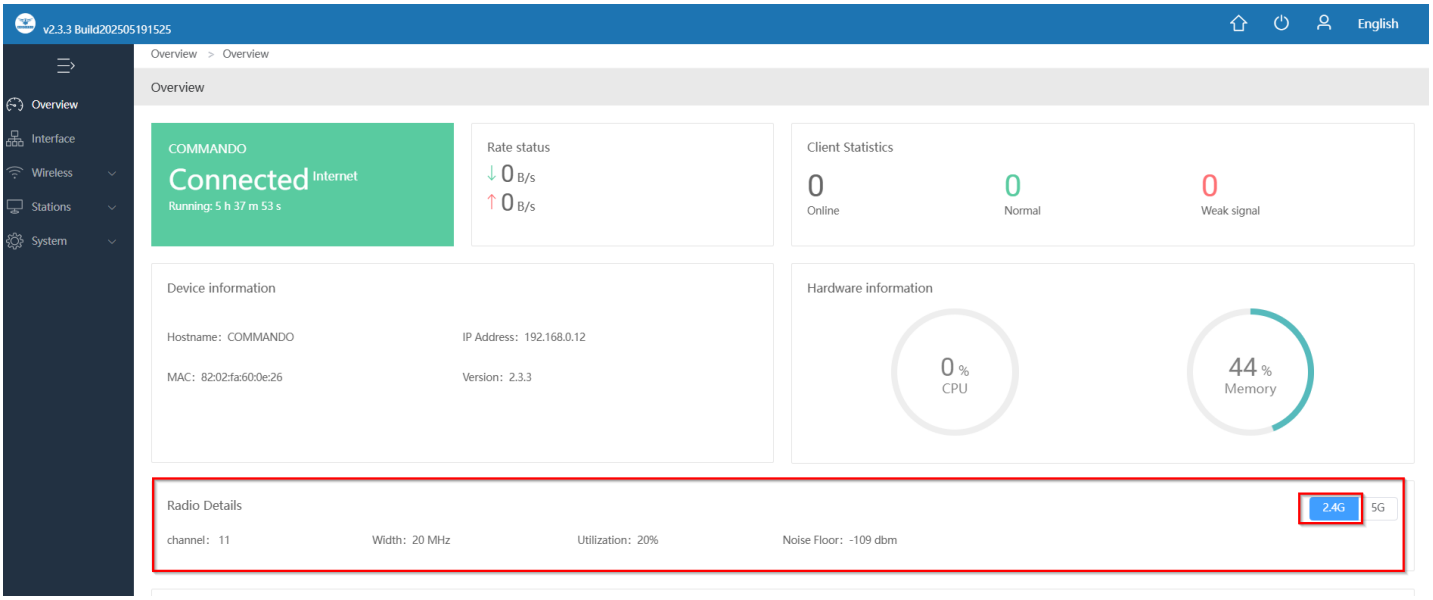


Fig 1.5.1 RF information for 2.4G of AIR-AP3000AX

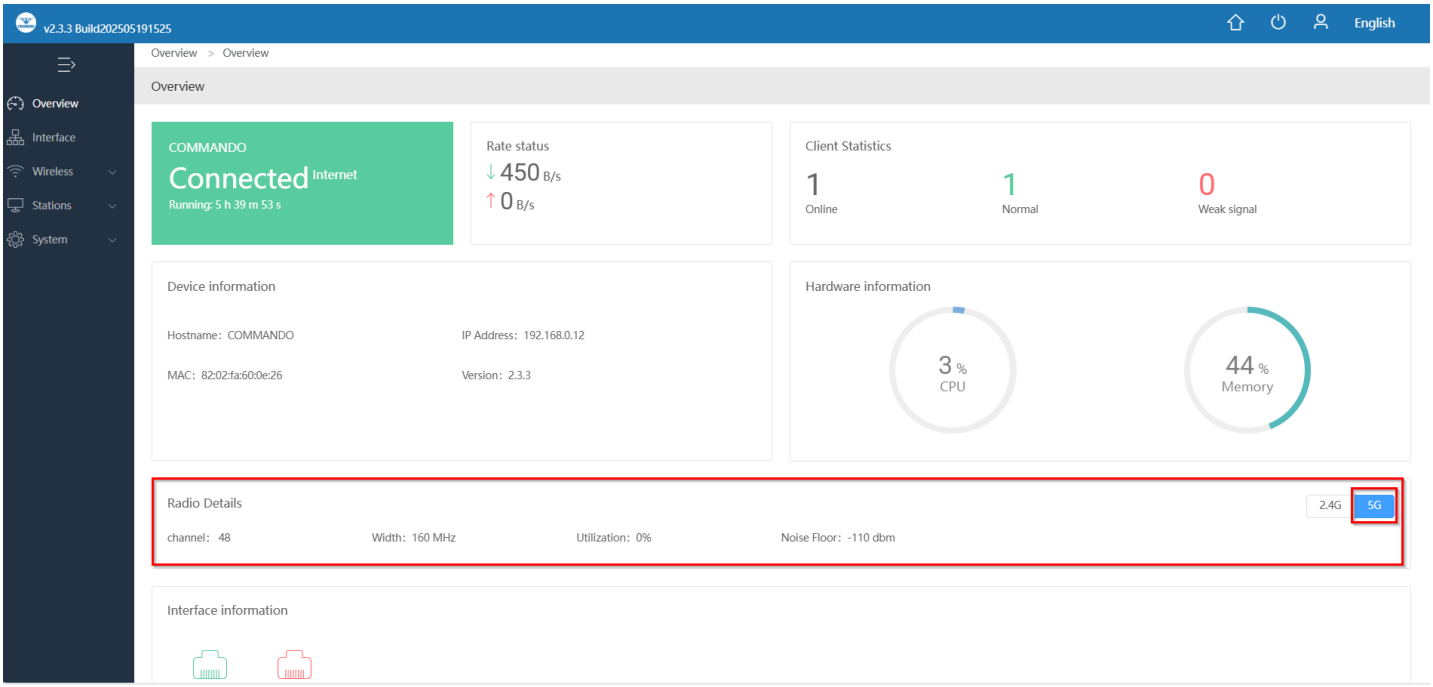


Fig 1.5.2 RF information for 5G of AIR-AP3000AX

1.6 Interface Information

Displays the current enabled WAN, LAN port(s). All Interface Status automatically refresh in 5 sec intervals. Green means active and red means inactive.

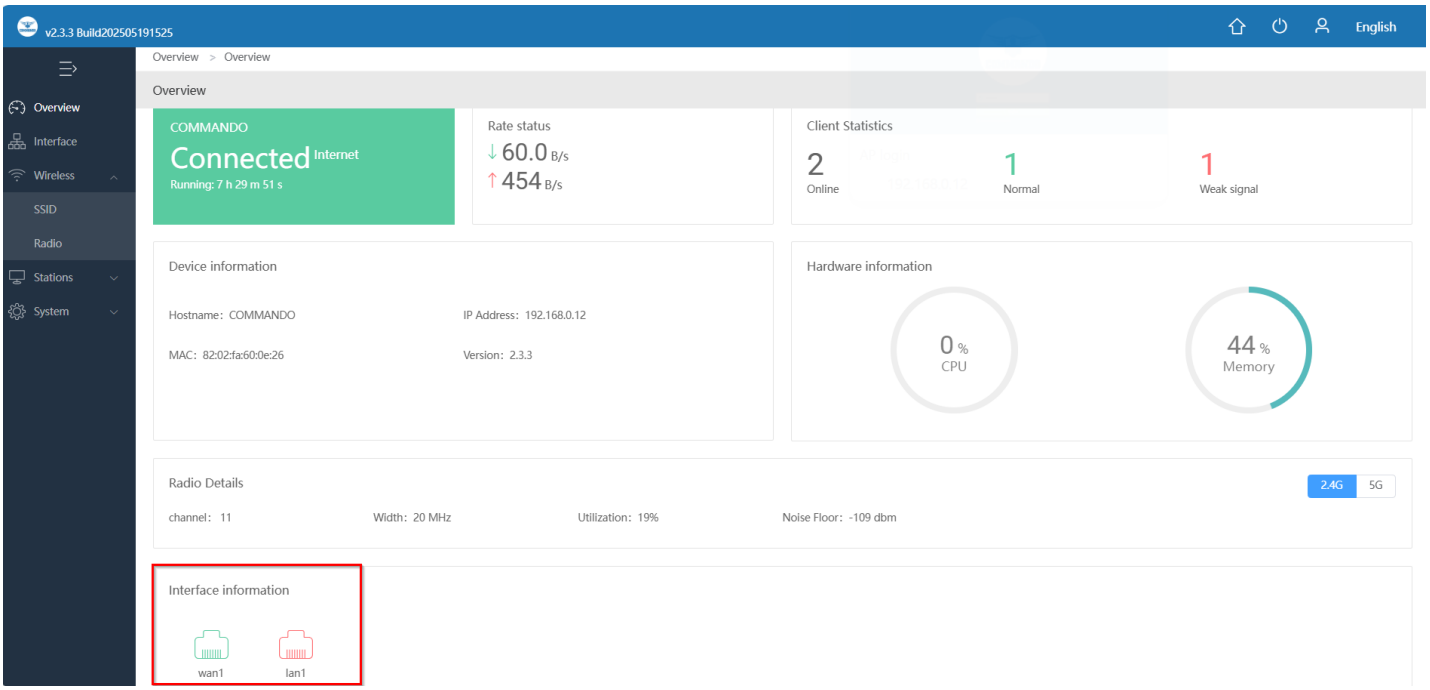


Fig 1.6.1 Interface Status of AIR-AP3000AX

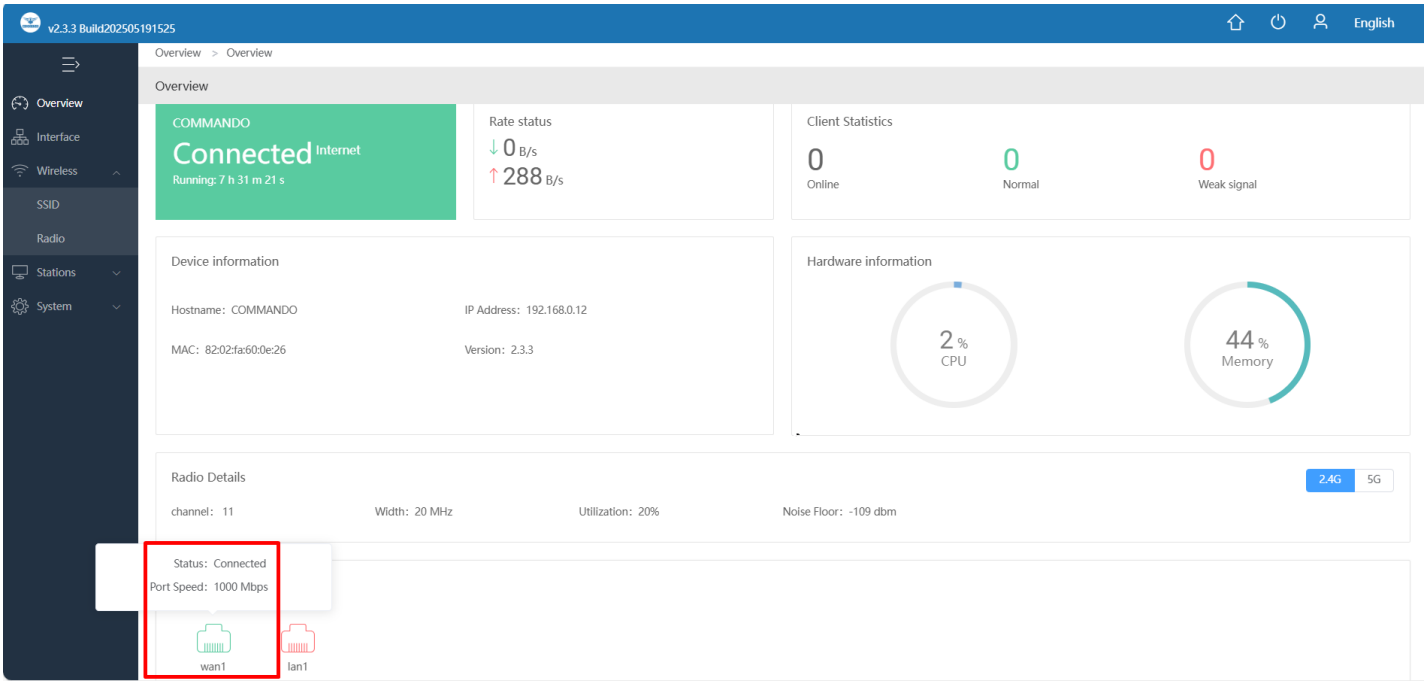


Fig 1.6.2 Physical connection of AIR-AP3000AX

Important Note:

1. In FIT mode, we can set basic setting and can not set port, WiFi, User and System Setting.
2. In FAT mode, we can set all including port, WiFi, User and System Setting.

2. Ports settings

In port setting we can set Access method like DHCP or Manual static IP address along with subnet mask and default gateway. We can also set DNS manually with Preferred DNS and Alternative DNS.

For Changing port setting click on Ports setting

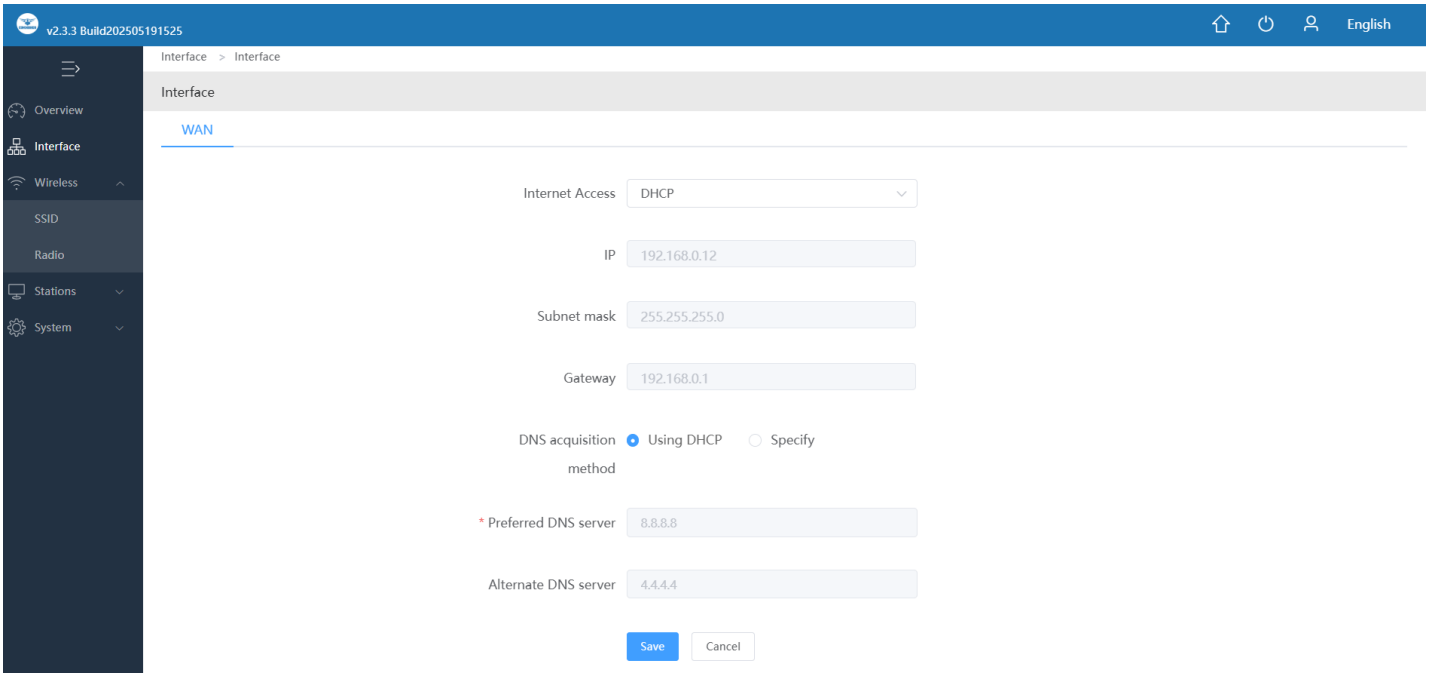


Fig 2.1 Port Setting of AIR-AP3000AX

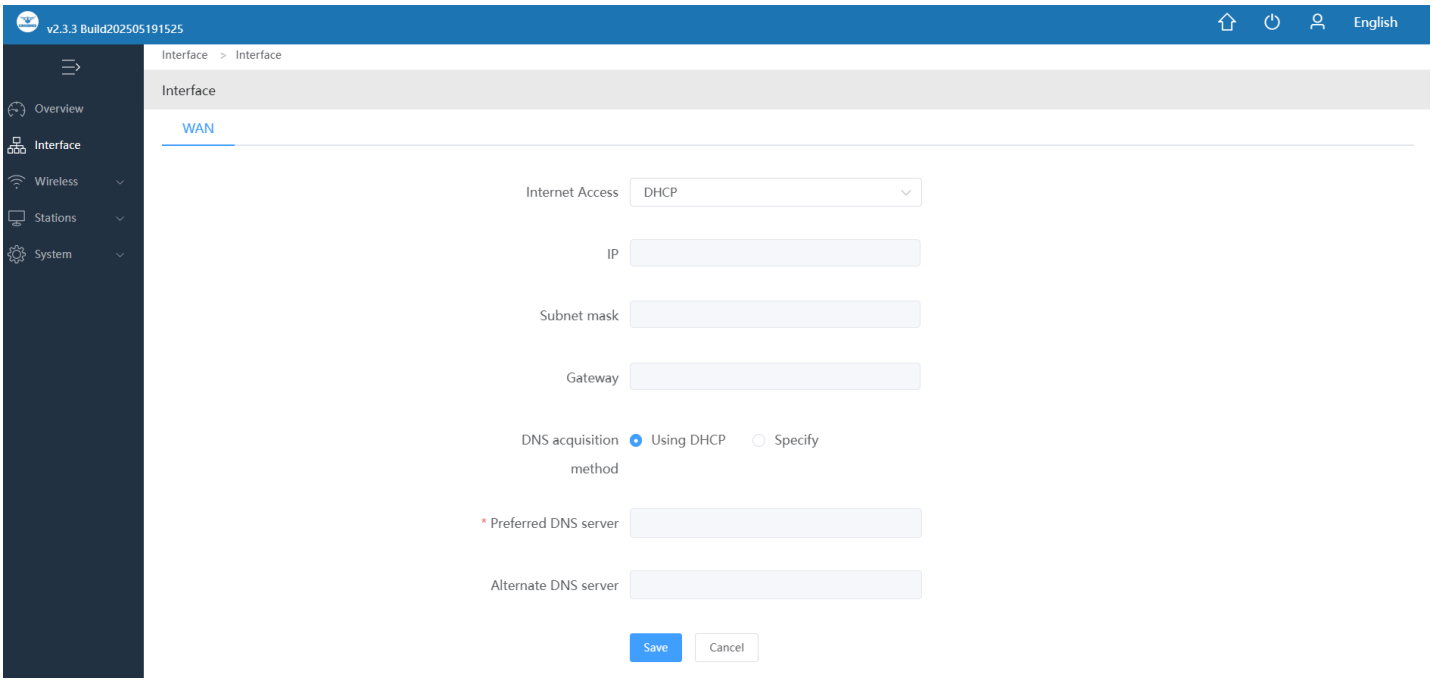


Fig 2.2 Default Port Setting DHCP of AIR-AP3000AX

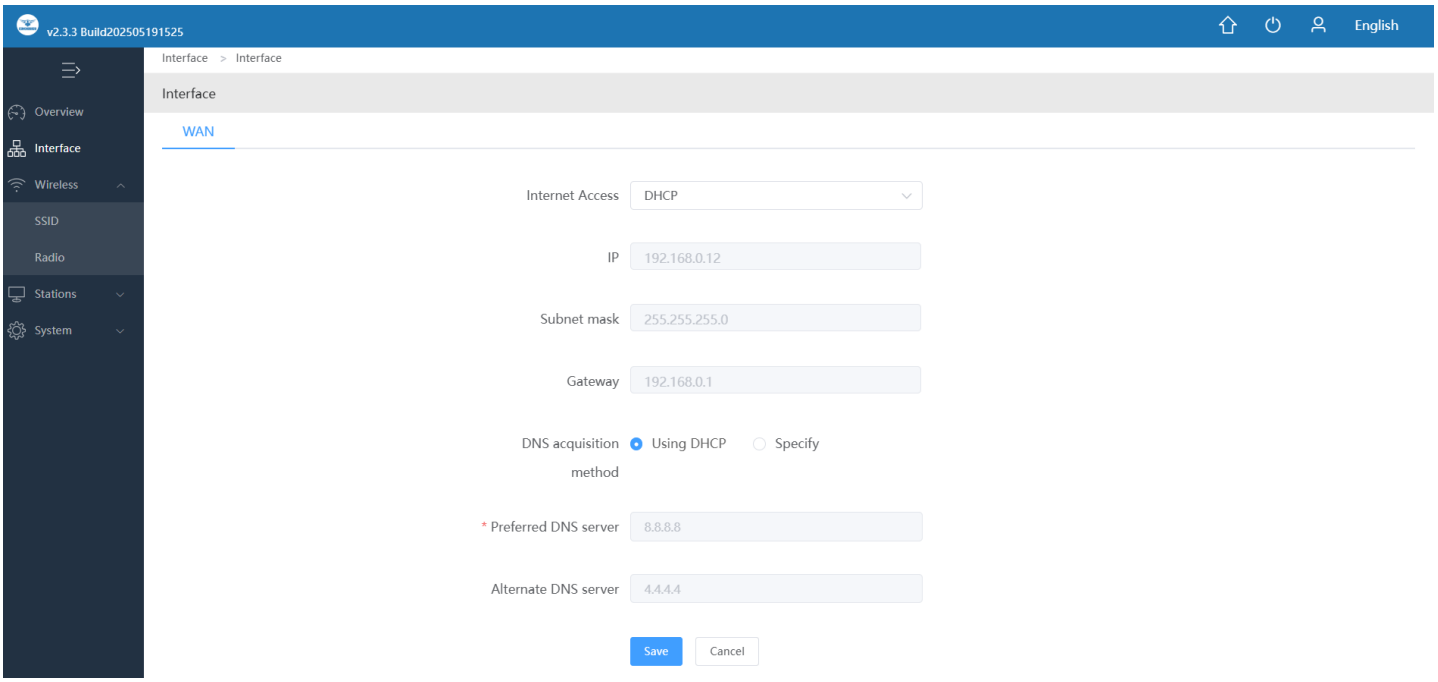


Fig 2.3 Port Setting DHCP of AIR-AP3000AX

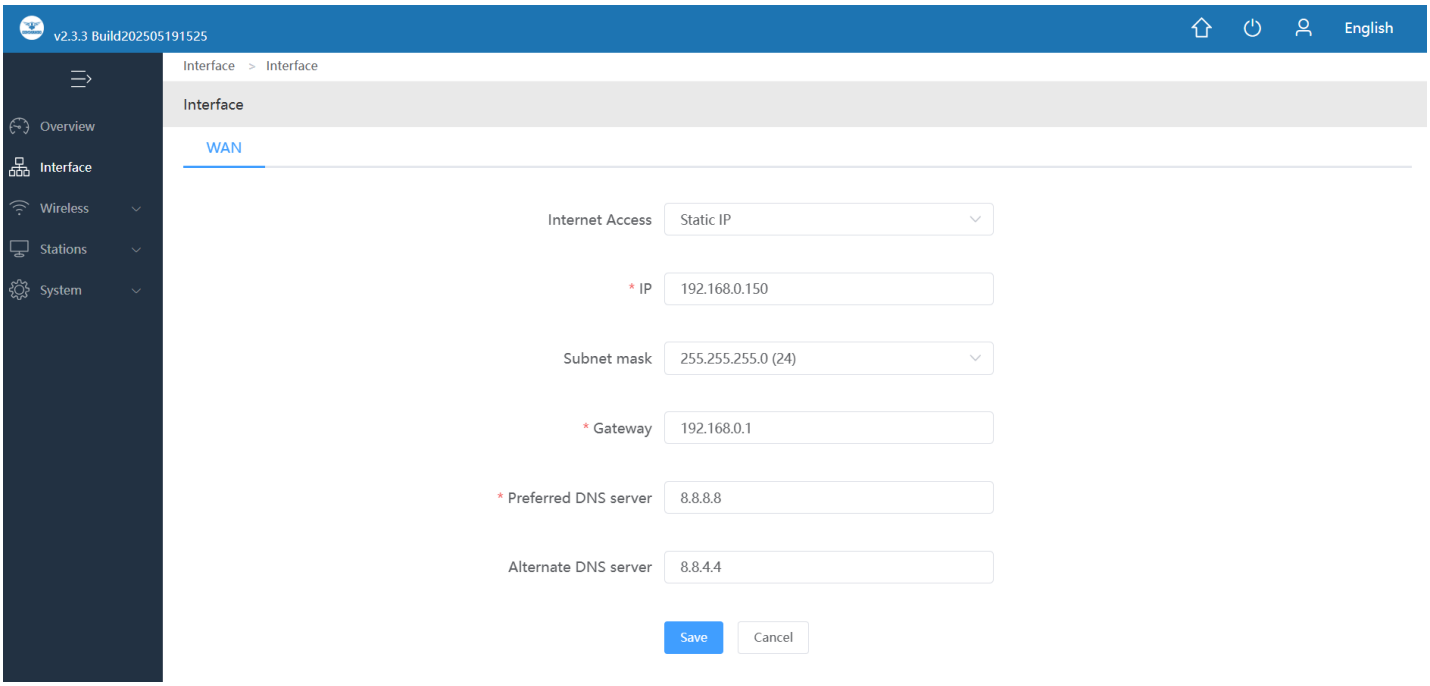


Fig 2.4 Port Setting DNS of AIR-AP3000AX

3. Wi-Fi Settings

In WiFi setting you can set the 2.4G/5G WiFi SSID and RF setting and Advanced settings.

1.1 SSID Settings

We can set 2.4G/5G WiFi with Basic Setting along with SSID setting. You can enable or disable WiFi by
WiFi Operating Status (Disable): On mean SSID is available for wireless clients. WiFi Operating Status (Enable): Off mean SSID not available.

Note:
1. By default Basic WiFi SSID “2.4G_default” and “5G_default” is turned ON.
2. By default no Password/authentication is required to connect to SSID. For Changing SSID

parameters Click on WiFi Setting> SSID Setting

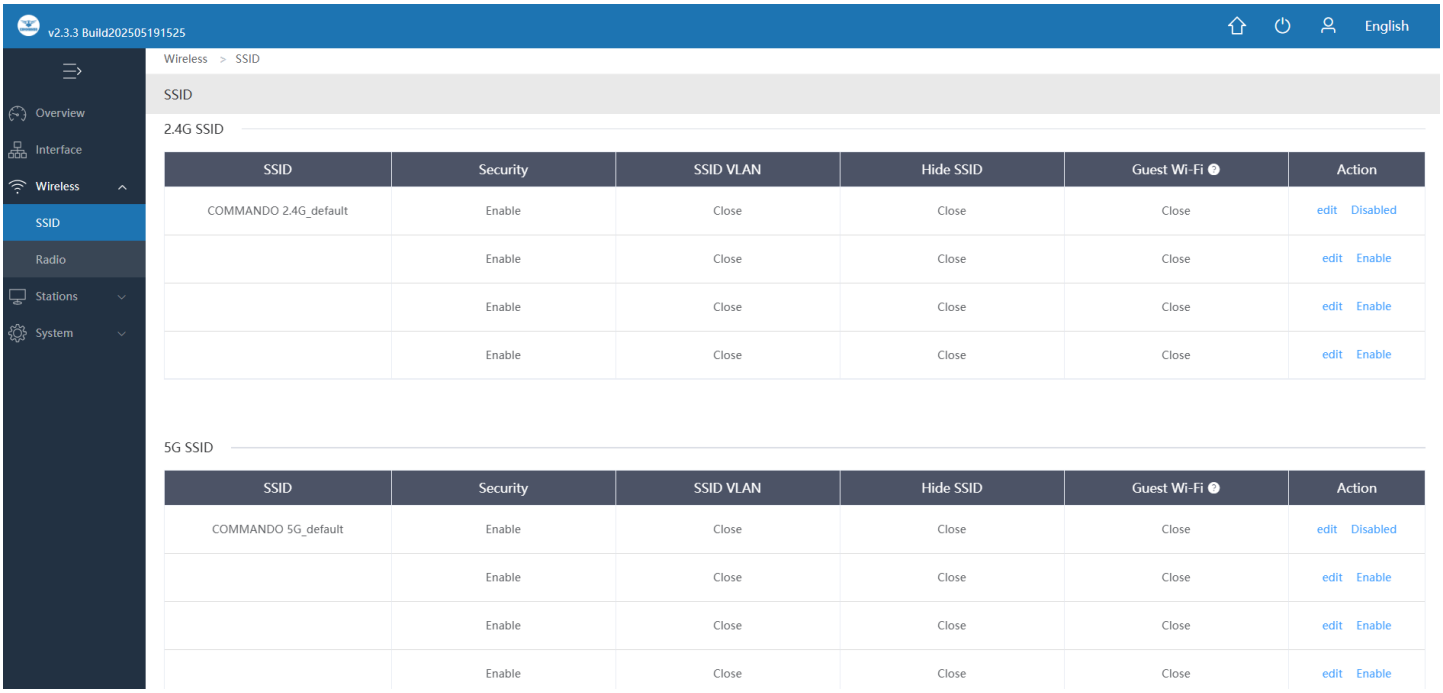


Fig 3.1.1 Default WiFi of AIR-AP3000AX

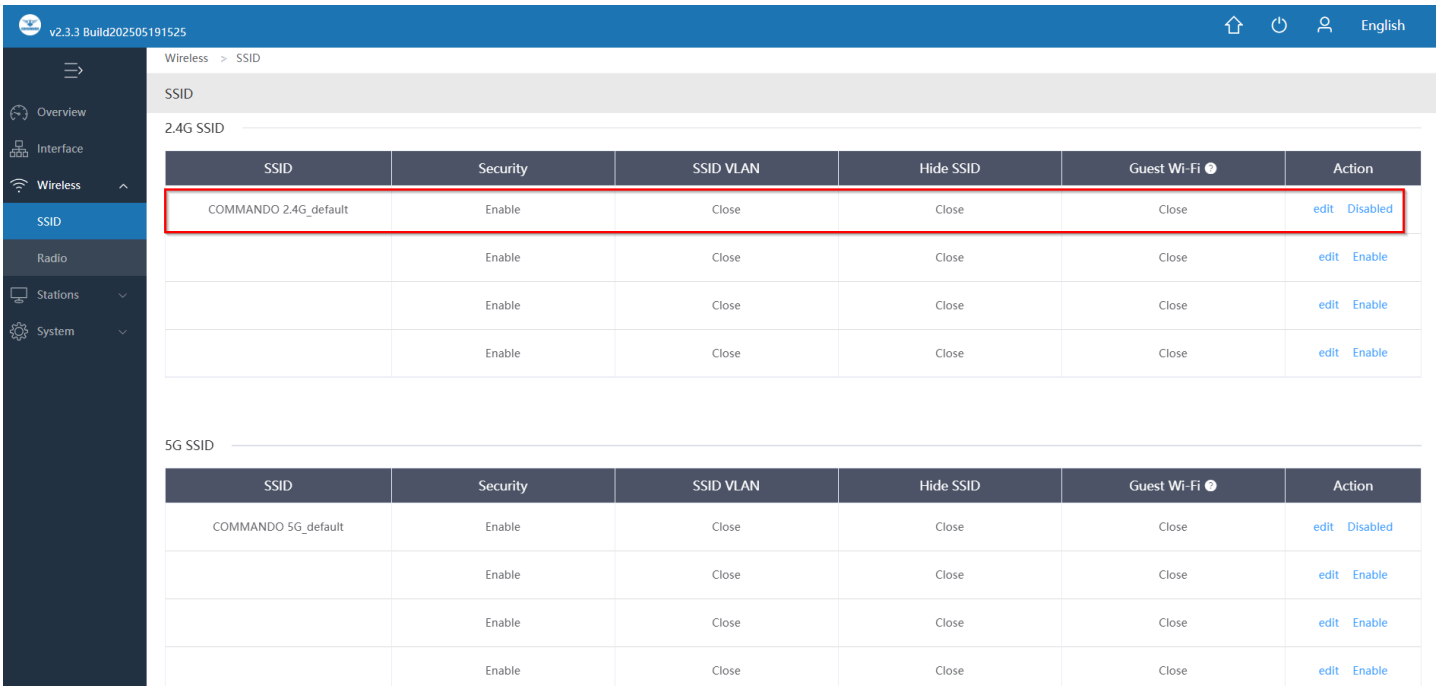


Fig 3.1.2 Default 2.4G WiFi enable of AIR-AP3000AX

How to change SSID (Wi-Fi Name)?

For changing SSID name and parameters, Click on WIFI Setting>>SSID Setting>>Edit.

In SSID Setting, various parameters like SSID name, Security type either Open, WPA-PSK, WPA2-PSK, WPA3- PSK, WPA-PSK+WPA2-PSK, WPA2-PSK+WPA3-PSK can be set. You can also set SSID VLAN and can also rate limit of Uplink speed limit and Downstream speed limit in KB/s . You can Hide SSID or configure Guest mode which Prohibit mutual visits and access to wired.

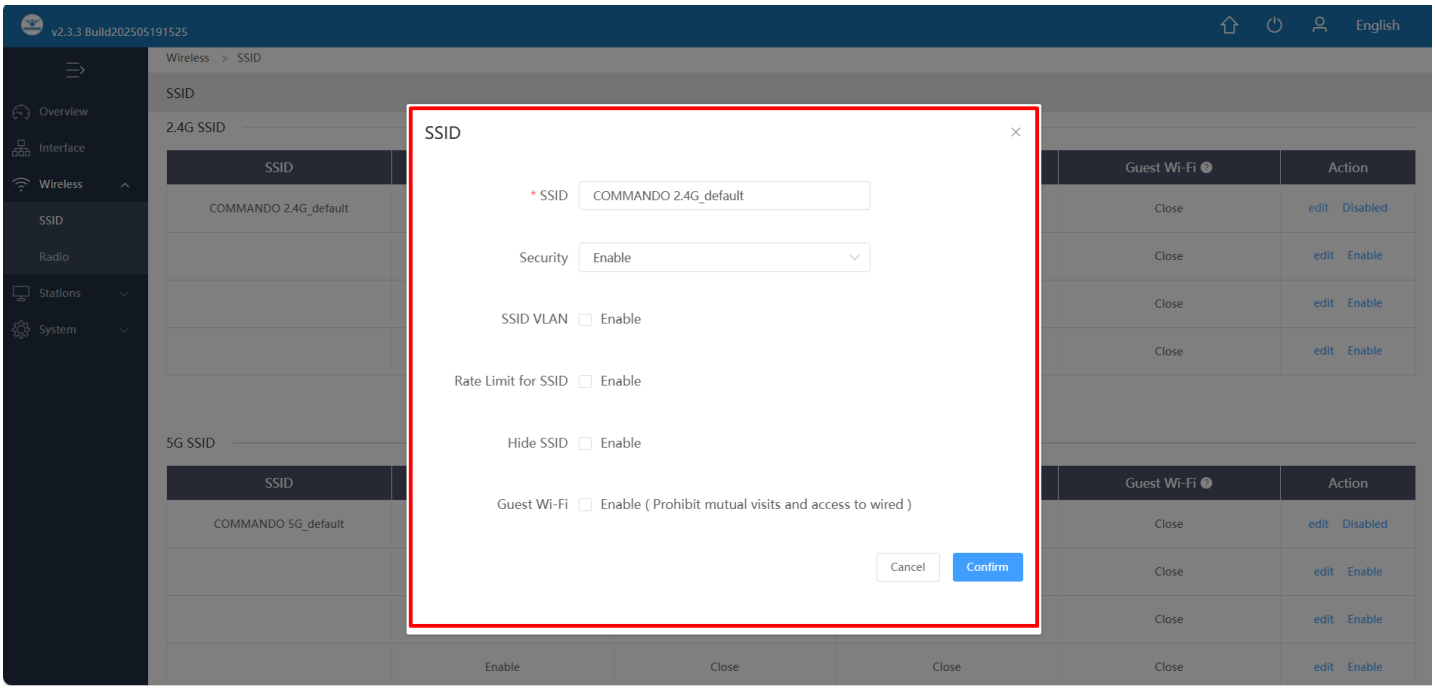


Fig 3.1.3 SSID Setting of AIR-AP3000AX

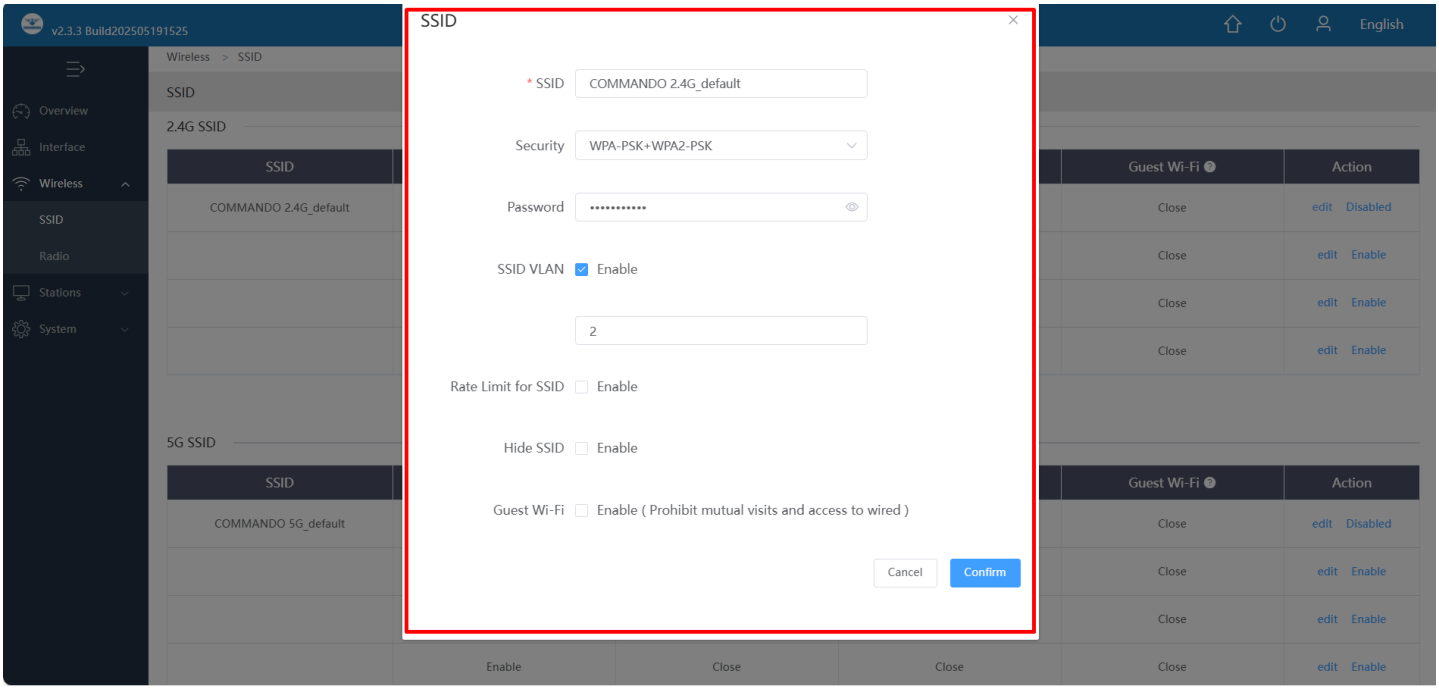


Fig 3.1.4 Setting security for AIR-AP3000AX

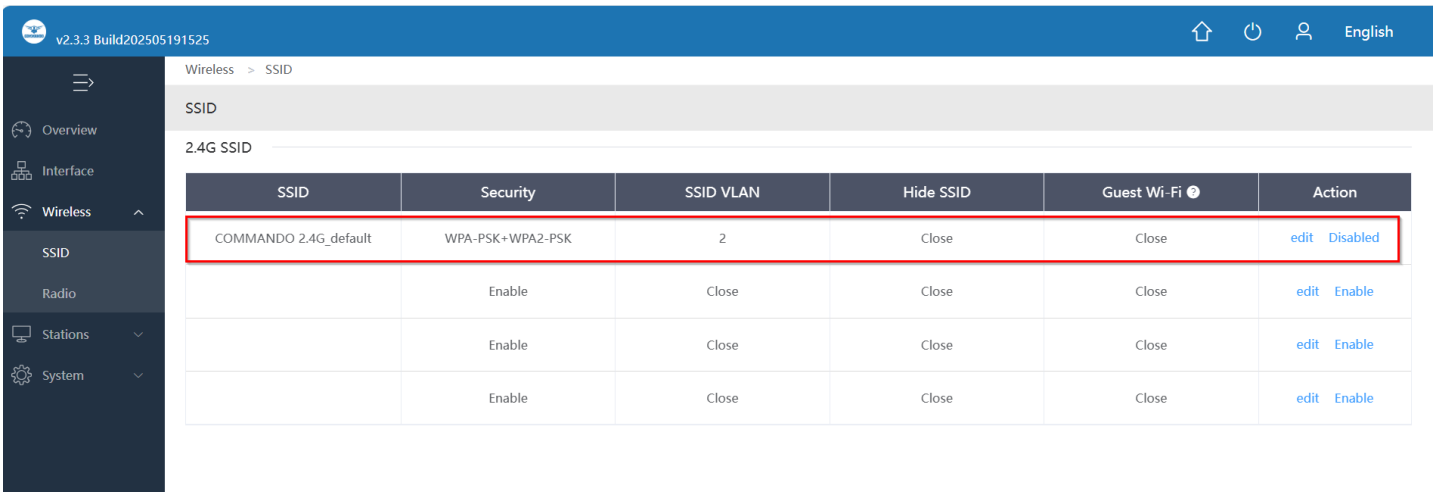


Fig 3.1.5 2.4G_default WiFi with security setting WPA-PSK+WPA2-PSK AIR-AP3000

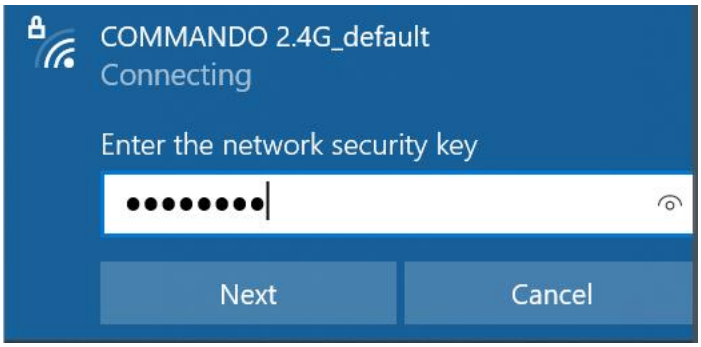


Fig 3.1.6 2.4G_default access with security setting to Wireless clients of AIR-AP3000AX

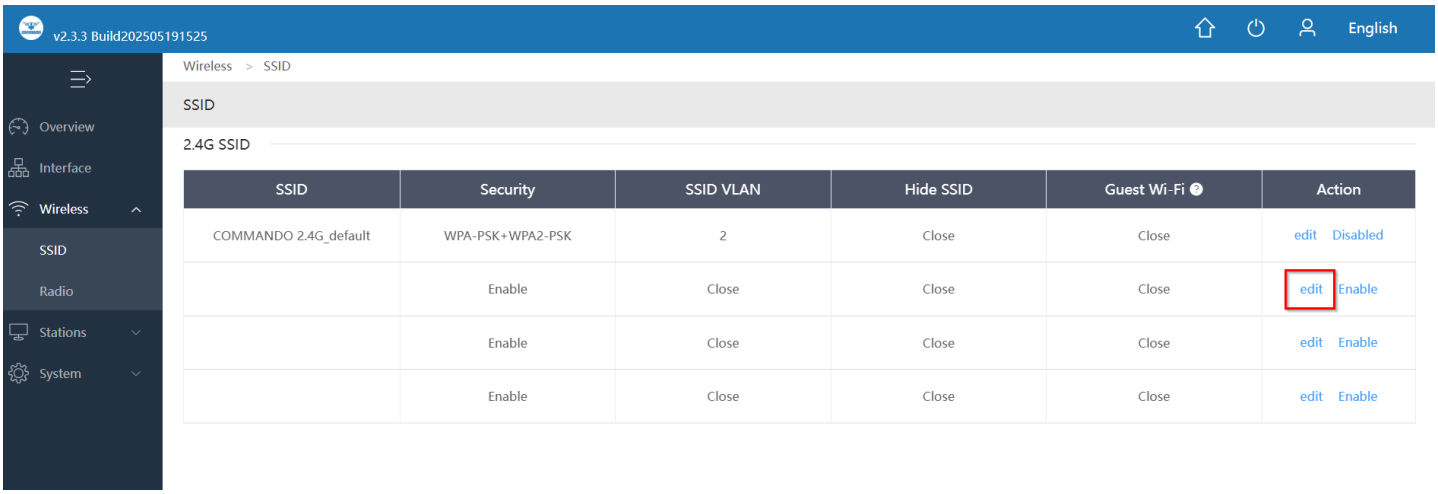


Fig 3.1.7 Enabling 2.4G VAP of AIR-AP3000AX

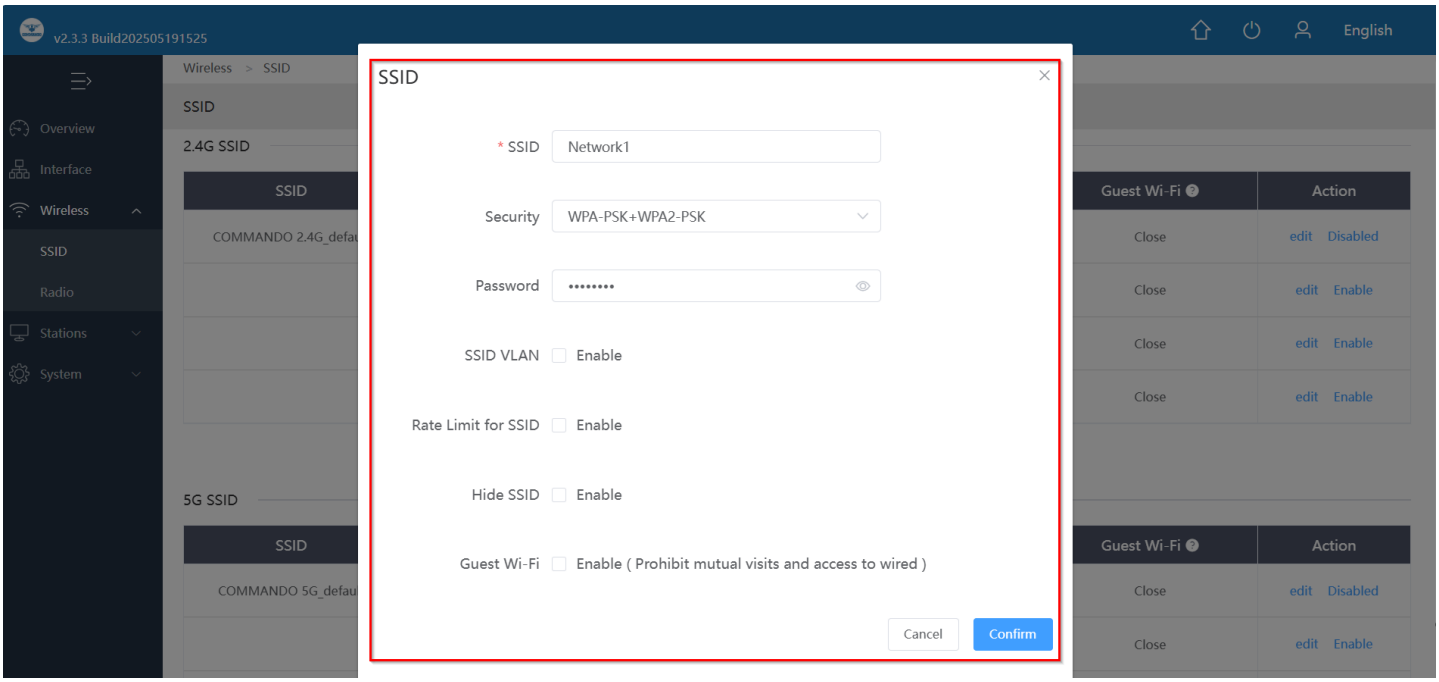


Fig 3.1.8 Setting 2.4G VAP 1 SSID and parameters of AIR-AP3000AX

Important Note: You can create SSID WiFi password as per your choice but wireless clients can connect only after enabling SSID.

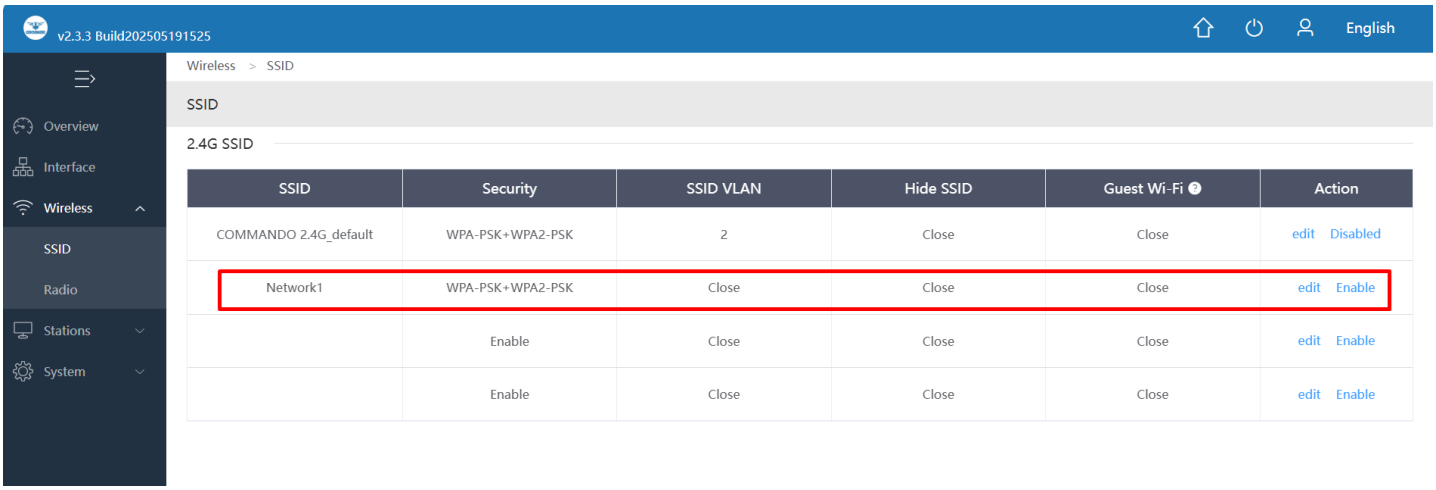


Fig 3.1.9 Wireless VAP 1 created in AIR-AP3000AX

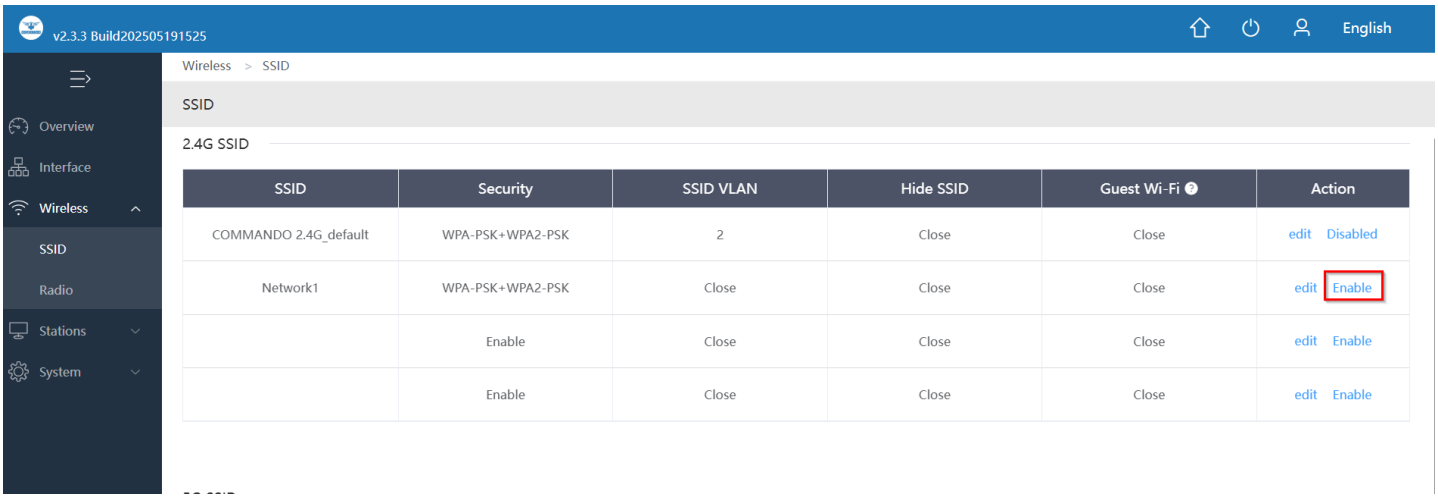


Fig 3.1.10 Enabling 2G WiFi VAP 2 of AIR-AP3000AX

Note: You can have Multi SSID up to 8 (4 in 2.4G band and 4 in 5G band) configured on AIR-AP3000AX. All created SSID will use same channel in 2G and 5G band and channel width as set in for band SSID. For each Virtual Access Point (VAP) can set different name, encryption and password.

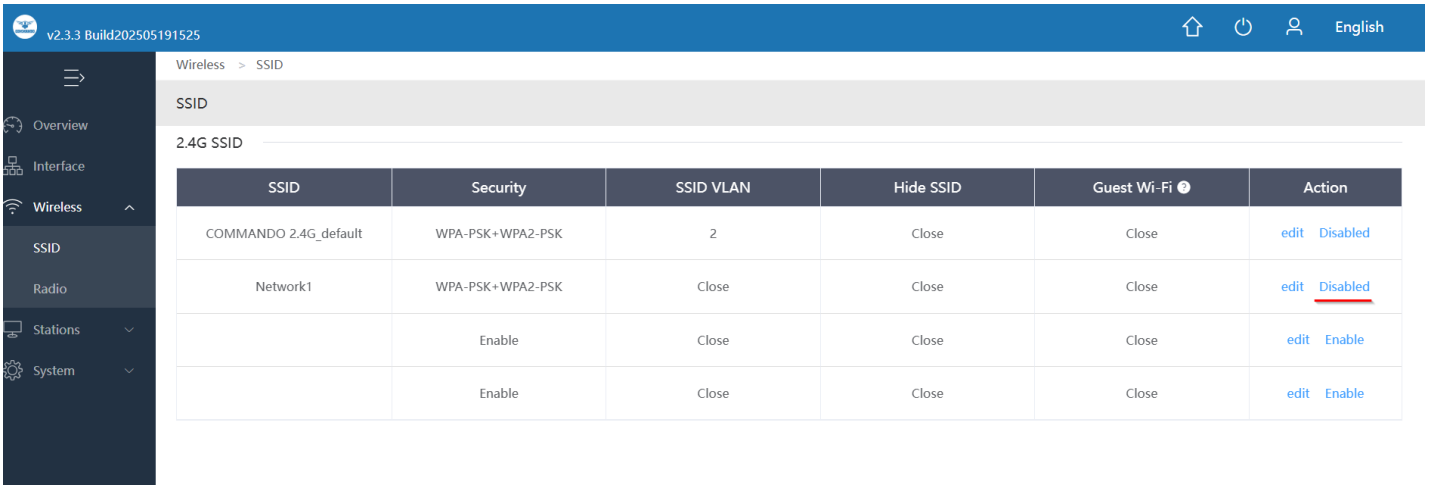


Fig 3.1.11 Enabling 2G WiFi Network1 of AIR-AP3000AX

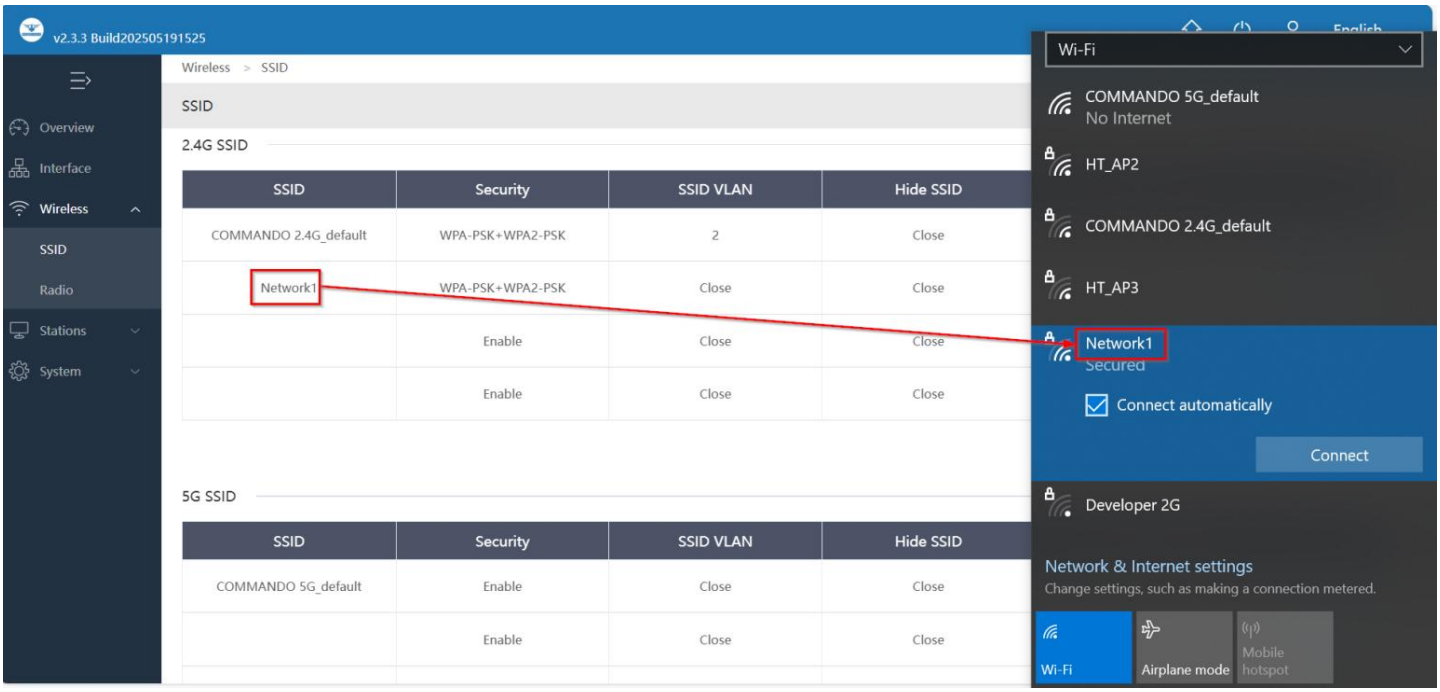


Fig 3.1.12 2G WiFi Network1 available for wireless clients AIR-AP3000AX

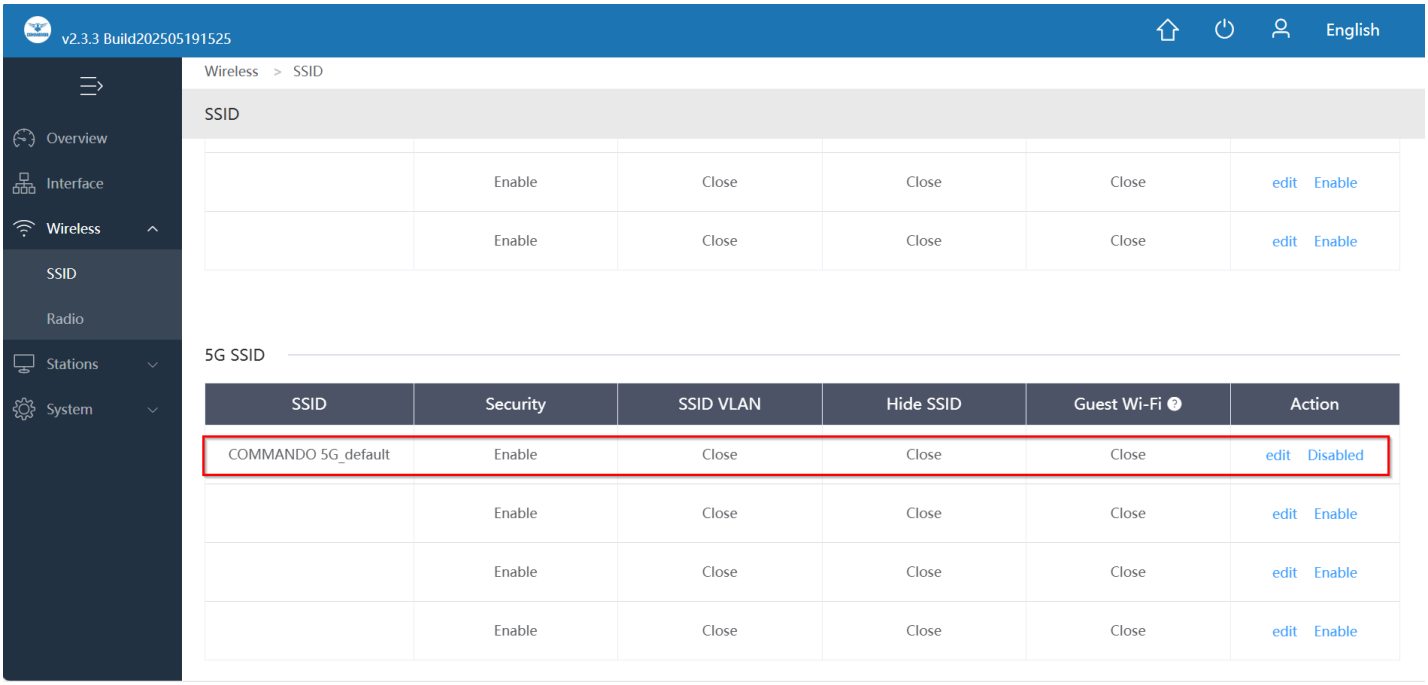


Fig 3.1.13 Default 5G WiFi SSID of AIR-AP3000AX

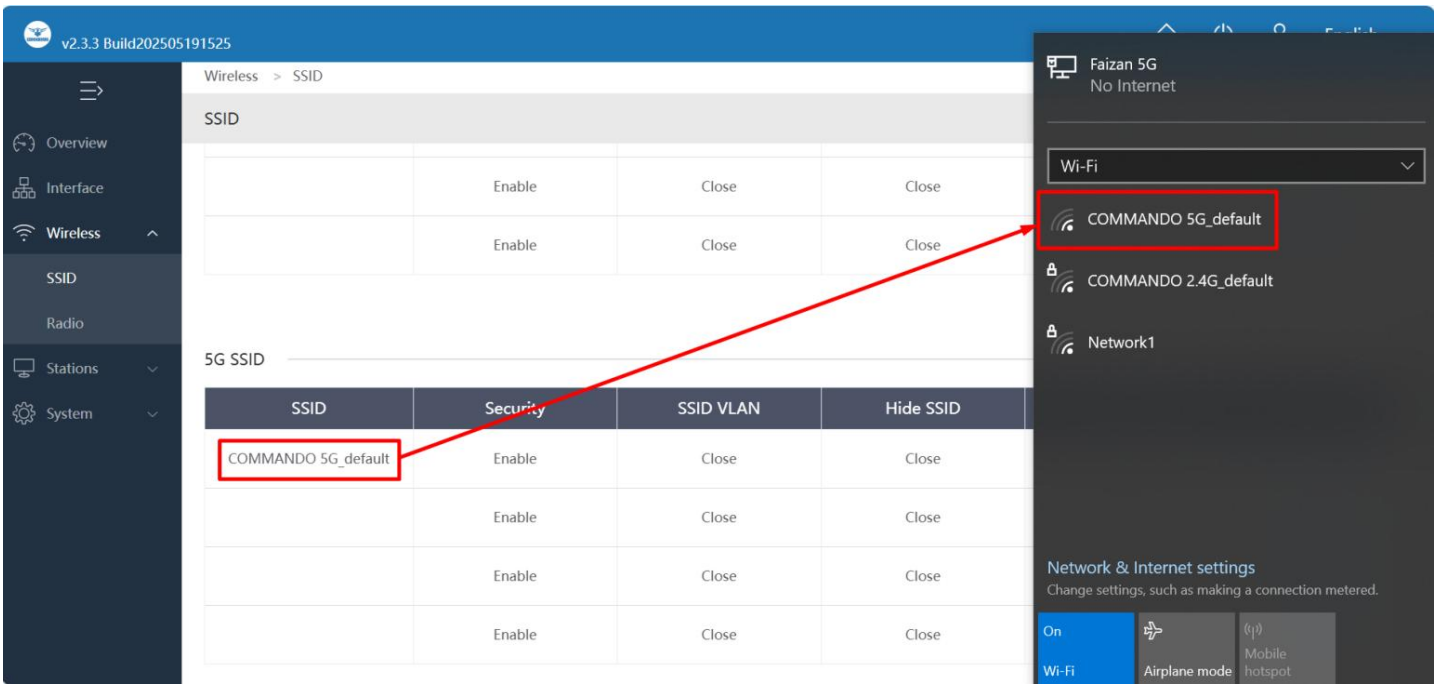


Fig 3.1.14 Default 5G WiFi SSID available for WiFi Clients of AIR-AP3000AX

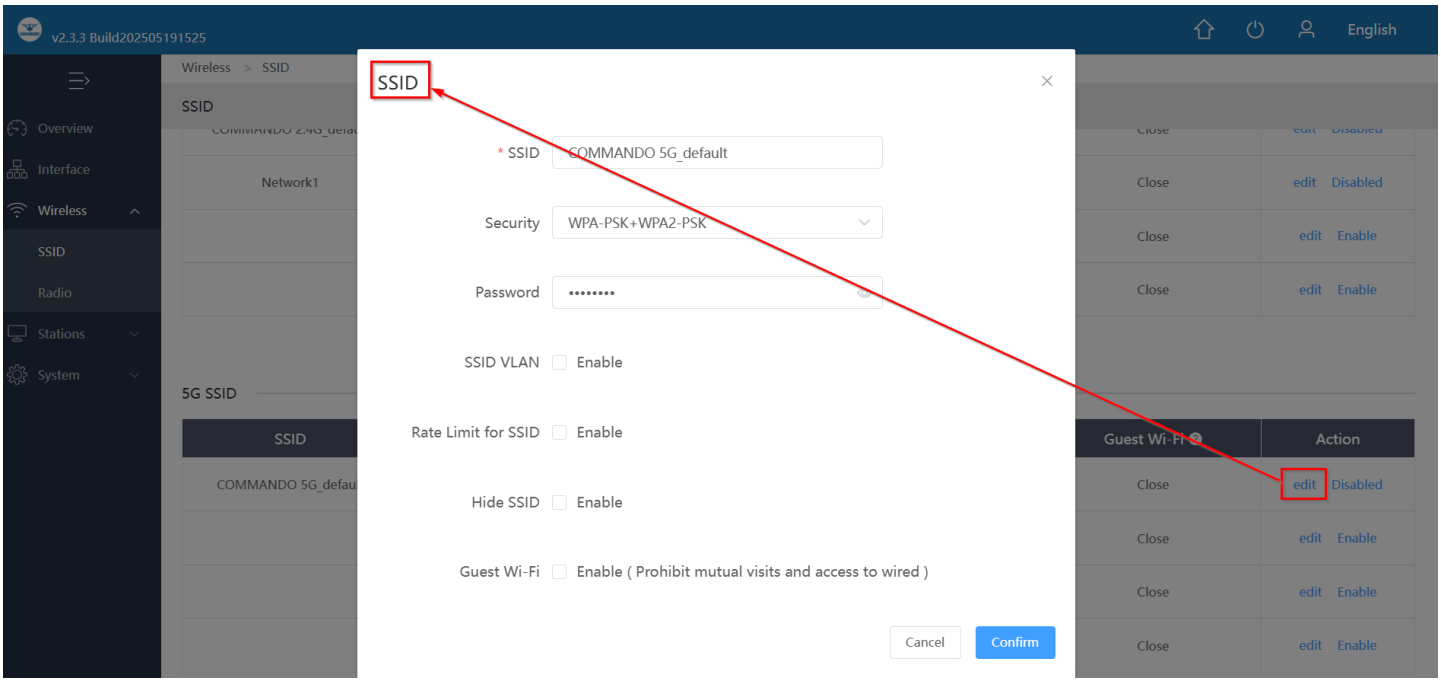


Fig 3.1.15 Edit 5G WiFi SSID setting of AIR-AP3000AX

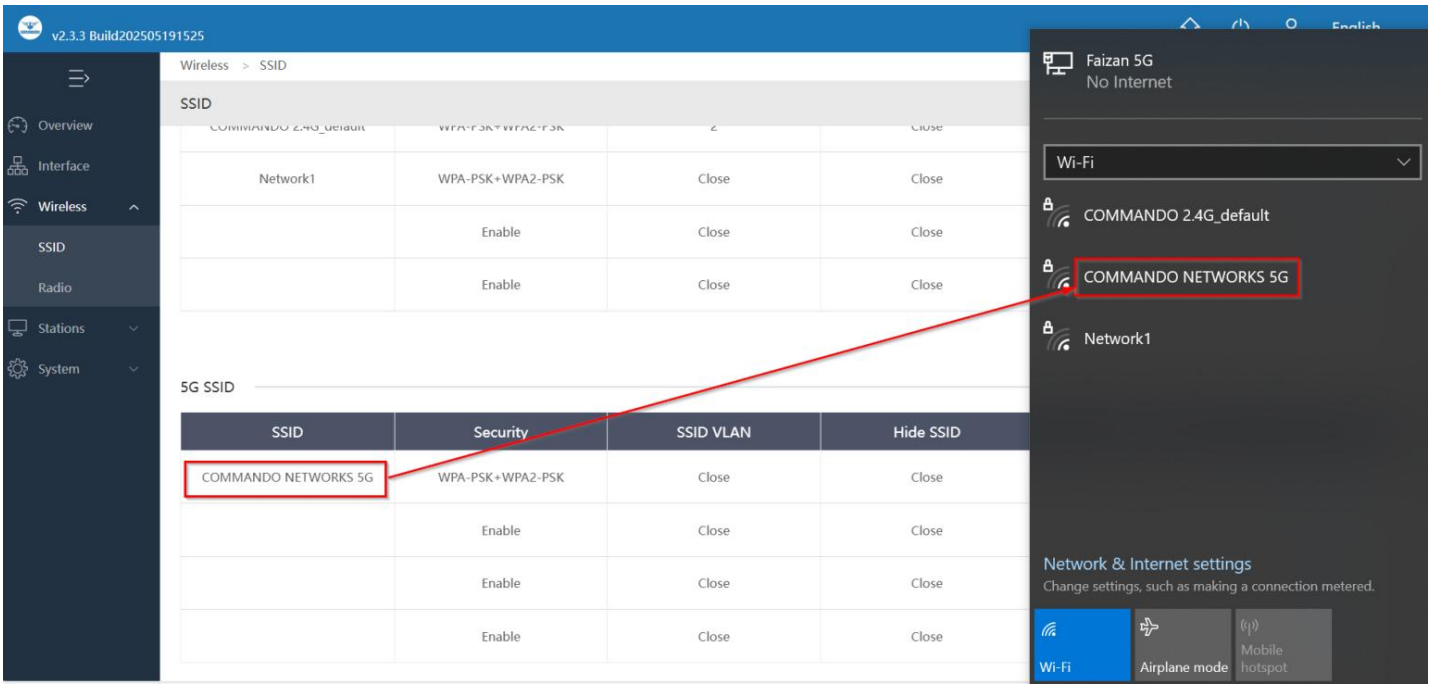


Fig 3.1.16 Setting 5G New SSID of AIR-AP3000AX

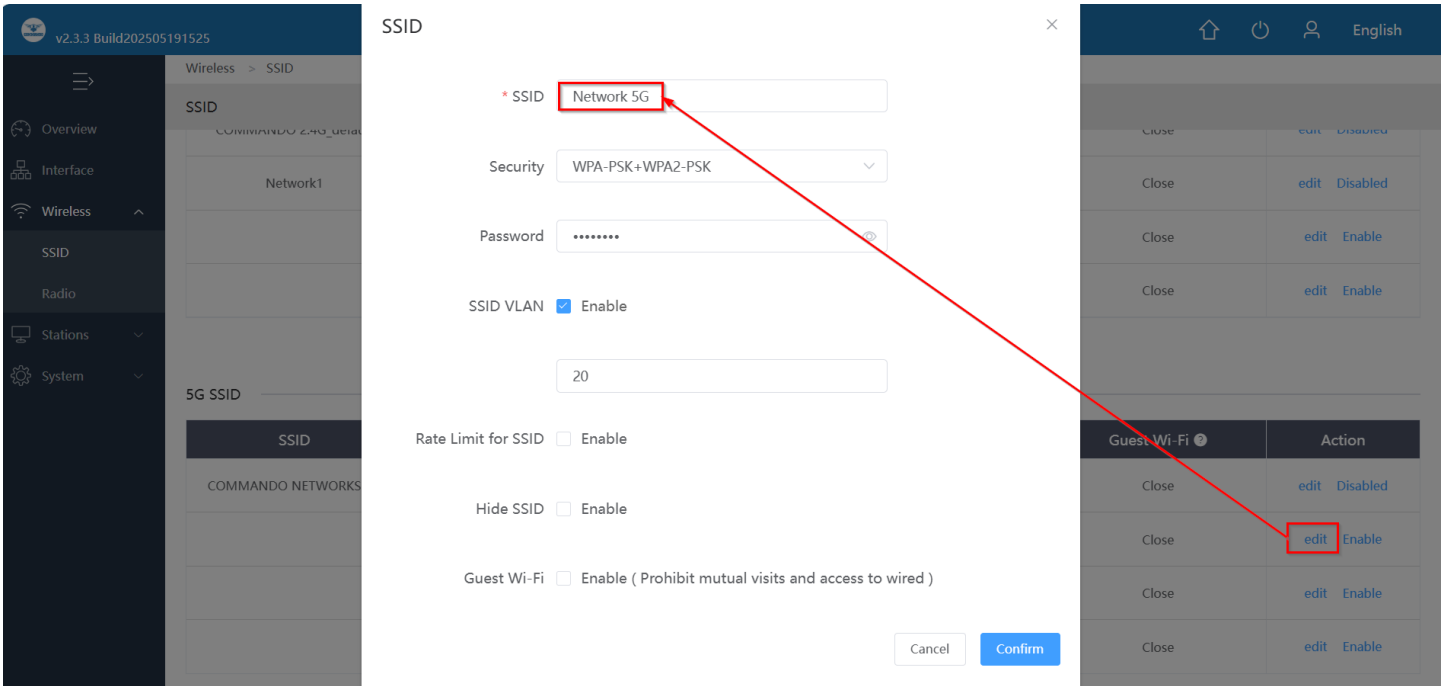


Fig 3.1.17 Setting VAP New SSID in 5G band of AIR-AP3000A

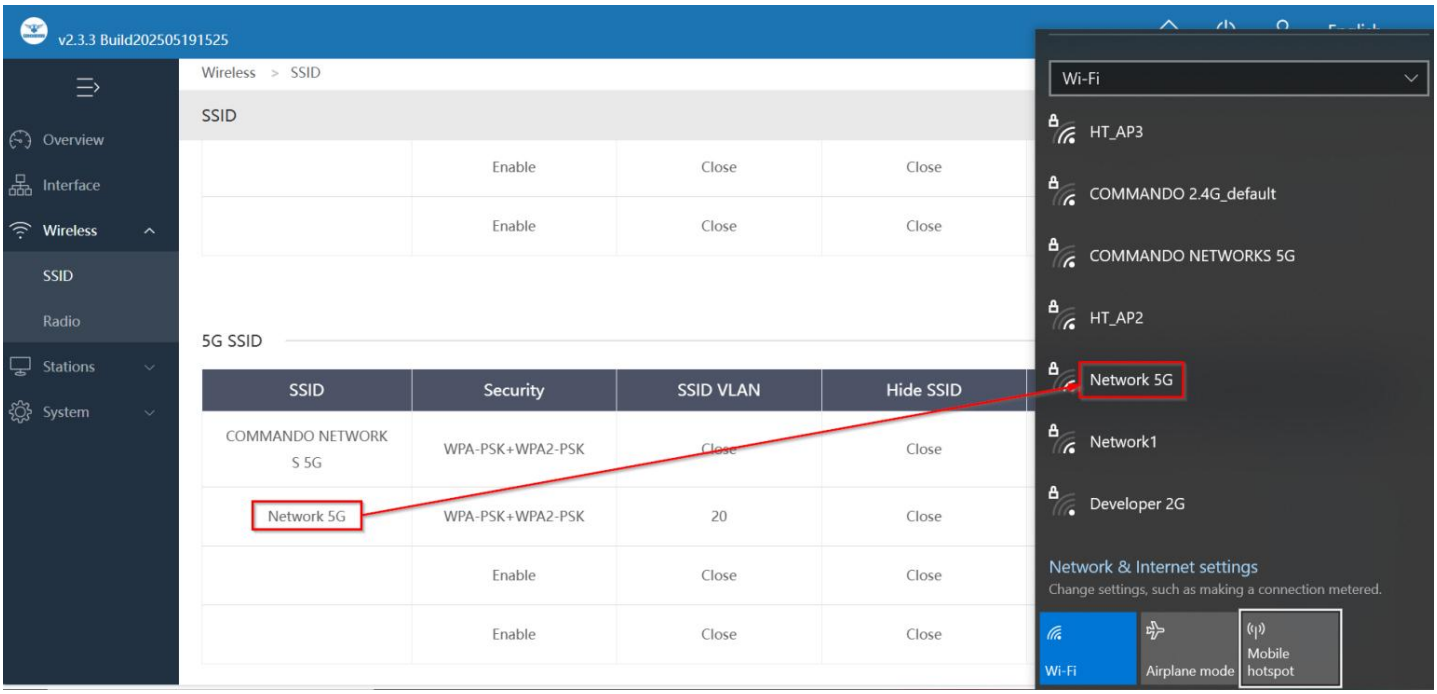


Fig 3.1.18 VAP New SSID available for wireless clients in 5G band of AIR-AP3000AX

RF settings:

It provides an automatic power and channel adjustment function with Dynamic Frequency Selection (DFS) which makes channel allocation scheme specified for wireless LAN, in 2.4G and 5G Wi-Fi. It is designed to prevent electromagnetic interference to ensures particular RF detection and management algorithms to attain a better RF coverage effect. When the signals of one AP is interfering with by strong external signals, the AP may automatically switch to an appropriate channel to avoid interference, which guaranteeing larger distance covered. If particular AP deployed in the network accidentally stops operating by power failure or PoE/PoE+ switch OFF, the RF management function compensates the resulting blind area of signals so that the wireless clients can still operate normally.

Setting Channel Bandwidth:

By default, the 2.4 GHz frequency uses a 20 MHz channel width and the 5 GHz frequency uses 160Mhz channel width. In crowded areas with a lot of frequency noise and interference, a single 20MHz channel will be more stable. 160Mhz channel width allows for greater speed and faster transfer rates but it doesn't perform as well in crowded areas.

Old Naming Convention	New Naming Convention
802.11b	Wi-Fi 1
802.11a	Wi-Fi 2
802.11g	Wi-Fi 3
802.11n	Wi-Fi 4
802.11ac	Wi-Fi 5
802.11ax	Wi-Fi 6

	Channel Width			
# Spatial Streams	20 MHz	40 MHz	80 MHz	160 MHz
1	86 Mbps	200 Mbps	433 Mbps	866 Mbps
2	173 Mbps	400 Mbps	866 Mbps	1.73 Gbps
3	288.9 Mbps	600 Mbps	1.3 Gbps	2.34 Gbps
4	346.7 Mbps	800 Mbps	1.73 Gbps	3.46 Gbps

Fig 3.1.19 RF speed in 2.4G and 5G band of AIR-AP3000AX

For changing RF 2.4G setting go to WIFI settings >RF settings >>2.4G

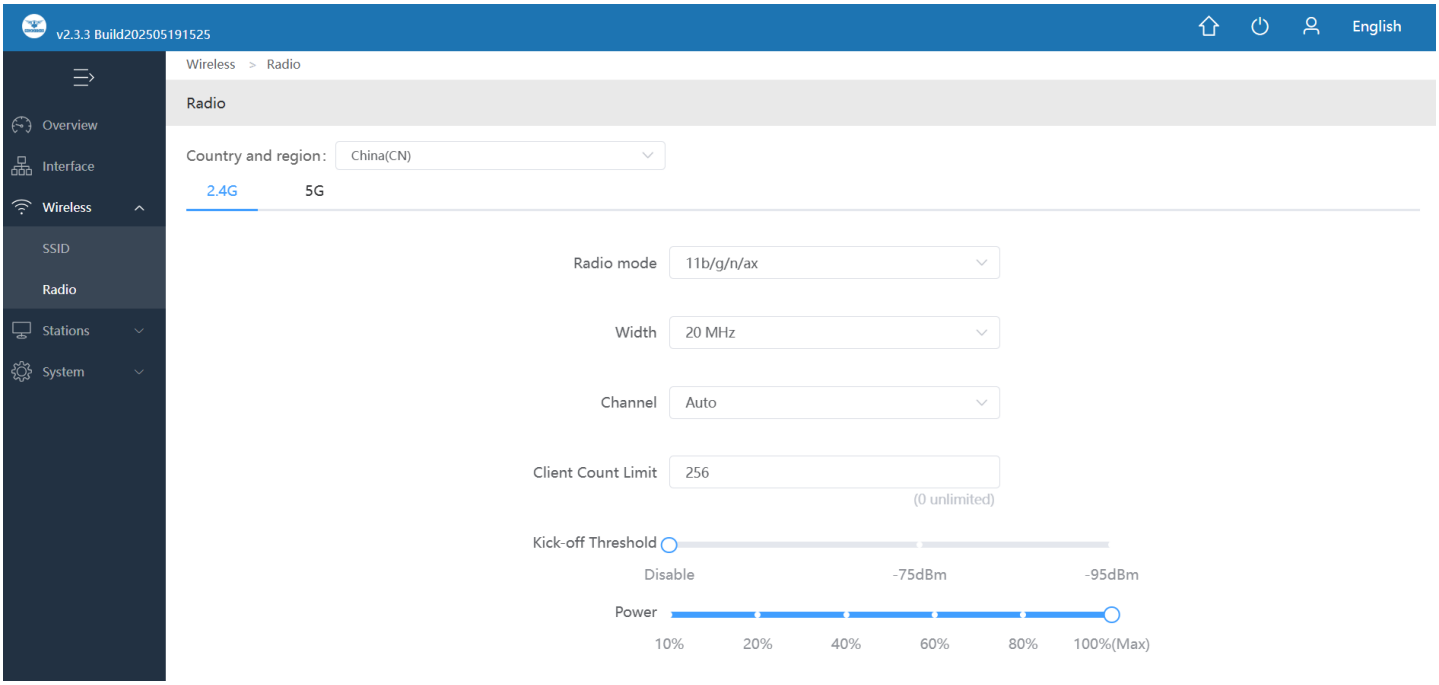


Fig 3.1.20 Changing Maximum Wireless client count in 2.4G band of AIR-AP3000AX

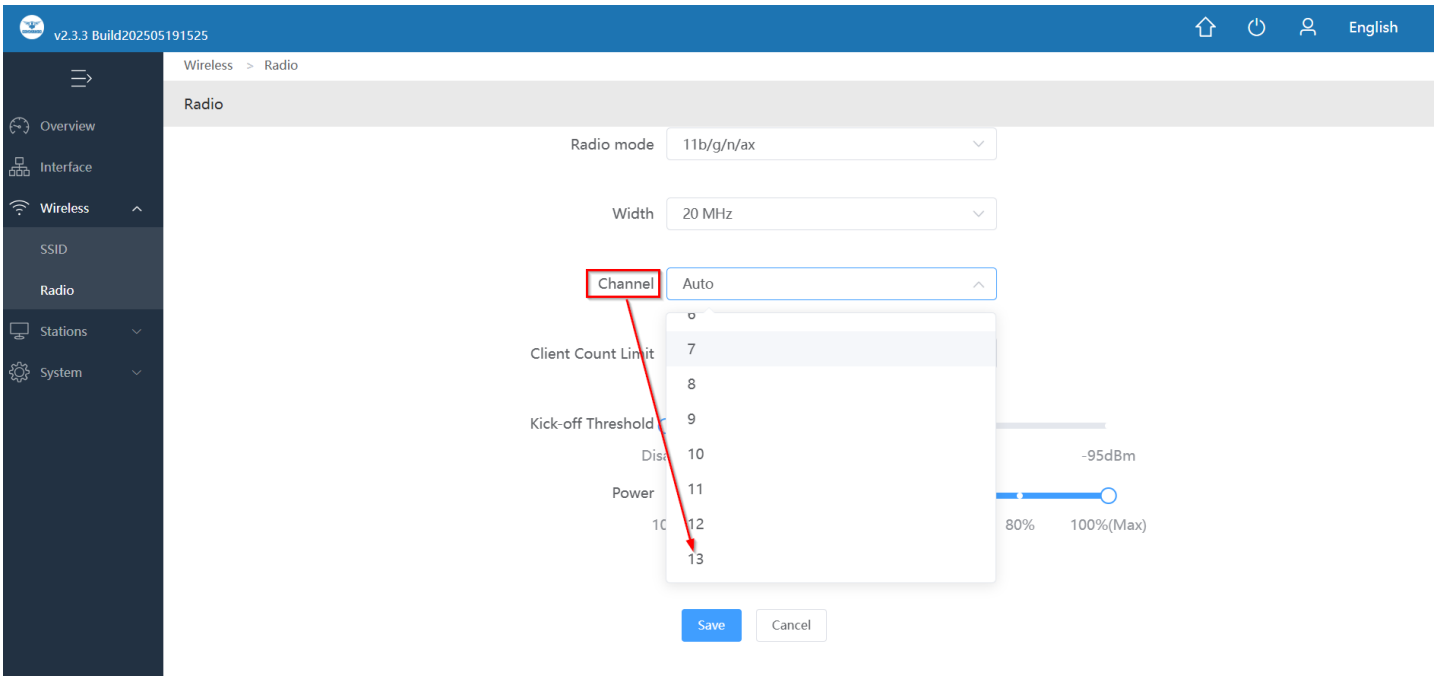


Fig 3.1.21 Changing Channels in 2.4G band of AIR-AP3000AX

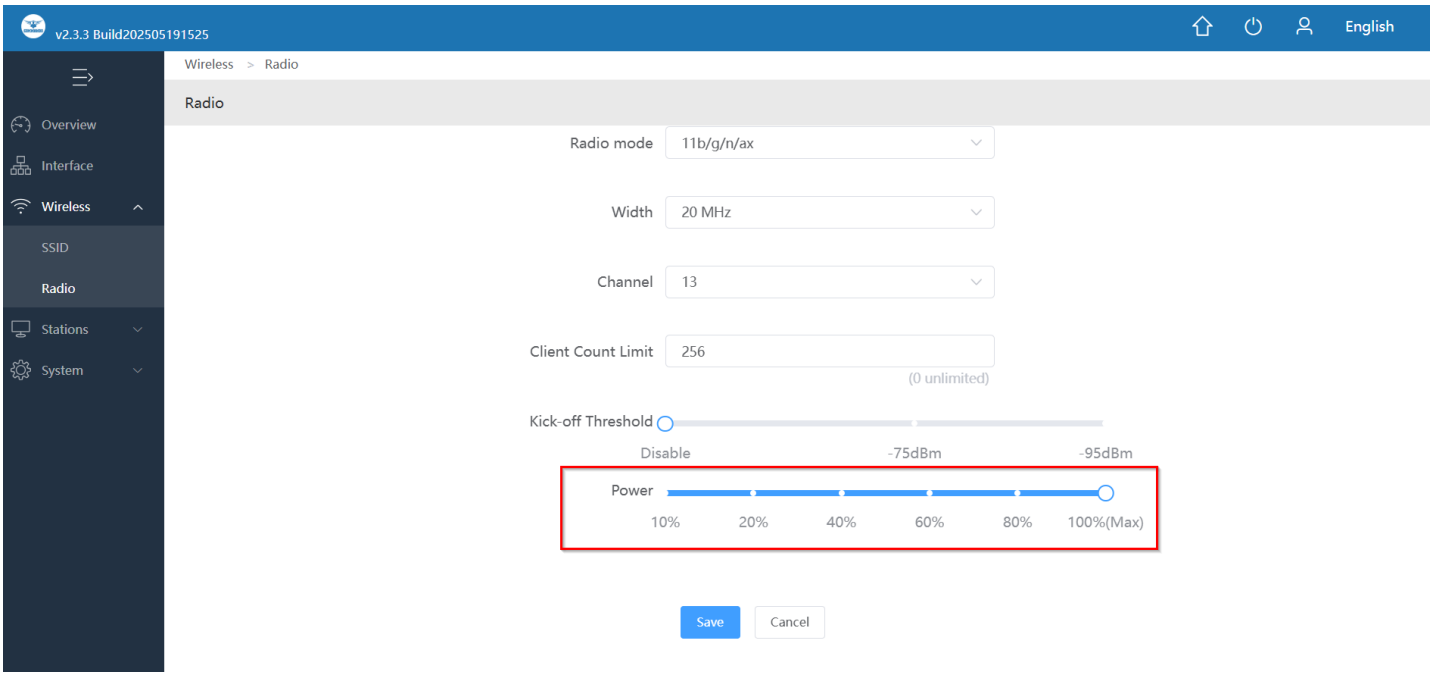


Fig 3.1.22 Changing Transmit Power in 2.4G band of AIR-AP3000AX

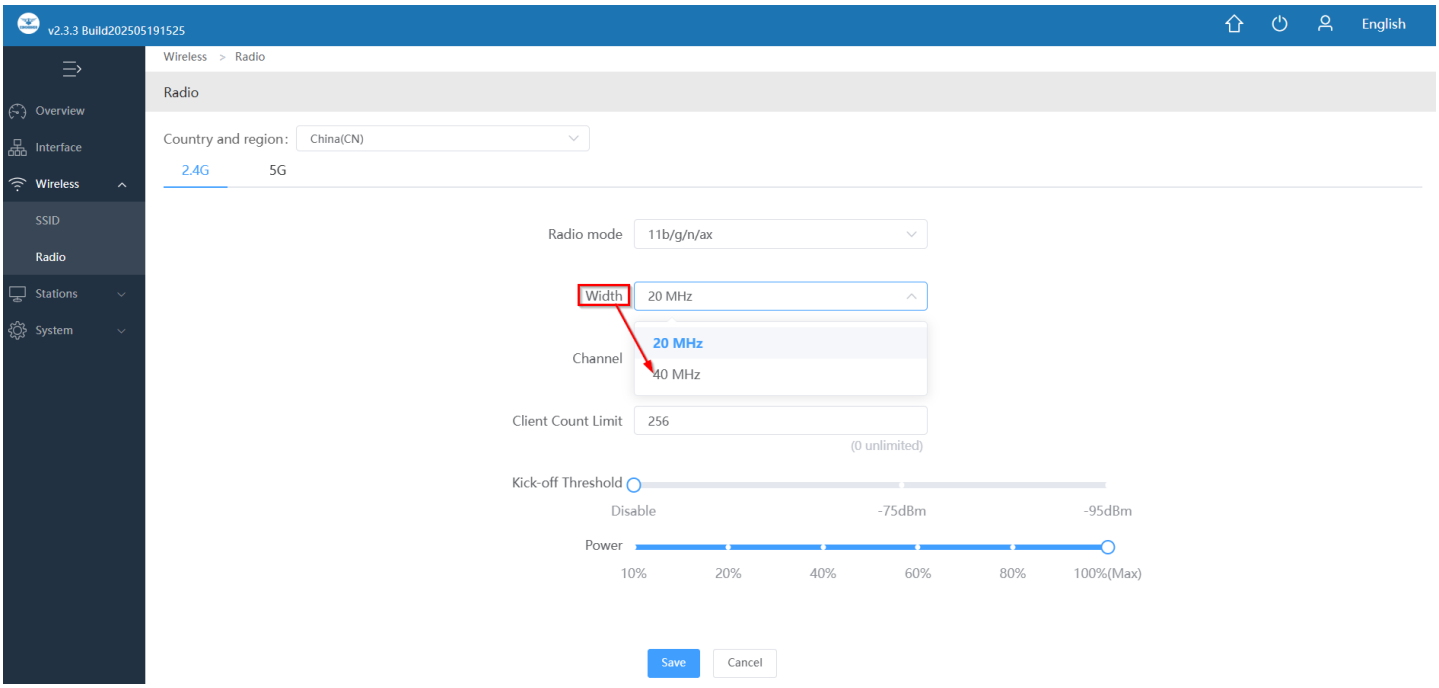


Fig 3.1.23 Changing Channel width in 2.4G band of AIR-AP3000AX

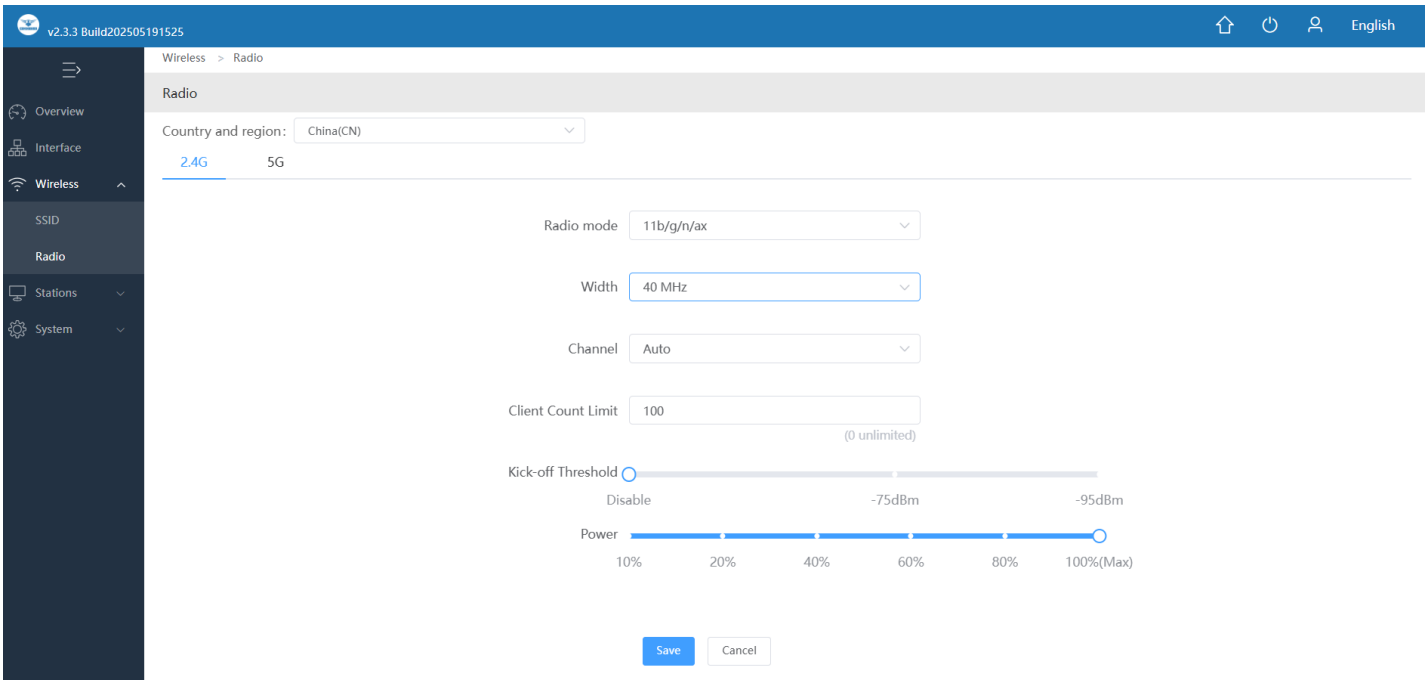


Fig 3.1.24 Configuration in 2.4G band of AIR-AP3000AX

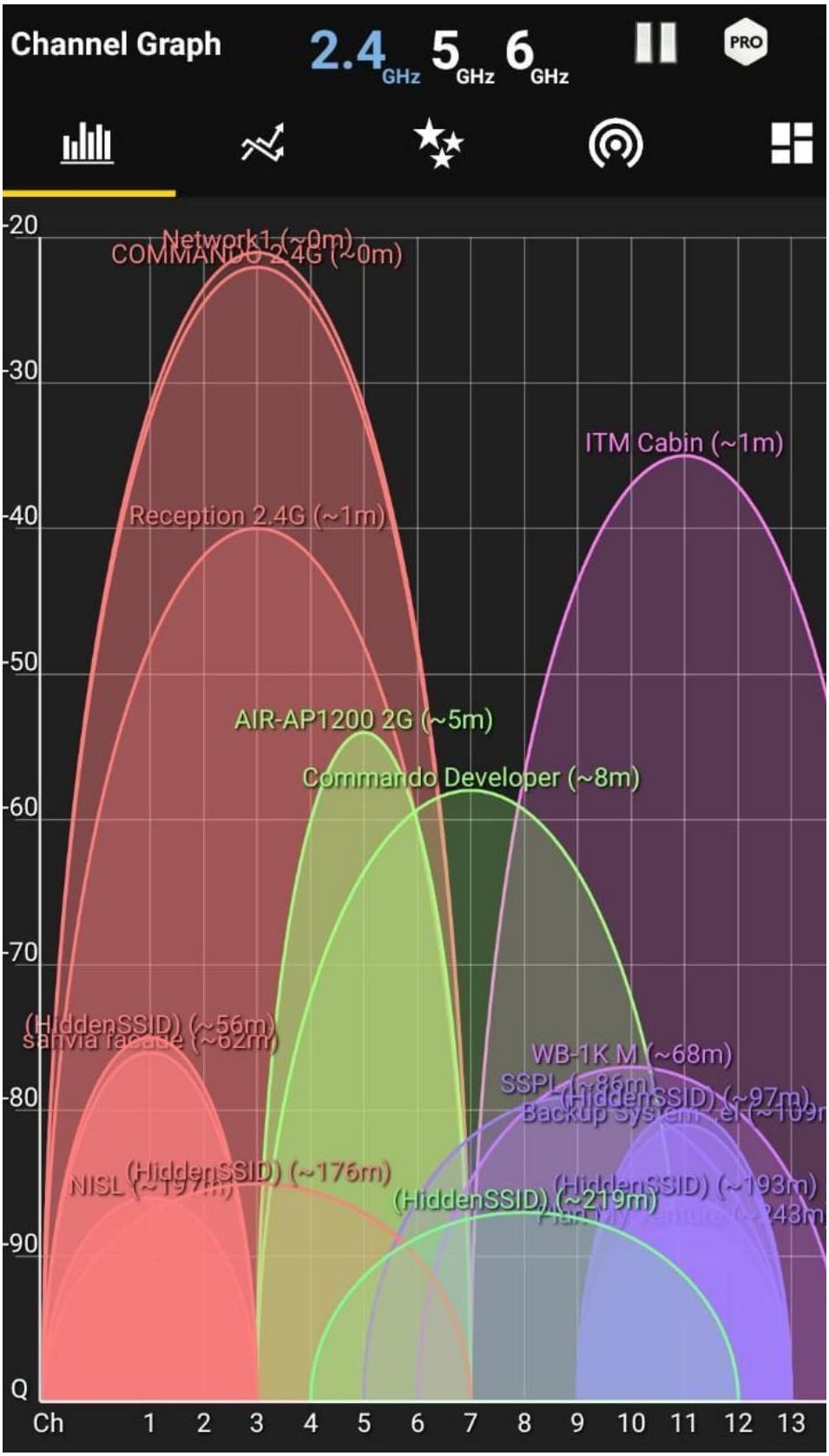


Fig 3.1.25 WiFi analysis 2.4G band of AIR-AP3000AX

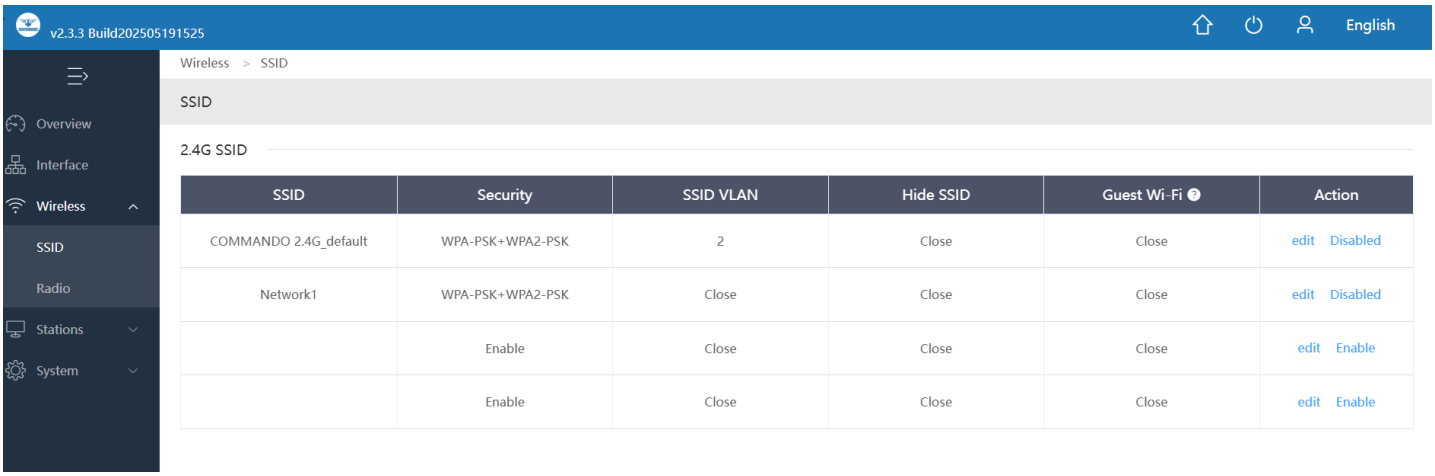


Fig 3.1.26 SSID used for 2.4G band along with desired RF parameter of AIR-AP3000AX

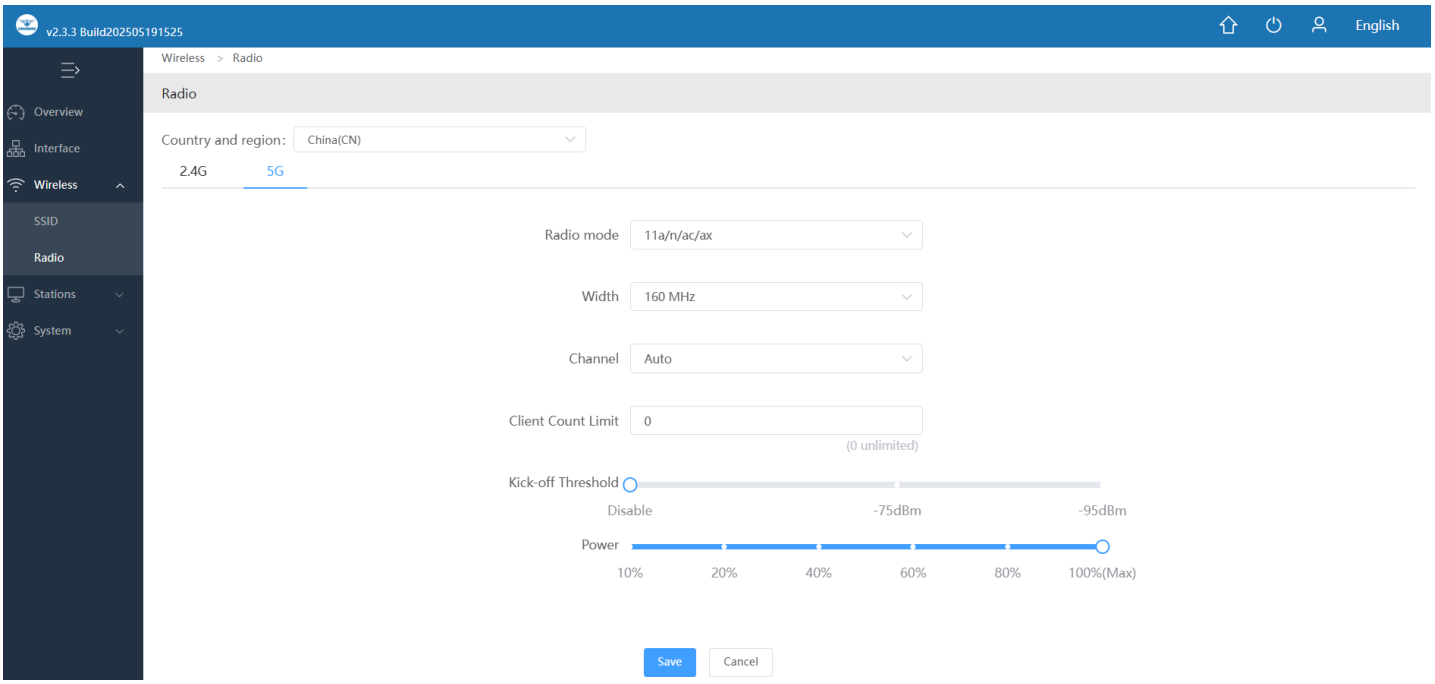


Fig 3.1.27 Default setting in 5G band of AIR-AP3000AX

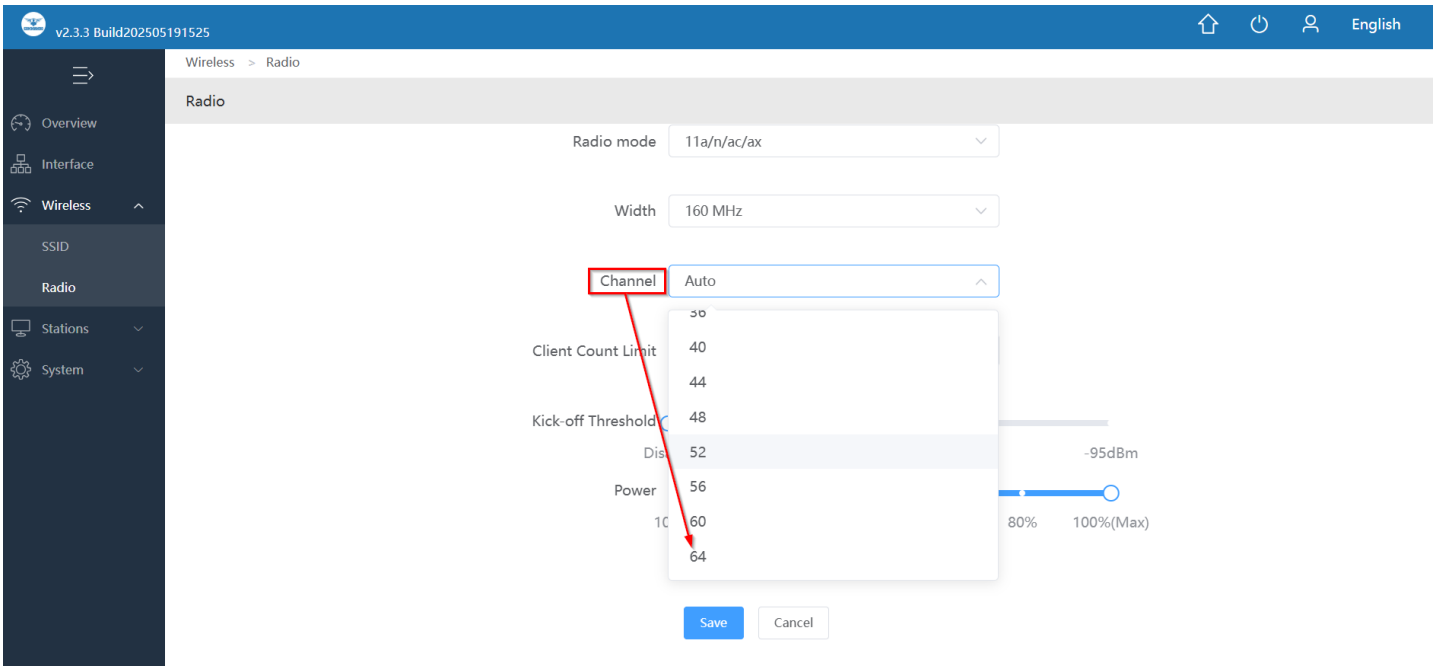


Fig 3.1.28 Changing Channels in 5G band of AIR-AP3000AX

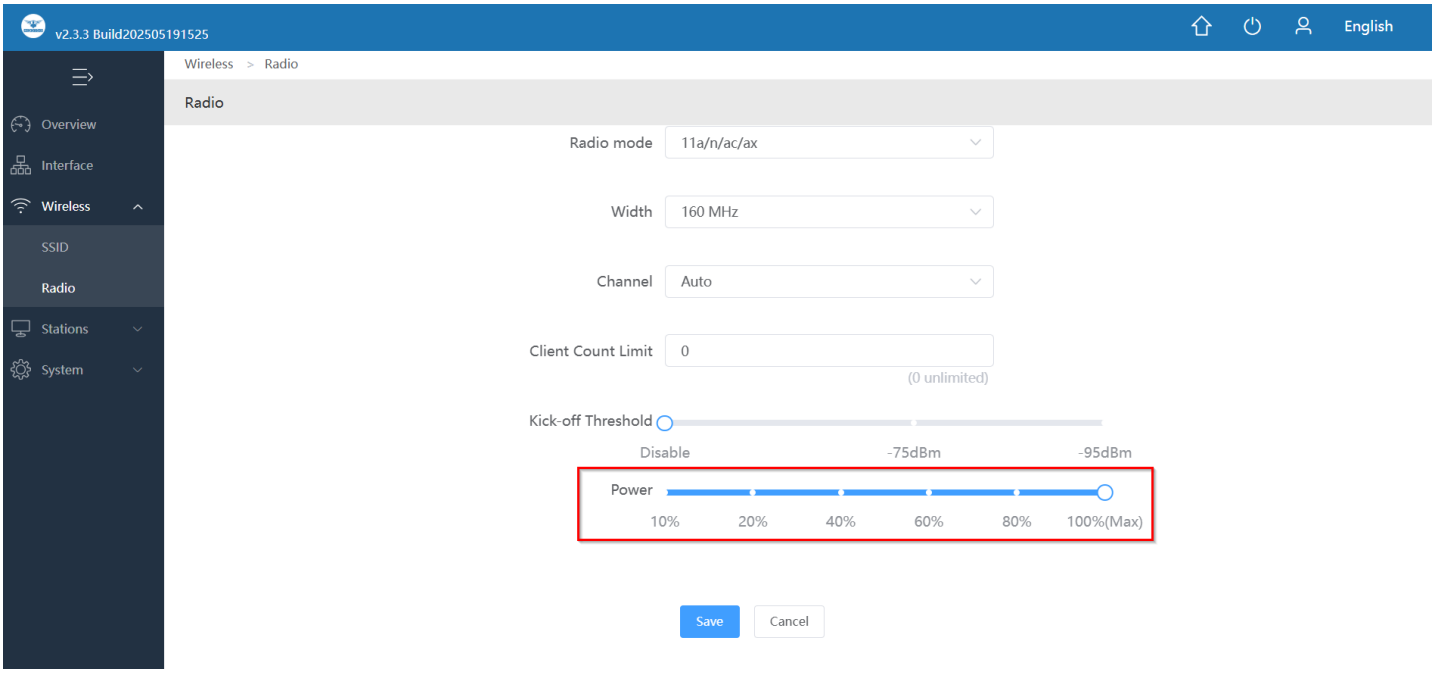


Fig 3.1.29 Changing Transmit Power in 5G band of AIR-AP3000AX

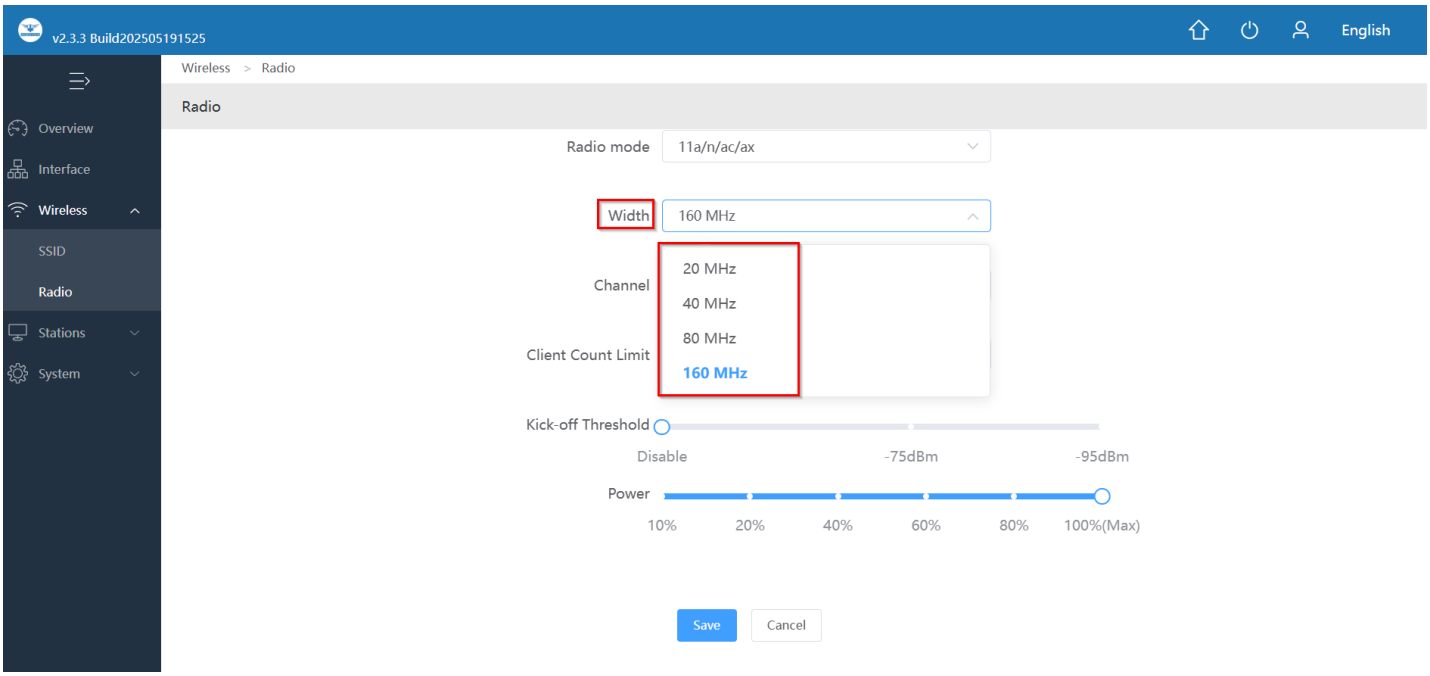


Fig 3.1.30 Changing Channel width in 5G band of AIR-AP3000AX

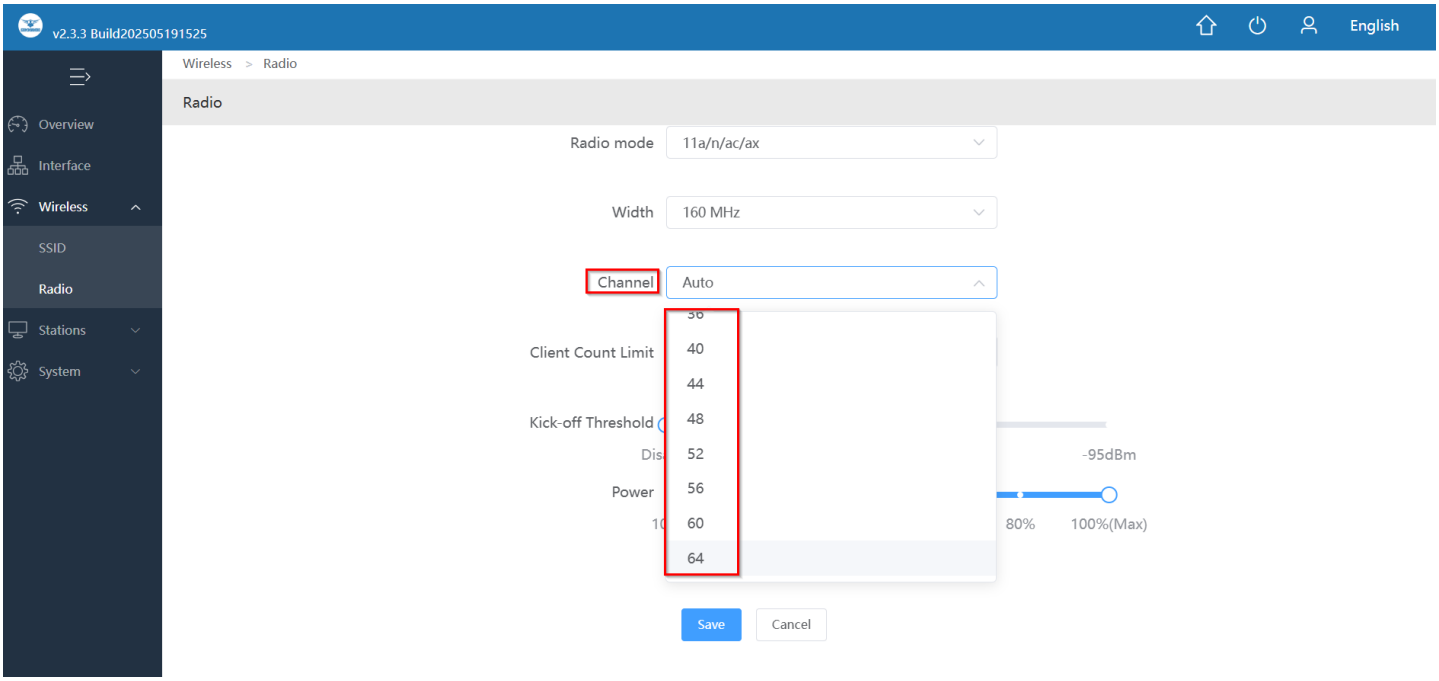


Fig 3.1.31 Configuration of channel in 5G band of AIR-AP3000AX

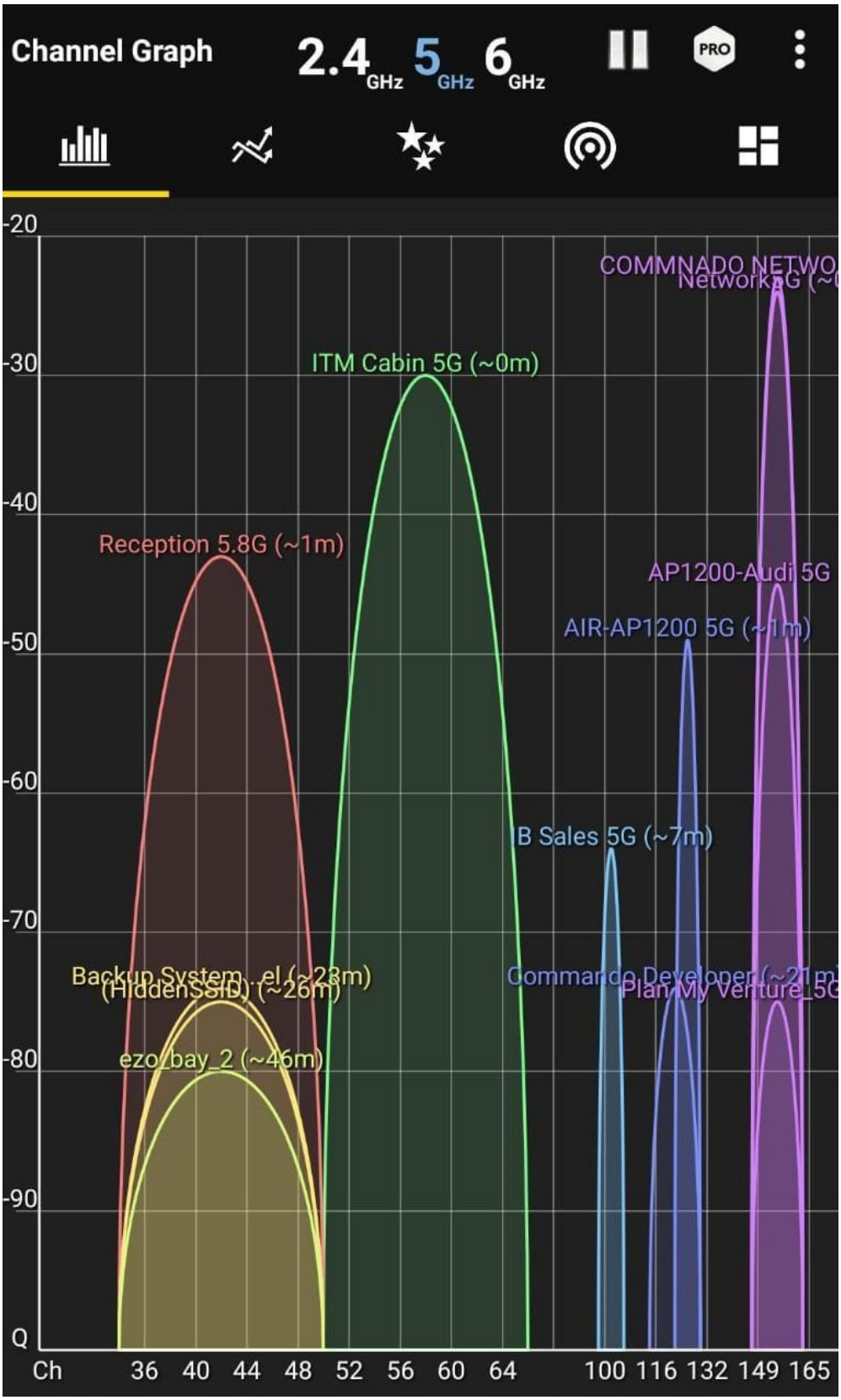


Fig 3.1.32 WiFi analysis of 5G band of AIR-AP3000AX

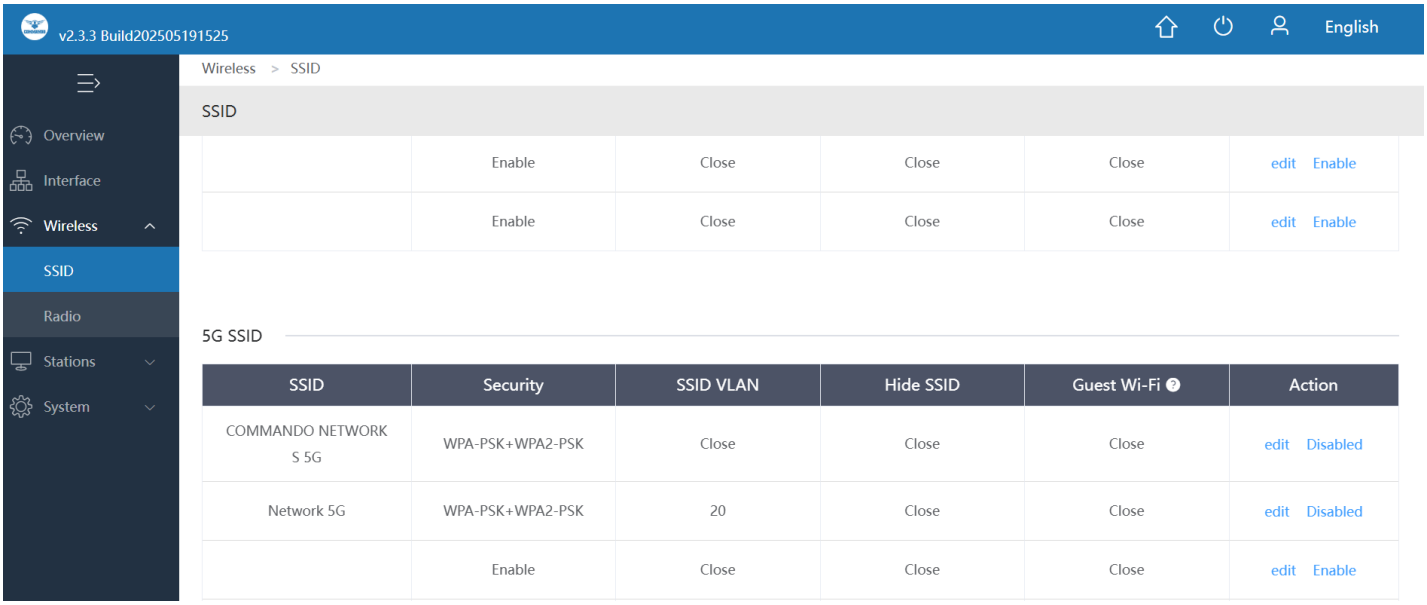


Fig 3.1.33 New SSID Network5G in 5G band of AIR-AP3000AX

4. User control

In user control get in User list of Wireless access user (Clients connected) along with Black and white list.

4.1 User list

Inbuilt intrusion prevention protects data and network clients and disallow unauthorized wireless client by blacklisting and white list.

For User List Click on, Stations >Station List

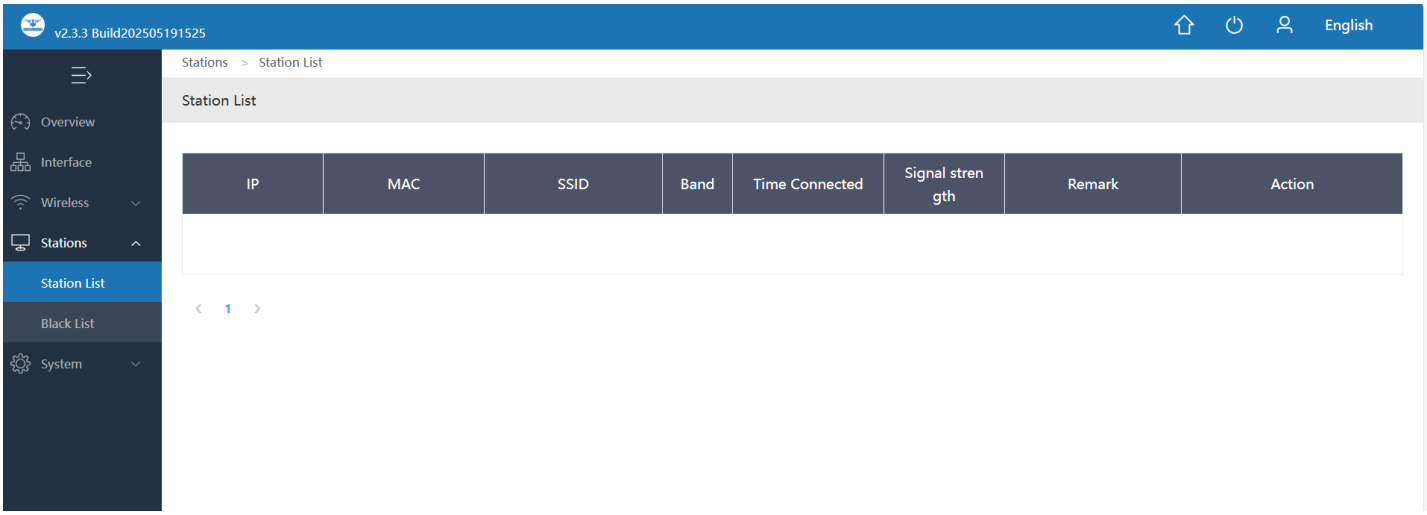


Fig 4.1.1 Default User List of AIR-AP3000AX

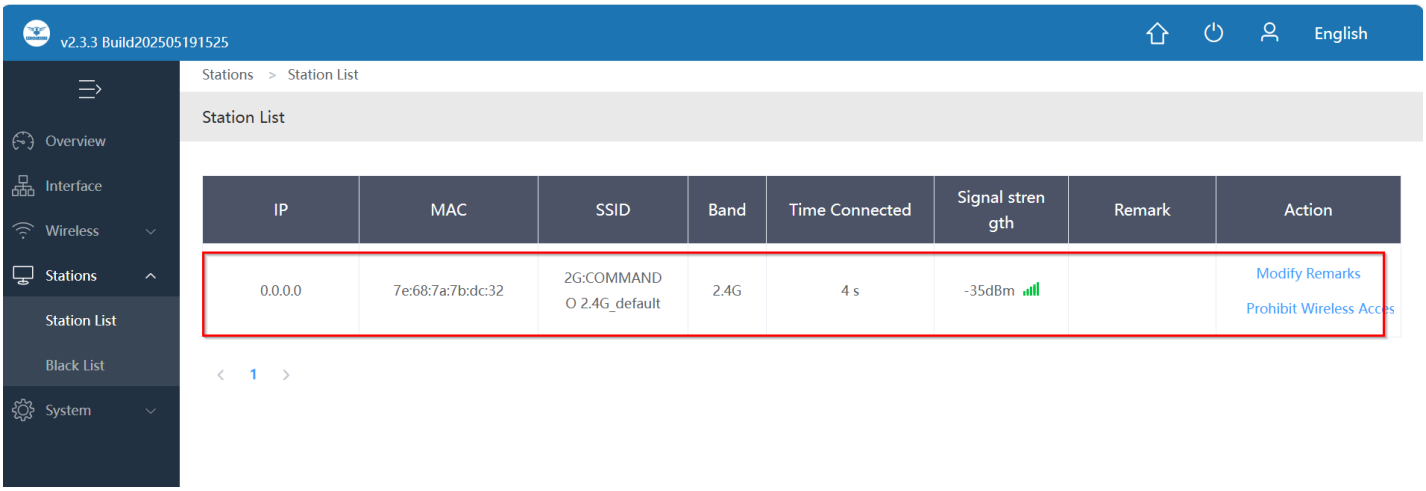


Fig 4.1.2 User List of AIR-AP3000AX

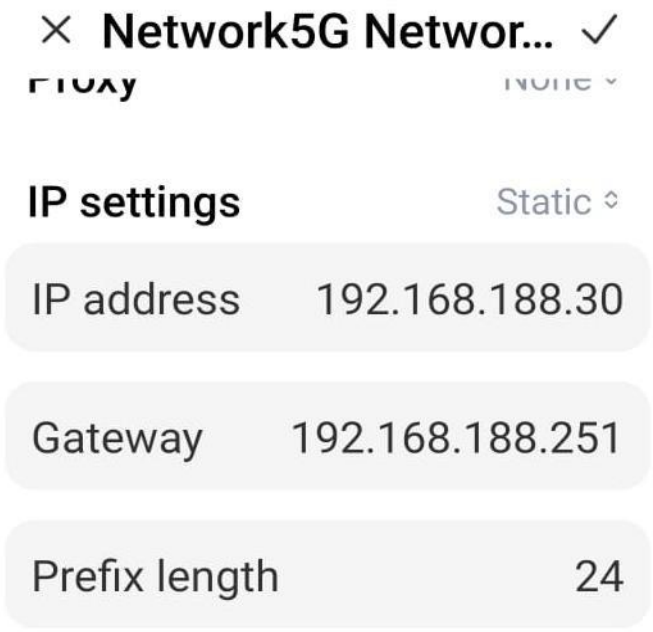


Fig 4.1.3 Connected wireless client of AIR-AP3000AX

Note:

You can also set DHCP Server is a network server that automatically provides and assigns IP addresses to wireless client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

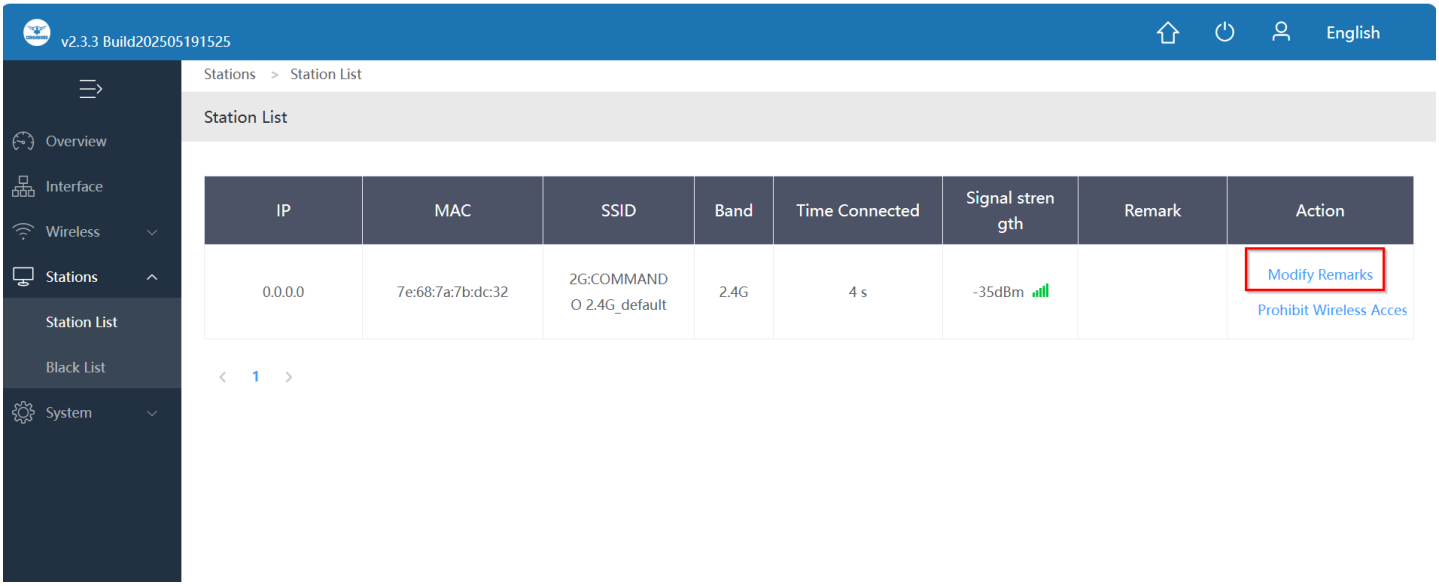


Fig 4.1.4 Modifying connected user notes of AIR-AP3000AX

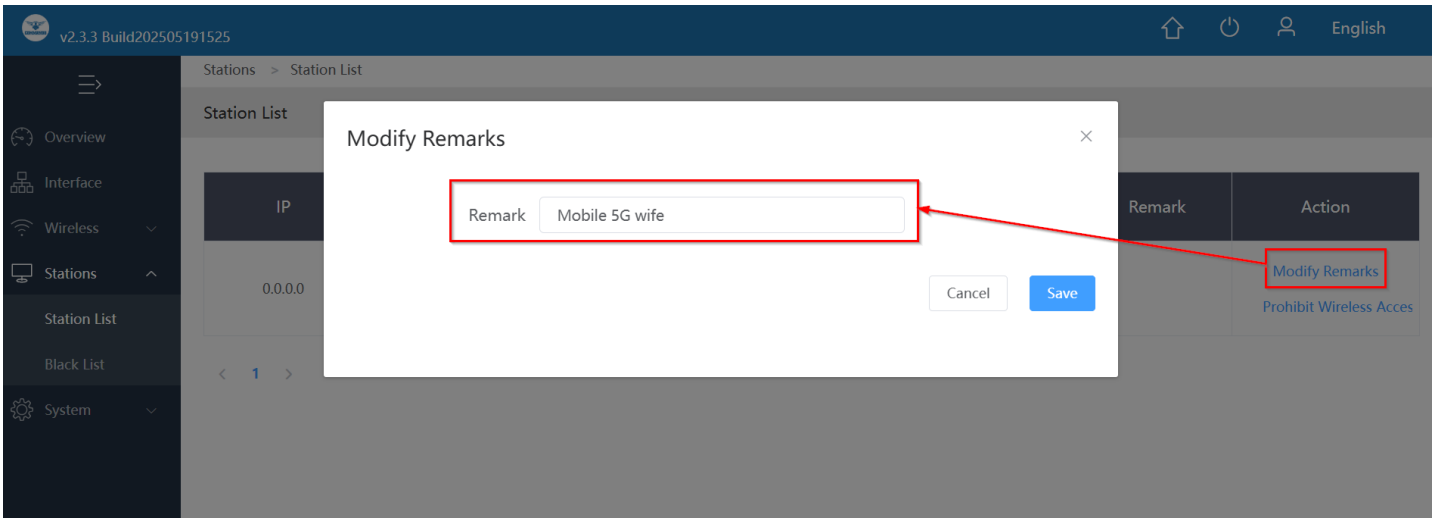


Fig 4.1.5 Changing User remarks AIR-AP3000AX

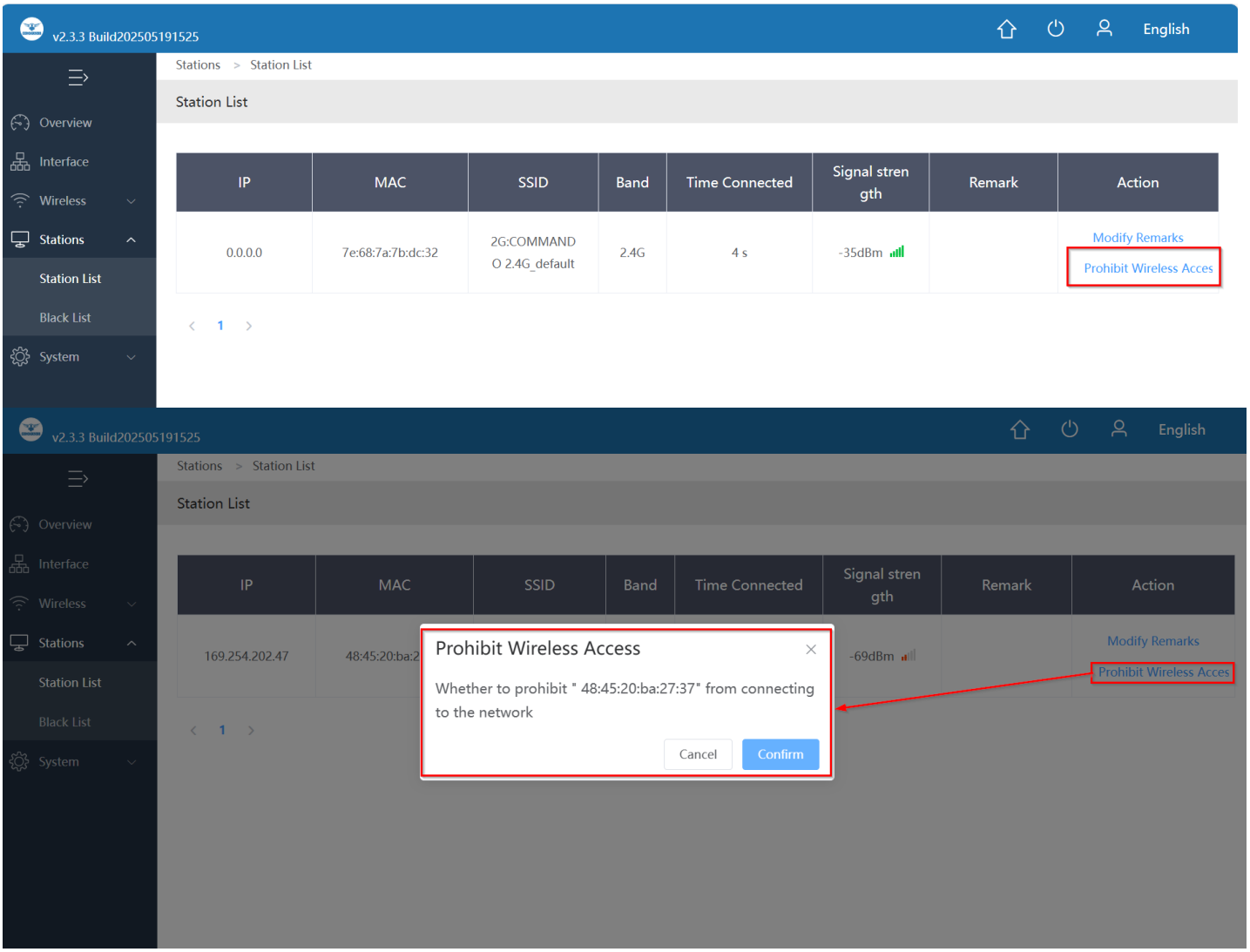


Fig 4.1.6 Disallowing user to access WiFi for AIR-AP3000AX

4.2 Black and white list

In Blacklist Mode, MACs which are listed are forbidden to access the wireless network. In Whitelist Mode all MACs except whitelist are allowed to access wireless network.

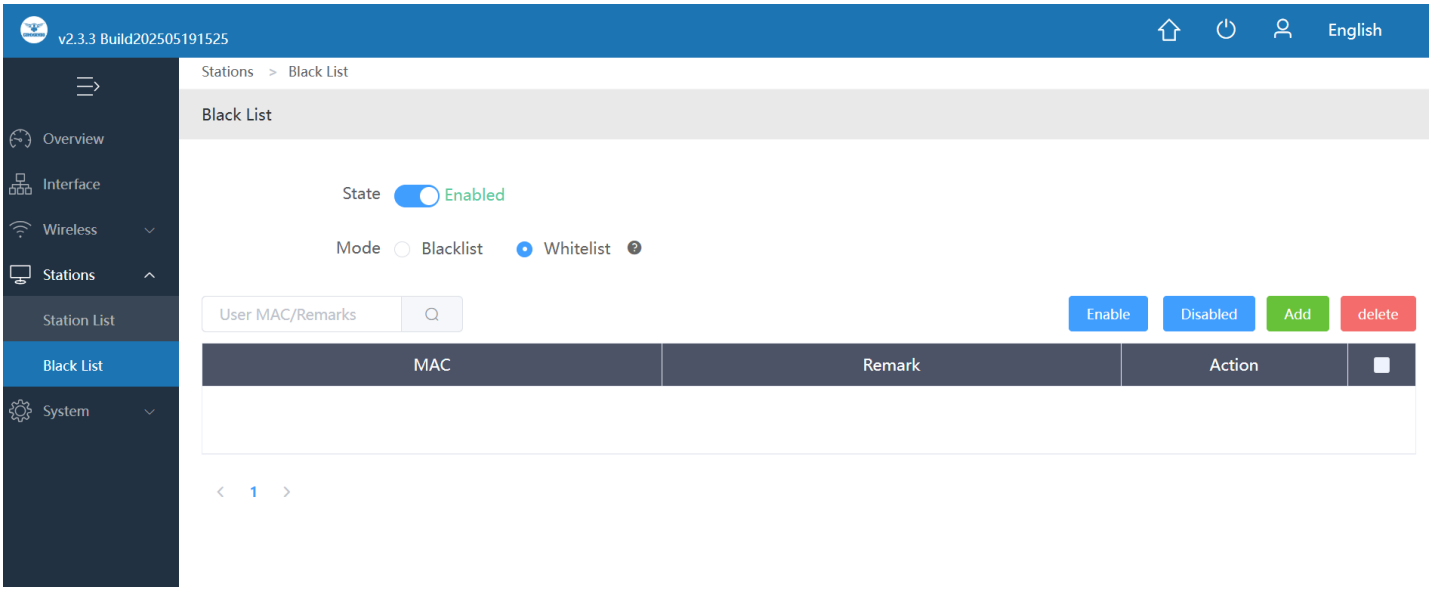


Fig 4.2.1 Black White List users in network.

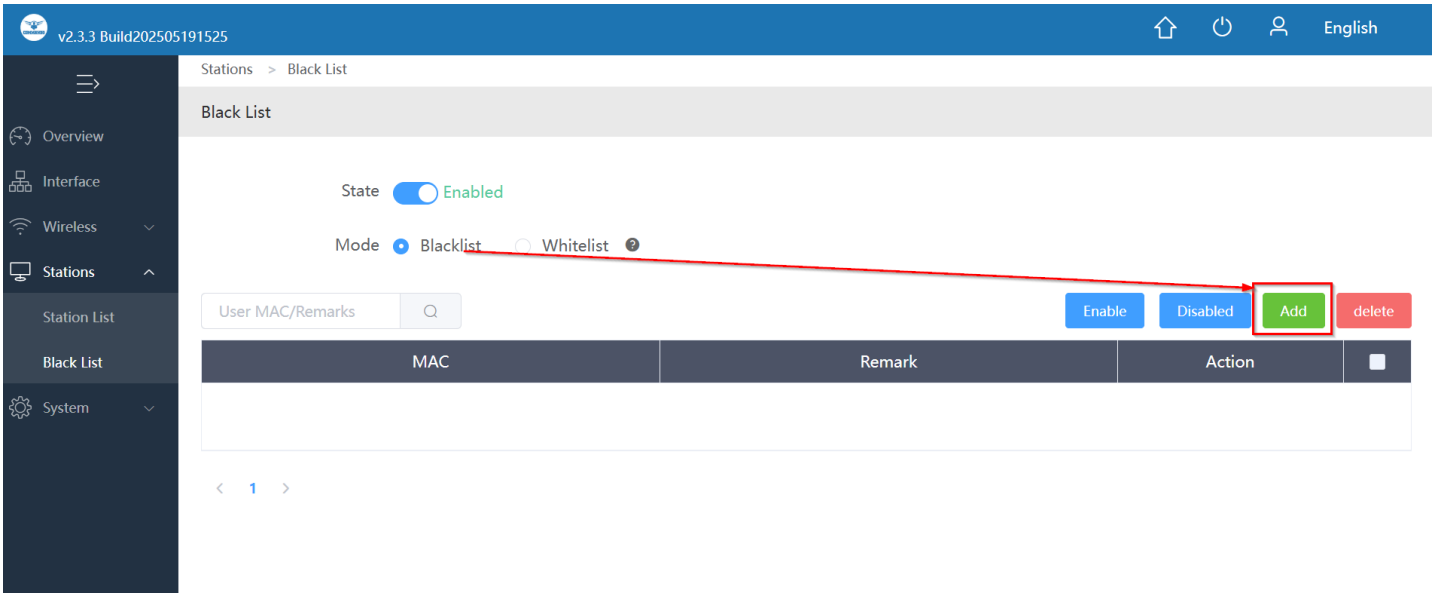


Fig 4.2.2 Add Blacklist Mac in AIR-AP3000AX

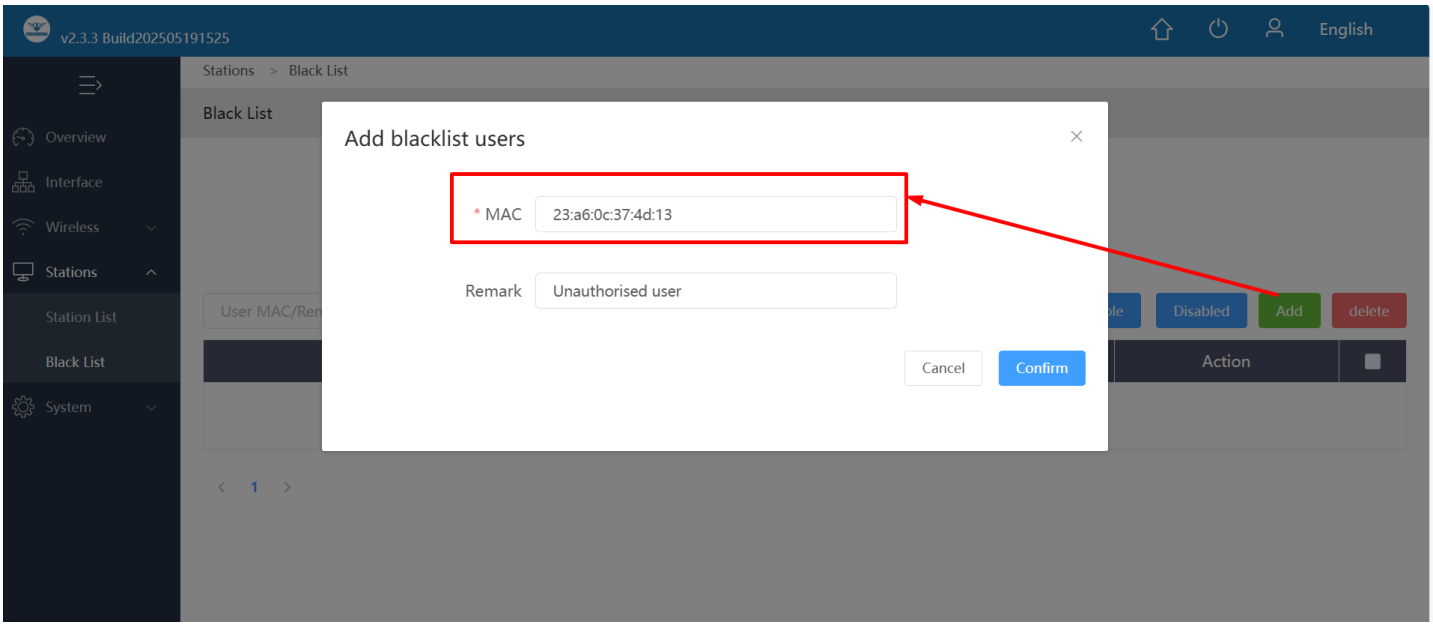


Fig 4.2.3 Add Blacklist User Mac in AIR-AP3000AX

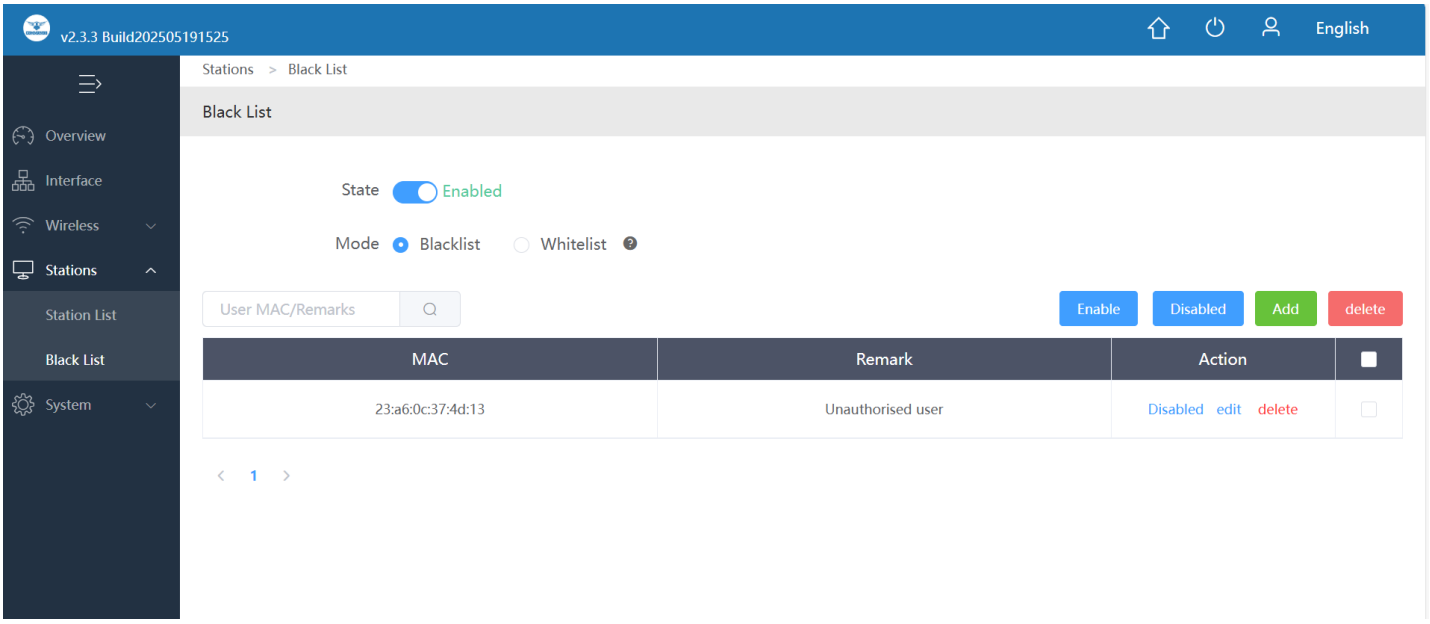


Fig 4.2.4 Blacklisted User in AIR-AP3000AX

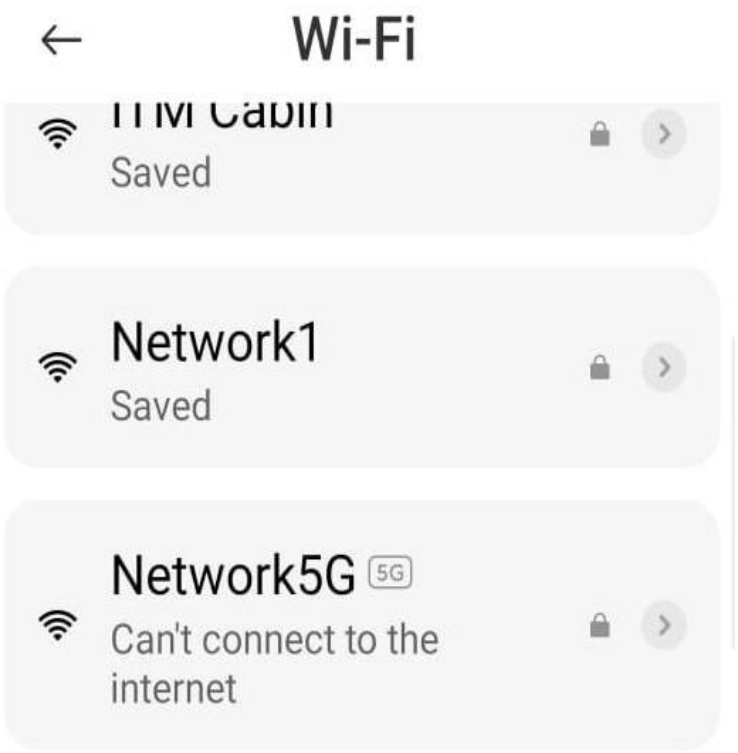


Fig 4.2.5 Status of wireless client after Blacklist in AIR-AP3000AX

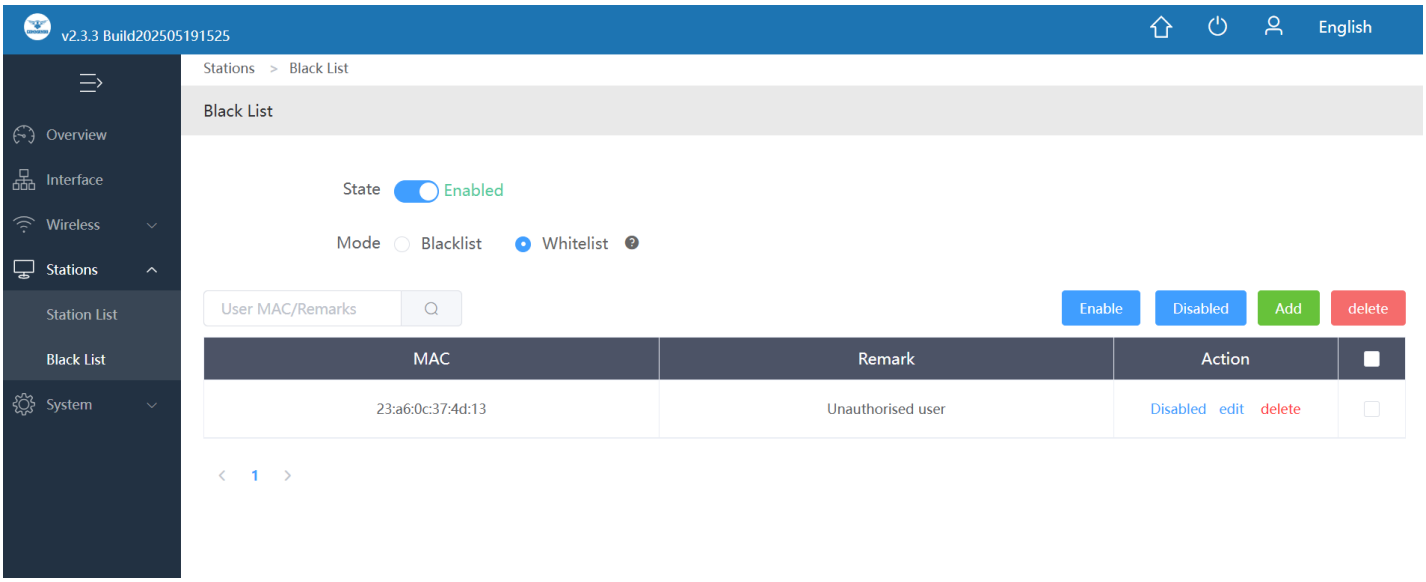


Fig 4.2.6 Add whitelist Mac in AIR-AP3000AX

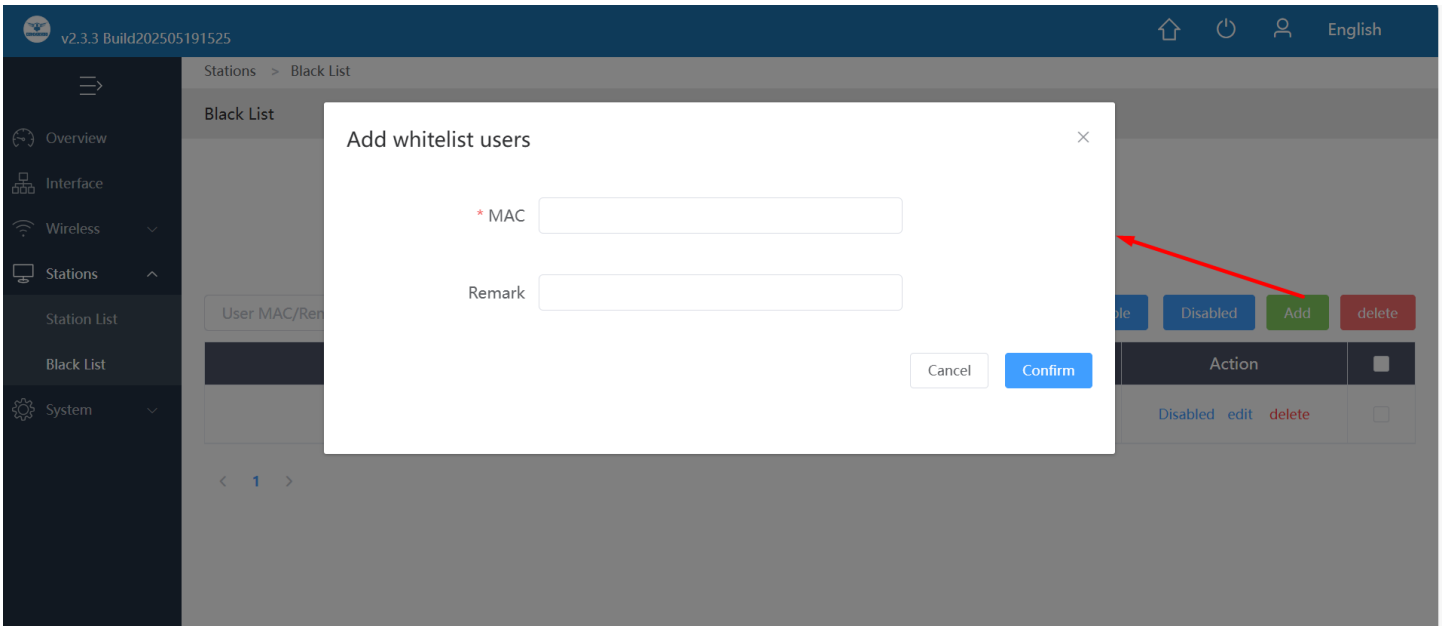


Fig 4.2.7 Add whitelist User Mac in AIR-AP3000AX

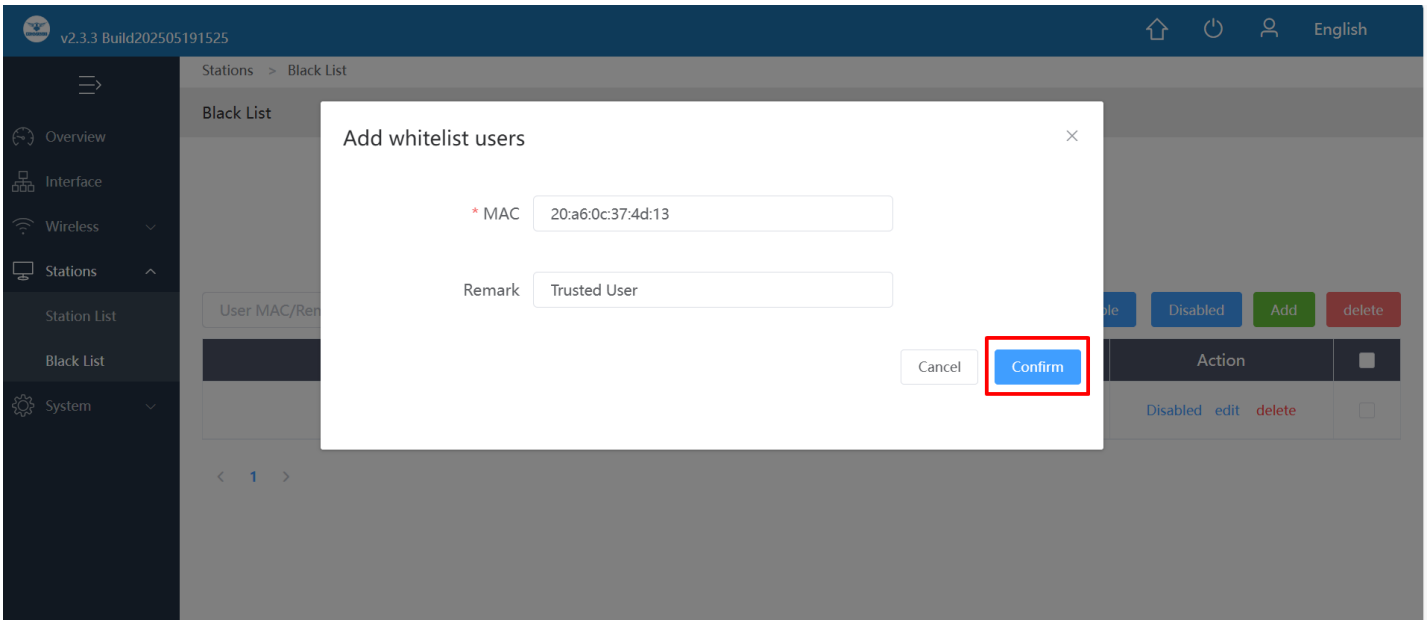


Fig 4.2.8 Add Whitelist User Mac in AIR-AP3000AX

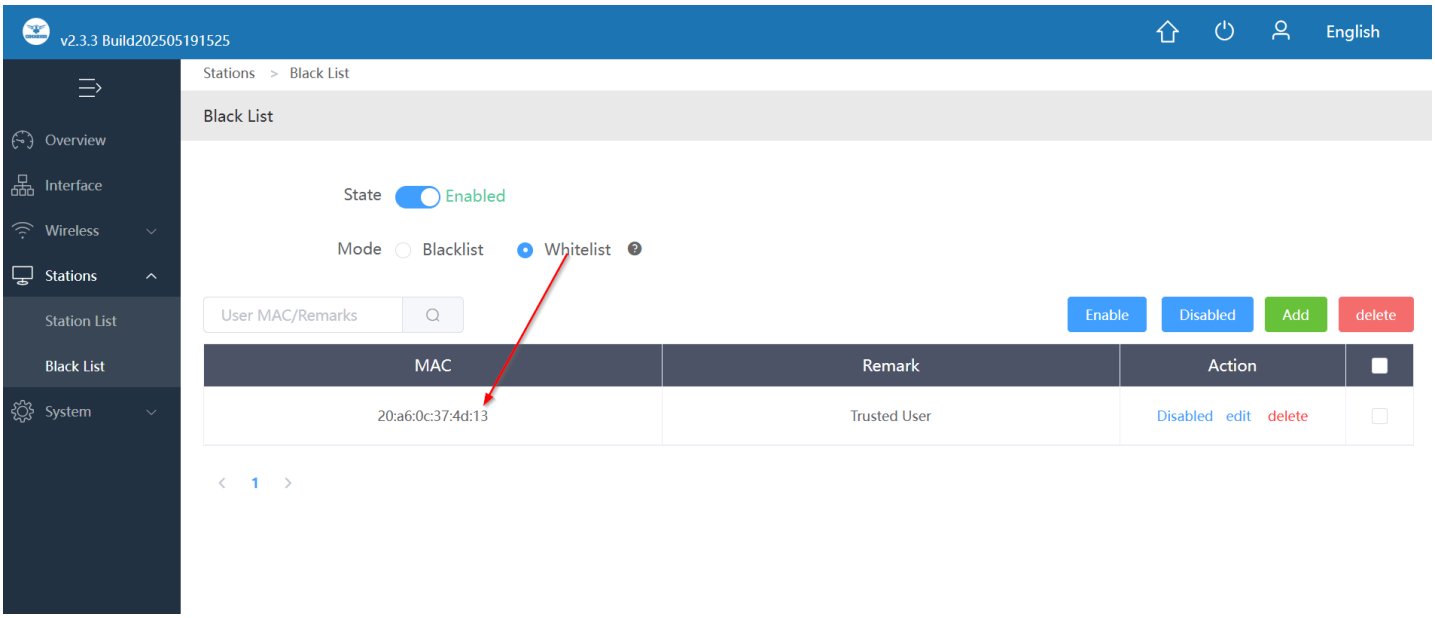


Fig 4.2.9 Whitelisted User in AIR-AP3000AX

5. System settings

In System settings you can do Basic, Timing, Login, Device reboot and Restore.

5.1 Basic Setting

In basic setting you can you can change Equipment Name, and AP Work Mode from FIT, FAT and Routing mode.

For Changing Basic settings, Click on System settings >Basic settings

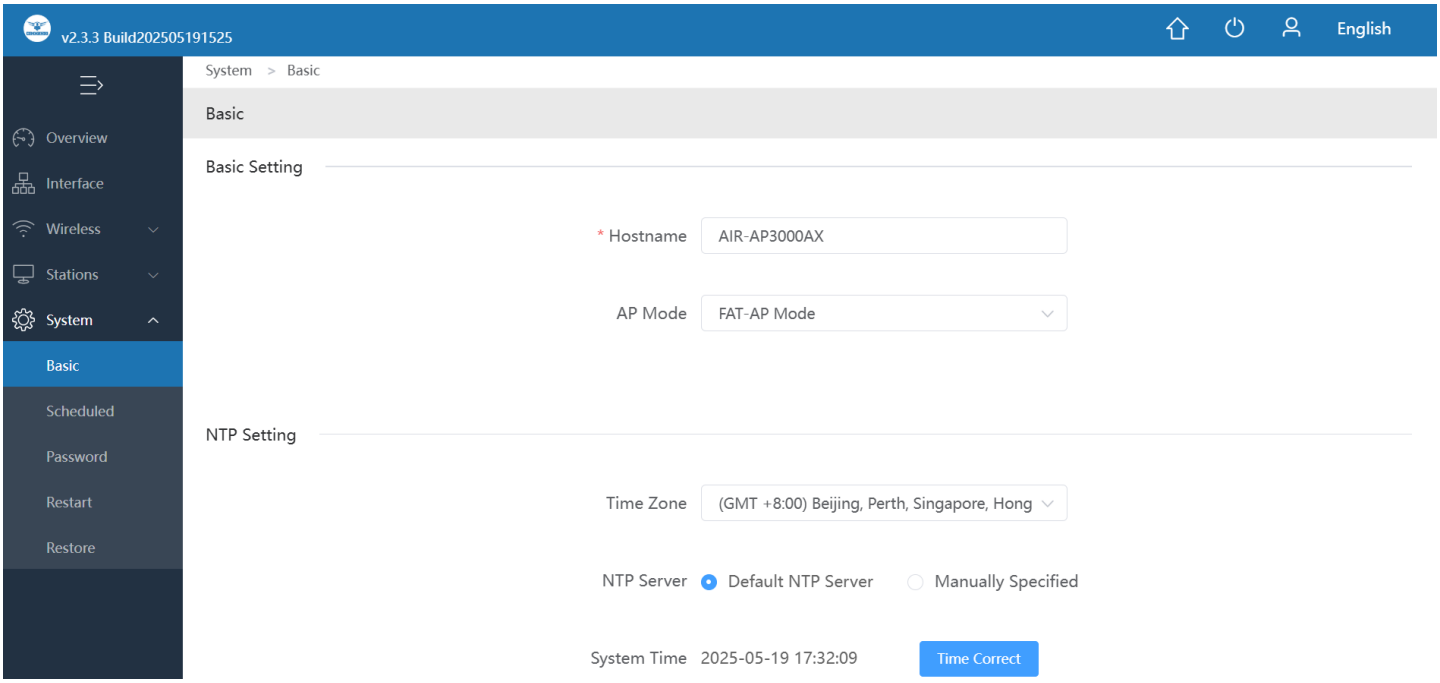


Fig 5.1.1 Default Basic setting of AIR-AP3000AX

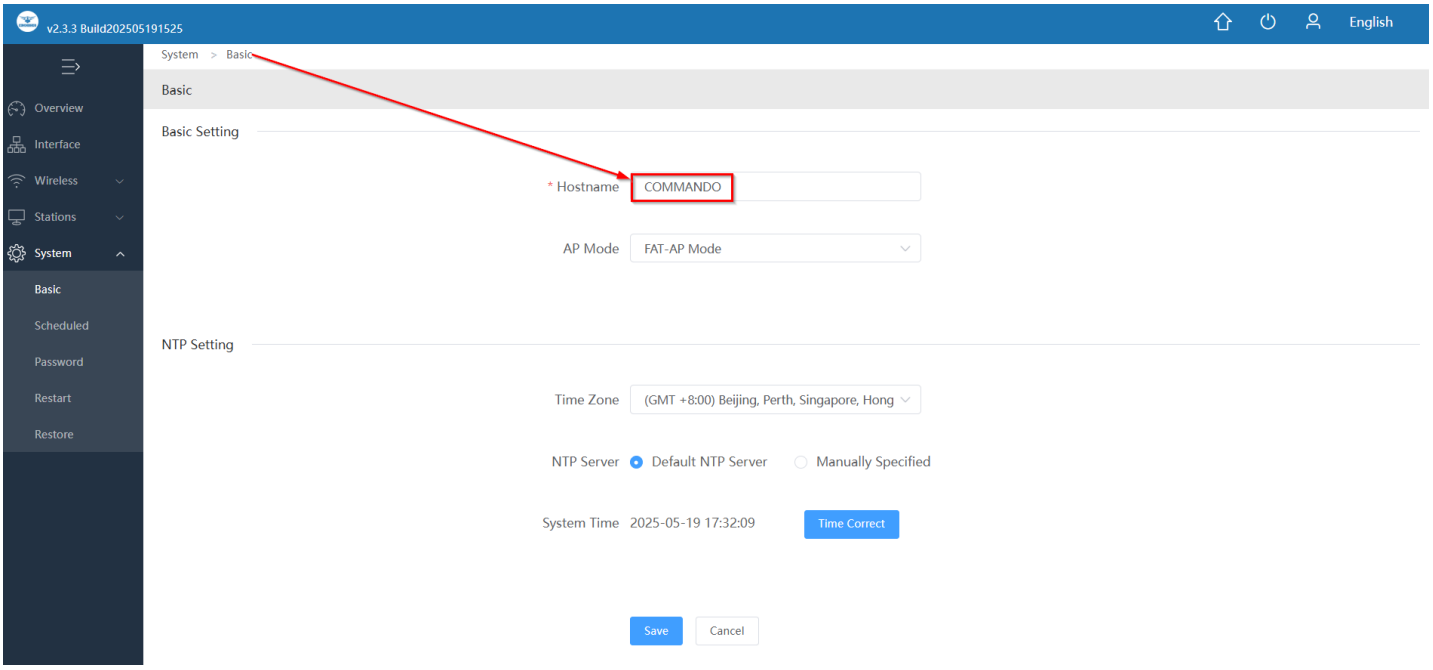


Fig 5.1.2 Change equipment name of AIR-AP3000AX

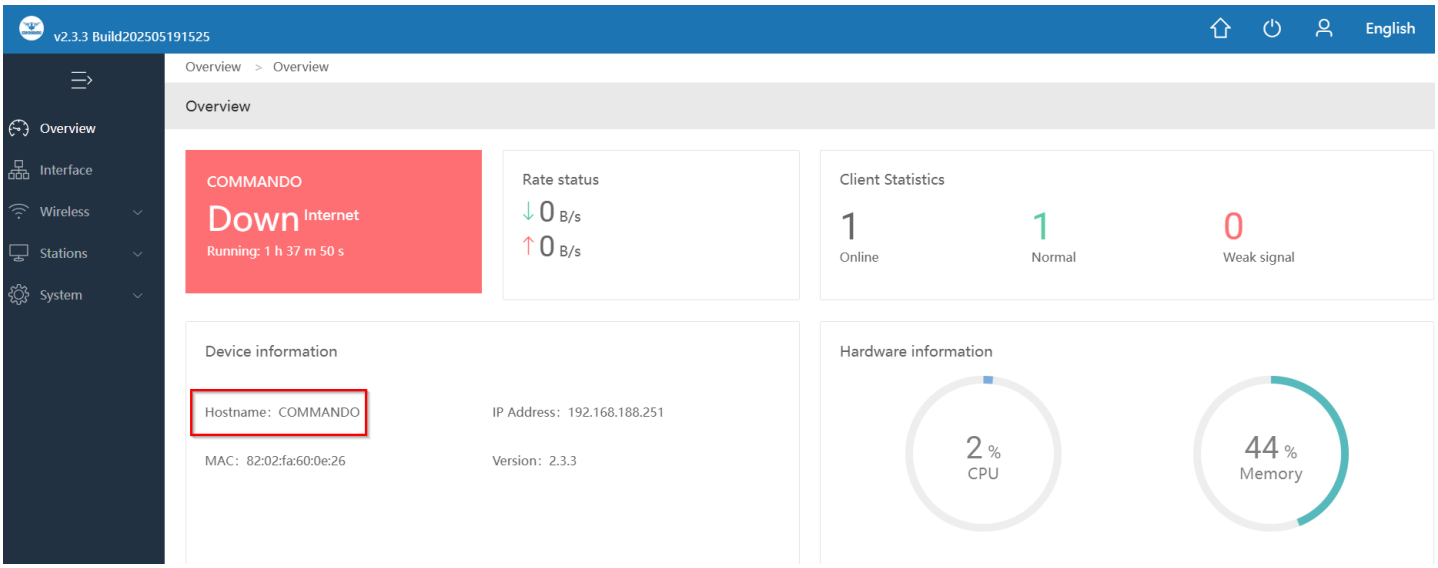


Fig 5.1.3 New Equipment name of AIR-AP3000AX

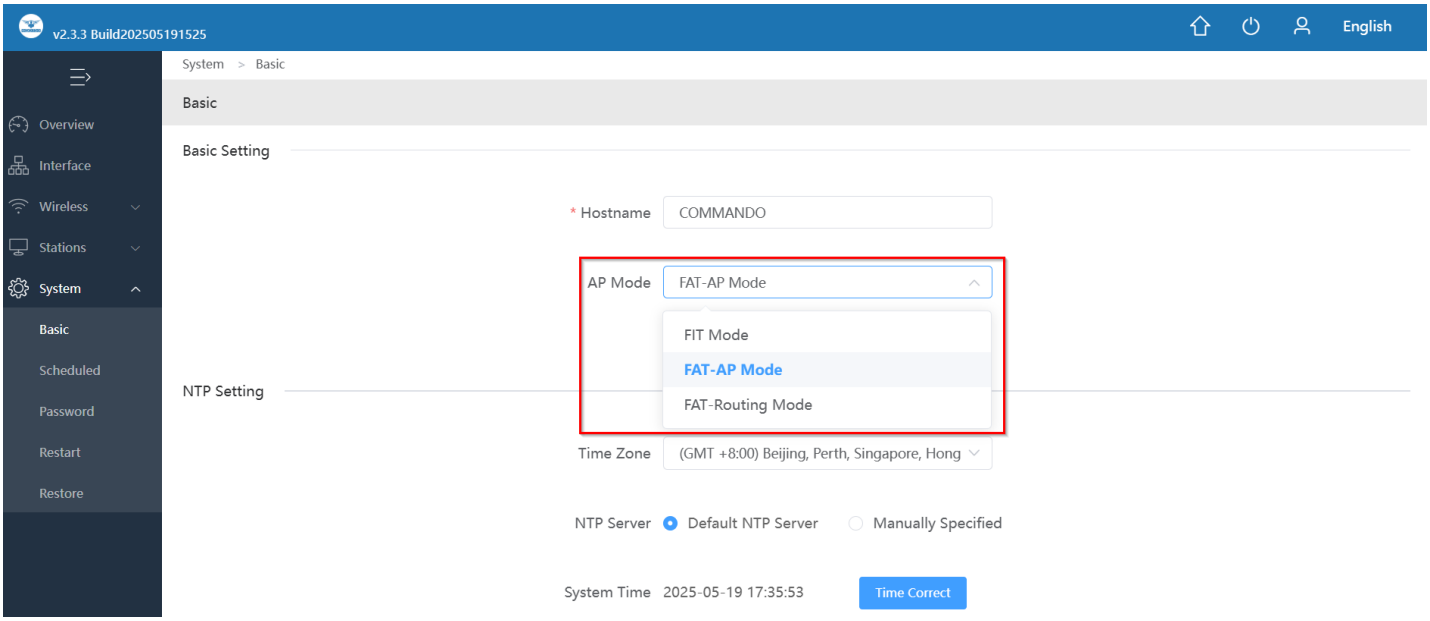


Fig 5.1.4 Default work mode of AIR AP3000AX Note:- Default work mode of AP is FIT mode.

5.2 Timing Setting

With System Time you can schedule WiFi availability and unavailability to wireless users and also can configure Scheduled reboot.

For Changing Timing setting click on, System settings >Timing setting

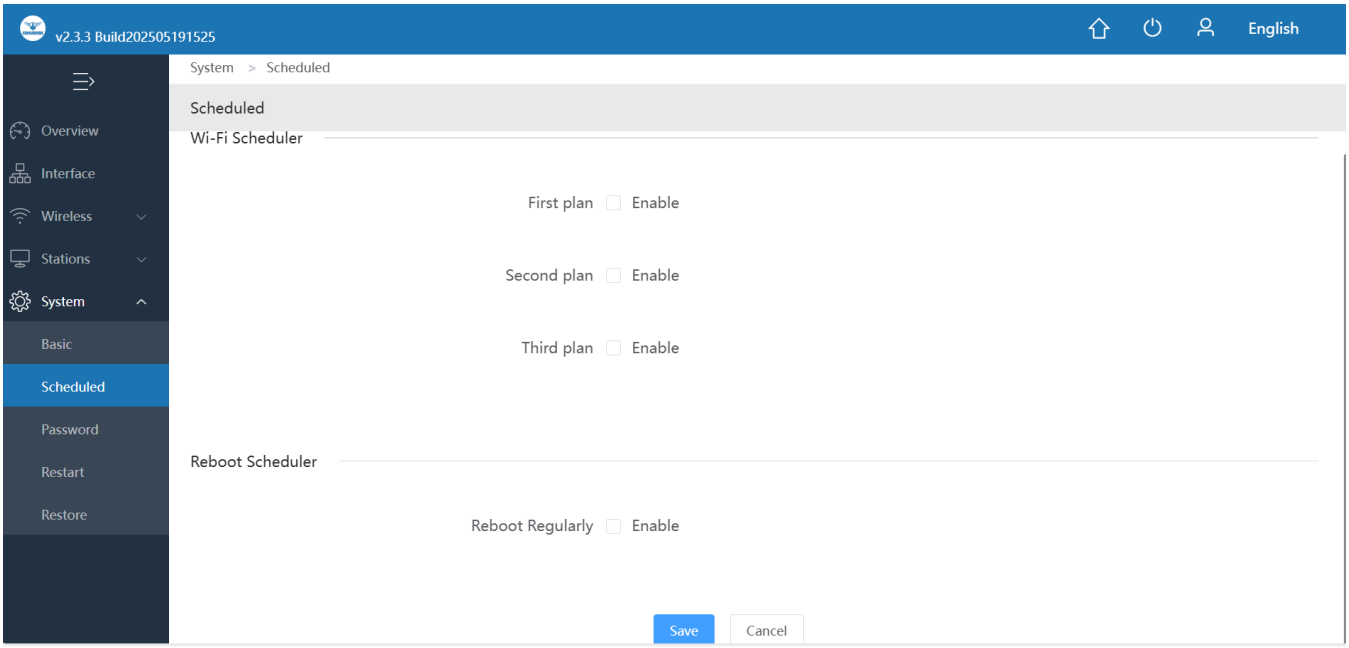


Fig 5.2.1 Default timing setting for AIR-AP3000AX

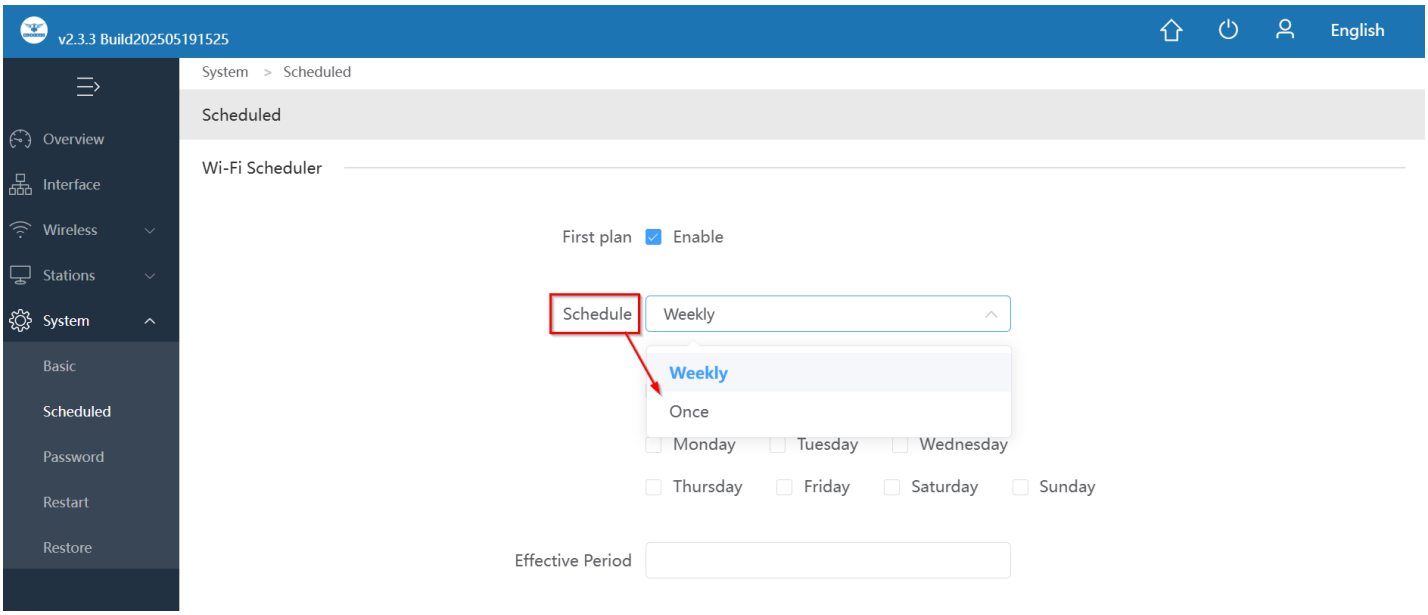


Fig 5.2.2 Setting schedule for wireless availability for AIR-AP3000AX

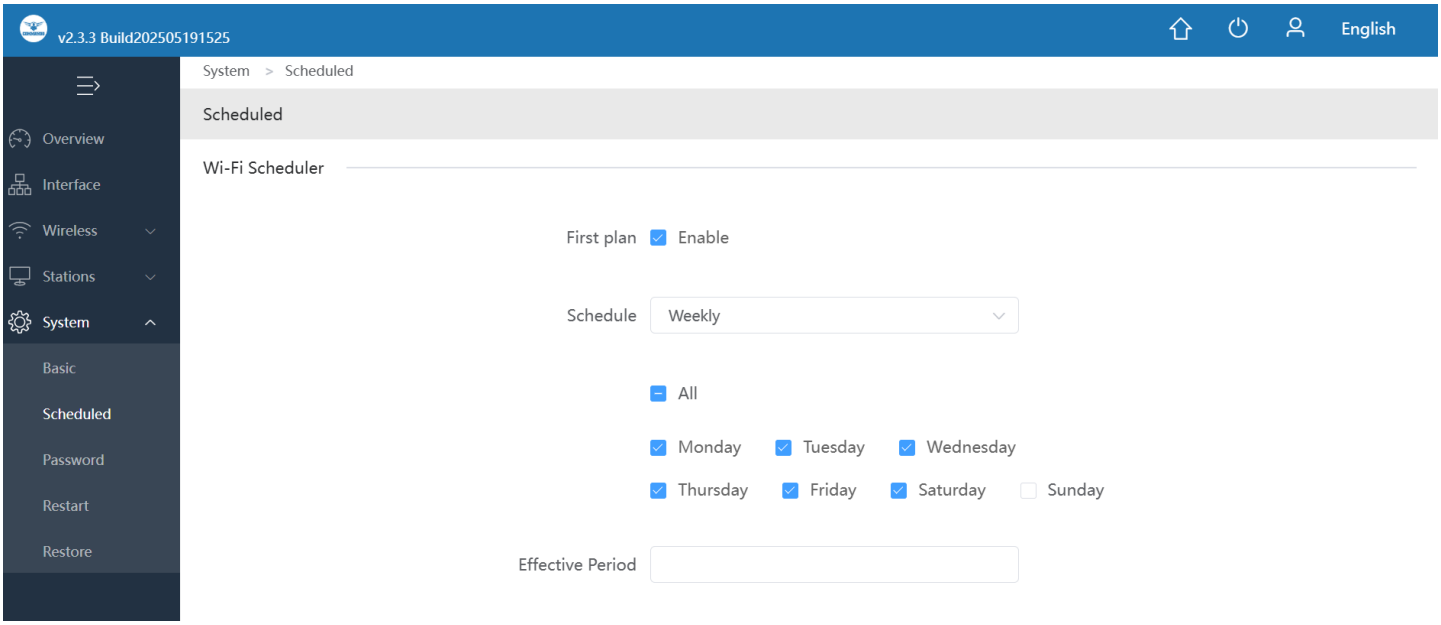


Fig 5.2.3 Setting Days and period for AP available AIR-AP3000AX

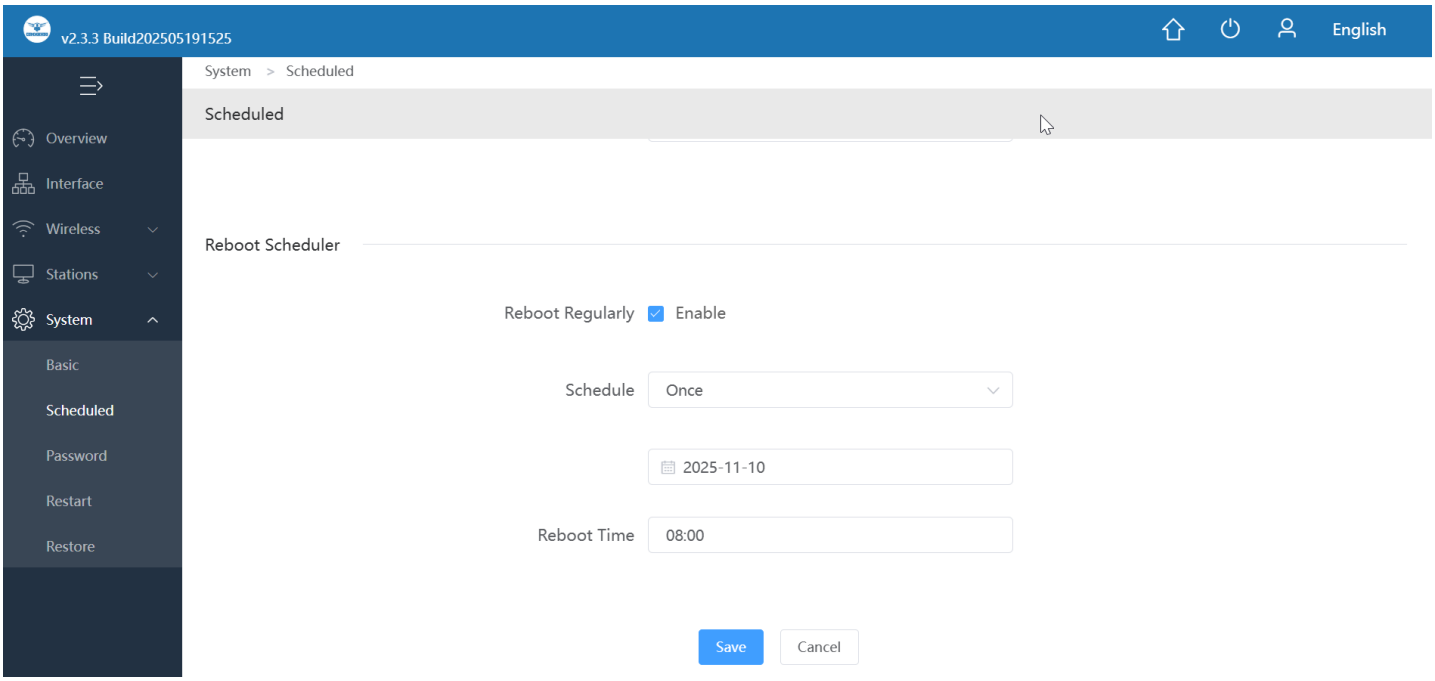


Fig 5.2.4 Setting reboot for AP available AIR-AP3000AX

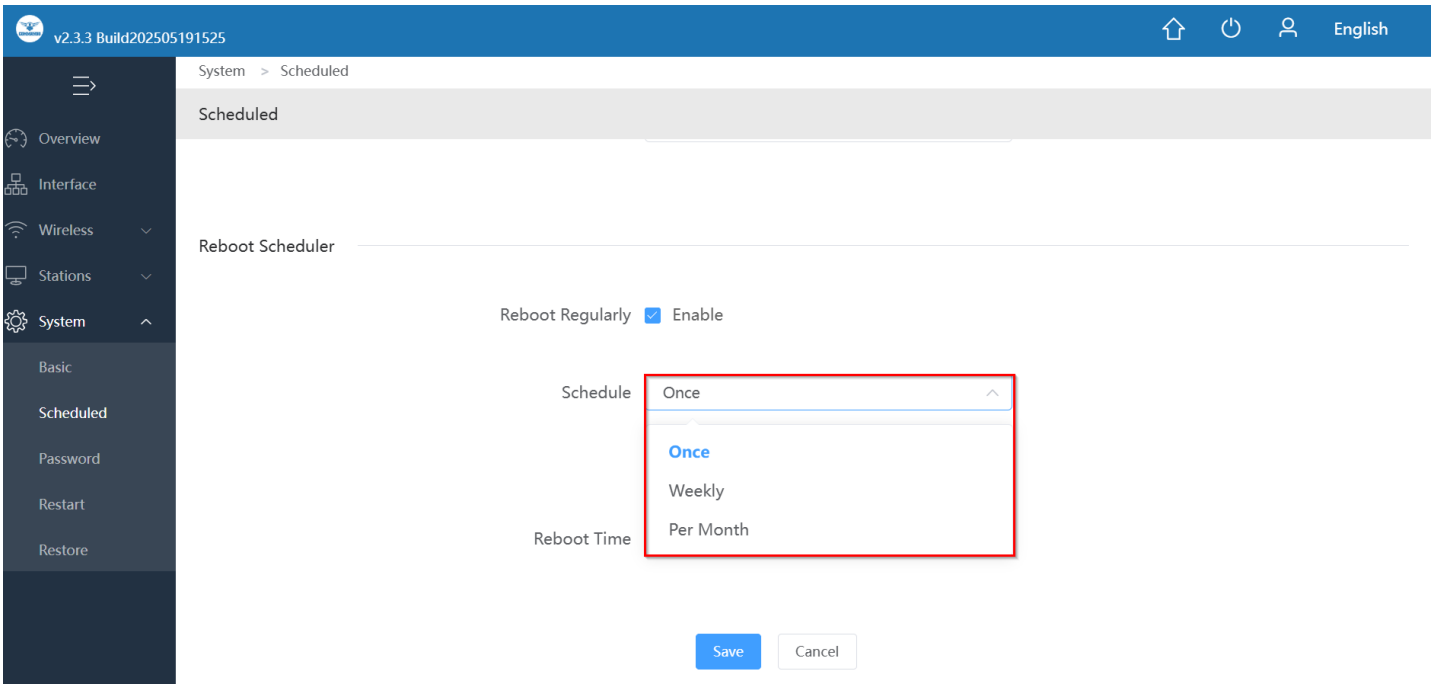


Fig 5.2.5 Selecting reboot frequency for AP available AIR-AP3000AX

5.3 Login Management

You can create password as per your choice and even change the admin password for login to device.

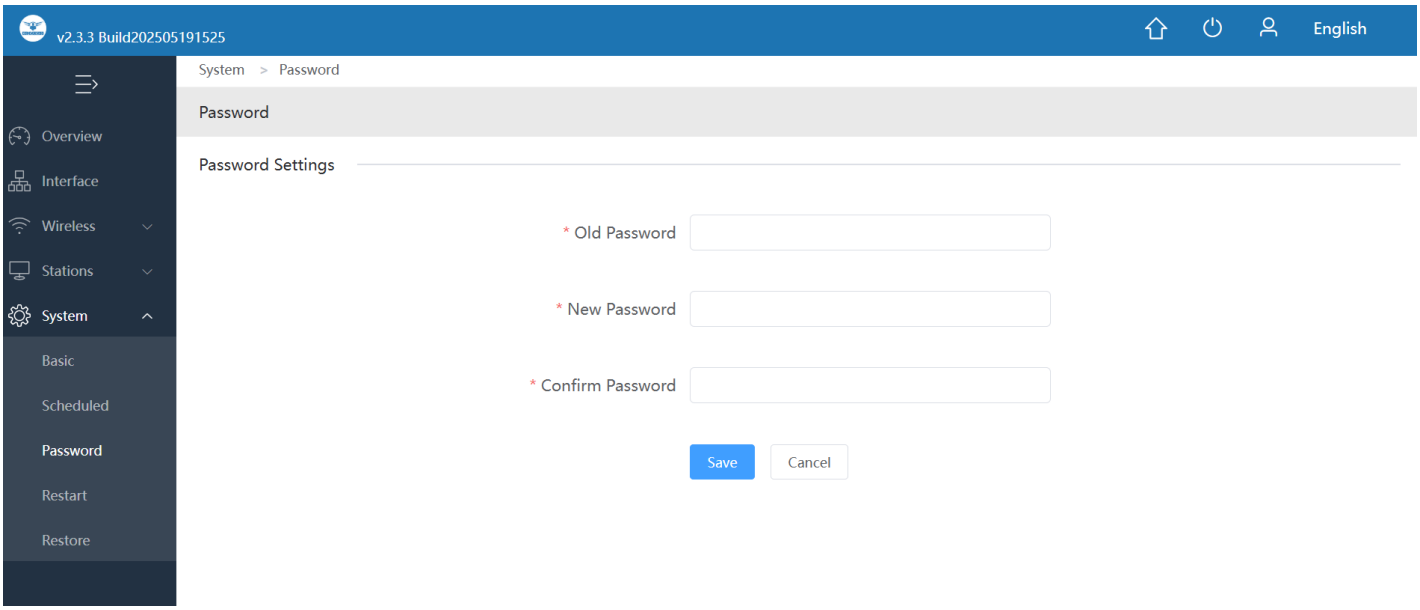


Fig 5.3.1 Default Login setting for AIR-AP3000AX

Note:- The factory default password is admin or commando depending on firmware version is mentioned in backside of device.

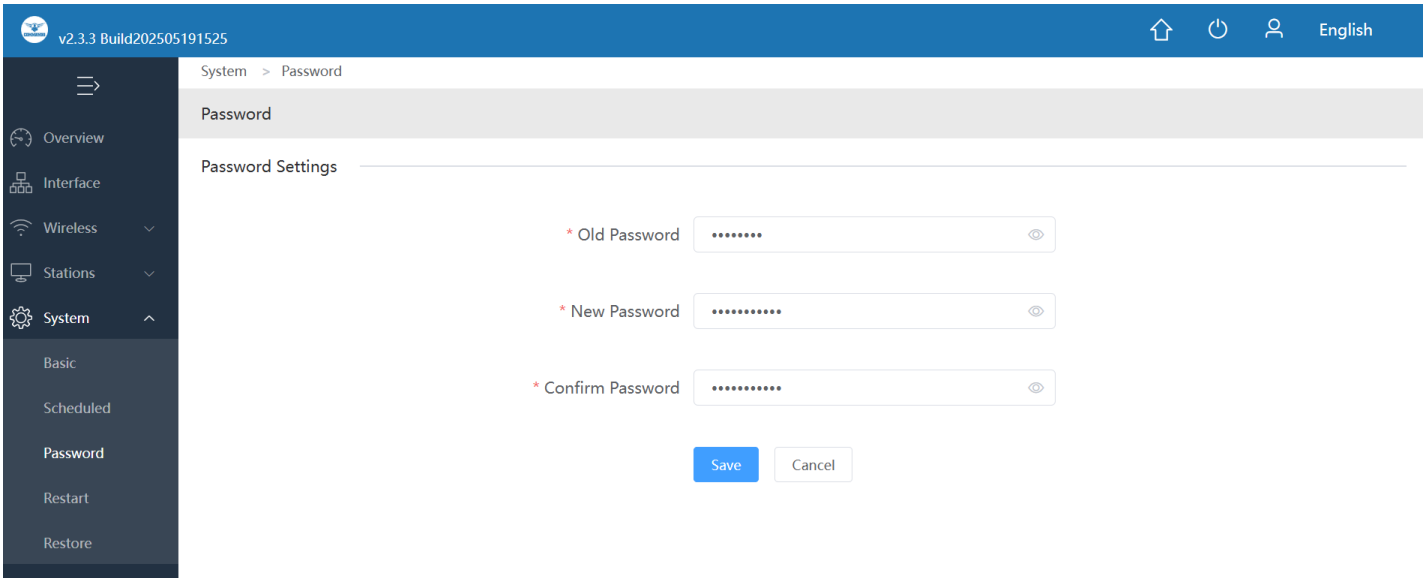


Fig 5.3.2 Setting New Password for AIR-AP3000AX

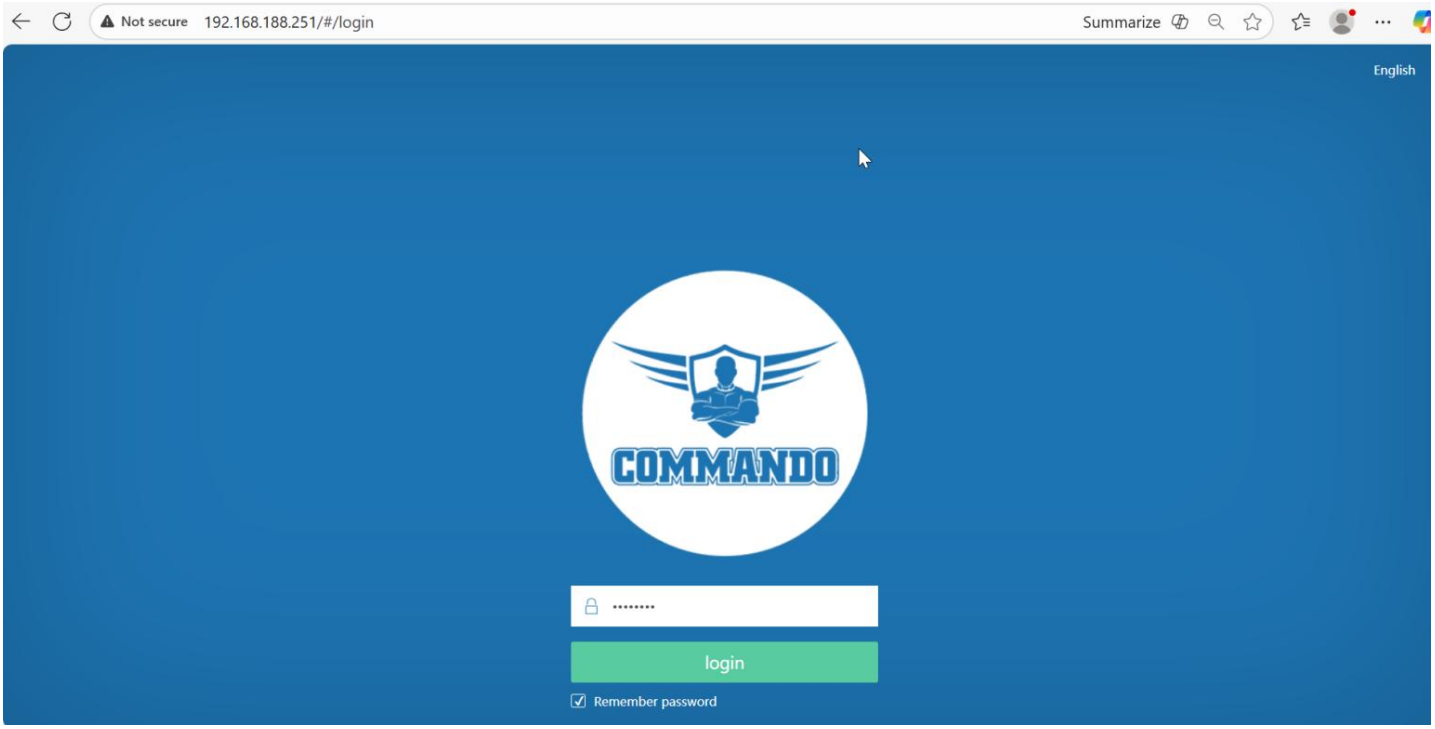


Fig 5.3.3 Login page for new password of AIR-AP3000AX

Recommendation: It is strongly recommended to change default password admin or commando which is used to access device.

5.4 Device reboot

It possible to reboot the AP by restart command. The Internet connection will be temporarily interrupted while rebooting.

To reboot AP, click System setting> Device Restart

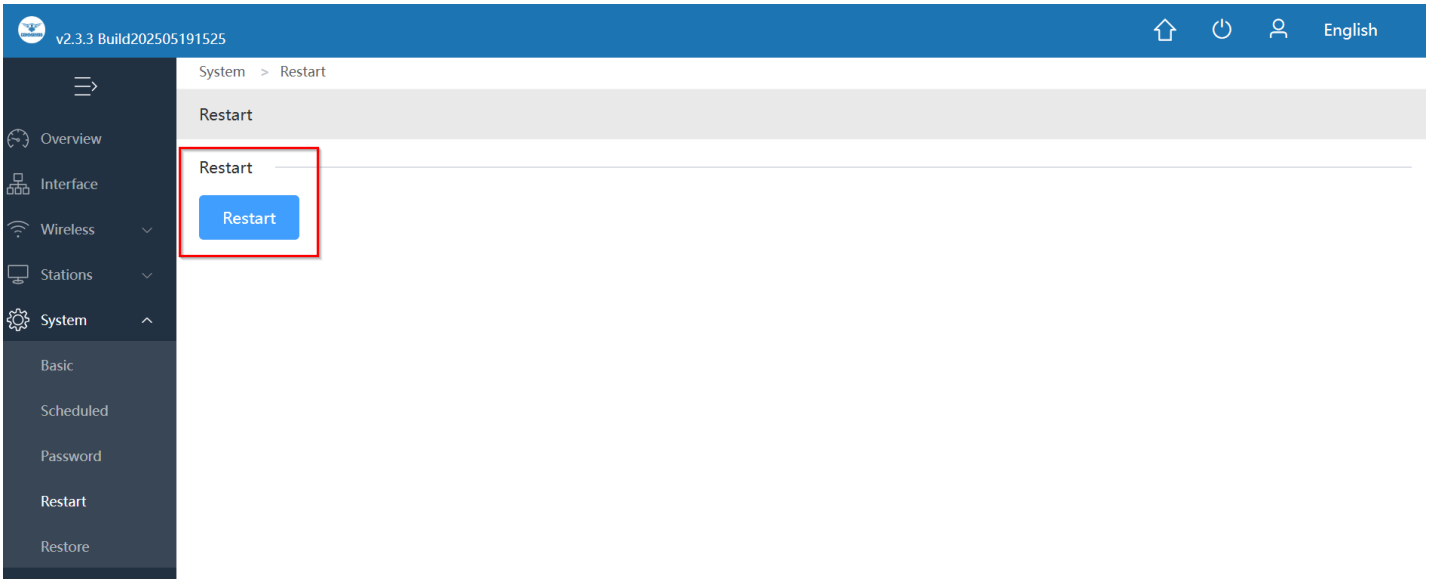


Fig 5.4.1 Default Device restart for AIR-AP3000AX

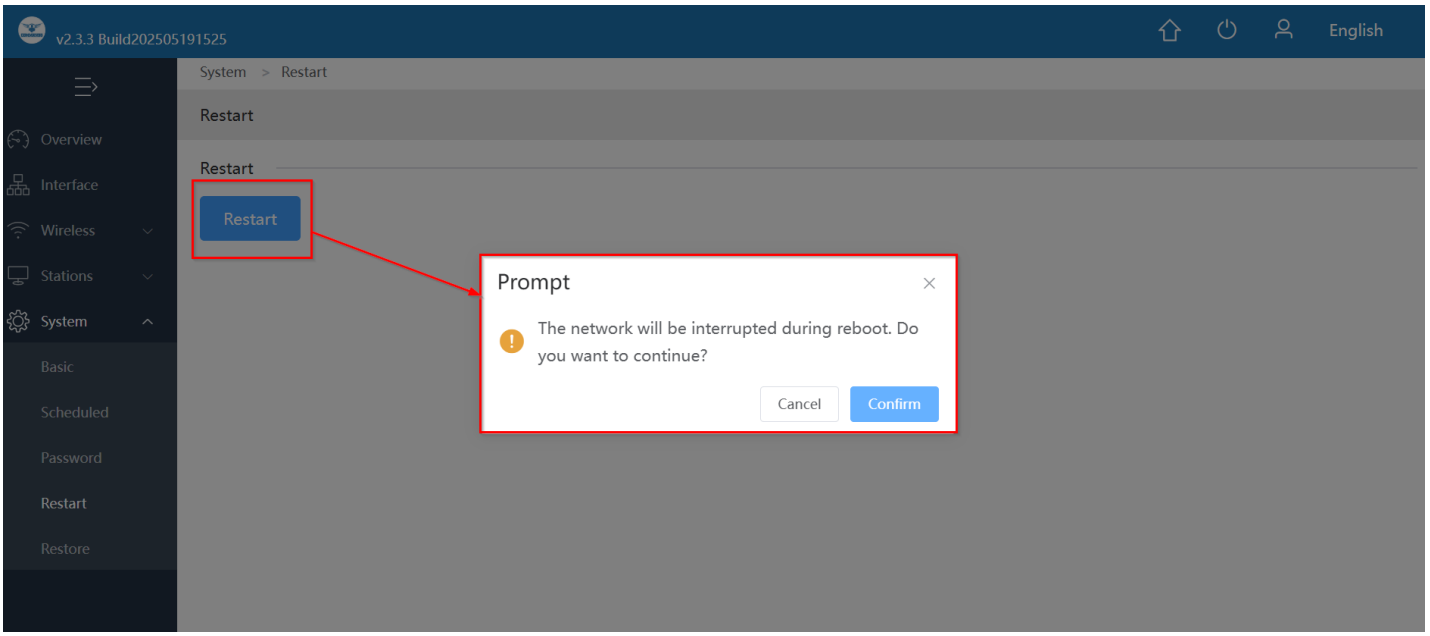


Fig 5.4.2 Restart for AIR-AP3000AX

5.5 Restore

Restore AP to known factory default configuration or to Reset to factory default settings. The Restore configuration feature allows end users to reset the AP to factory default settings. You can restore the AP to its factory default settings by the Restore button or by Restore Default option in this page. It must be noted that once the AP is reset, all the current configuration settings will be lost. Use the the page to restore the AP to the factory defaults or use the button to restore the AP to old configuration.

To restore AP to factory setting, Click on System setting> Restore

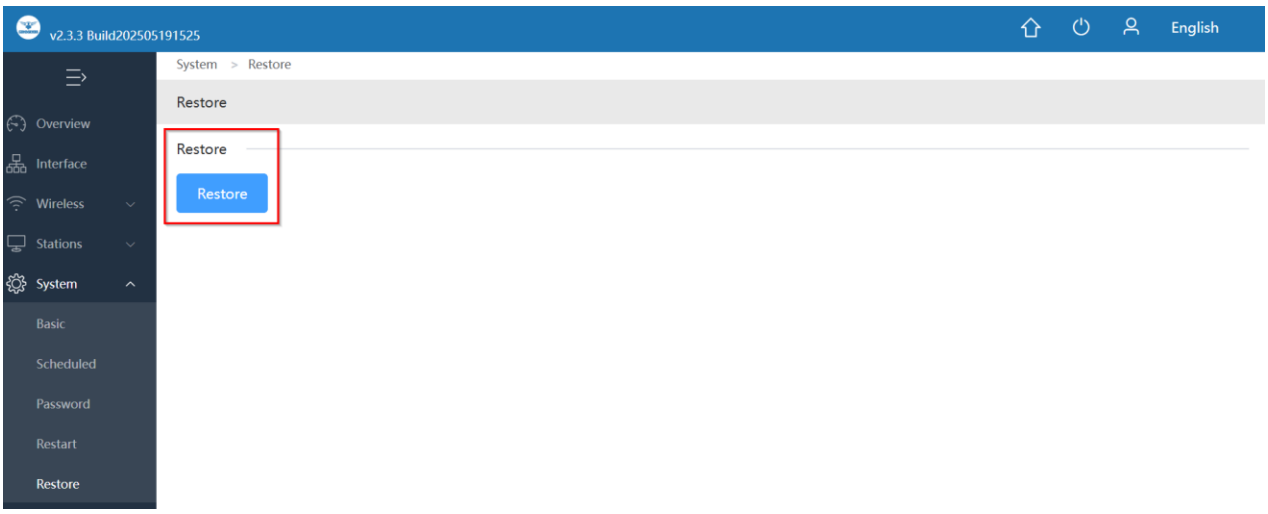


Fig 5.5.1 Default Restore button for AIR-AP3000AX

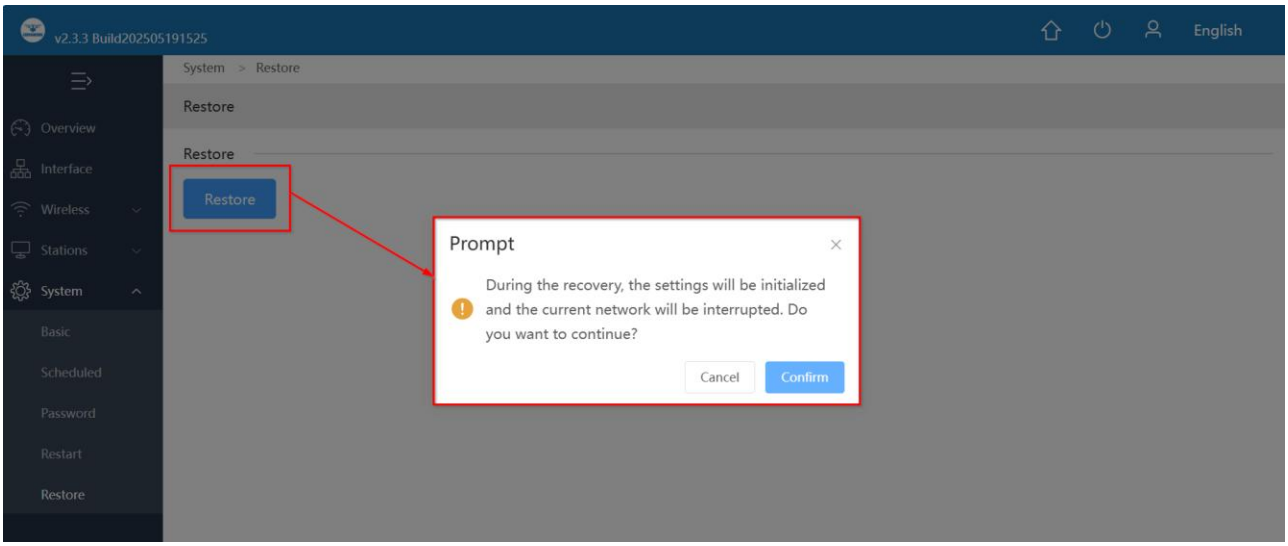


Fig 5.5.2 Restoring AP to factory default for AIR-AP3000AX

2. COMMANDO AIR-AP3000AX FIT mode works with RouteX Controller

COMMANDO AIR-AP3000AX supports FIT mode works with RouteX Controller, which can provide cloud-based access and functions as follows.

Monitoring

Interface, Terminal, protocol, Policy, System, Flow Control.

System Setup

Basic Setting, Disk management, Cloud Account, Advanced Settings like ALG Set, Administration, Upgrading, Reboot.

Network

Interfaces, DHCP, DNS, IP/MAC Group, Static Routes, VLAN,VPN Client, UPNP NAT, Port Mapping, IPv6, IGMP Agent.

Flow Control

Multi-WAN features Load Balancing/protocol/Port Forward/Domain Name/Upload/Download, Smart Flow Control, IP/MAC Limiters, protocol Library.

Access Controller

Wireless overview, AP Configuration, AP group, AP Firmware Upgrades, Wireless blacklist and whitelist, User Information.

1. **Wireless overview:** Open Access Controller with ON/OFF button. The connected AP will automatically enter the AP device list and can Manage AP. Running State of AP status with Online AP, Offline AP, fast roaming, 5G first along with terminal statistics like 2.4G online, 5G online, peak online, active terminal, inactive terminal. Wireless Network Rating with traffic statistics, terminal association details with Access evaluation, Access times, Average access success rate with Network transmission quality.

2. **AP Configuration:** Access Point Configuration with All groupings, All Status like Online/Offline/Upgrading, All Frequency like (2.4G+5G) & IP/MAC/Model/Remarks. Interference Analysis with Start Searching AP, MAC, Remarks, BSSID, BSSID Remark, SSID, Signal Value, Channel along with Import or Export configuration files. Default Configuration for 2.4G, 5G Radio with other Setting like SSID1 Name.

SSID1 Security No Password, SSID1 VLAN Close, Hide SSID1 Name Open, SSID rate limit Open, Guest Mode Open (Isolate guest devices discovery and access to wired network) Channel Auto, AP Signal 80% default Channel width. This channel width 20/40 MHz in 2G band and 5G band can change to 80Mhz or self-adaptation, Airtime scheduling, Advanced settings like Beacon frame power.

Follow AP signal strength Beacon frame interval 200ms, RTS threshold0, Low-rate access license Allow all, Management frame rate 1Mbps.

3. **AP group:** AP Group Add/Delete with Group name, Number of AP, channel, Maximum belt capacity, SSID, Actions. With Add button click we can set Group name with 2.4G/5G control state information.

4. **AP Firmware Upgrades:** Access Point Upgrades with MAC/Model, Upgrade All, Batch Upgrade with information like MAC Address, Current Version, Latest Version, Status, AP Remarks, Actions

5. Wireless blacklist and whitelist: With Add, Import, Export, Enable, Disable, Delete which also shows Mode, Terminal MAC address, SSID, AP, week, time, comment, Status, Actions

6. User Information: User Information with IP/MAC/SSID, All Frequency (2.4G/5G), All users along with weak signal users and normal users showing information like IP Address, MAC, AP Information, SSID, Signal, Connect Time, Tx, Rx, Comment, Actions.

Authentication

Captive Portal, VPN Server, Authentication Account, Push Notification.

Behavior

Behavior Audit with Mark MAC Address, MAC Control, Website Control, URL Control, Application protocol Control, Secondary Routing, QQ, Blacklist/Whitelist.

Firewall

ACL Rules, ARP binding, Connection Limiter, Advanced Firewall. Advanced application-->Dynamic DNS, SNMP, Application across three layers, Wake on LAN, FTP Server, HTTP Server, UDPXY Set.

Services

Ping Test, Capture Packet, Trace Route, IP Sub-netting, Speed Test, Diagnostics, Watchdog.

Log

User Logs, Function Logs, System Logs.

COMMANDO AirX Ceiling AP's also can be controlled from cloud captive portal with RouteX controller with Cloud Login https://commandonetworks.com.cn.

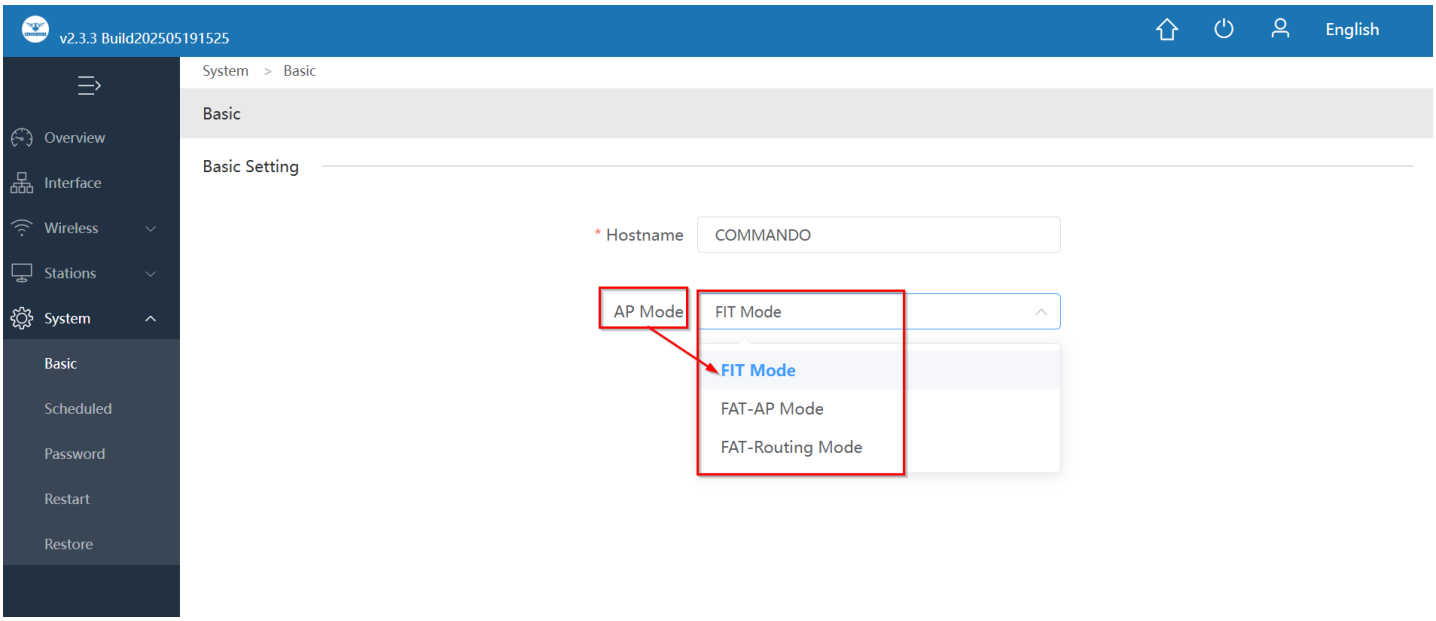


Fig 1. Selection of FIT mode of operation for AIR-AP3000AX Page

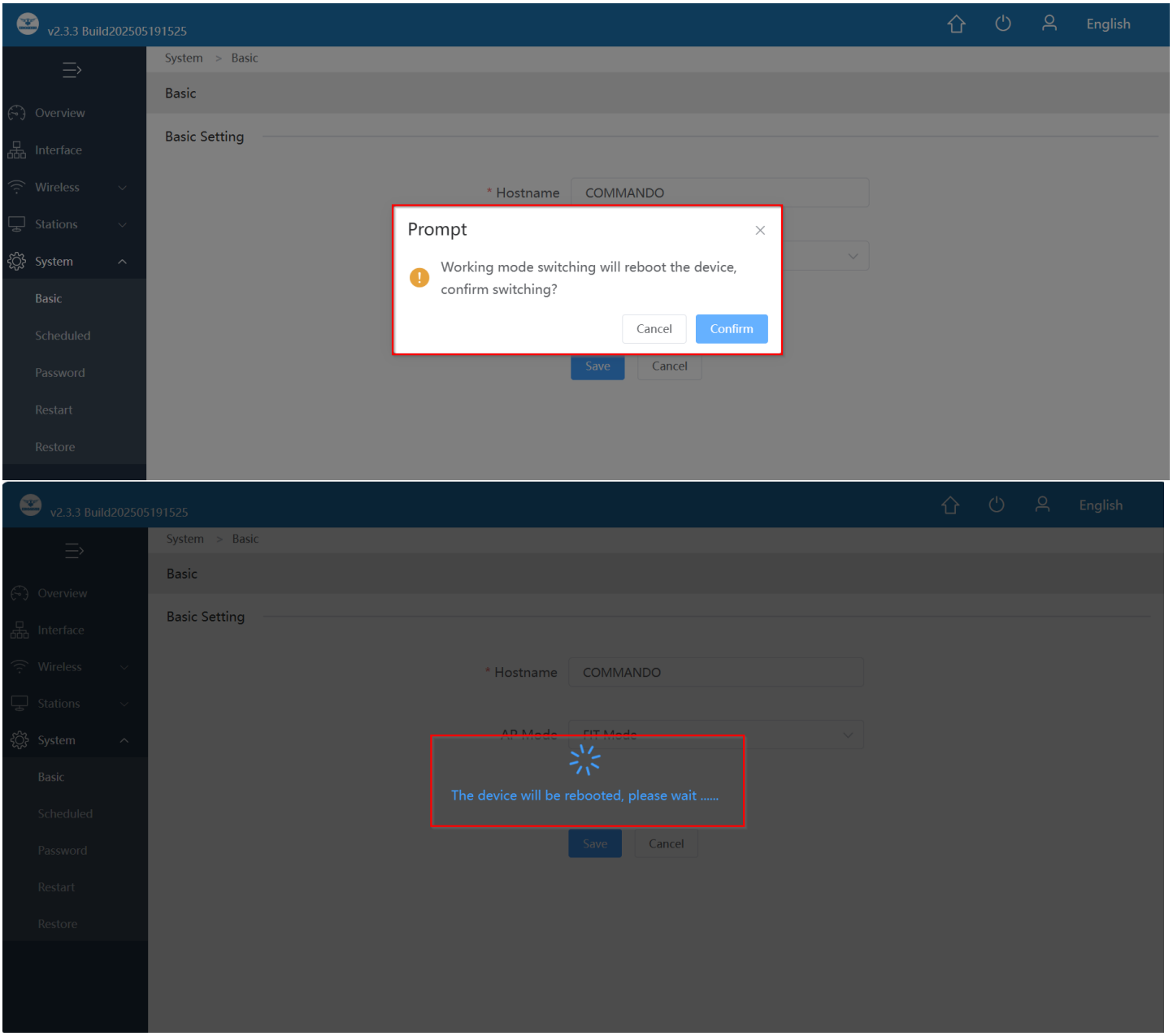


Fig 2. Switching FIT mode of operation for AIR-AP3000AX Page

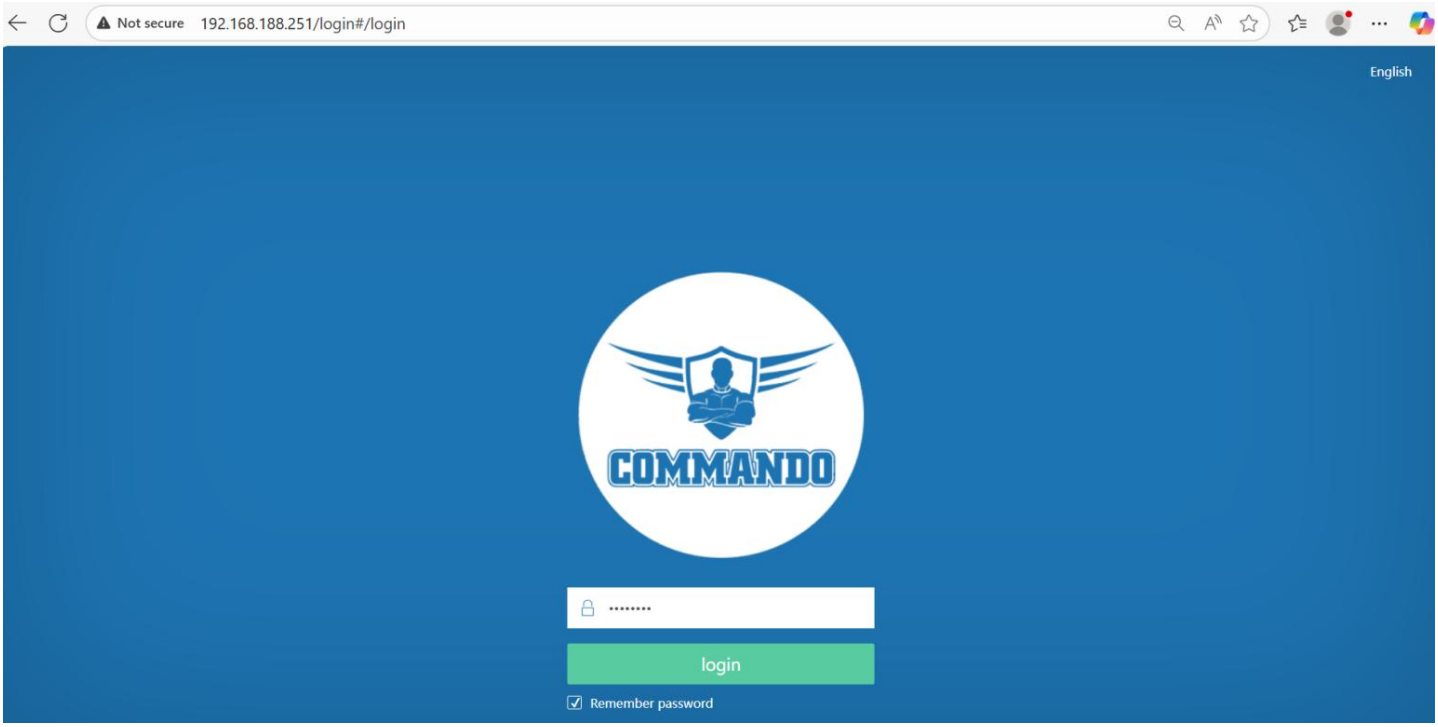


Fig 3. After switch to FIT mode login page

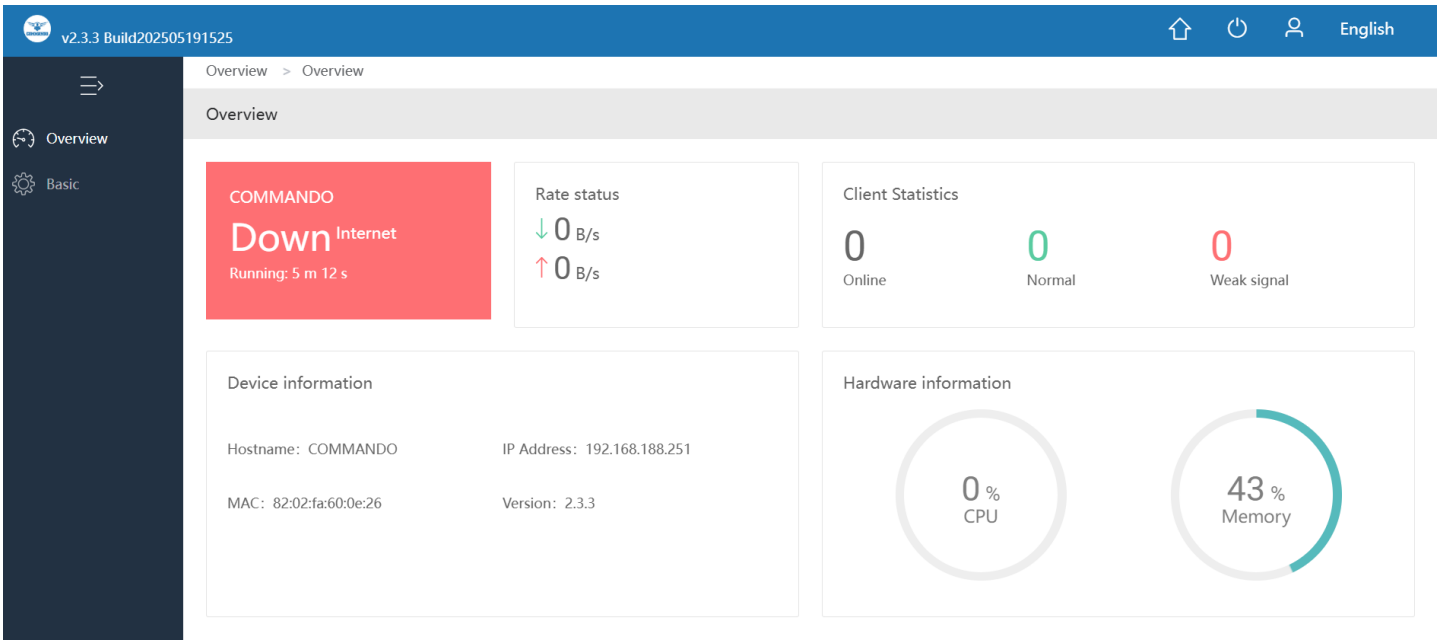


Fig 4. Switching FIT mode of operation for AIR-AP3000AX Page

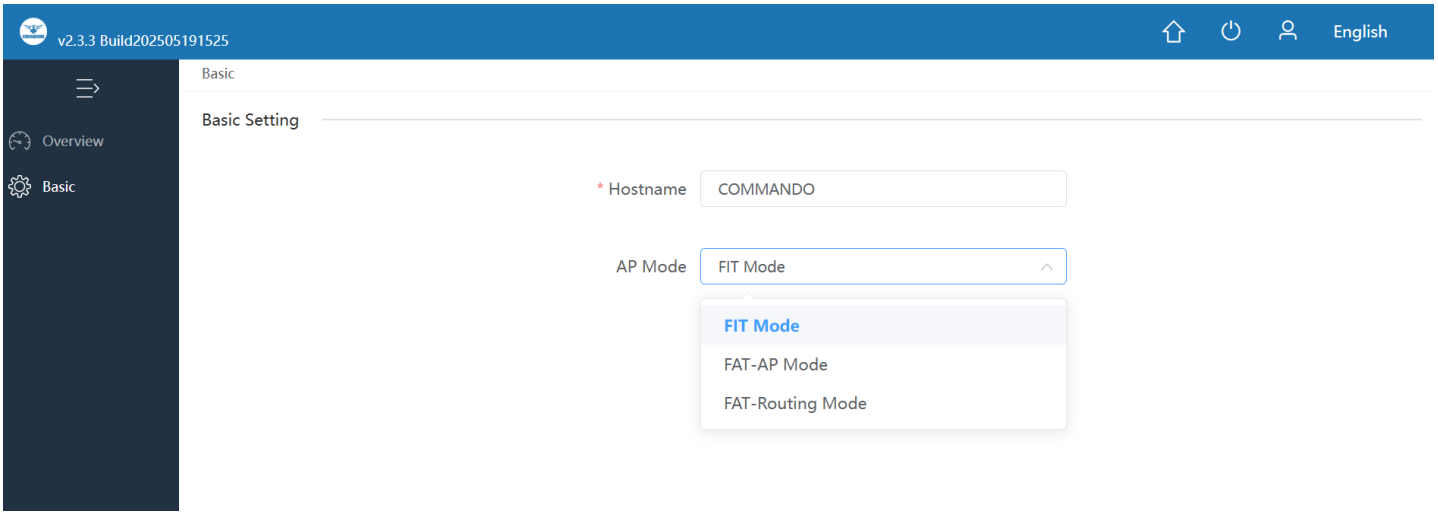


Fig 5. Basic settings available in FIT mode.

Connect with RouteX Controller.

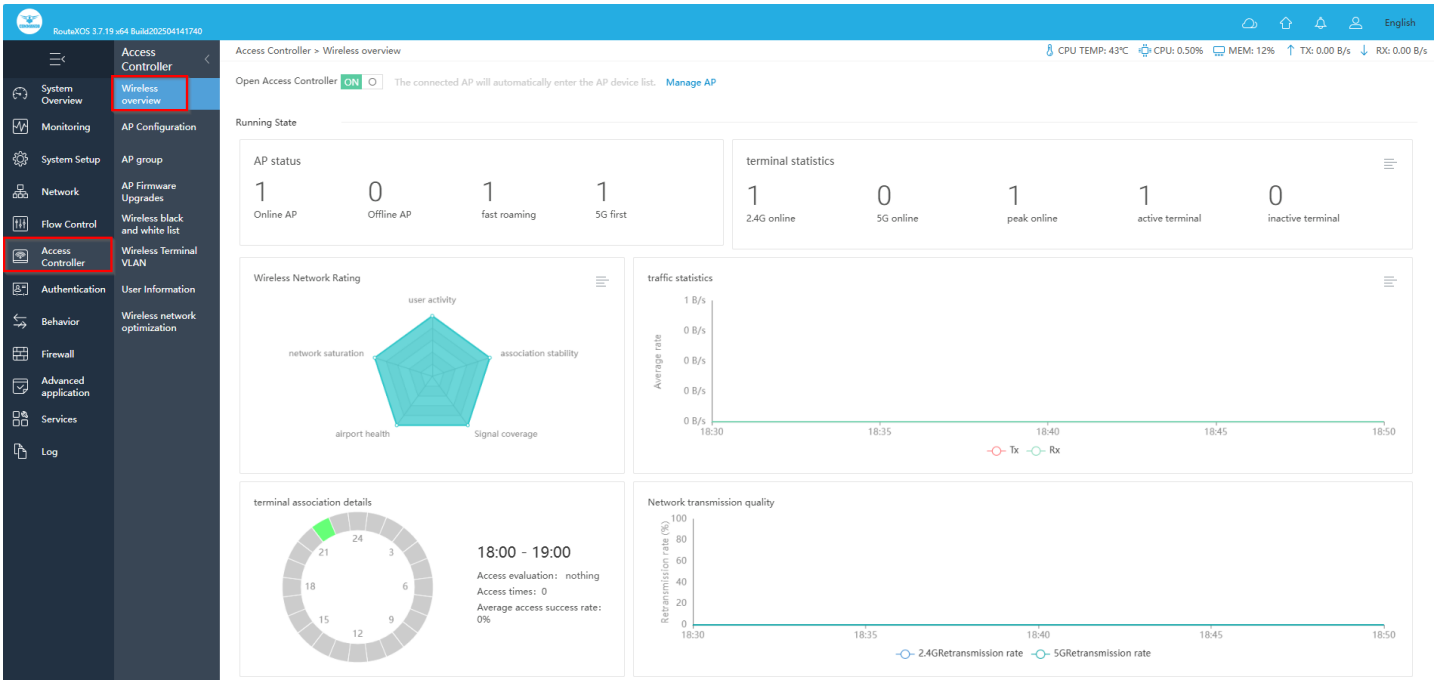


Fig 6. Wireless overview

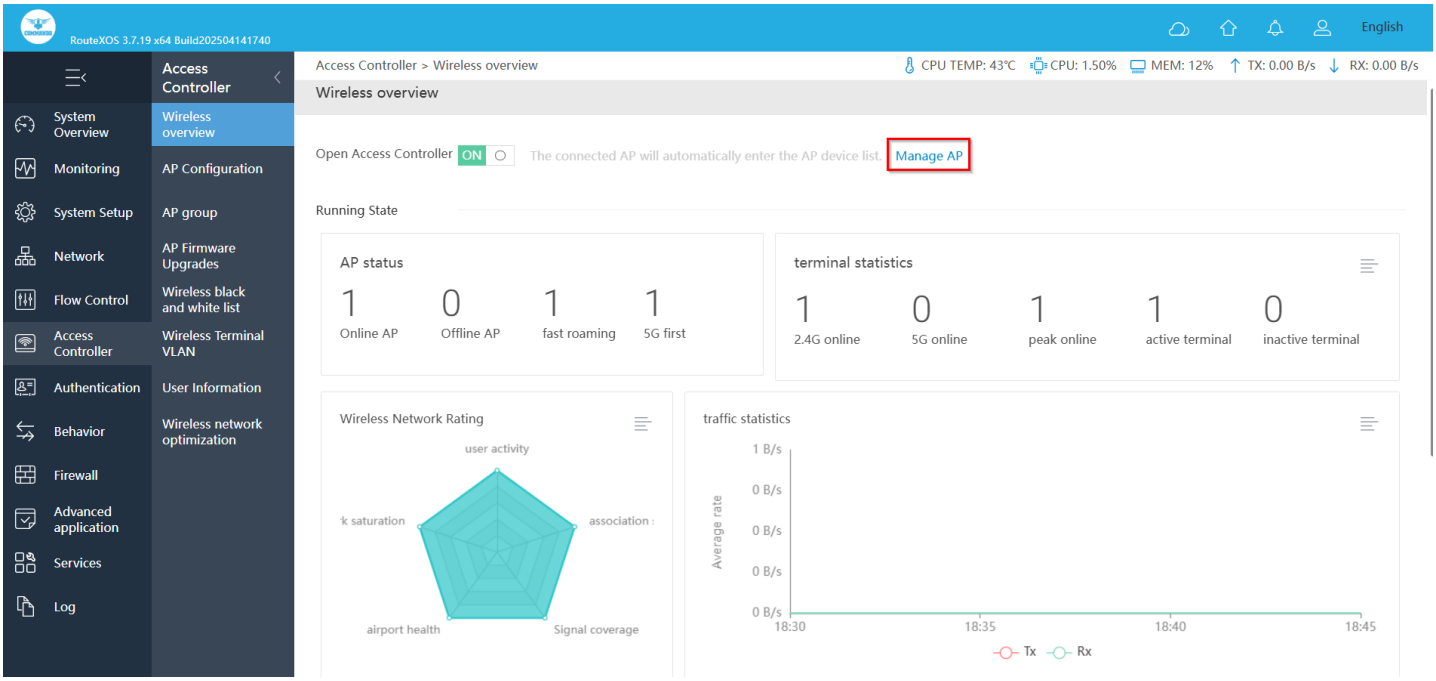


Fig 7. Can manage AP

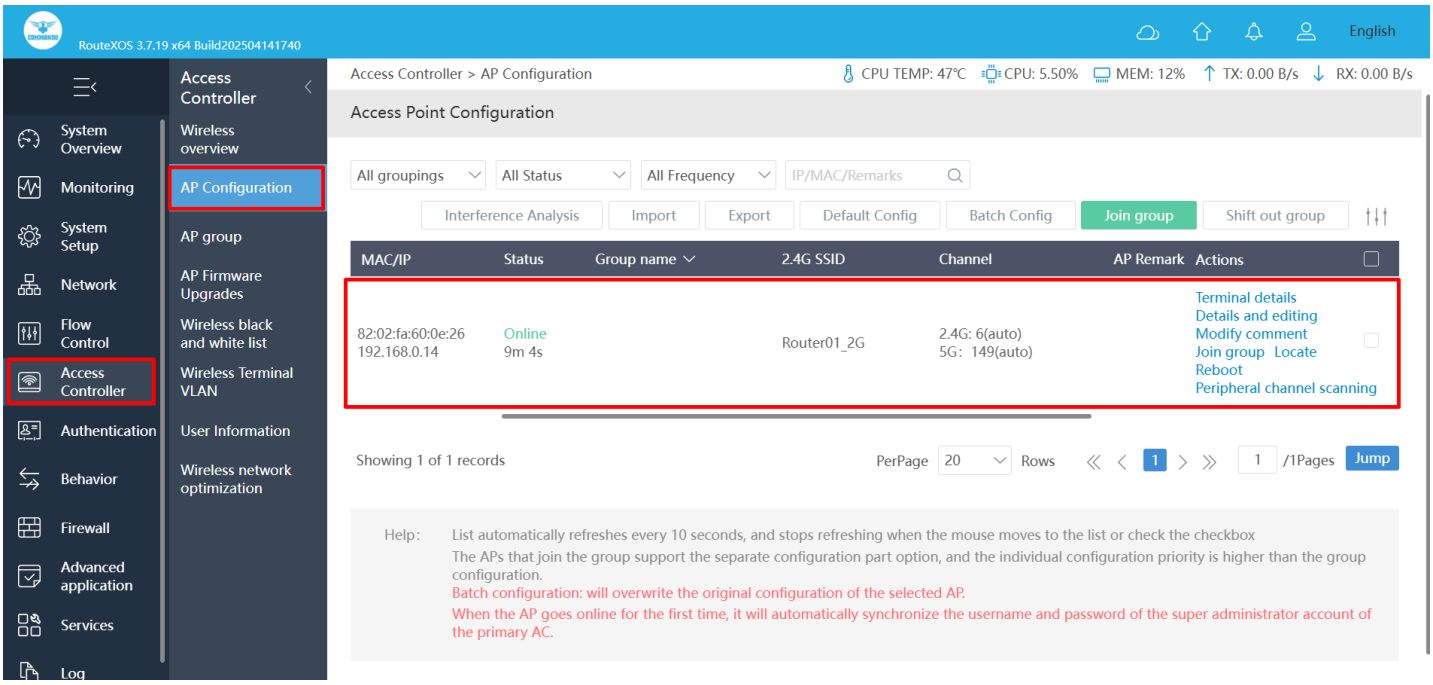


Fig 8. Default AP Configuration page in RouteX Controller.

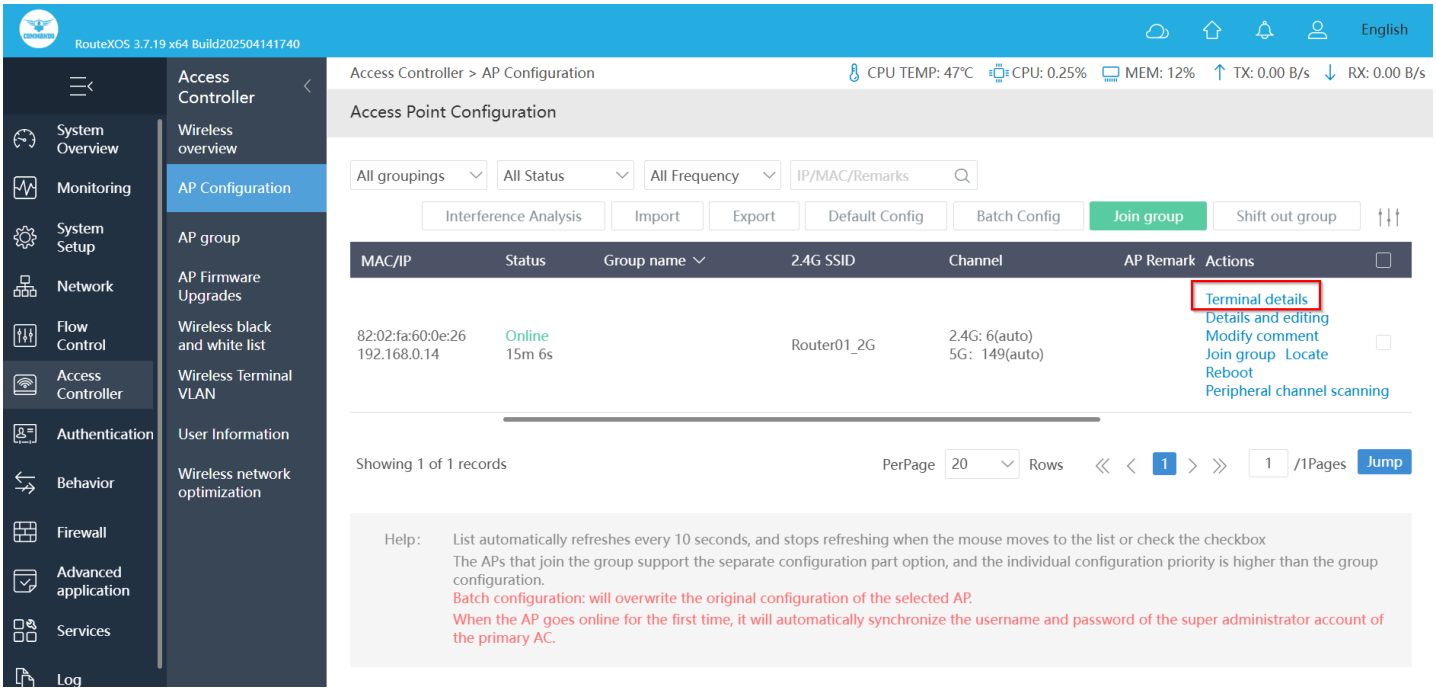


Fig 9. Connected Device to this AP.

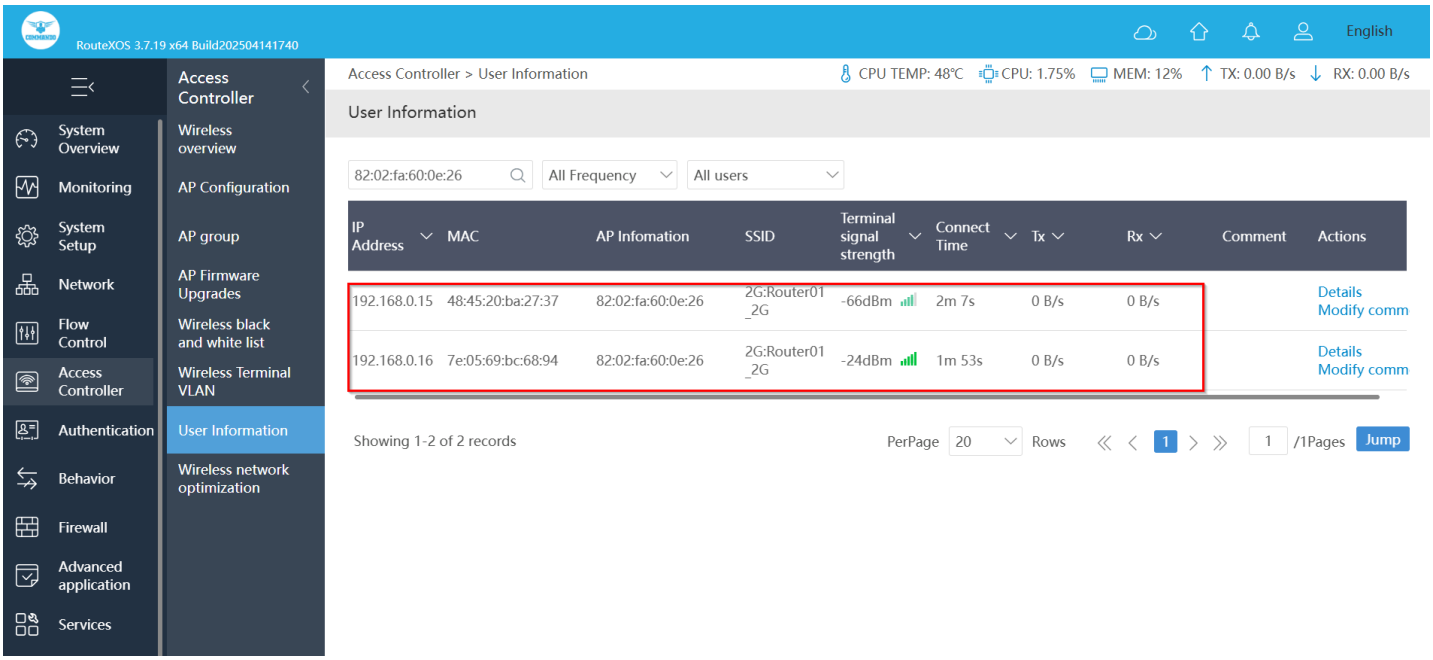


Fig 10. User information.

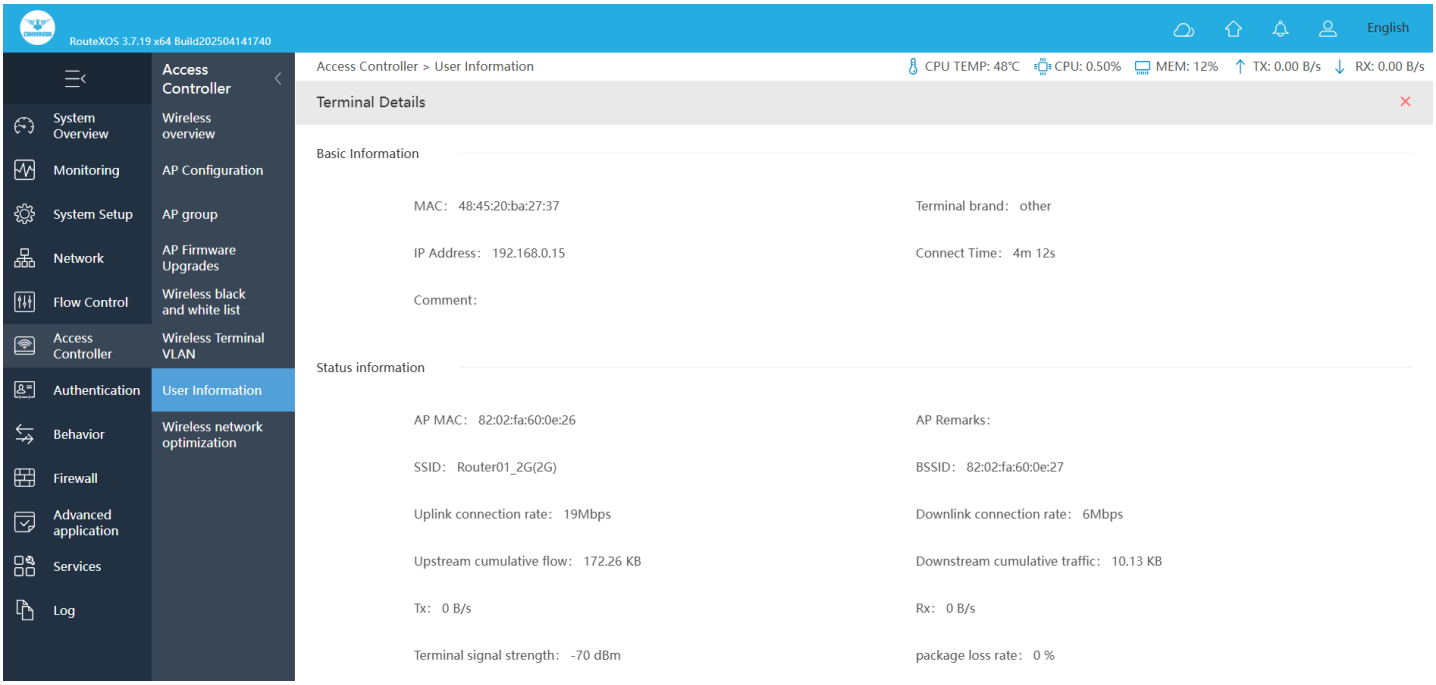


Fig 11. User information details.

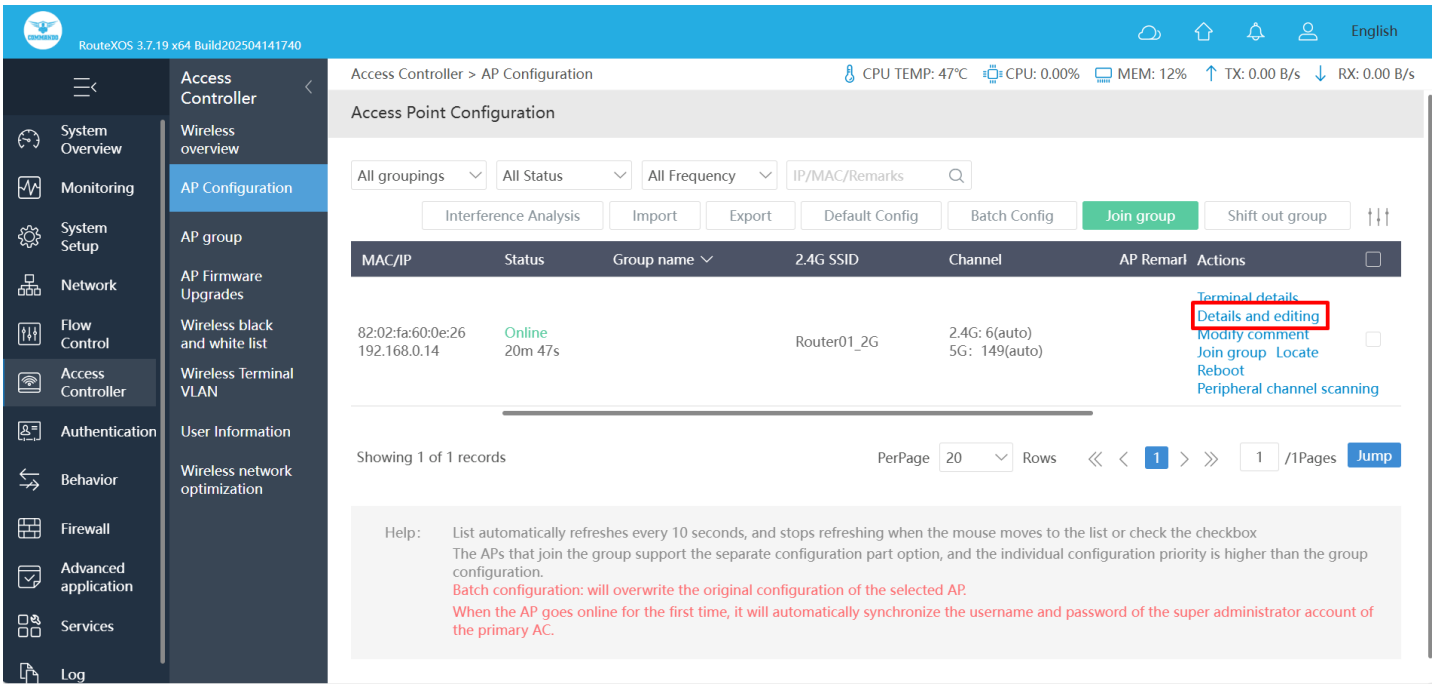


Fig 12. Check details and edit option.

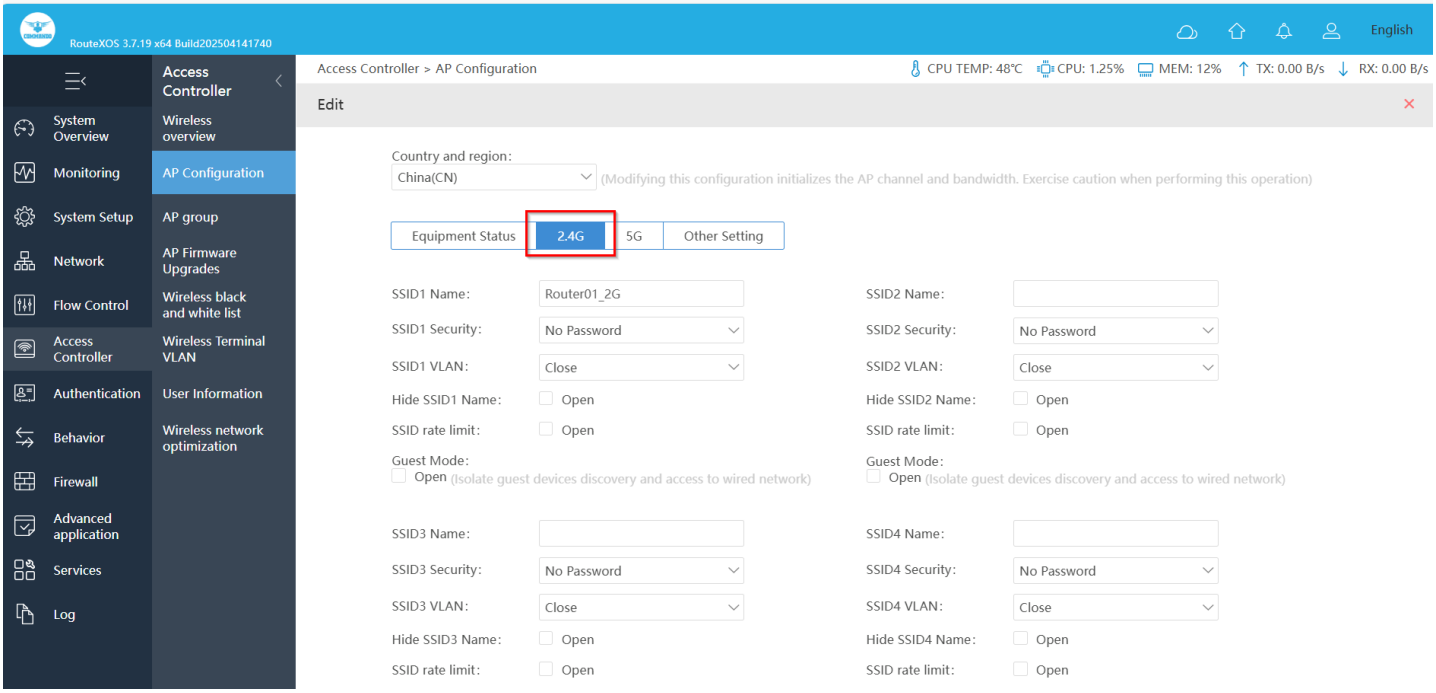
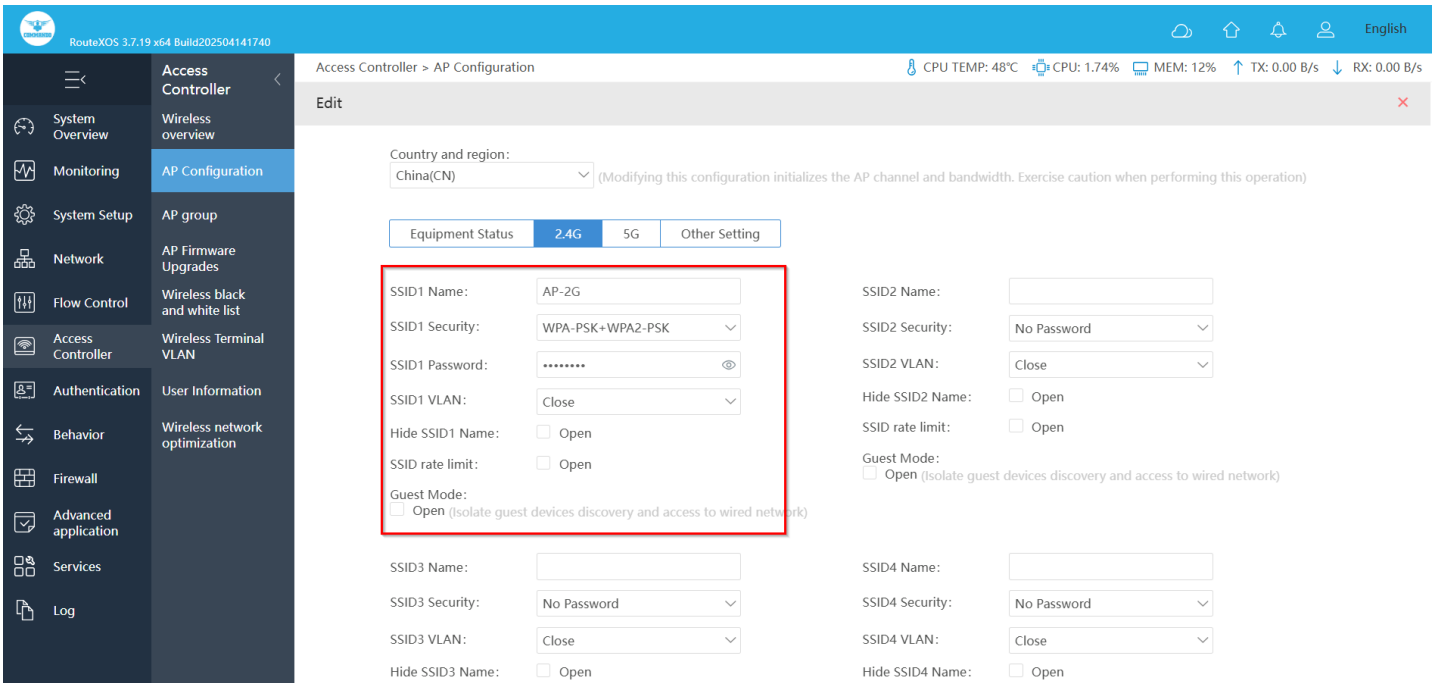


Fig 13. Default WiFi in FIT mode via controller.



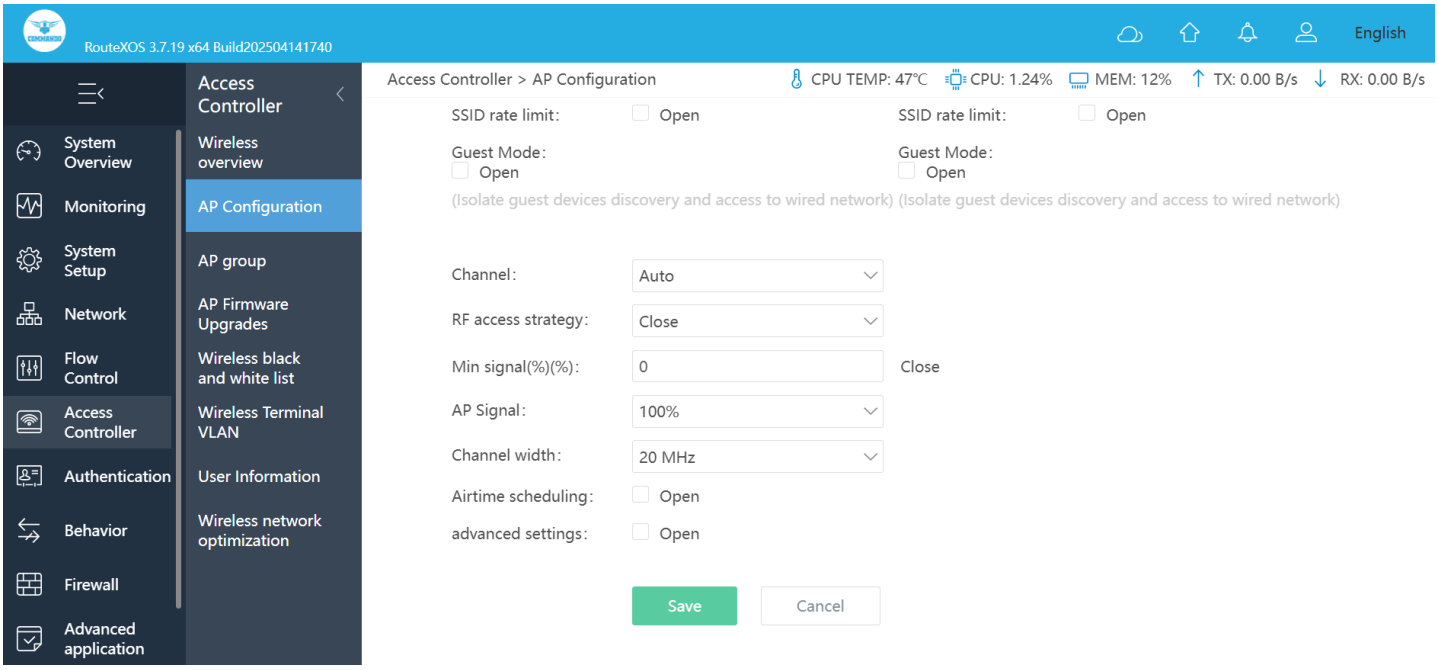


Fig 14. Set SSID and password for 2.4G.

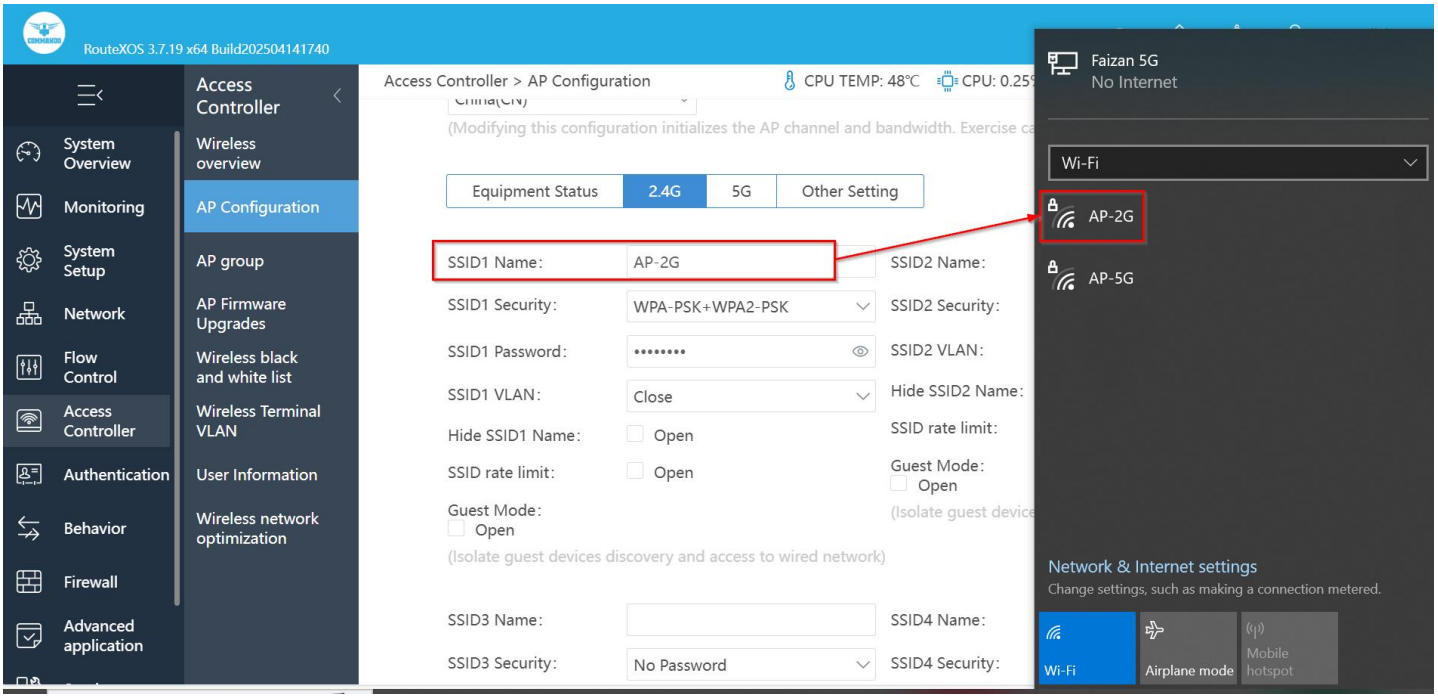


Fig 15. 2G WiFi AP-2G available for wireless clients AIR-AP3000AX

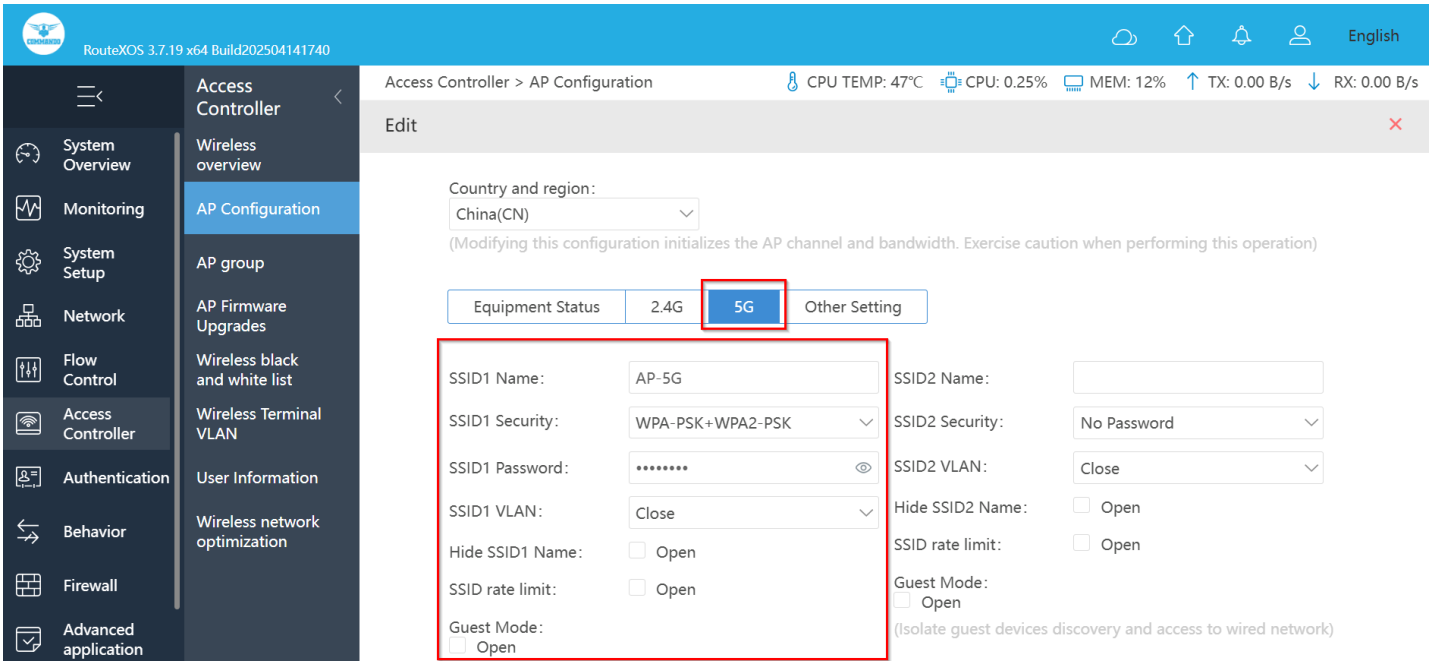


Fig 16. Set SSID and password for 5G.

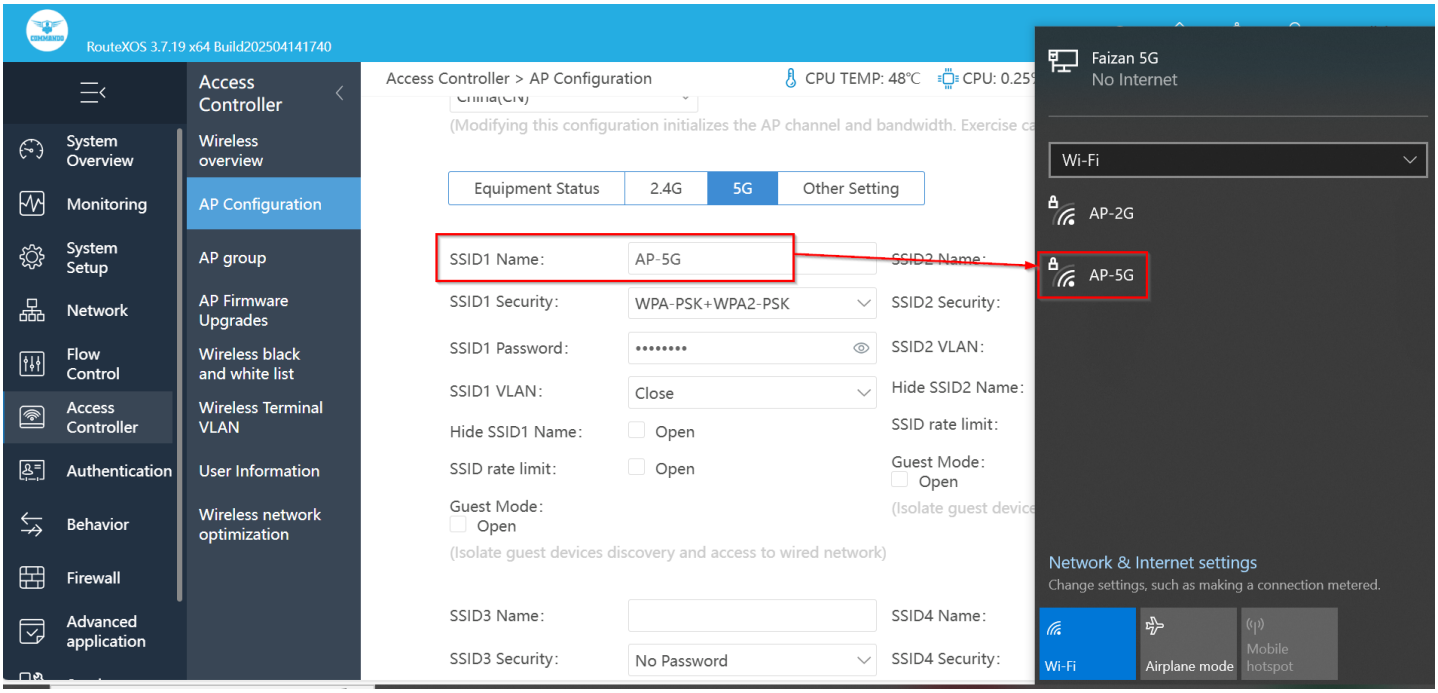


Fig 17. 5G WiFi AP-2G available for wireless clients AIR-AP3000AX

With Other Settings you can schedule WiFi availability and unavailability to wireless users and also can configure Scheduled reboot.

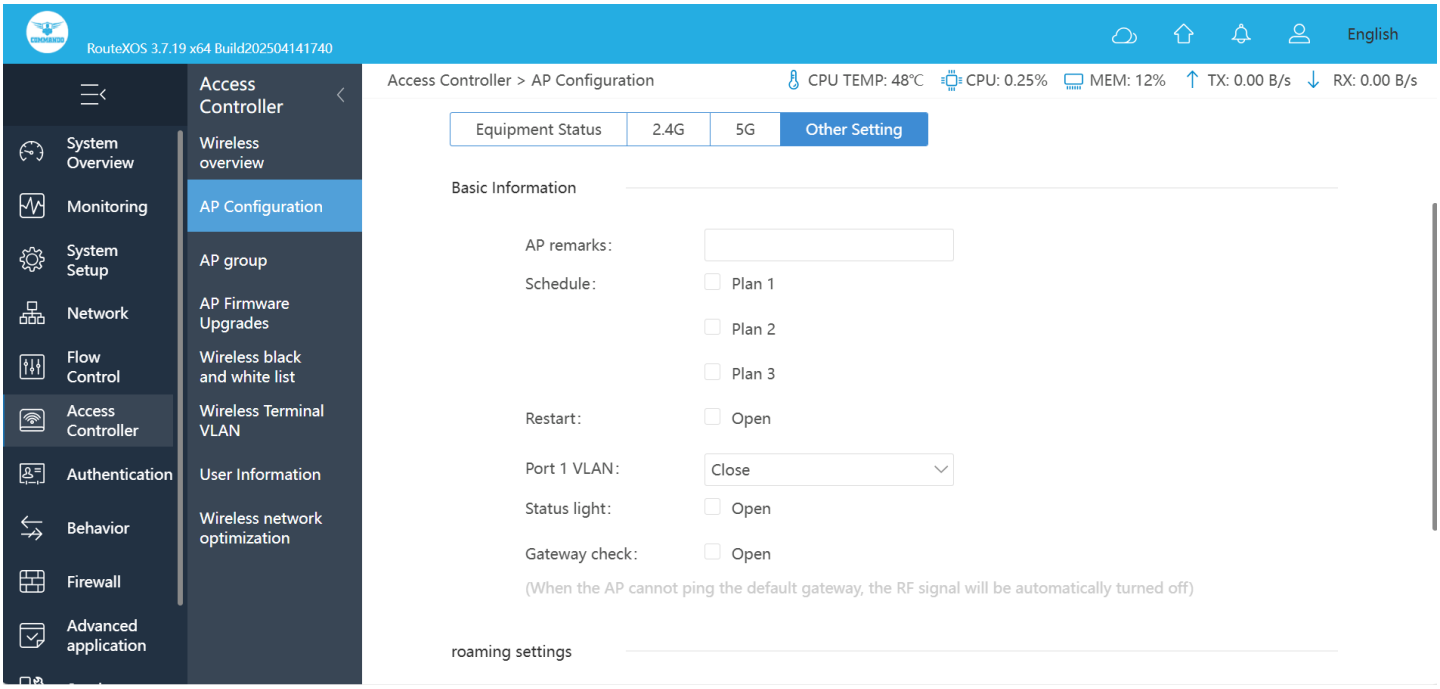


Fig 18. Default timing setting for AIR-AP3000AX

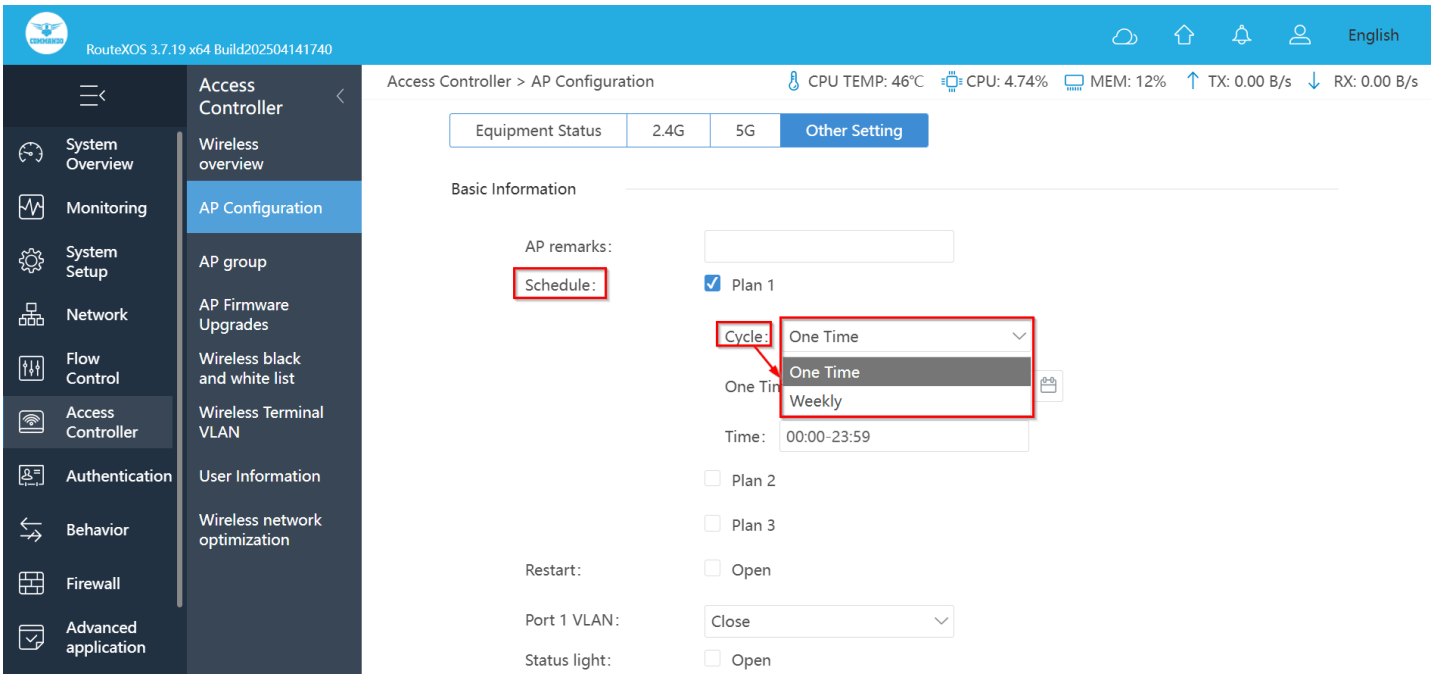


Fig 19. Setting cycle for wireless availability for AIR-AP3000AX

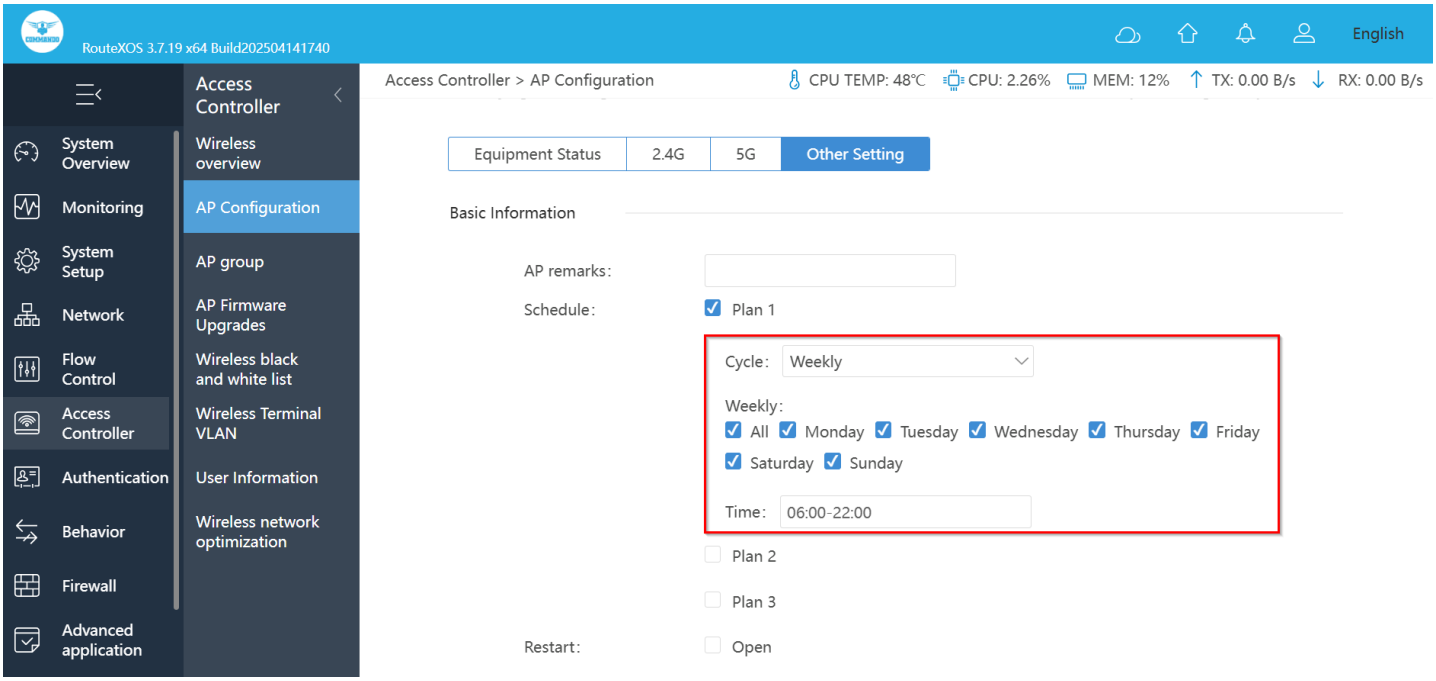


Fig 20. Setting Days and period for AP available AIR-AP3000AX

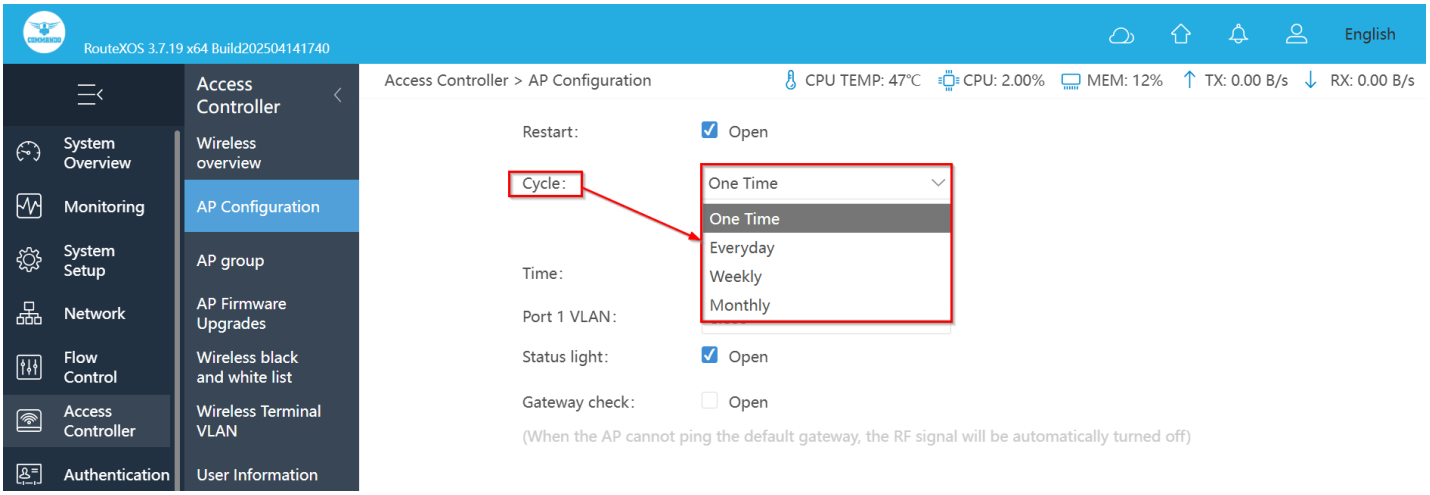


Fig 21. Selecting reboot frequency for AP available AIR-AP3000AX

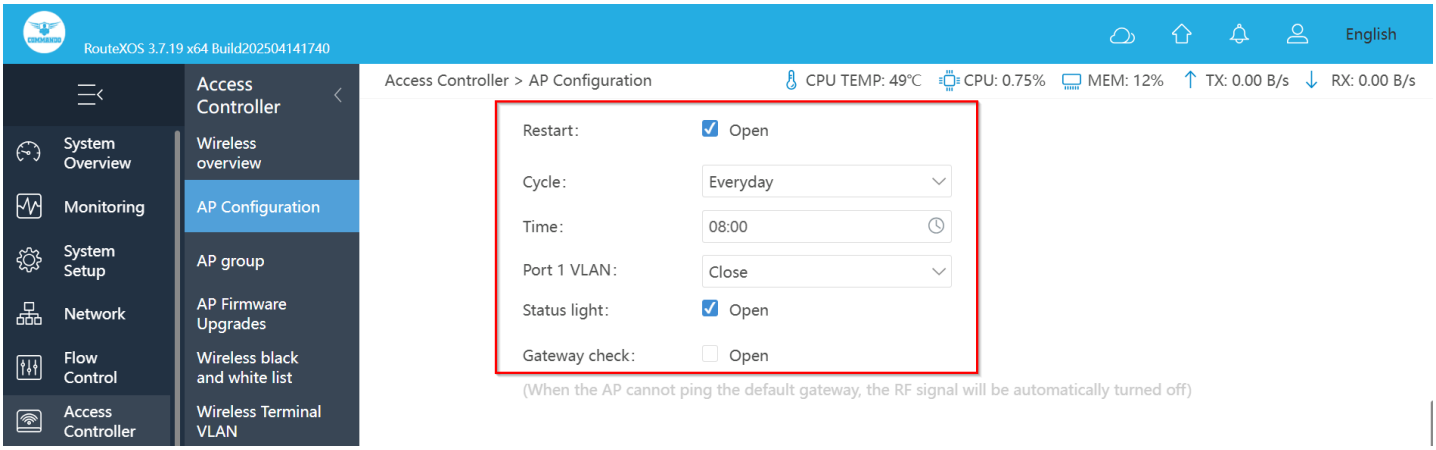
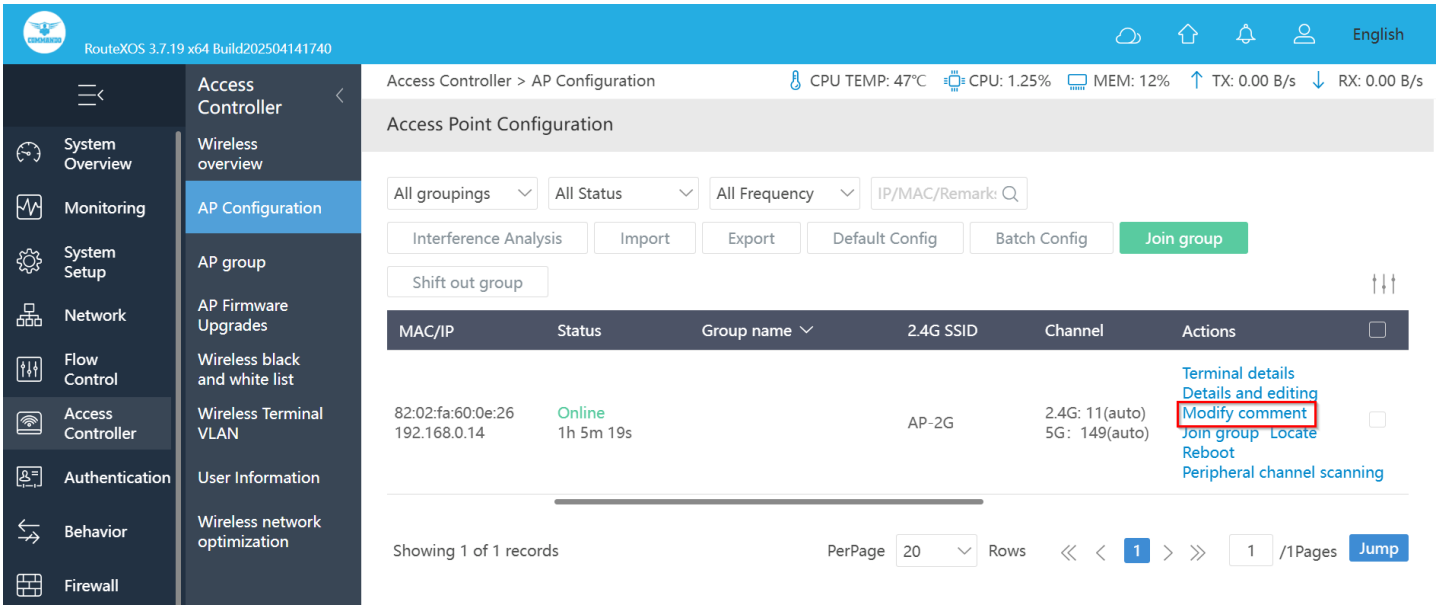


Fig 22. Setting restar for AP available AIR-AP3000AX



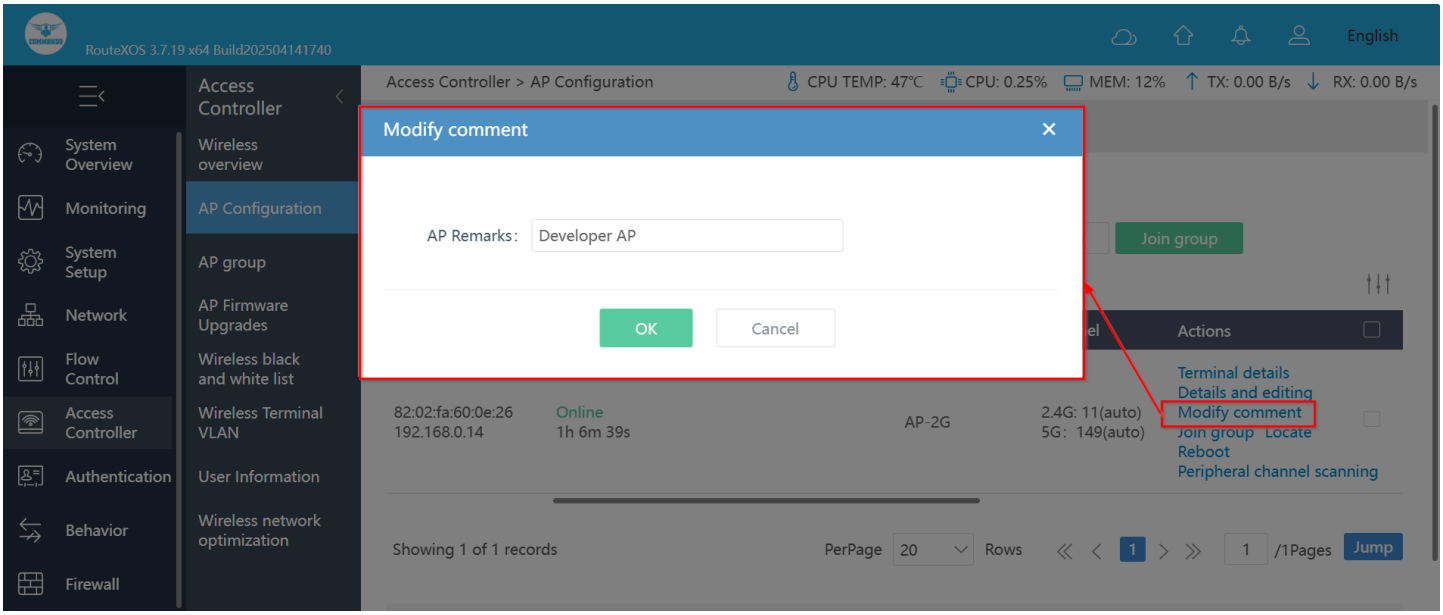


Fig 23. Setting to modify AP remark or comment.

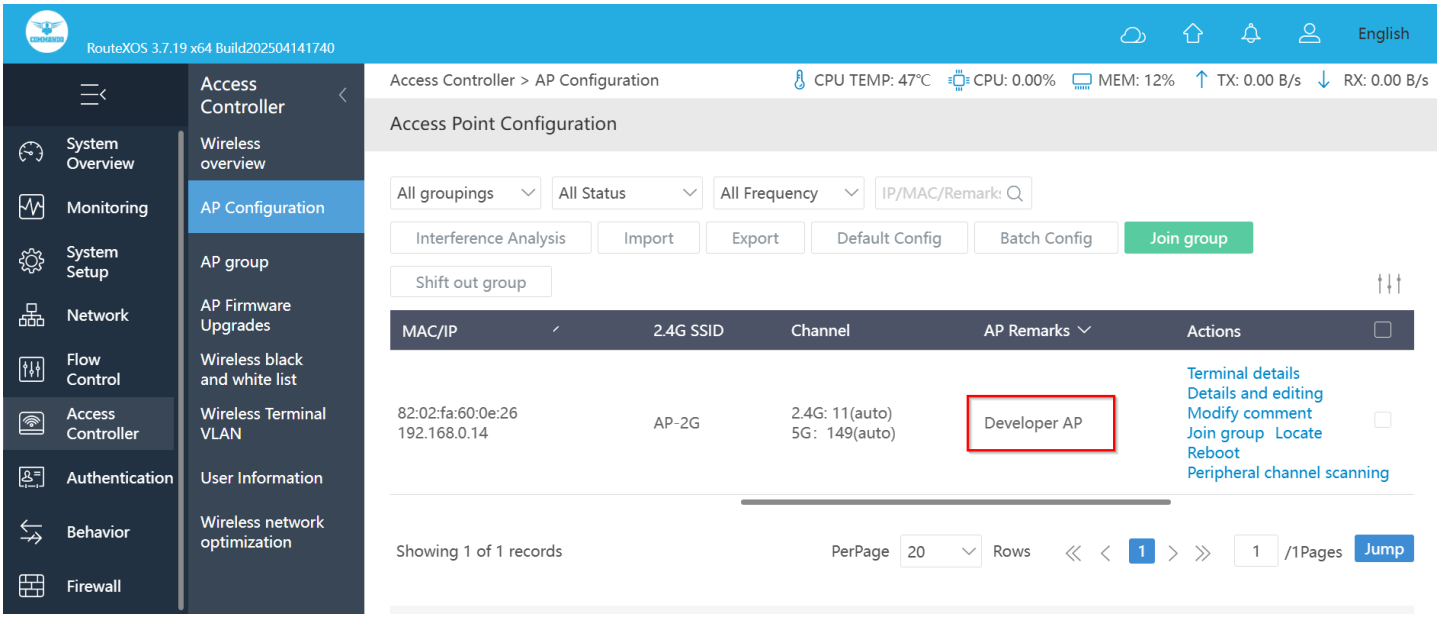


Fig 24. Added AP remark.

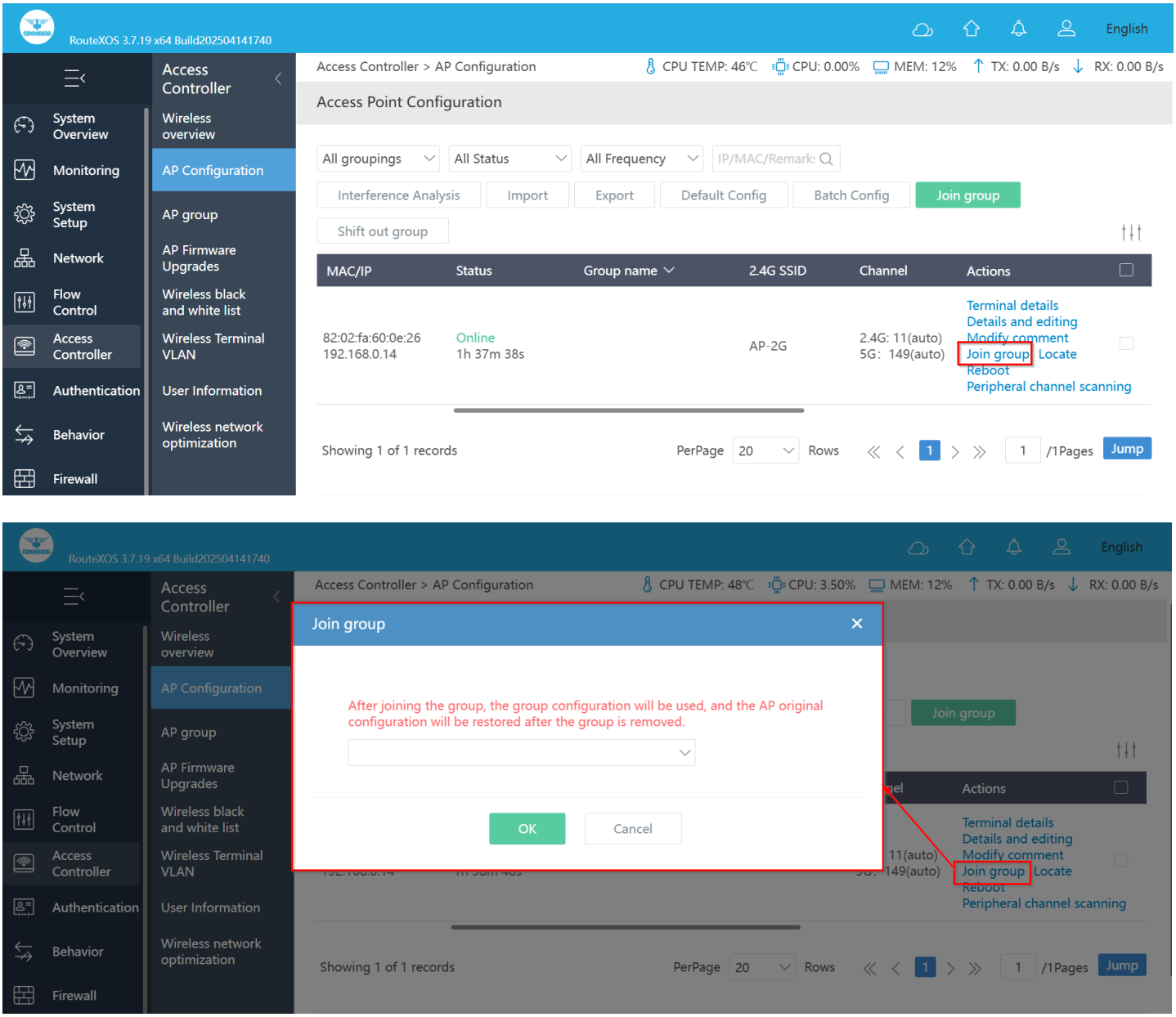


Fig 25. Join group option

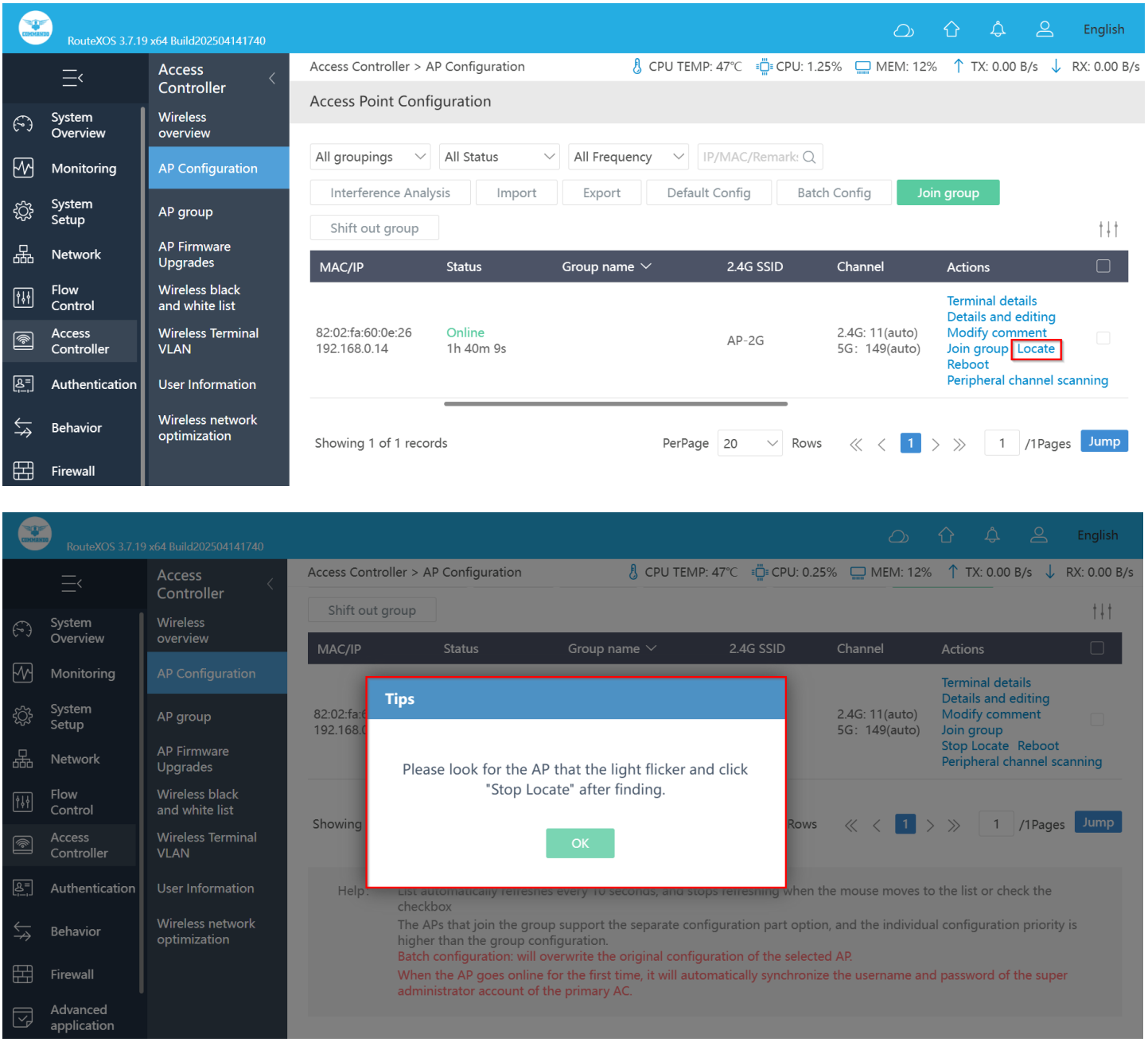


Fig 26. Locate option

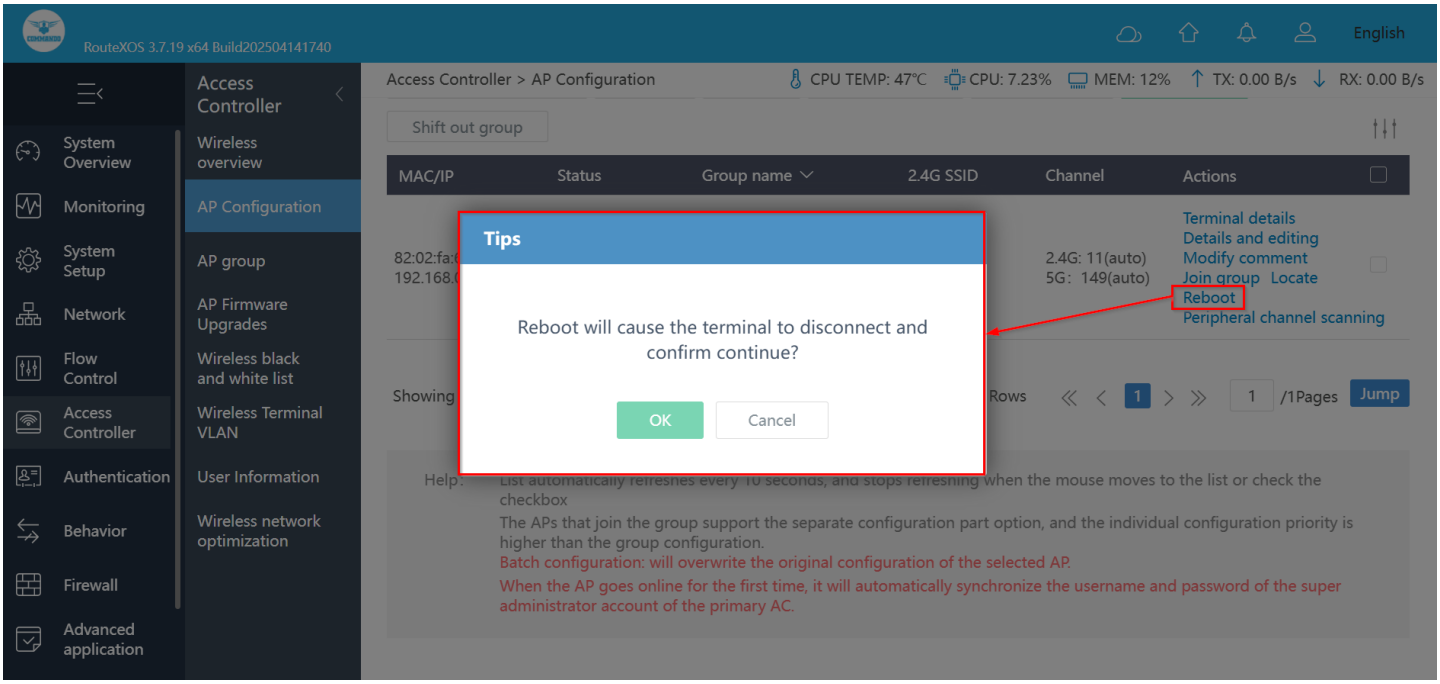
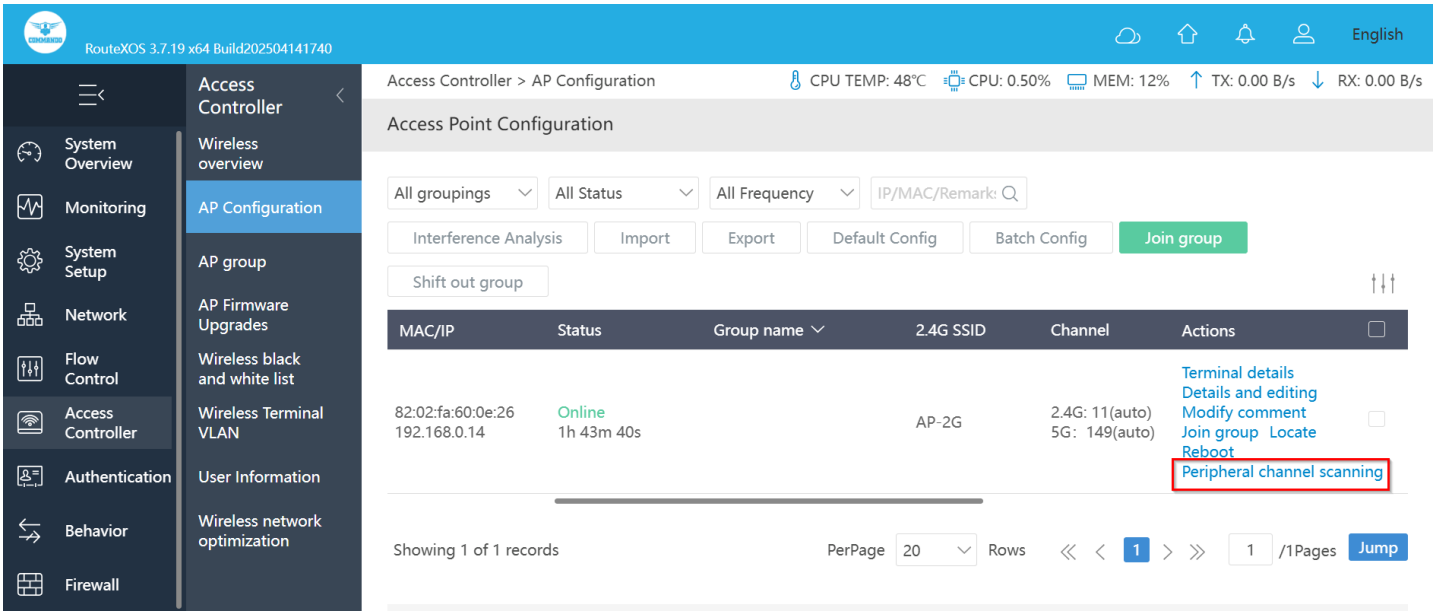


Fig 27. Reboot the AP



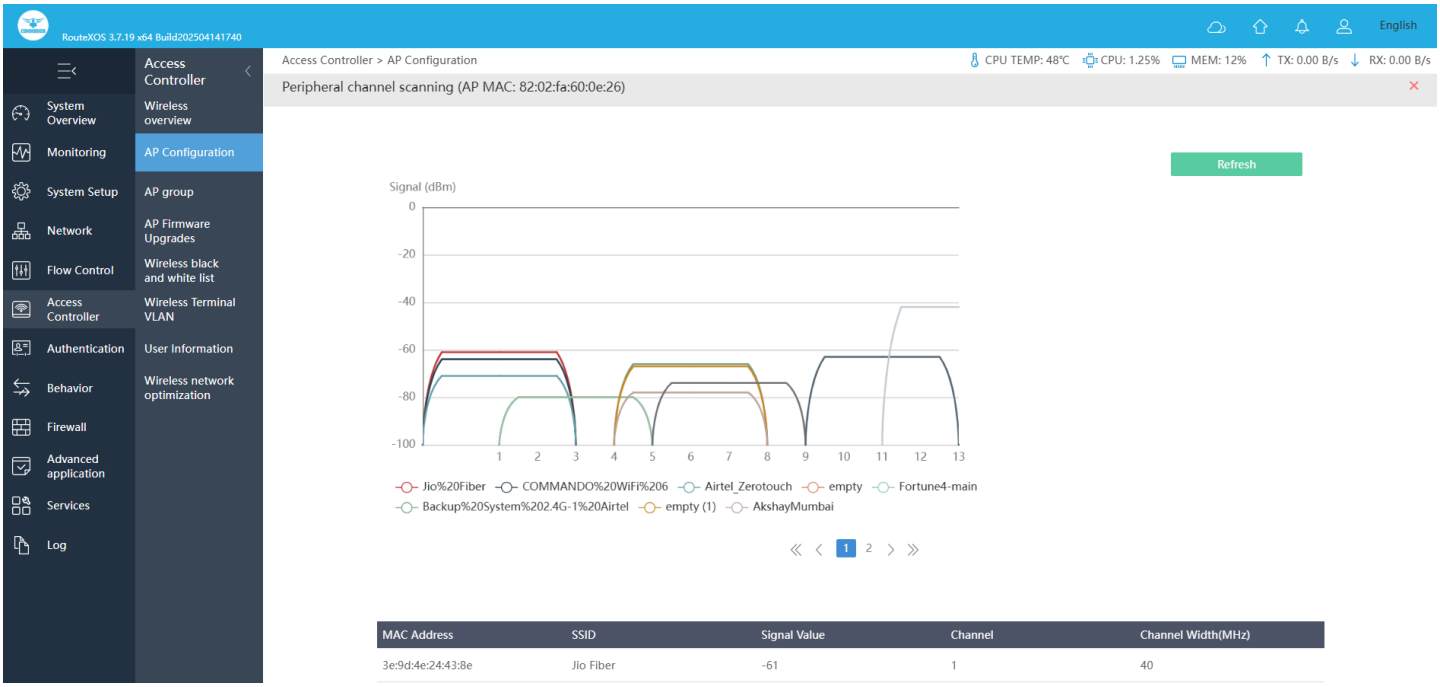


Fig 28. Peripheral Channel Scanning

6. COMMANDO Cloud

In FIT mode this AP can connect with cloud and You can configure cloud settings under this option.

What is cloud service?

Cloud service focuses on managing the router. You can view and manage your devices, such as check the running status, modify the configuration, and set the authentication for captive portal.

How to connect to cloud service?

Into cloud platform http://commandonetworks.com.cn/#/ ---> gets the binding code ---> enters the binding code in router and remark name ---> saves and completes the binding.

How to manage?

Wait about 3 minutes, you will see this device in your cloud account, you can manage and operate using your cloud account.

How to unbind the cloud?

Log in to cloud platform on the PC side and complete the unbundling of corresponding routes in the routing list -- equipment management -- routing information overview page.

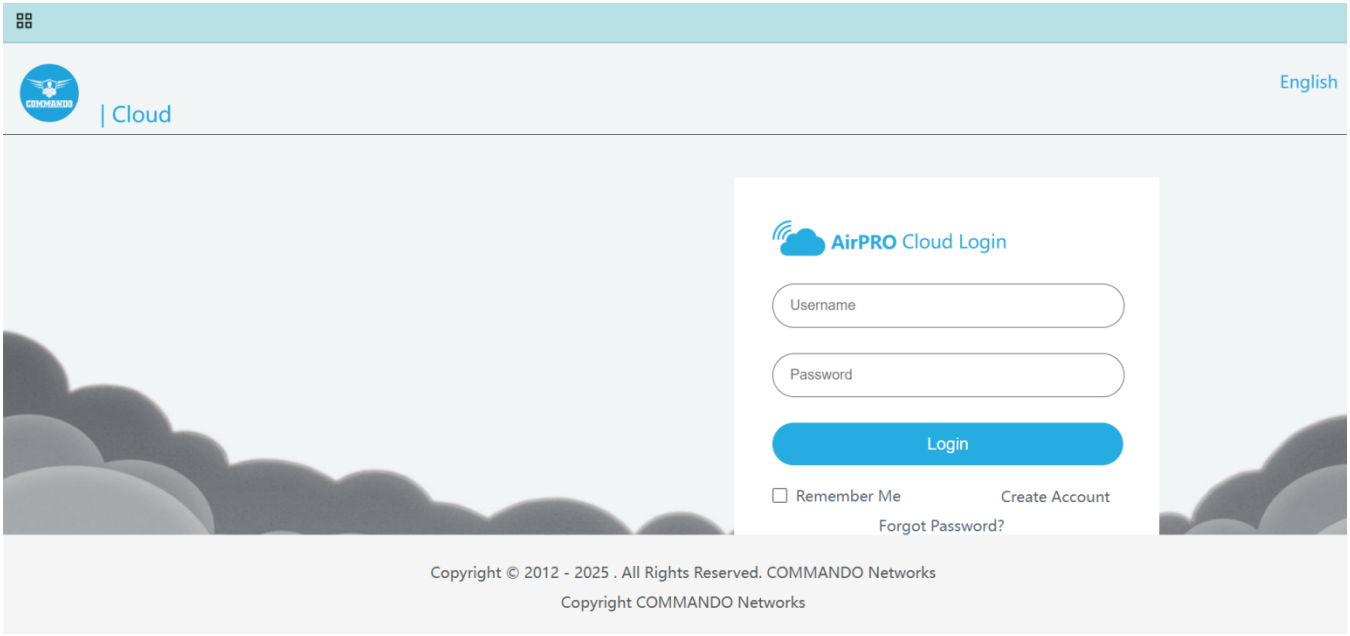


Fig 6.1 Cloud Login page

How to create the account in COMMANDO cloud for login?

Go to any browser and type http://commandonetworks.com.cn. Then AirPRO cloud login page as follows will appear.

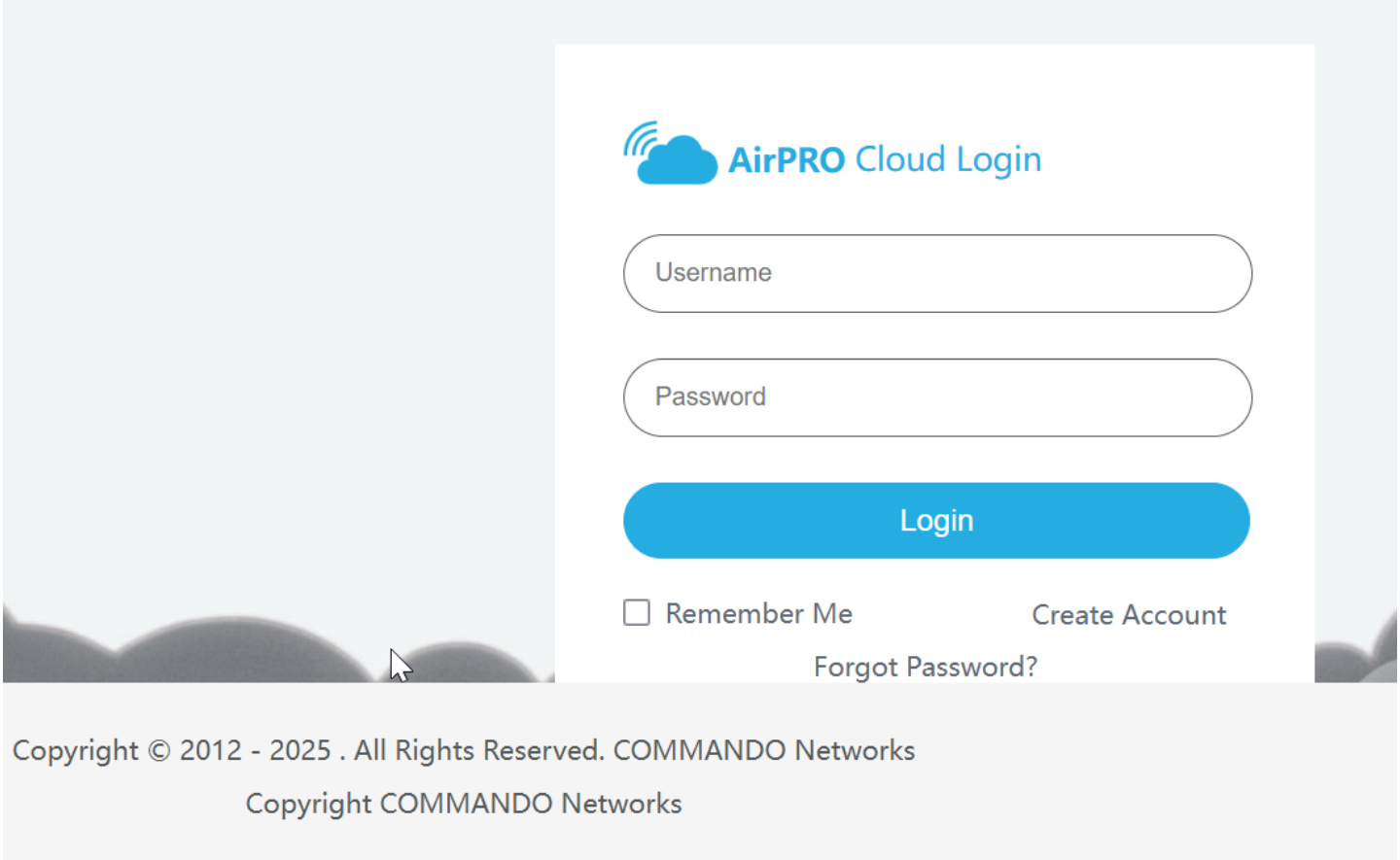


Fig 6.2 Create Cloud Login page

Click on the create account (This process is for creating new account).

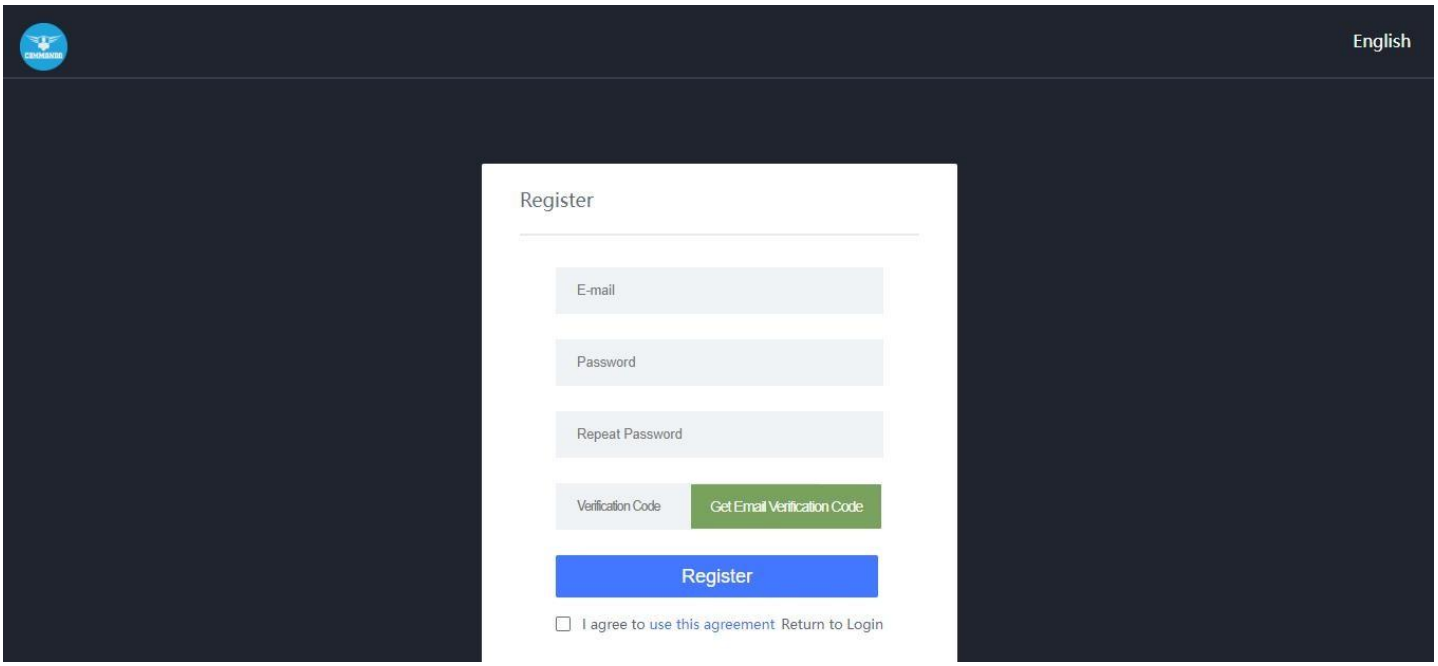


Fig 6.3 Register Cloud Login Email and password page

You can choose register Cloud Login Email and password as per choice of administrator. Note: Email ID should be a valid Email ID.

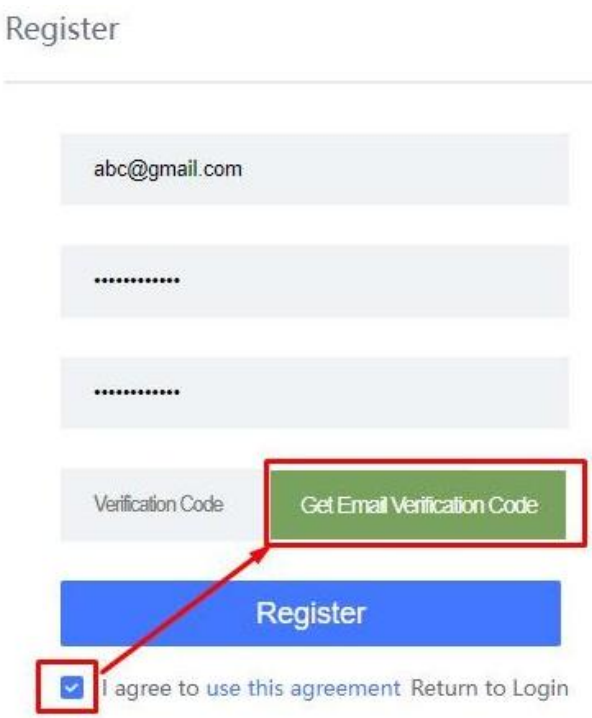
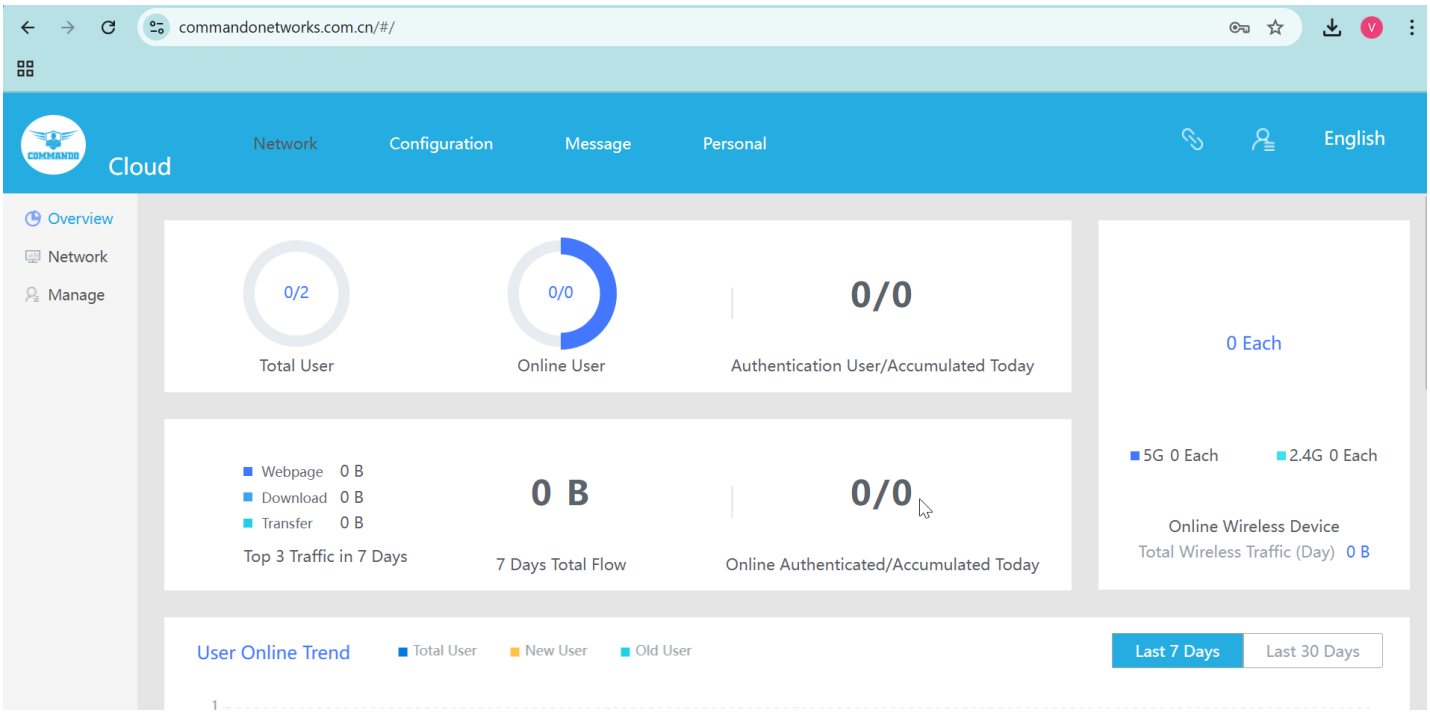


Fig 6.4 Email Verification code page

With help of RouteX Controller Controller you can bind with Cloud and can configure AP from cloud itself. How to bind RouteX Controller with COMMANDO cloud login?



Login in the portal with created email credential and copy cloud binding code.

Fig 6.5 Cloud Binding page

Then take access of RouteX Controller connected to internet and go to System Setup > Cloud Account and bind that copied code to router ID.

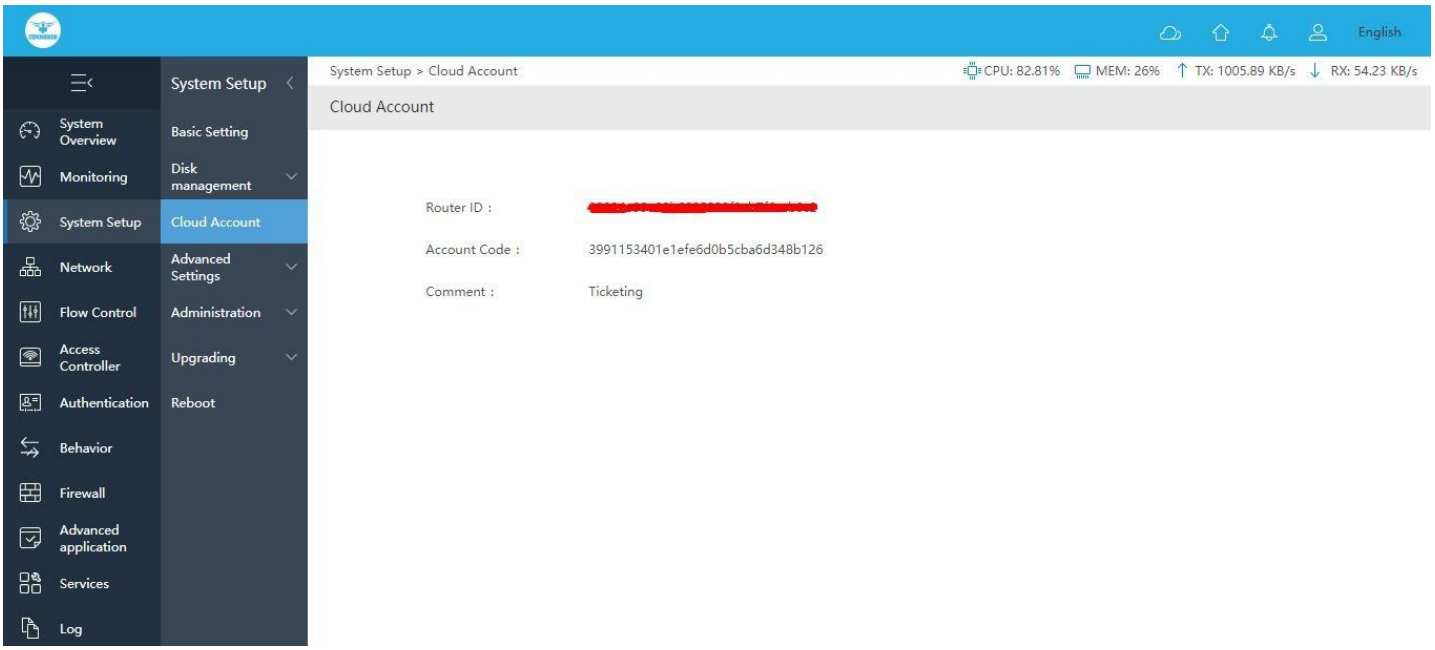


Fig 6.6 RouteX Controller Cloud Account Binding page

After binding code the cloud portal can access and configure RouteX Controller from anywhere in the world if having correct login credential.

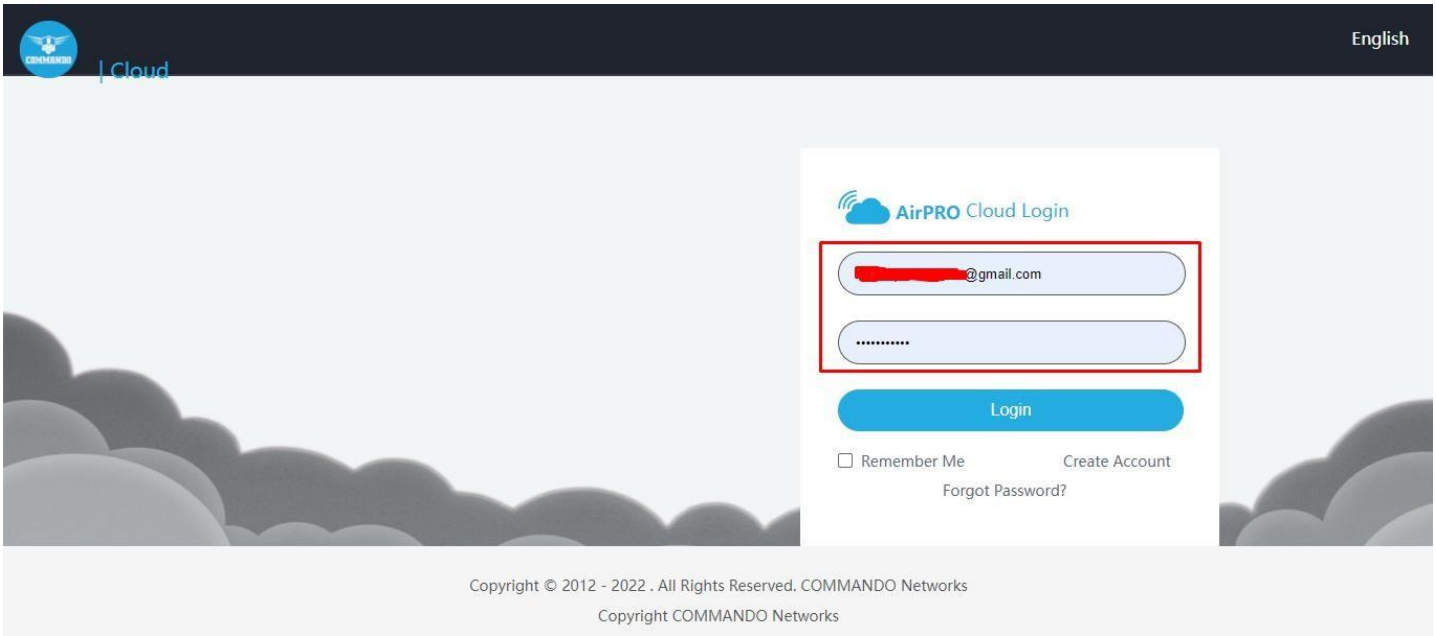


Fig 6.7 Cloud login after binding page

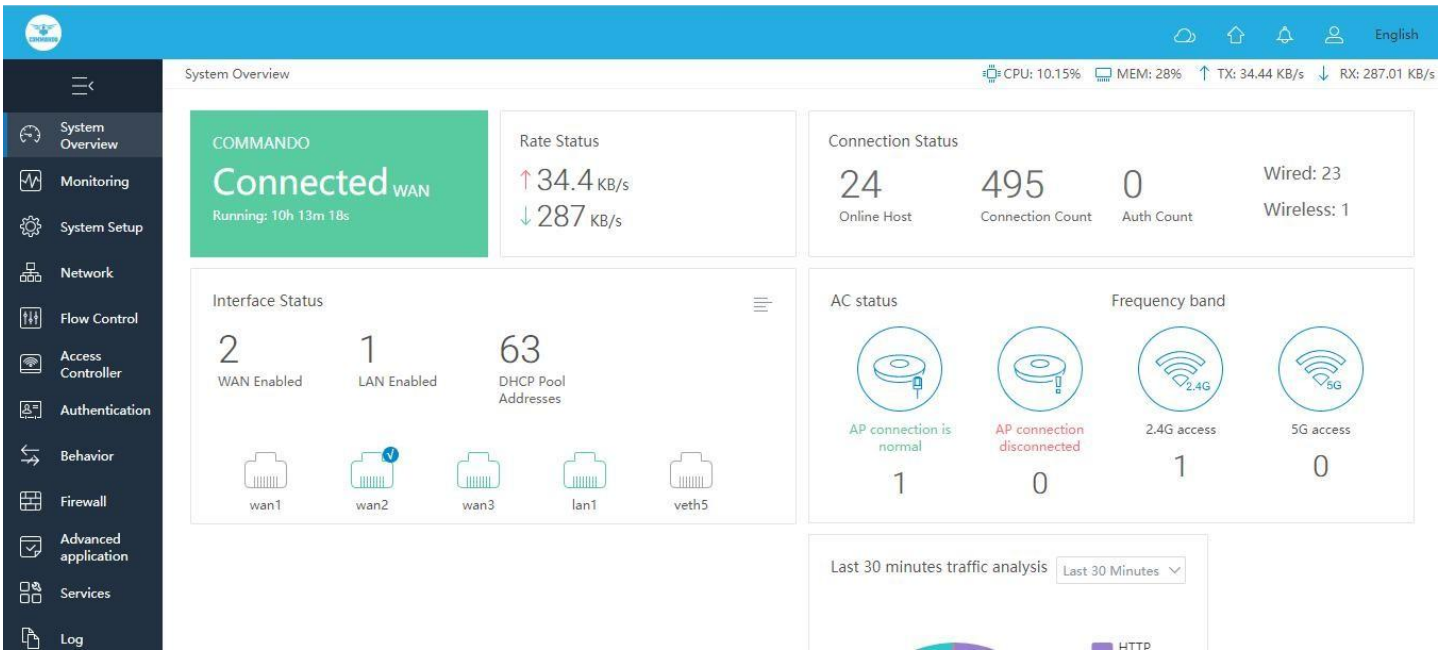


Fig 6.8 RouteX Controller device live access page

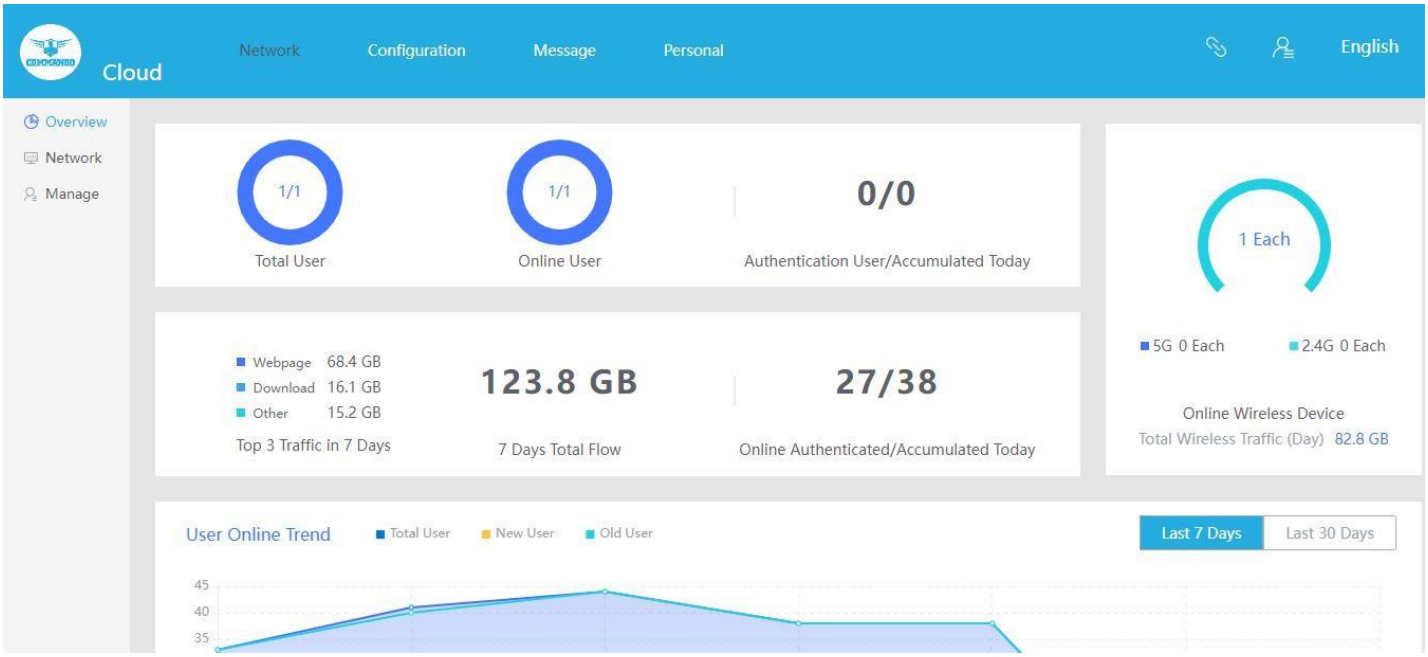


Fig 6.9 RouteX Controller cloud live access page

If password is forgot then following process to be followed.

How to recover from lost cloud portal password?

For recover from lost cloud portal password go to the cloud portal of COMMANDO and click Forgot Password.

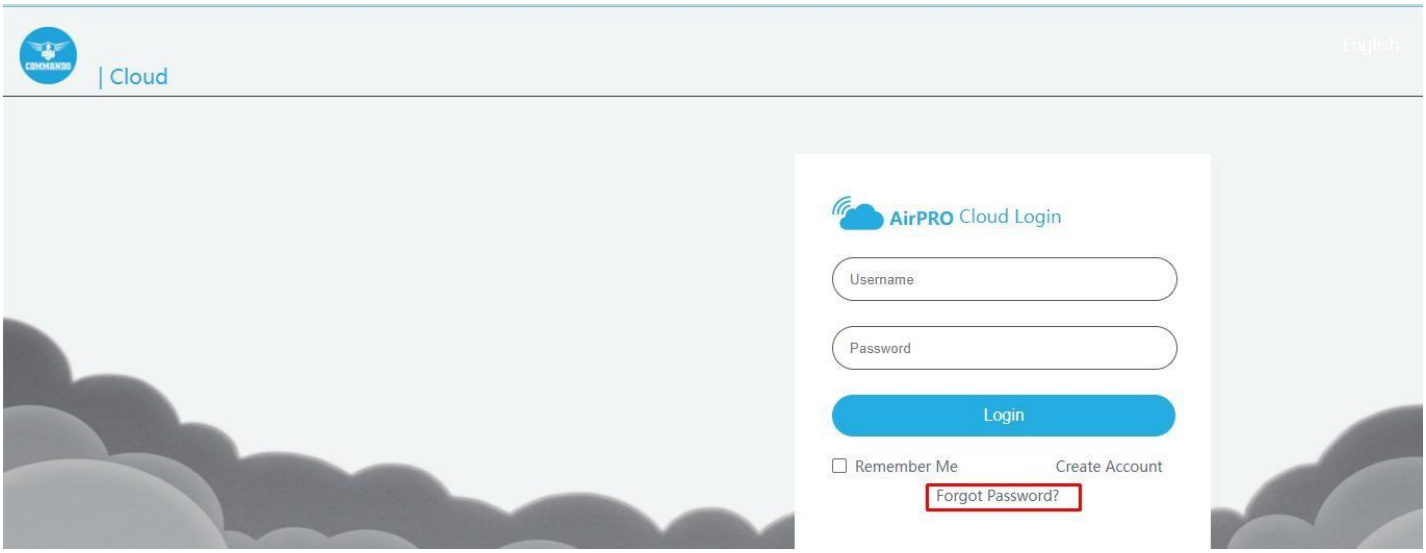


Fig 6.10 AirPRO forgot password page

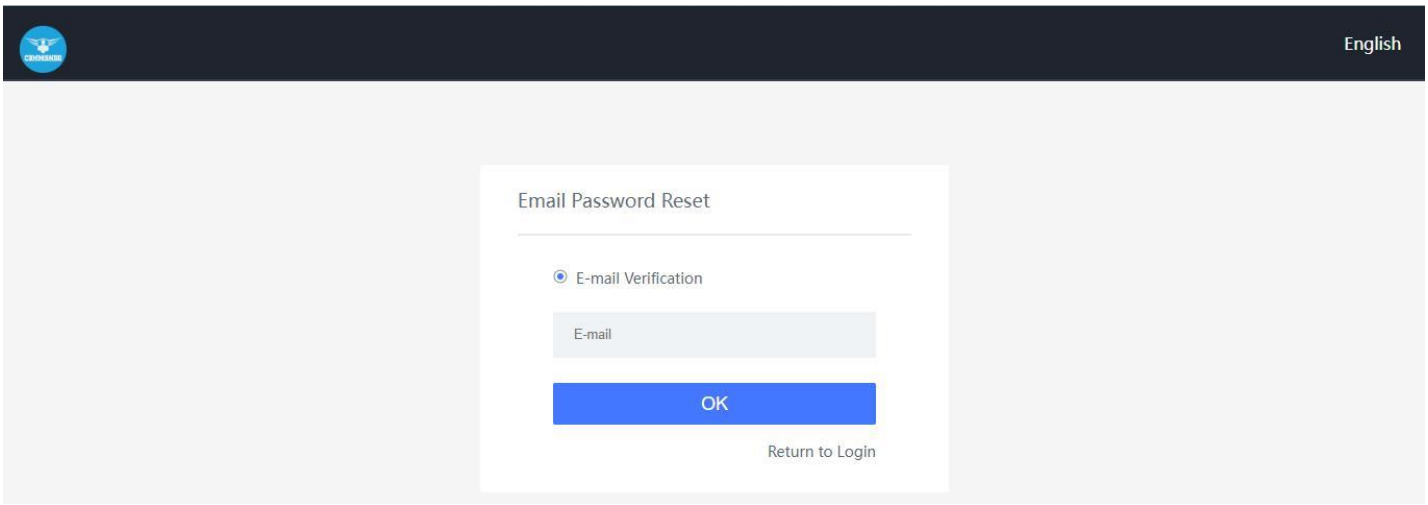


Fig 6.11 AirPRO Email for password reset page

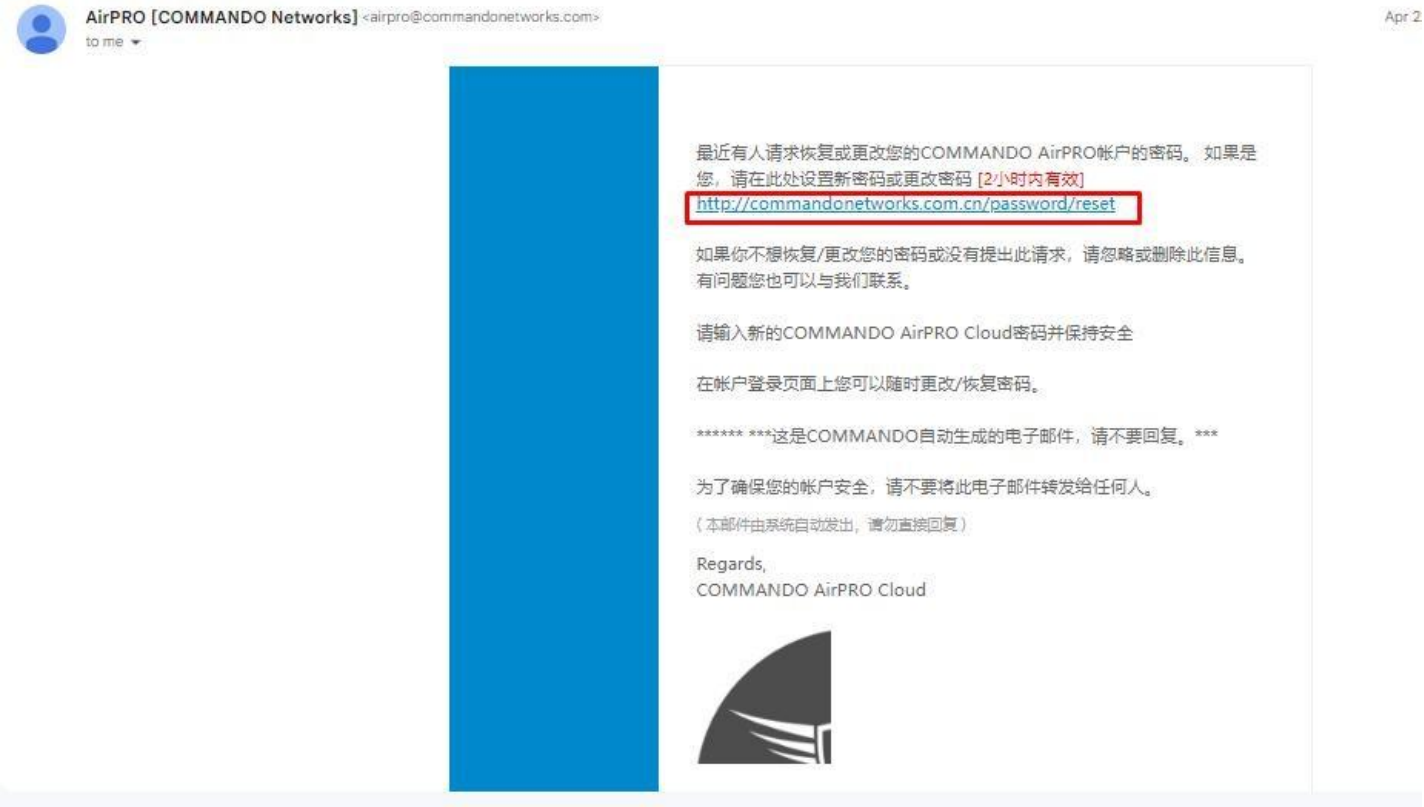


Fig 6.12 AirPRO Email received for password reset page

The reset email will send on email provided for request to recover or change the password for COMMANDO AirPRO account. Set a new password or change your password and said link will be valid for 2 hours only. http://commandonetworks.com.cn/password/reset. If you do not wish to recover/change your password or did not make this request, please ignore or delete this information. You can also contact COMMANDO support for any query.

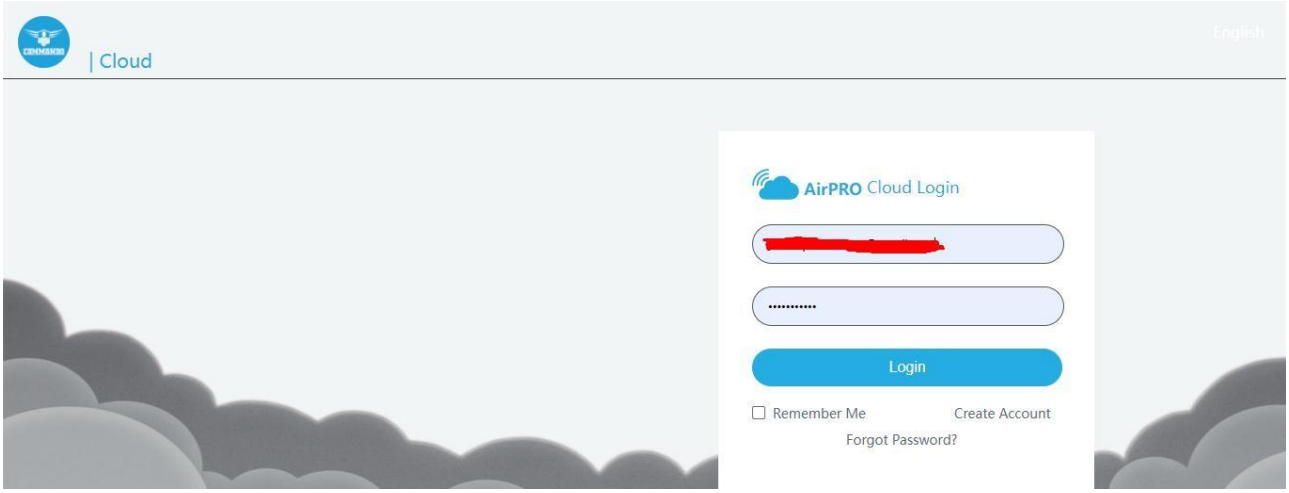


Fig 6.13 AirPRO cloud login after password reset page

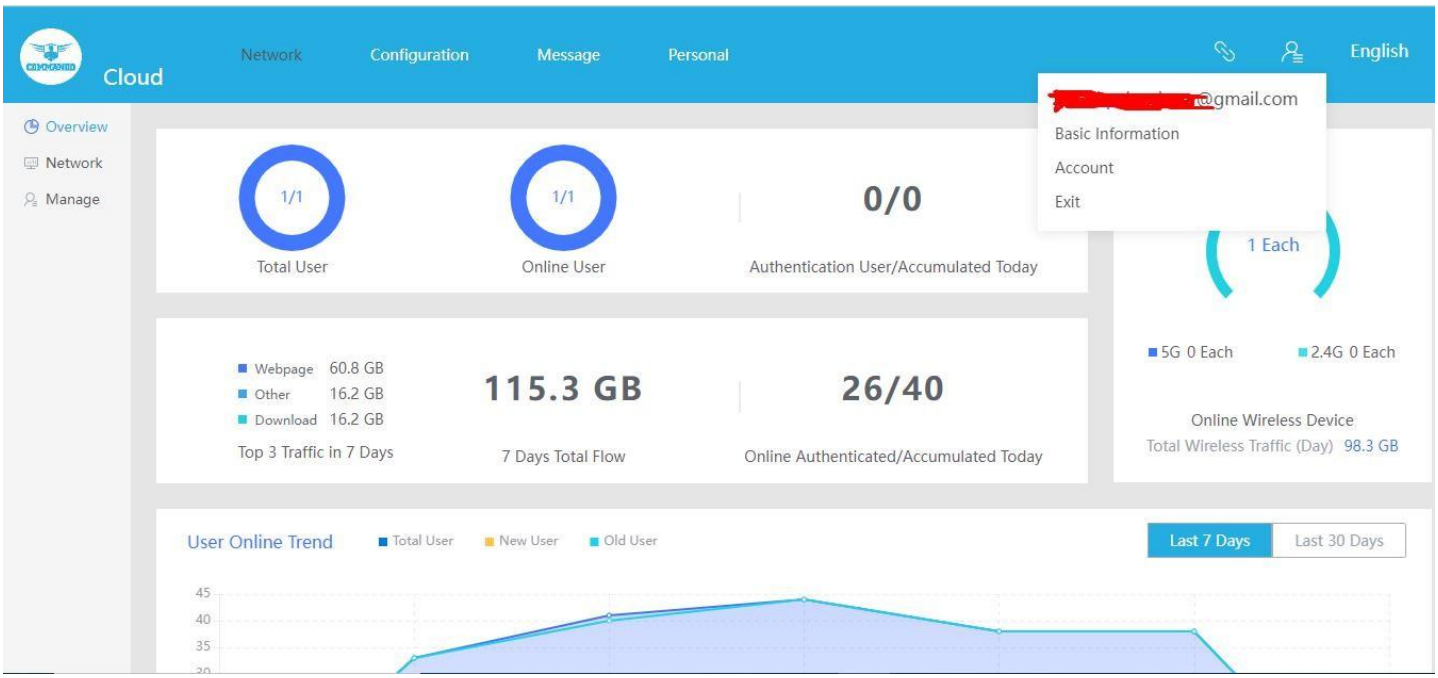


Fig 6.14 AirPRO cloud login page

Fig 6.15 Cloud User Language setting page

6.1 AirPRO Cloud Overview

A cloud-managed access point or networking solution allows business owners to manage Wi-Fi and network infrastructure over the cloud with zero maintenance charges, centralize control painlessly. This means businesses can connect to the cloud by subscribing to a pay-as-you-go, on-demand model.

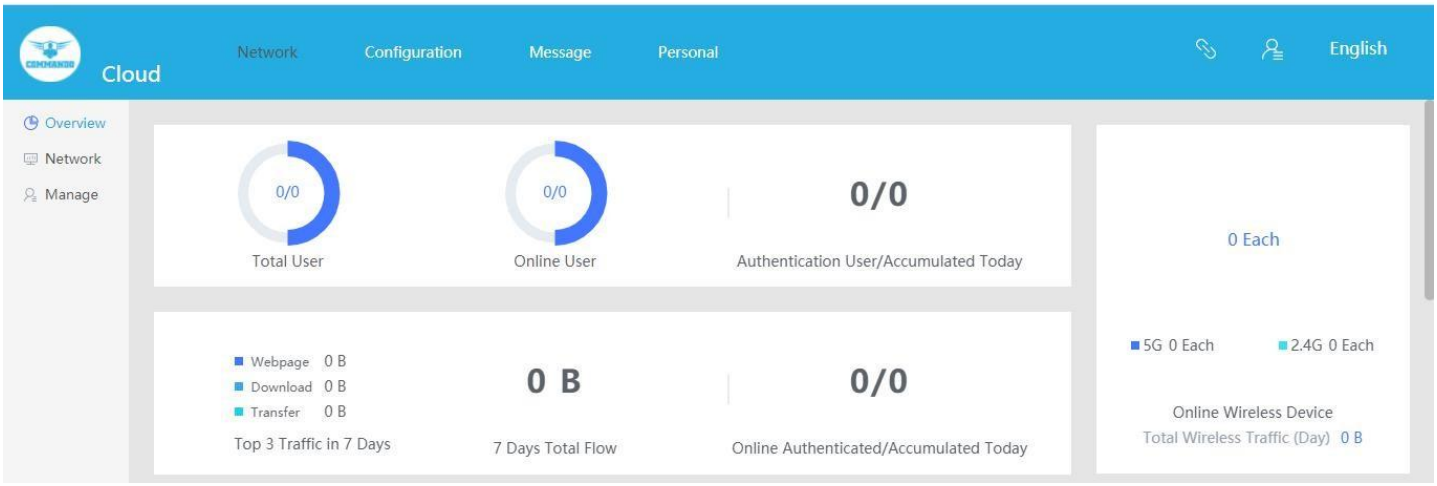


Fig 6.1.1 Default Cloud Overview page

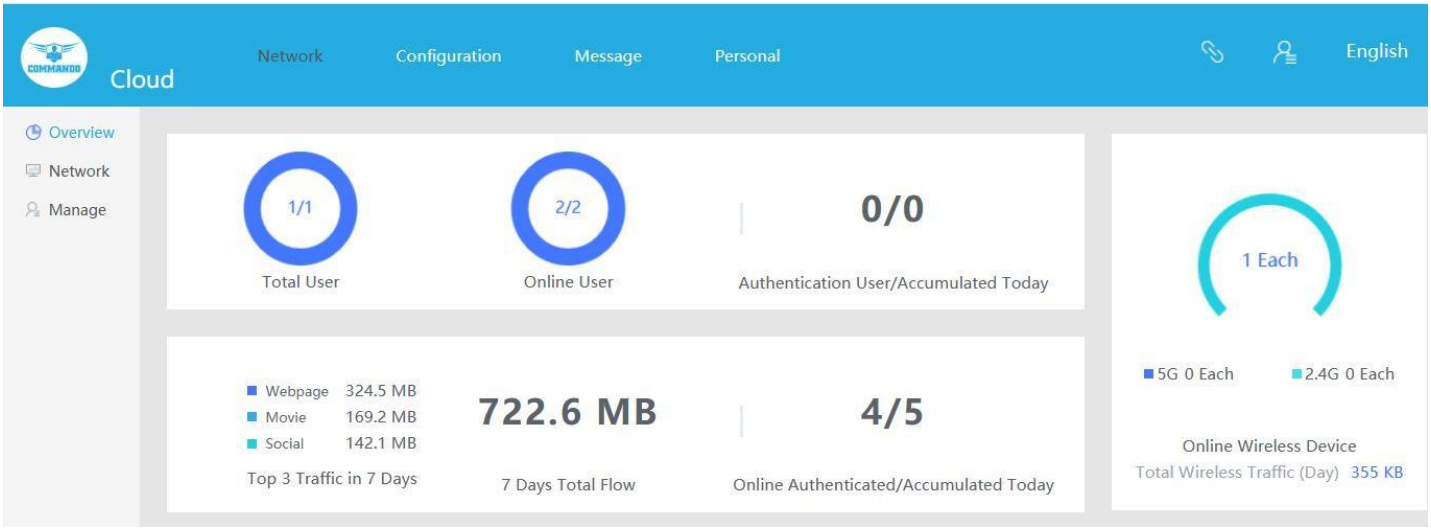


Fig 6.1.2 Cloud Overview page

Fig 6.1.3 Cloud User online trend page

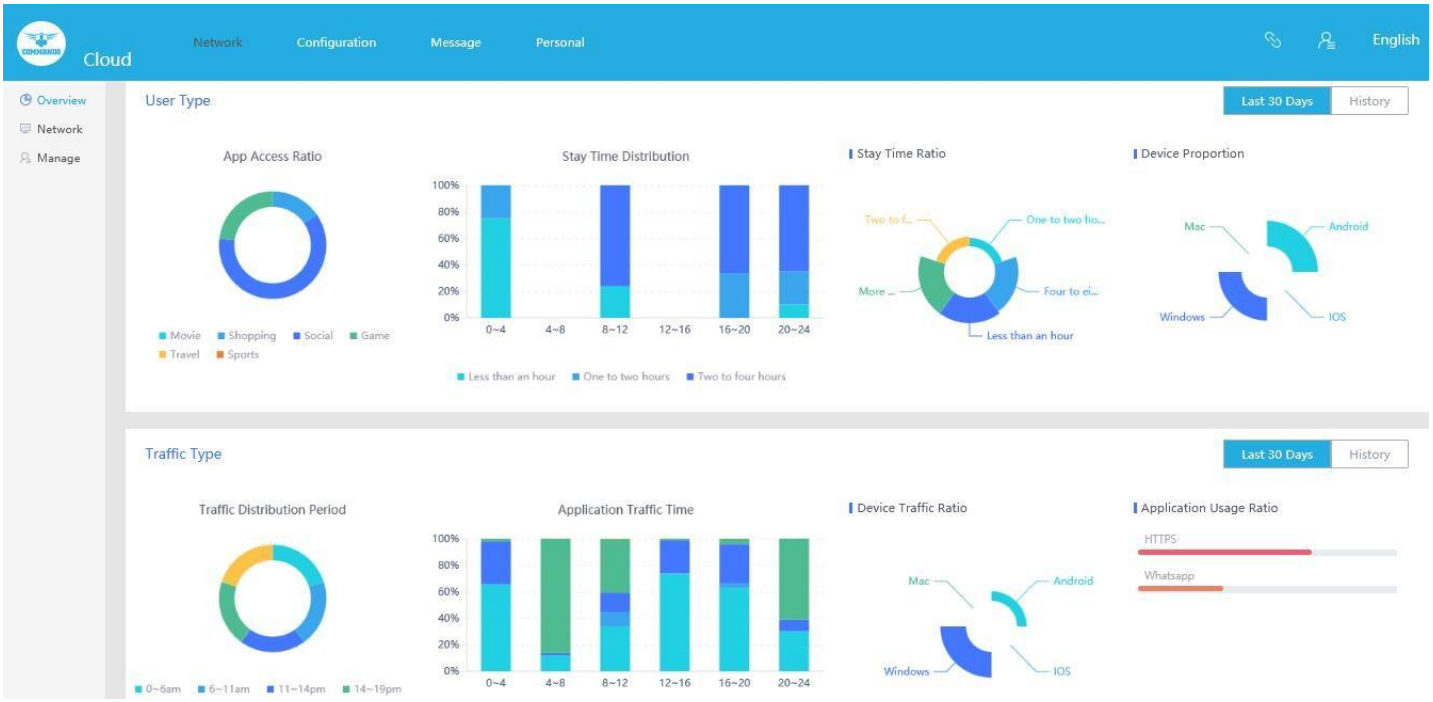


Fig 6.1.4 Cloud User Type page

6.2 Network

Cloud Networking Solutions are Designed to Enhance Your access and IT infrastructure in which some or all of an organization's network capabilities and resources are hosted cloud account.

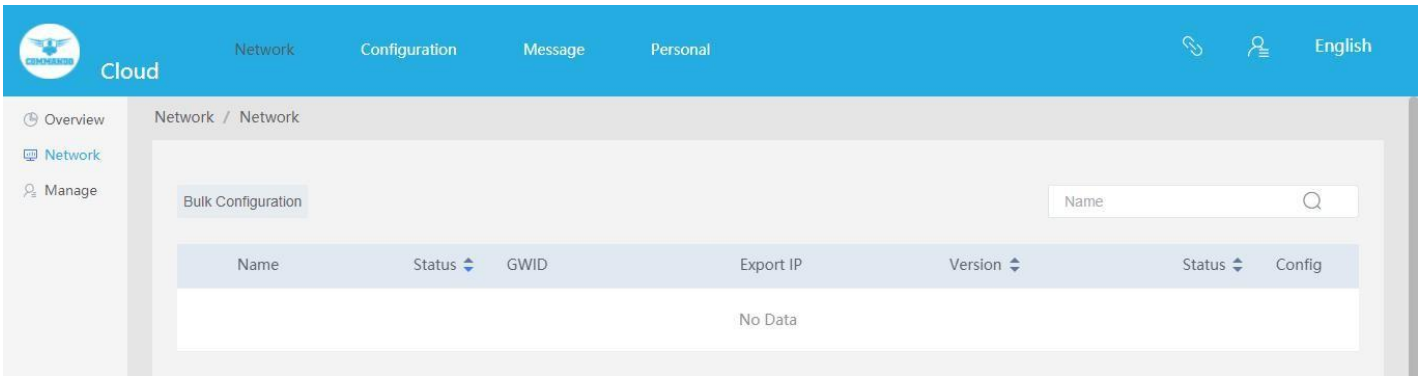


Fig 6.2.1 Default Bulk configuration page

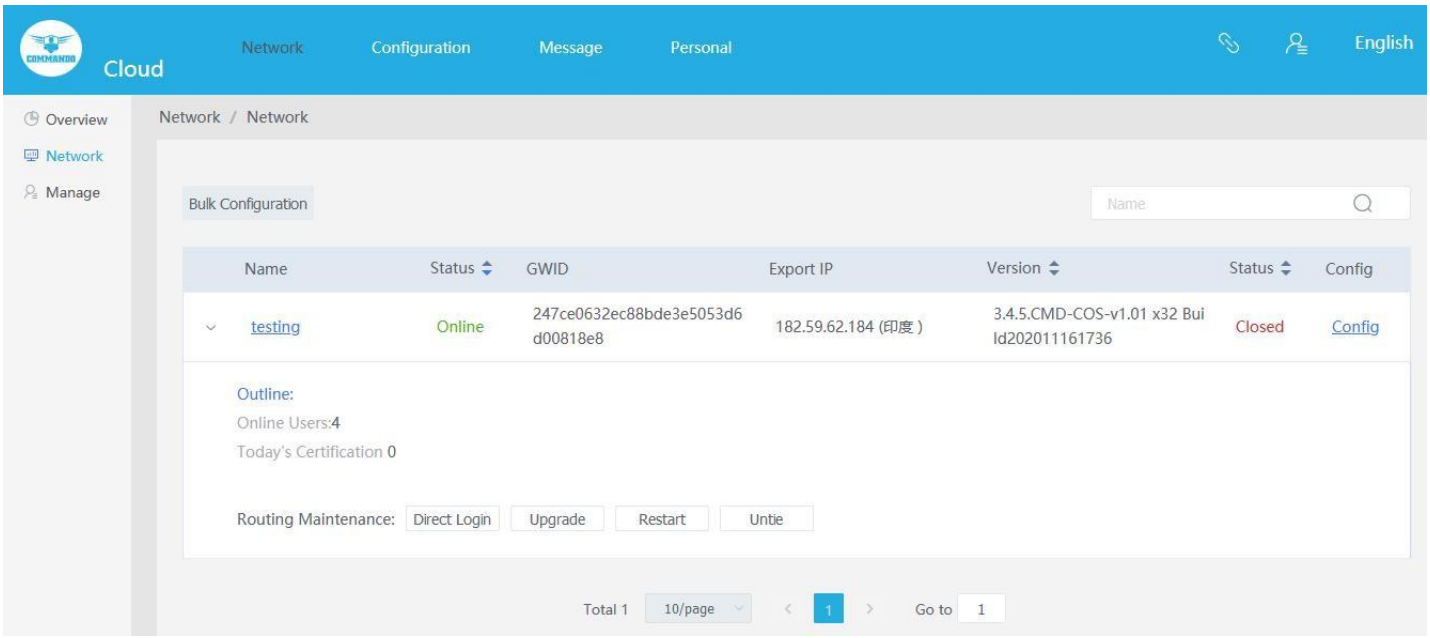


Fig 6.2.2 Bulk configuration page

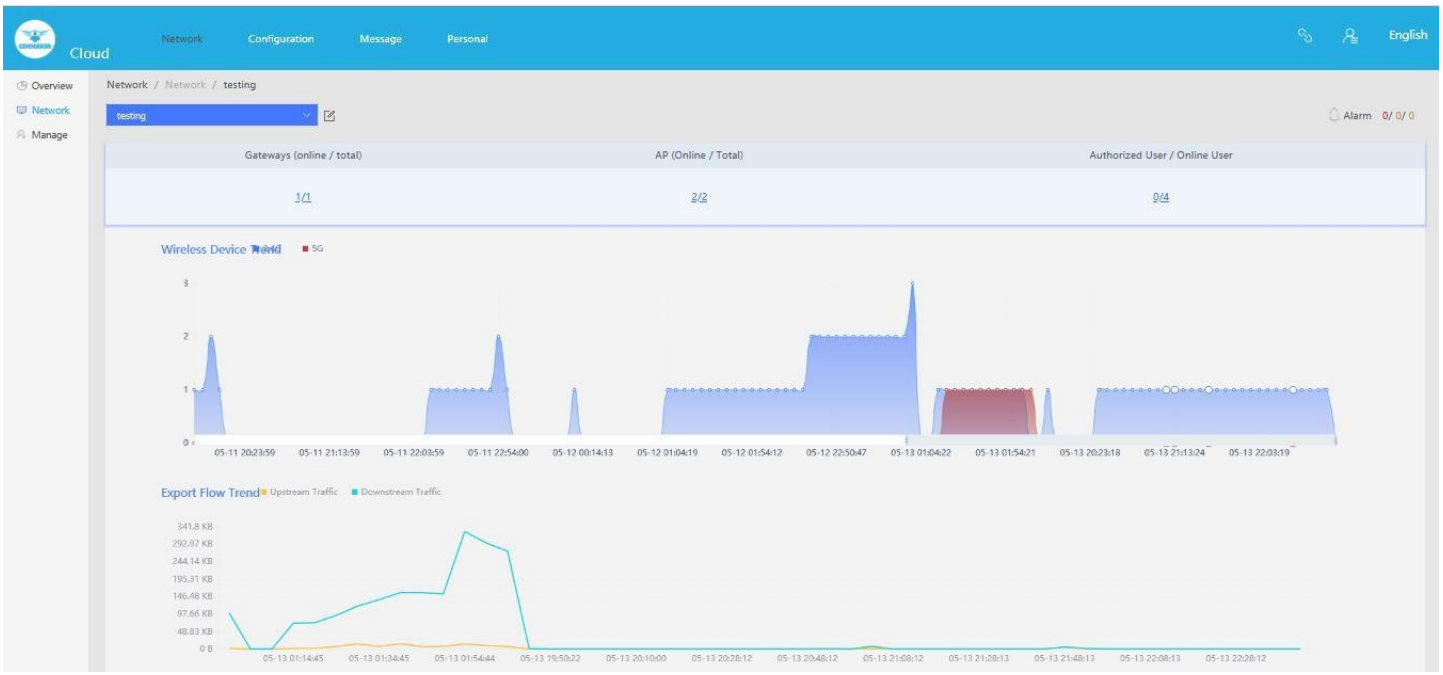


Fig 6.2.3 Network Devices listed in Cloud page

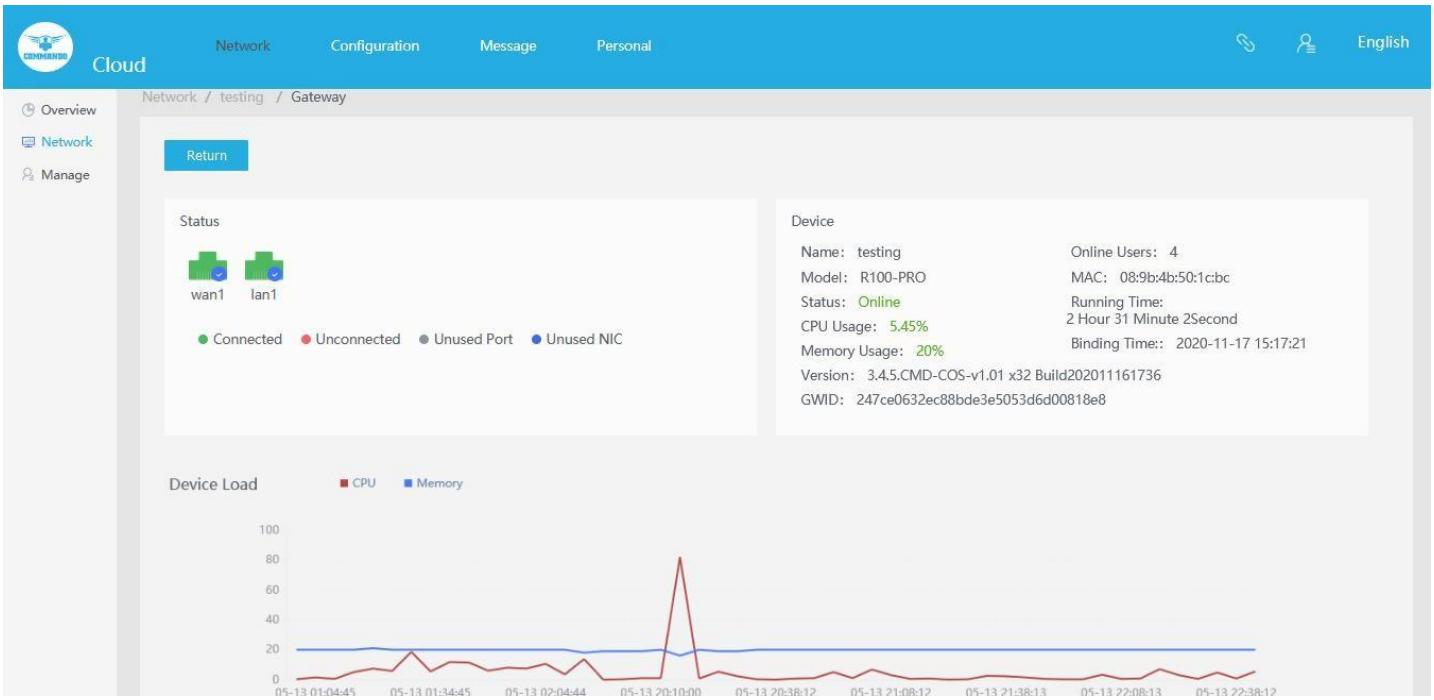


Fig 6.2.4 Gateway page

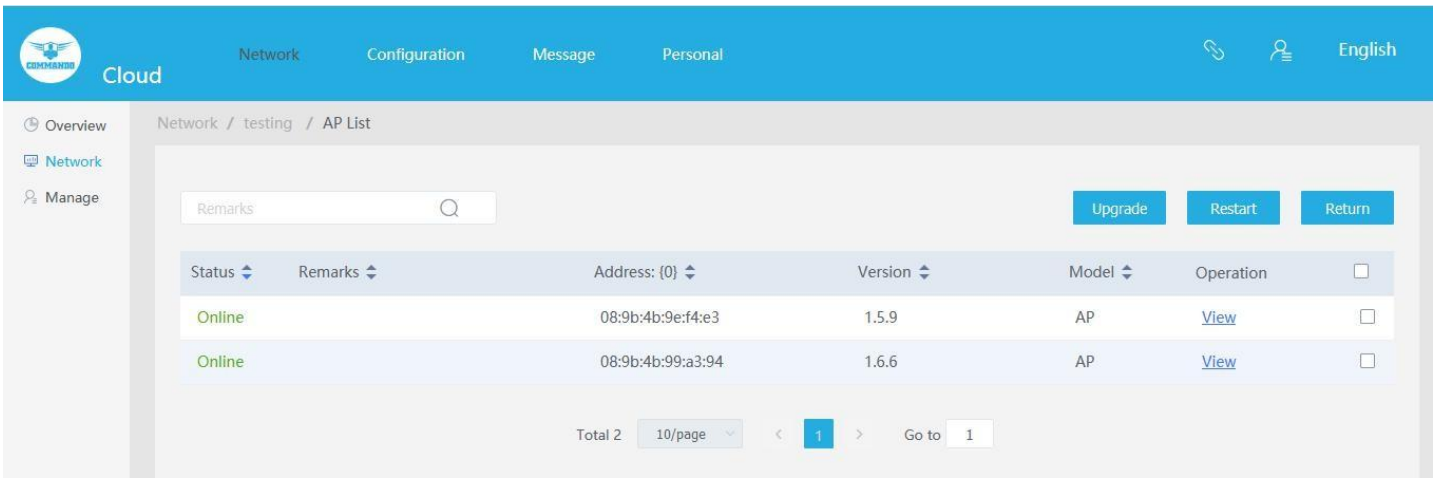


Fig 6.2.5 AP List page

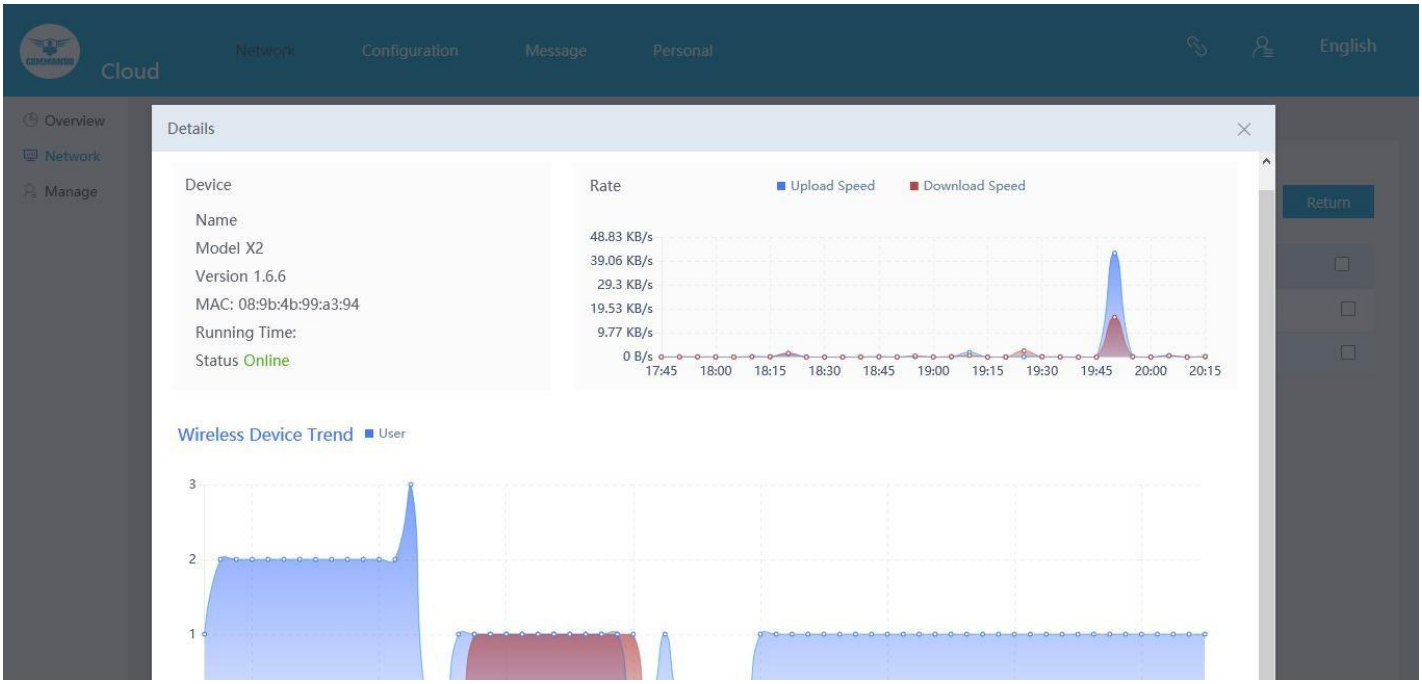


Fig 6.2.6 Bulk configuration for particular AP Device page

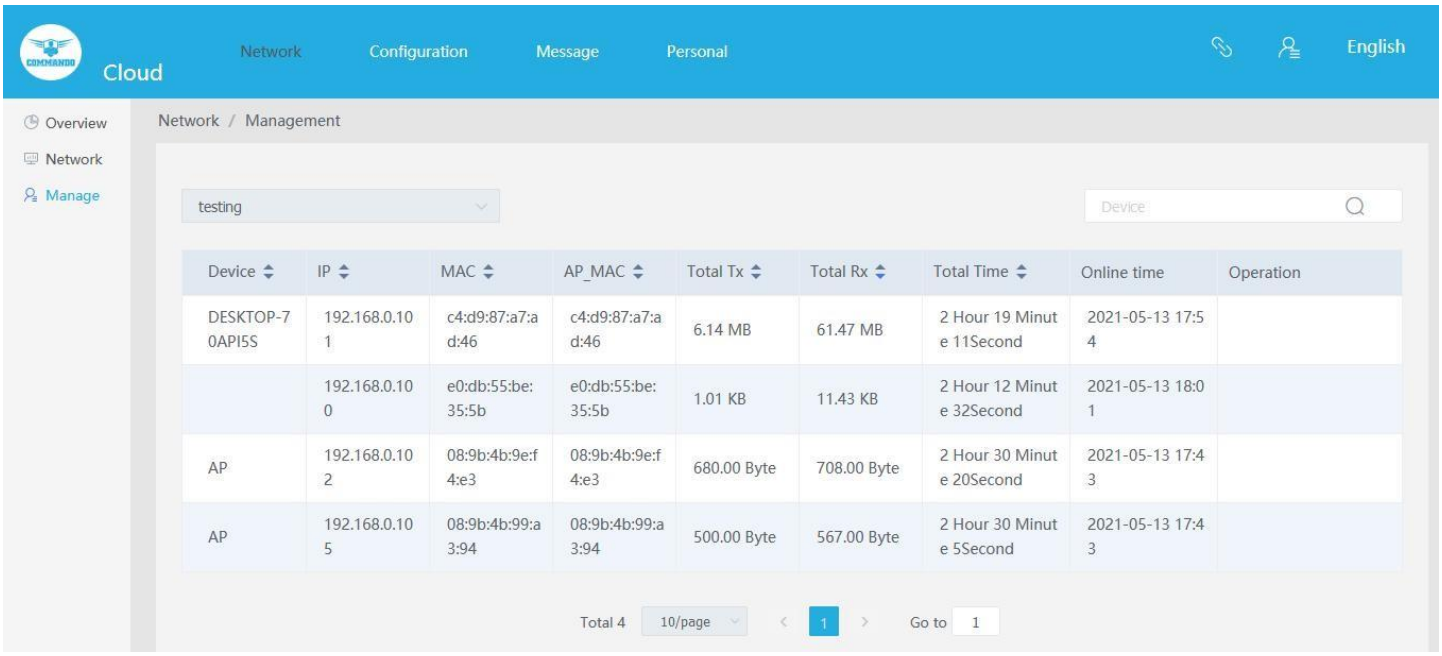


Fig 6.2.7 Network Management for all users' page

6.3 Configuration

The cloud authentication can be done with three server method namely Cloud Platform, Customize as per user requirement and Web-Radius. Cloud networking allows users to build networks using cloud-based services with help of certification process with Global Portal and WeChat Mini Program. A reliable cloud network provides centralized management, control and visibility, for example, managing devices in different physical locations using the internet. It can be used for connectivity, security, management and control.

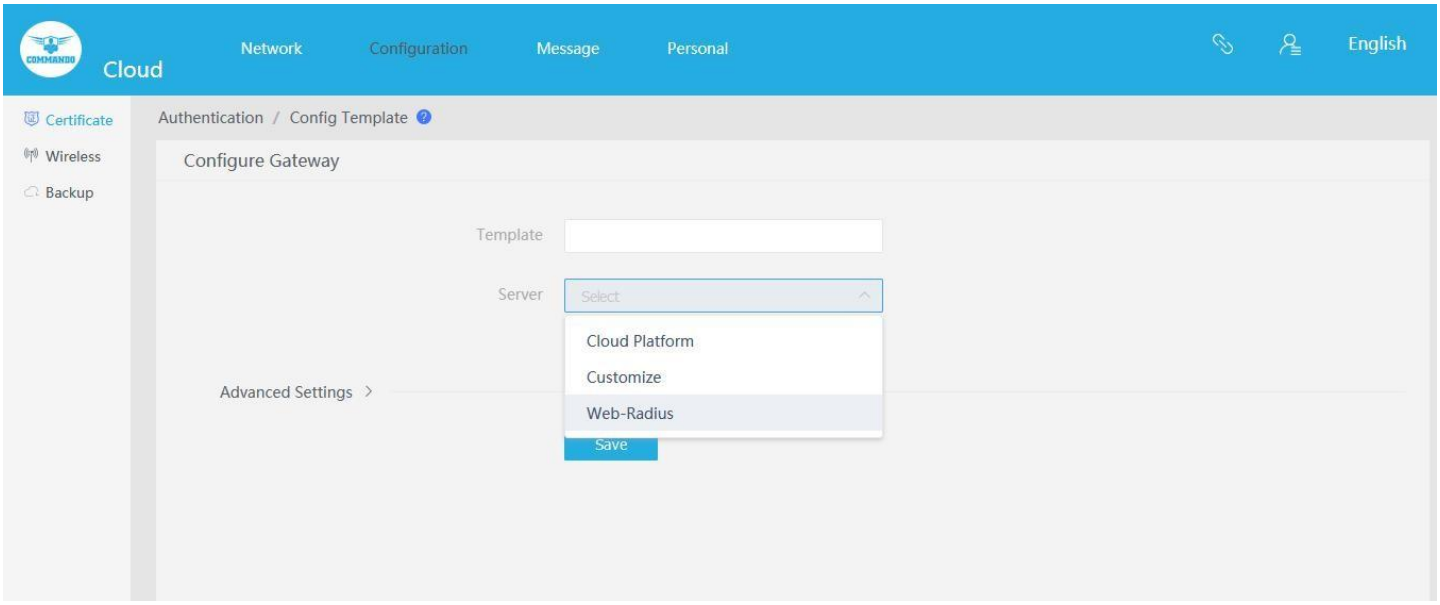


Fig 6.3.1 Default Server Authentication selection page

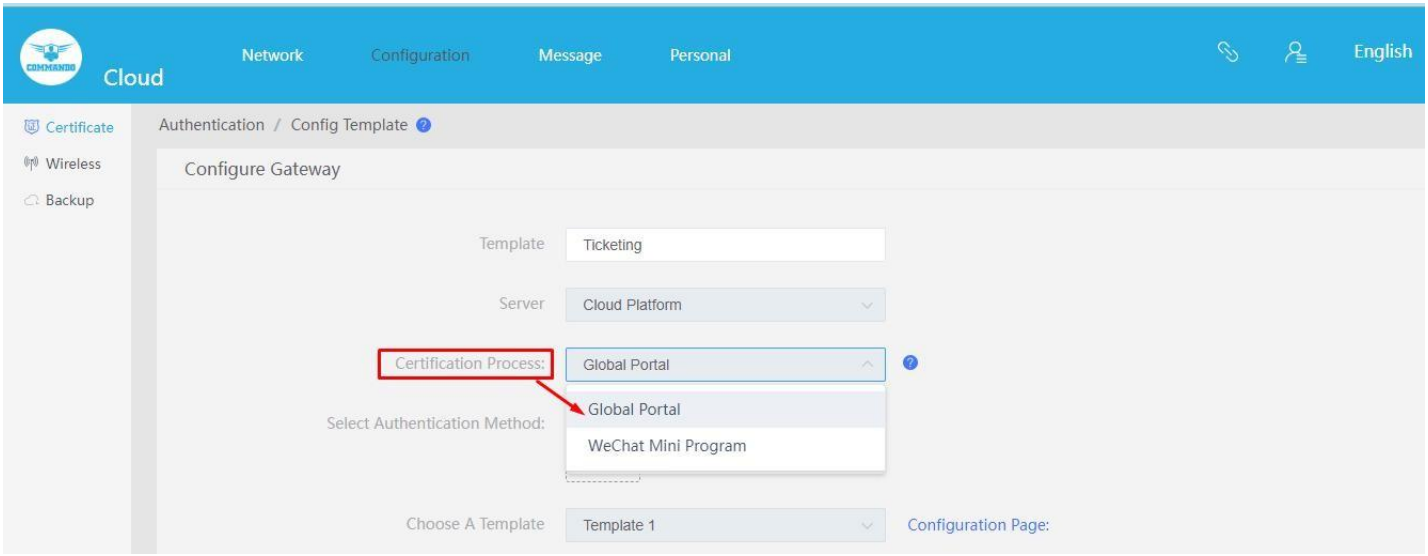


Fig 6.3.2 Certification Process selection option page

User can select various Authentication Method as per choice/requirement. You can choose multiple method of authentications simultaneously.

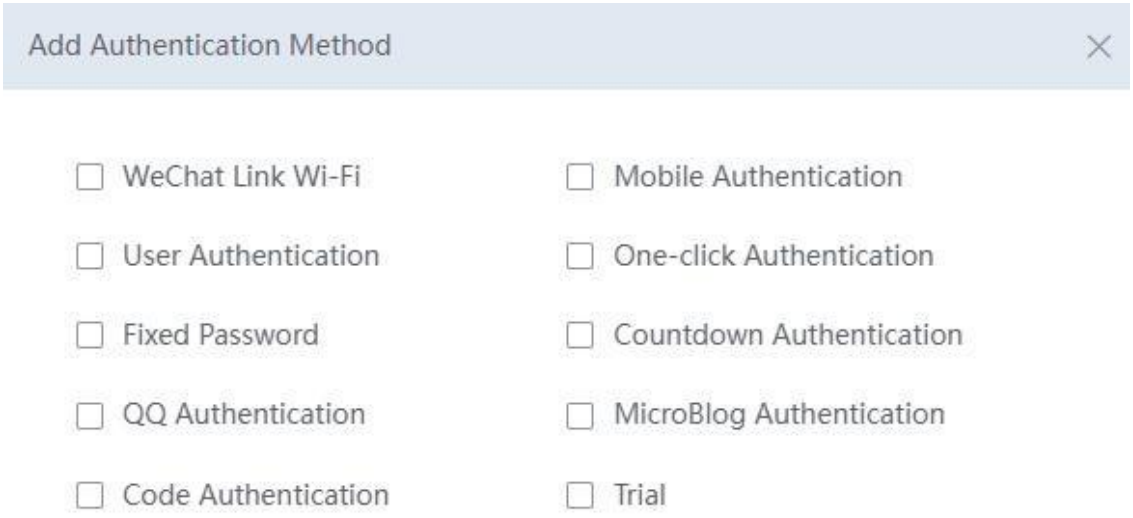


Fig 6.3.3 Authentication Method selection option page

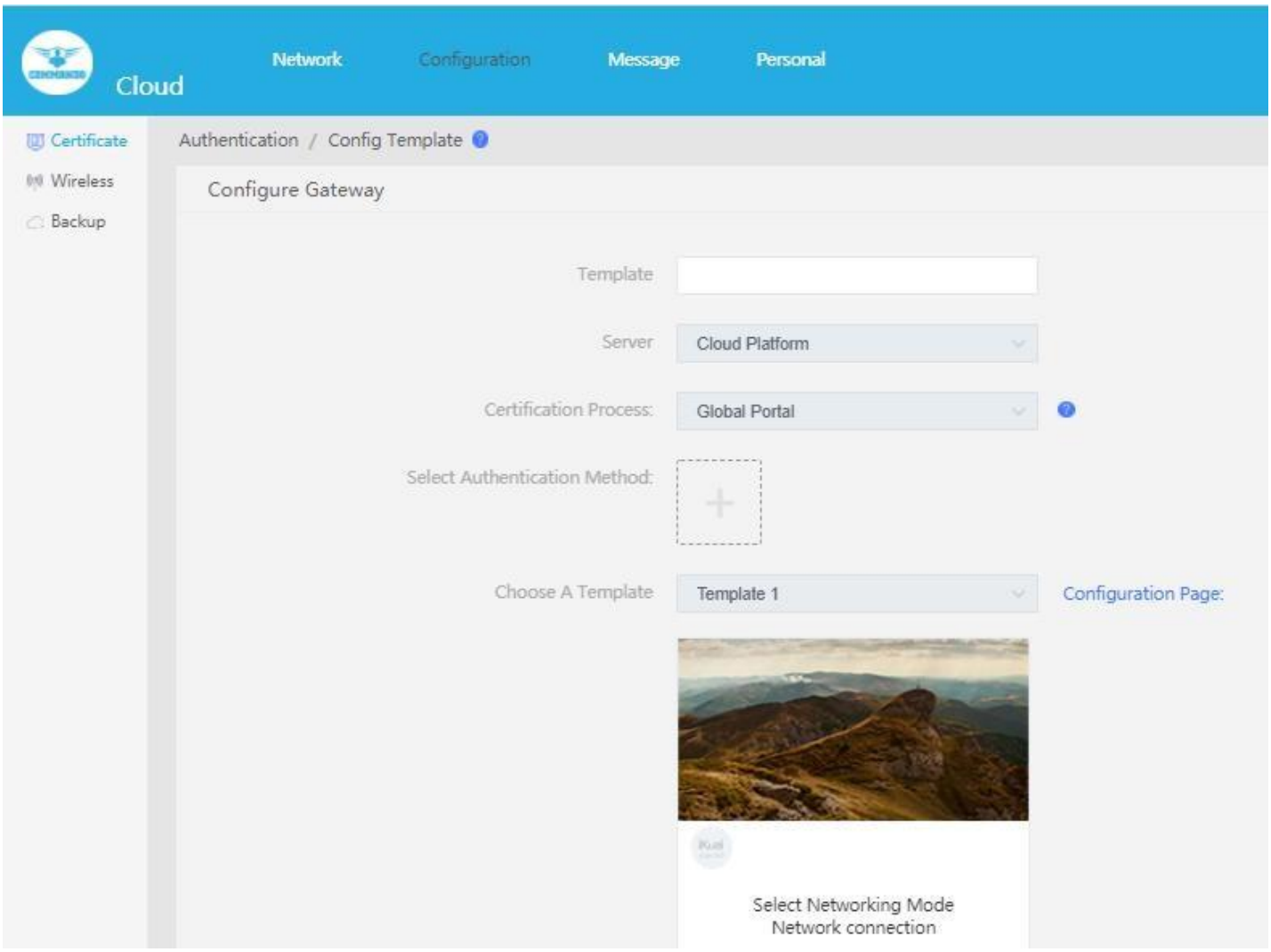


Fig 6.3.4 Default Cloud platform configure gateway page

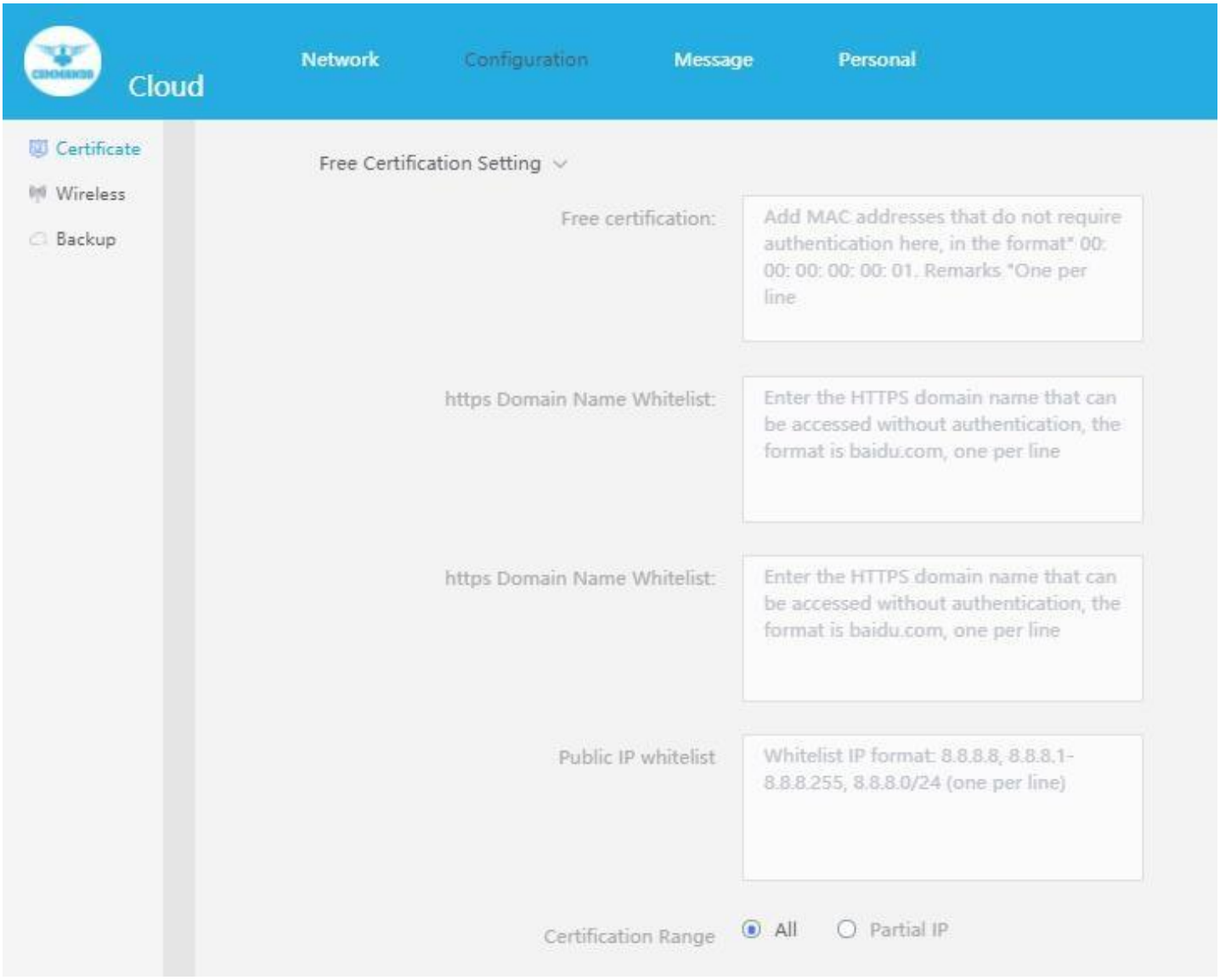


Fig 6.3.5 Default Authentication Free certification setting page

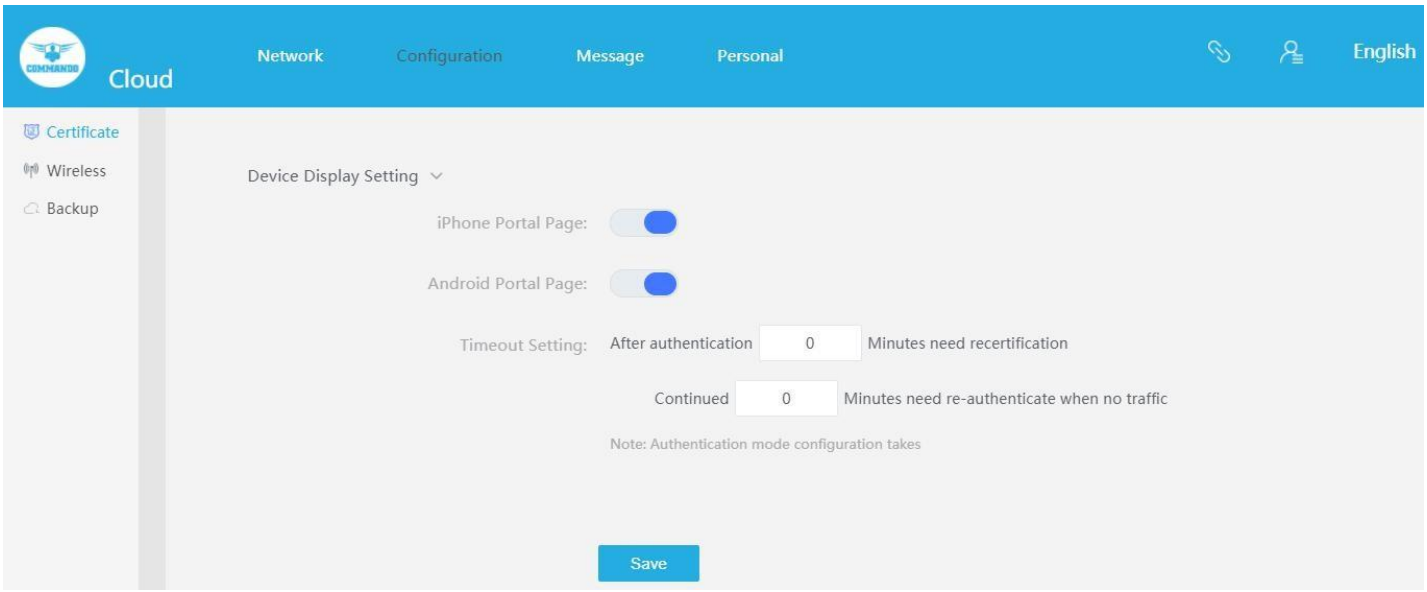


Fig 6.3.6 Default Authentication Device Display setting page

Example 1:

Let us set Authentication/Config Template for Configure Gateway with Template named Ticketing with authentication Server platform as Cloud Platform with Certification Process as Global Portal along with Authentication Method as One-click Authentication.

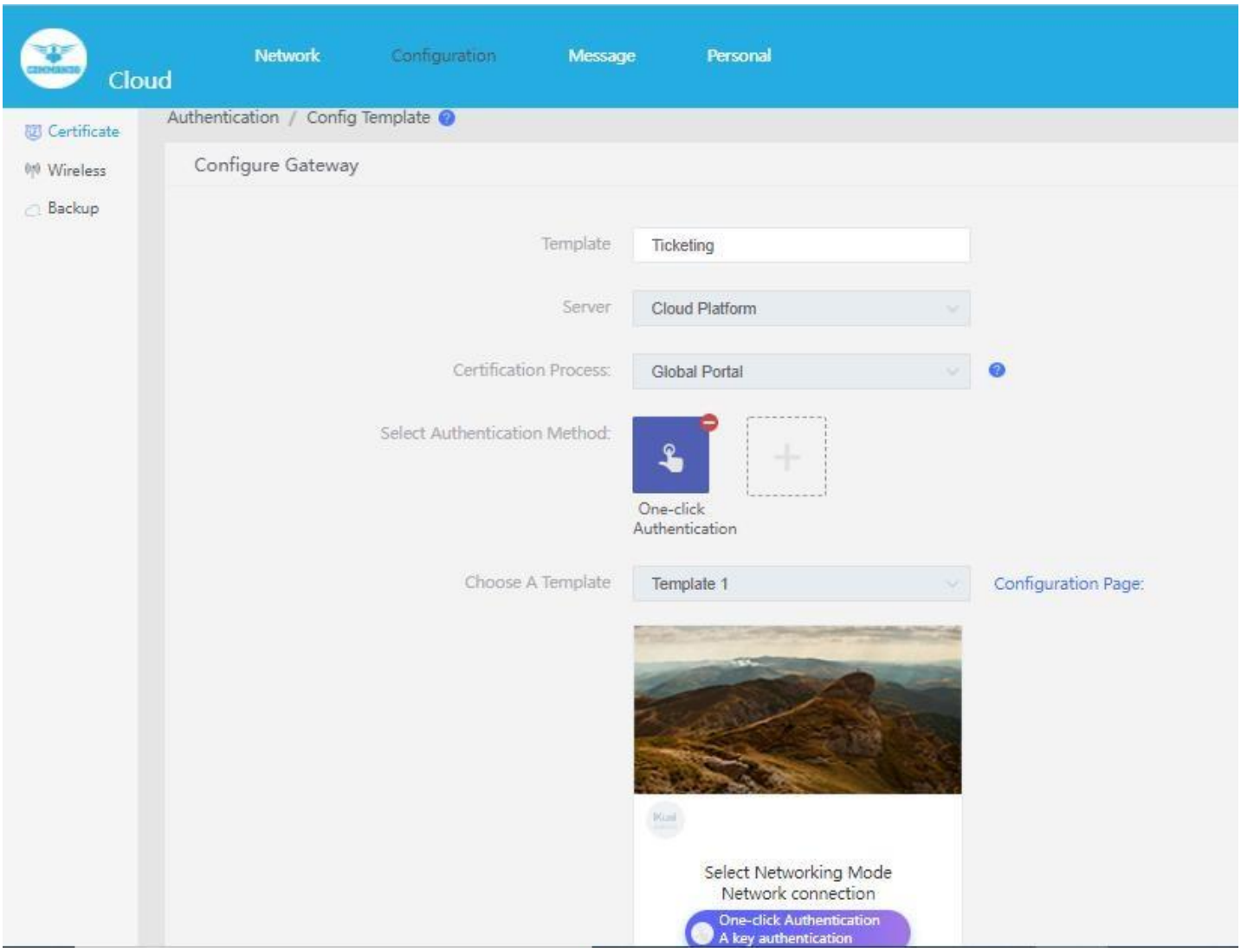


Fig 6.3.7 Authentication Config Template setting for example 1 page

Note: After adding a template, you can go to the" Network Management "page and use the" Bulk Configuration "option to deliver the template.

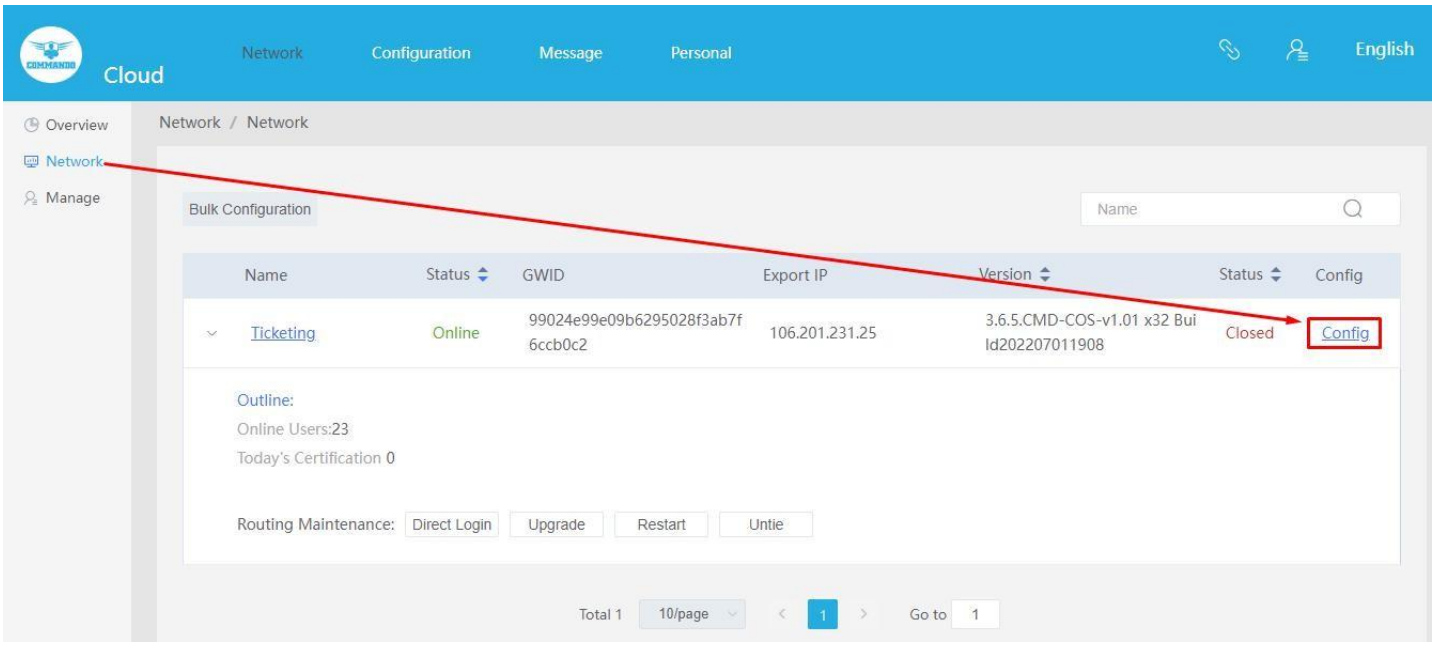


Fig 6.3.8 Authentication Configuration in network setting for example 1 page

Fig 6.3.9 Authentication web page for example 1 page

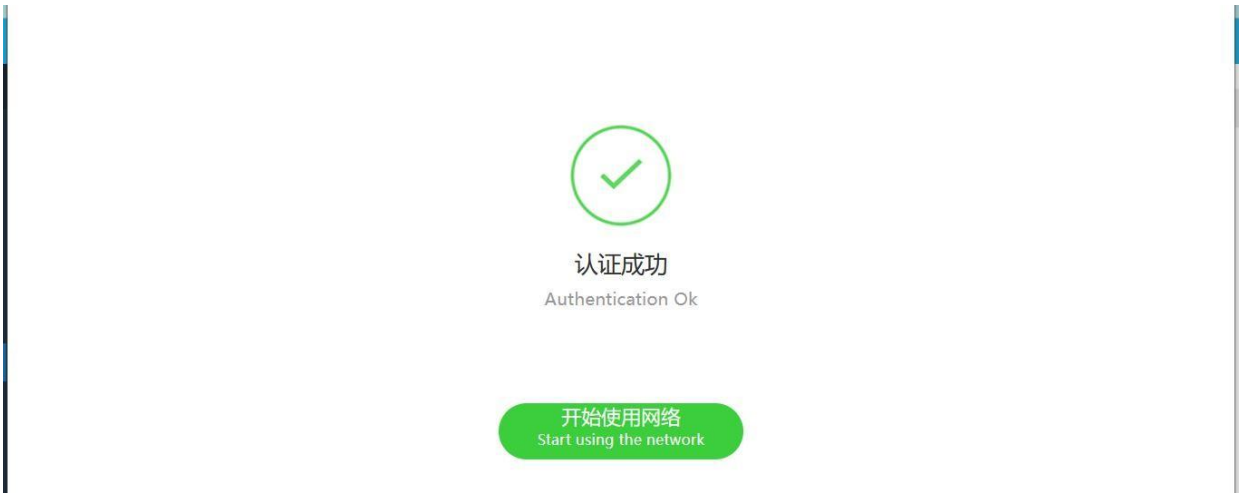


Fig 6.3.10 Authentication Successful web page for example 1 page

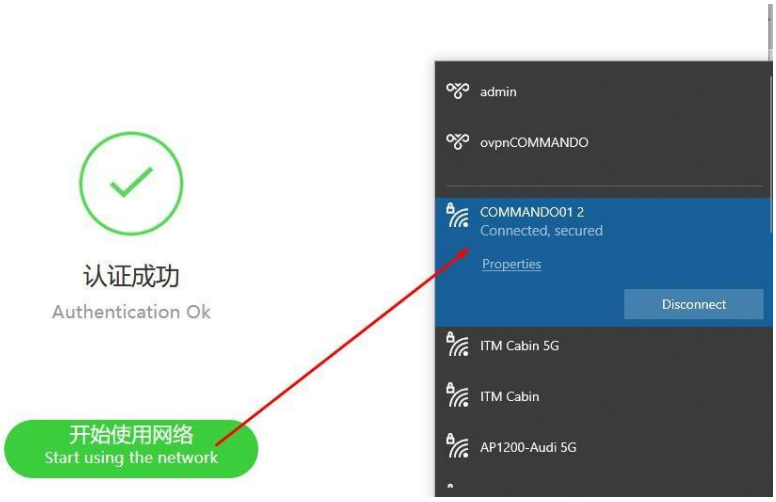


Fig 6.3.11 Wifi connected after Authentication Successful for example 1 page

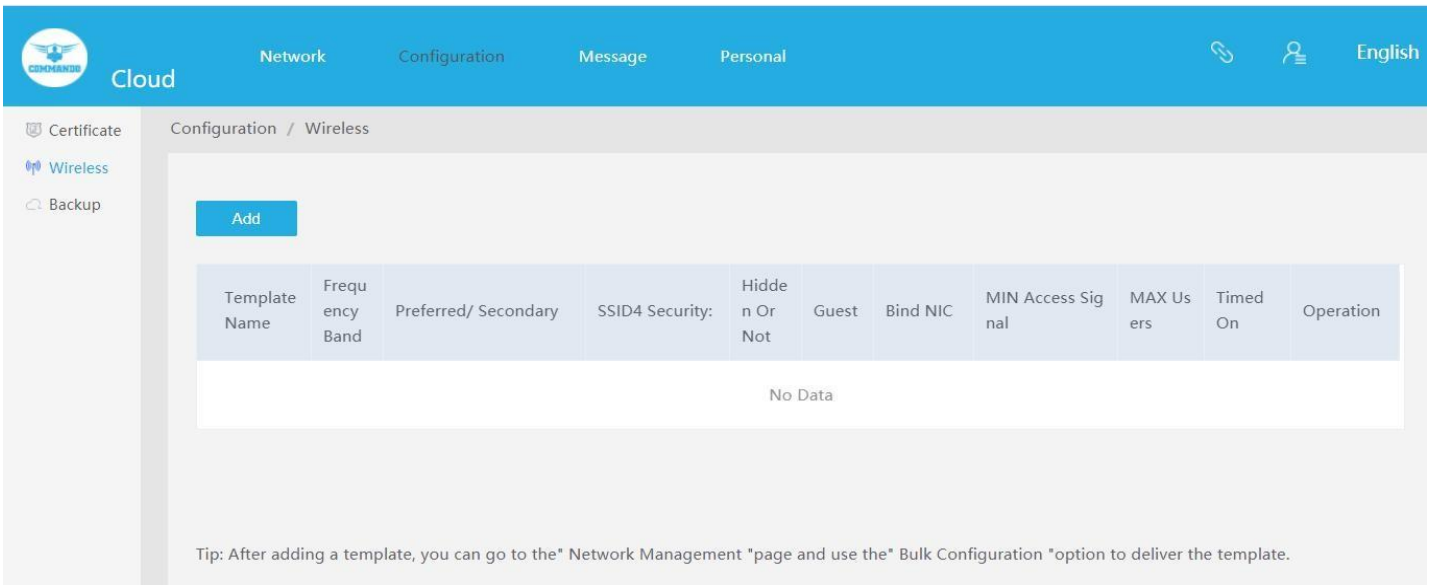


Fig 6.3.12 Default Wireless add setting page

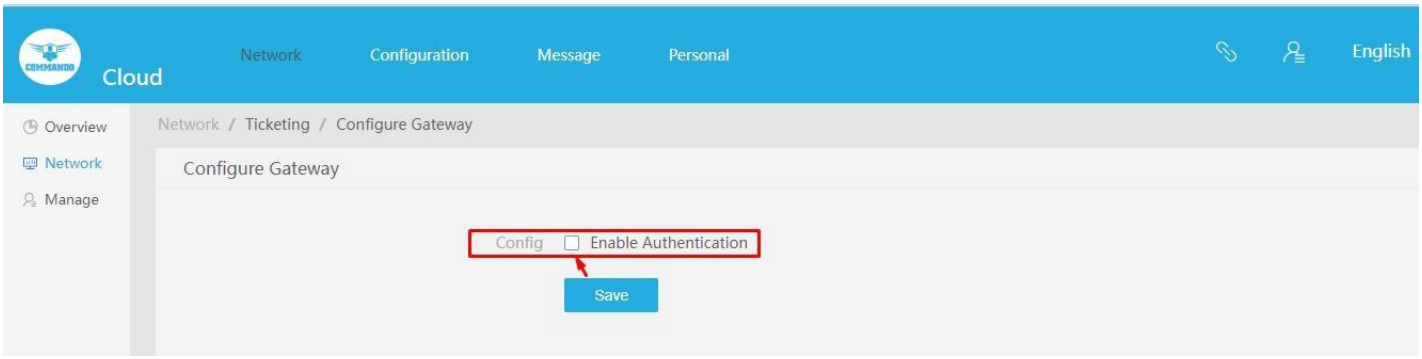


Fig 6.3.13 Default configure gateway setting page

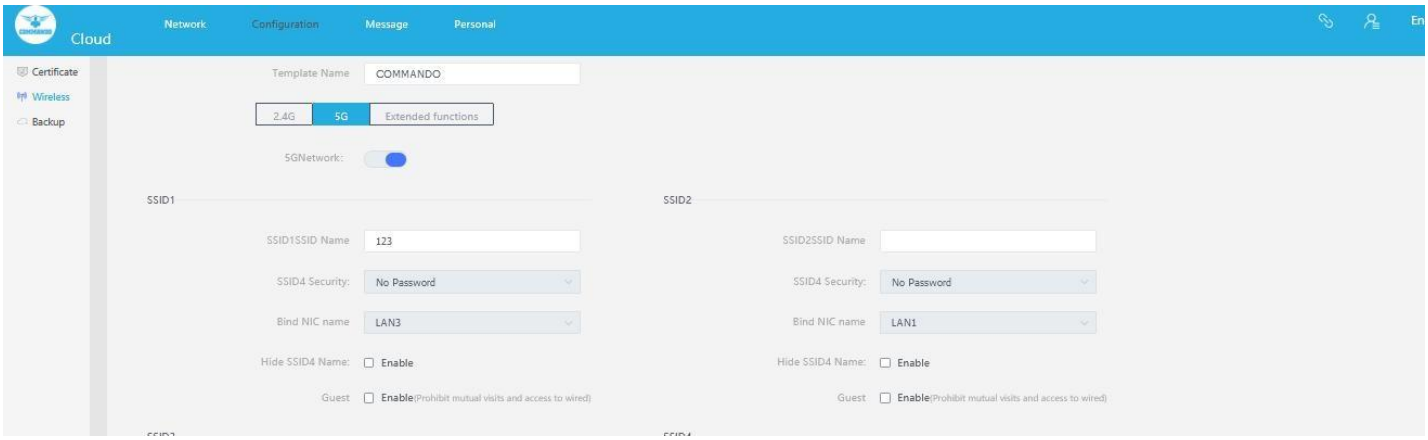


Fig 6.3.14 Default Add 5G Wireless setting page

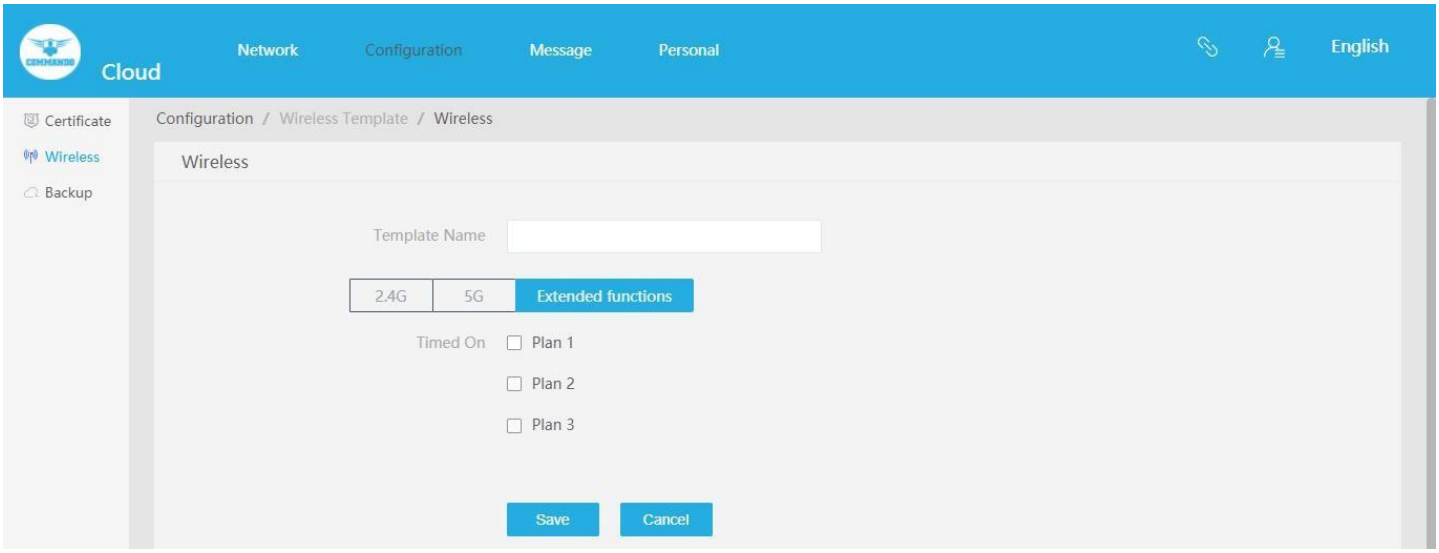


Fig 6.3.15 Default Wireless Configuration Extended function setting page

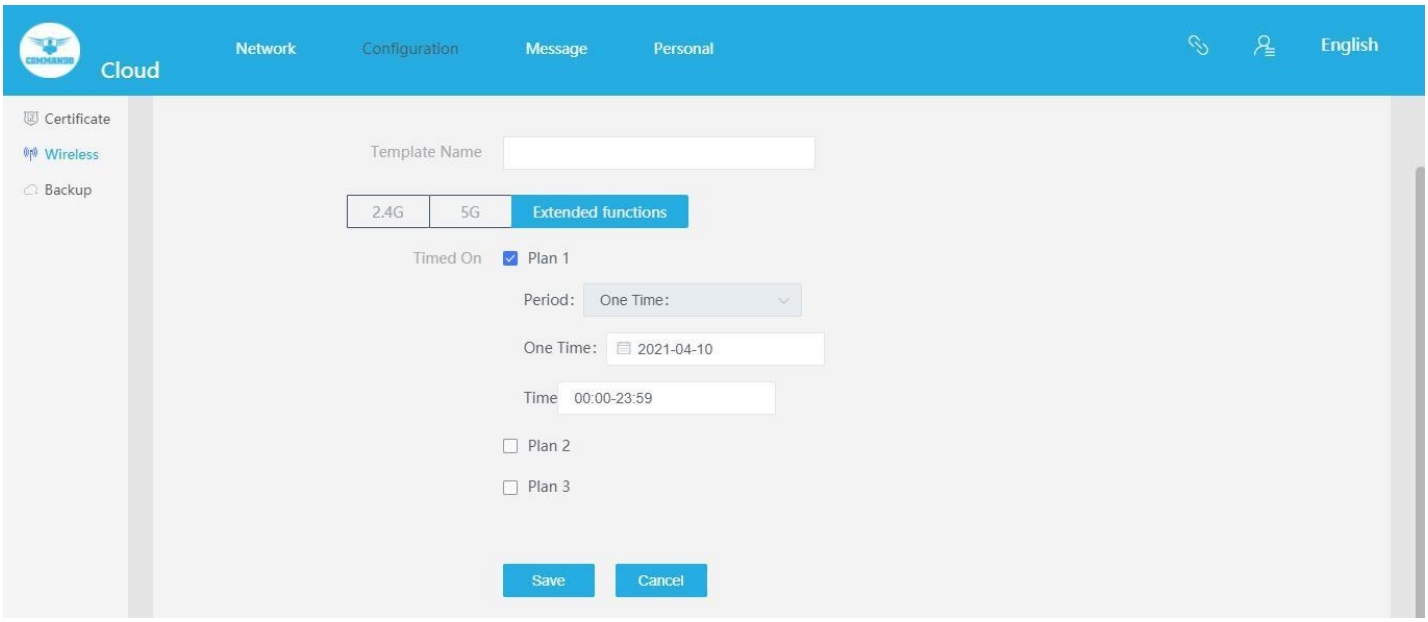


Fig 6.3.16 Default Wireless Configuration Extended function for Plan 1 setting page

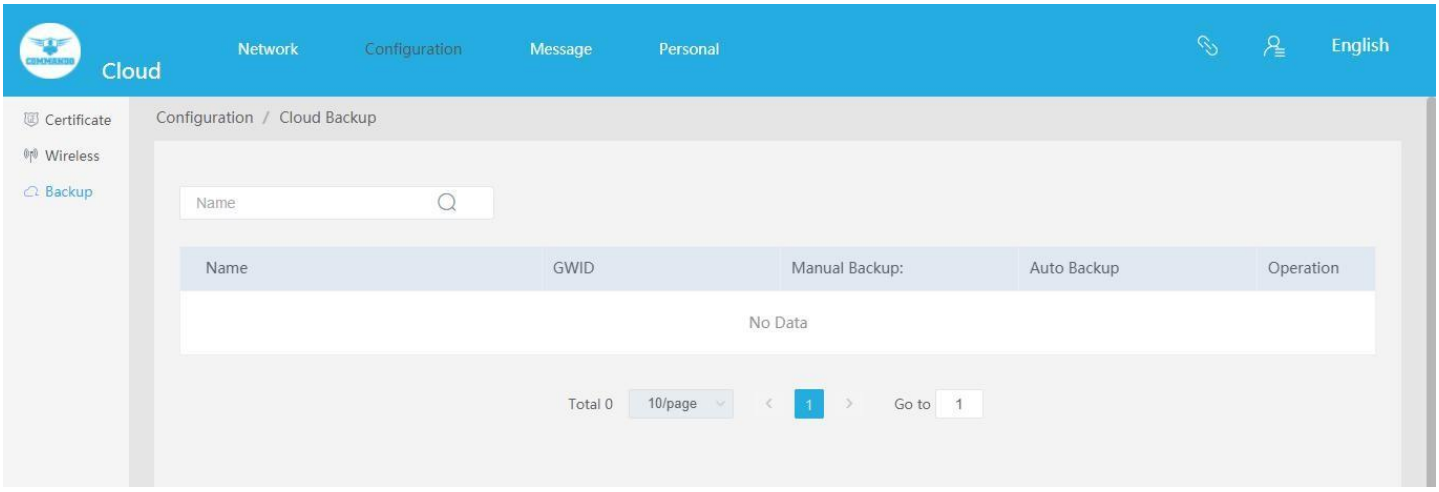


Fig 6.3.17 Default Configuration backup setting page

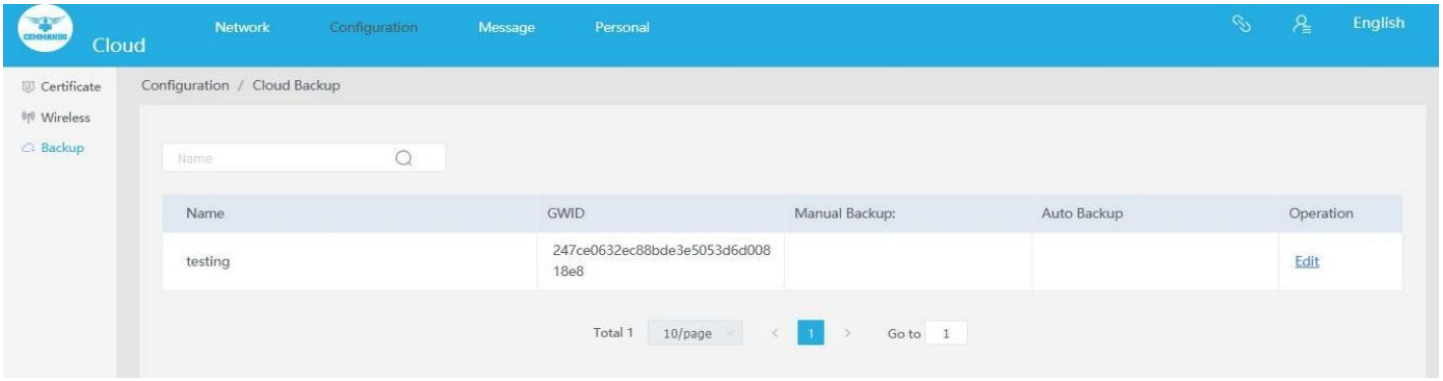


Fig 6.3.18 Default Backup Configuration setting page

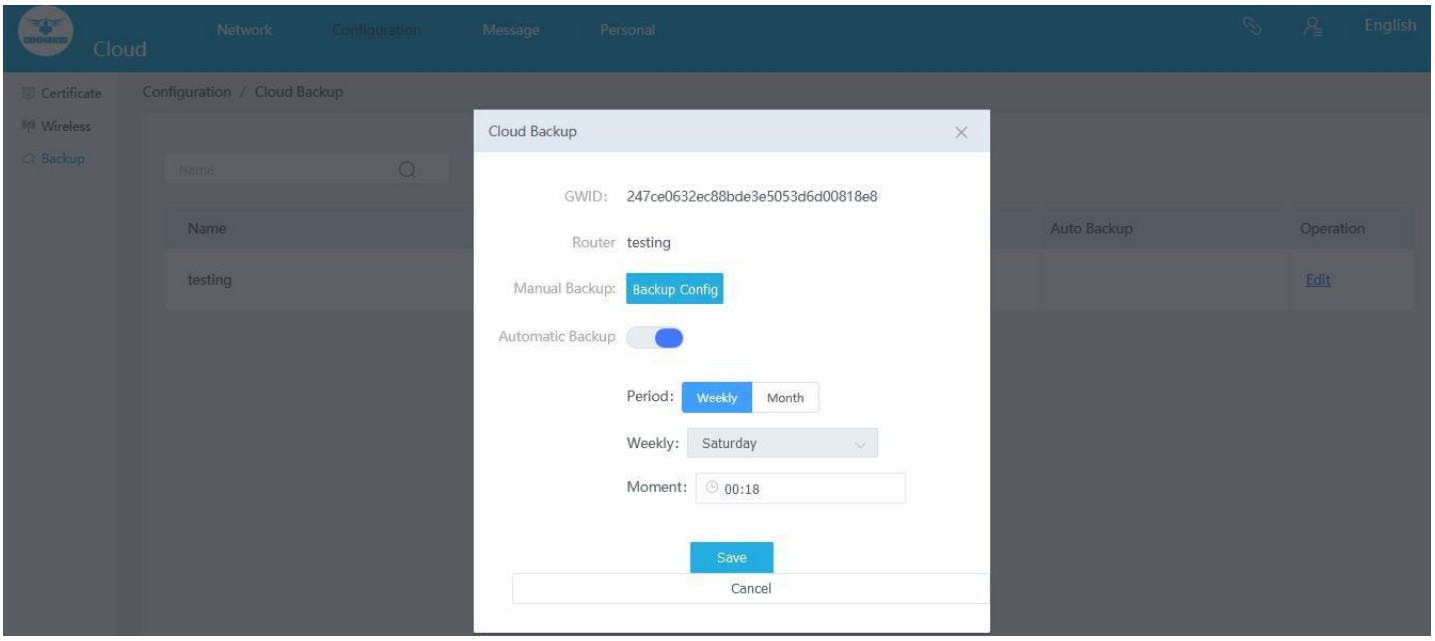


Fig 6.3.19 Default Cloud Backup Configuration setting page

6.4 Message

Messages can be Log, Login or logout, Upgrade or Restart and Configuration or Operation.

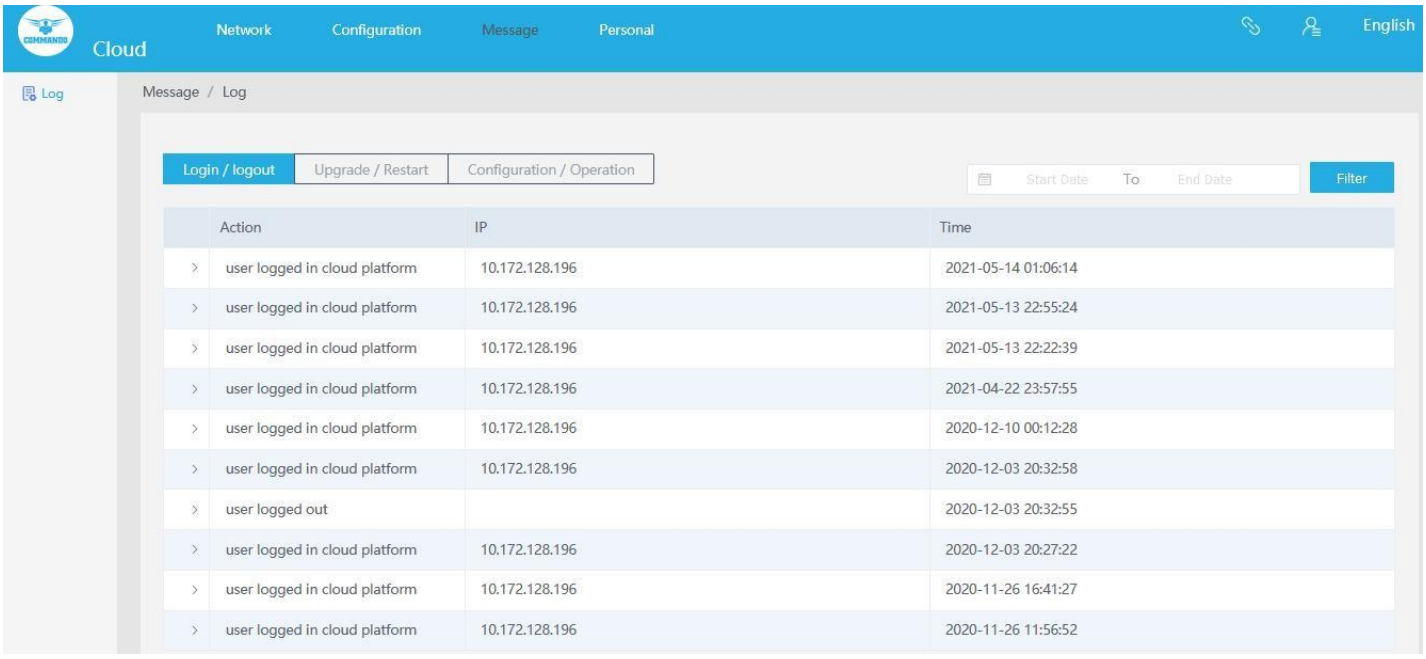


Fig 6.4.1 Default Login and Logout page

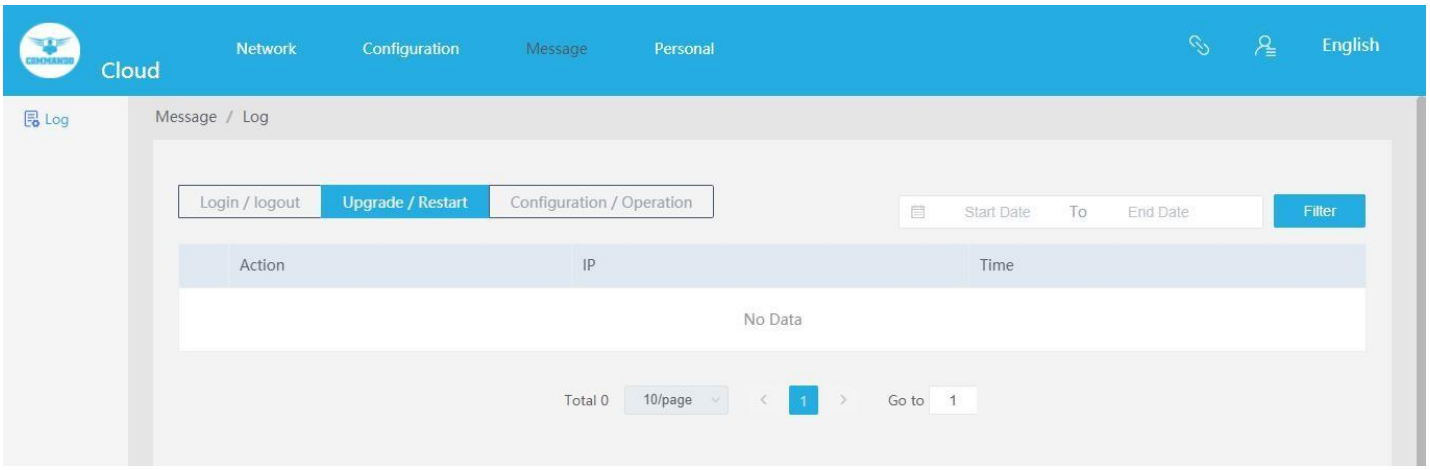


Fig 6.4.2 Default Upgrade and Restart page

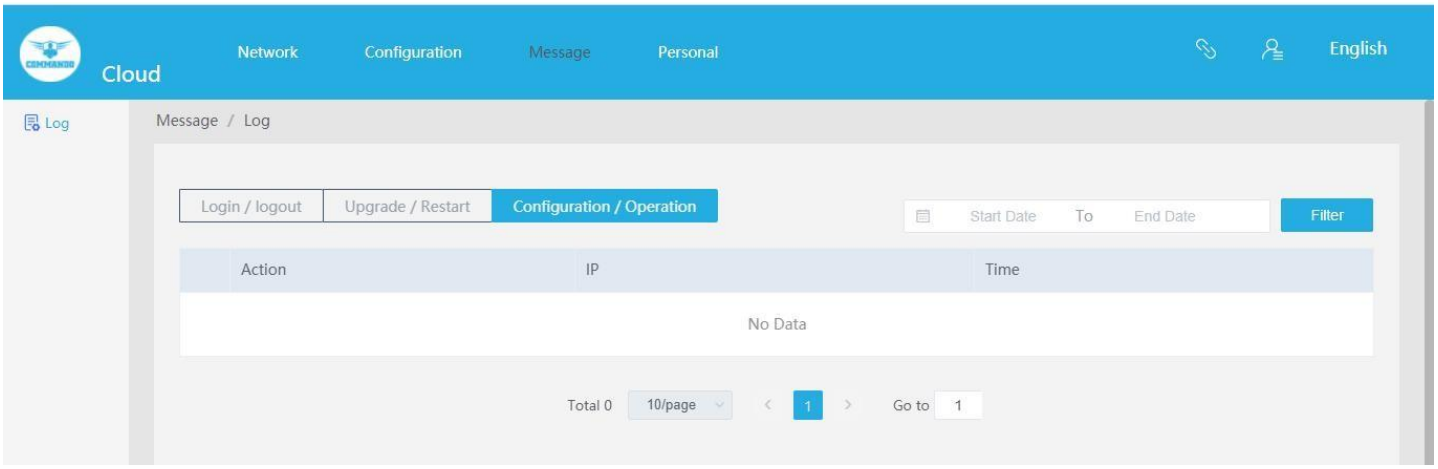


Fig 6.4.3 Default Configuration and operation page

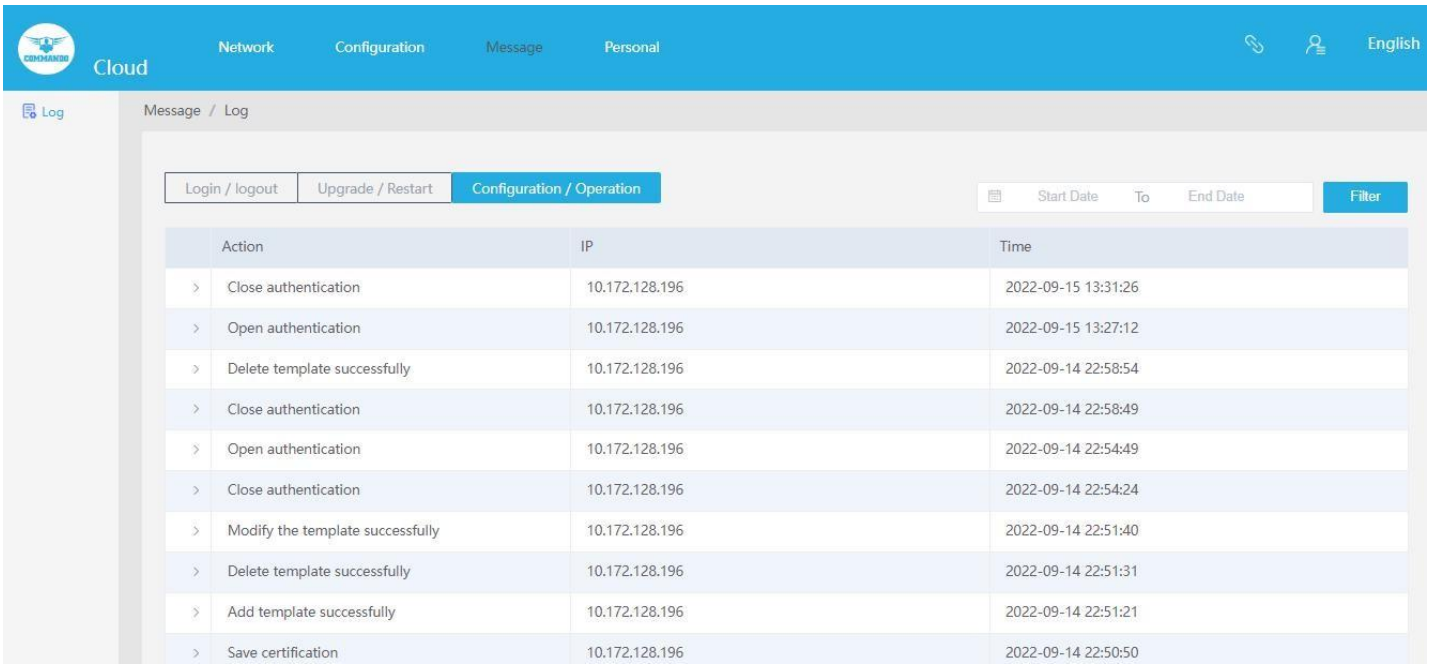
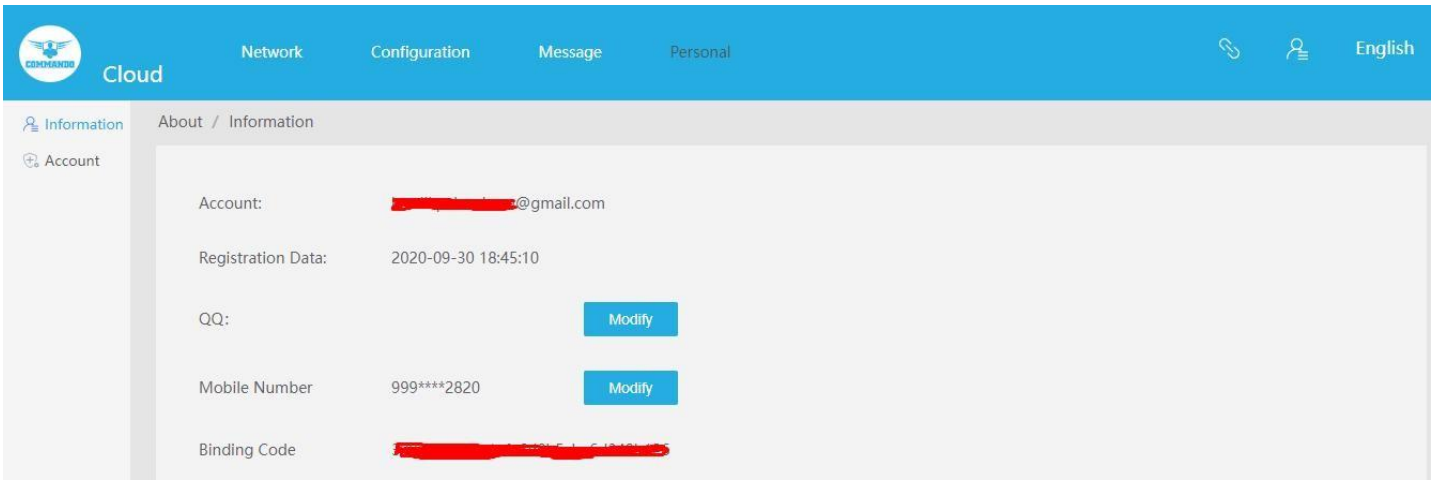


Fig 6.4.4 Configuration and operation page

6.5 Personal



Personal Information is available on this page.

Fig 6.5.1 Default Personal Information page

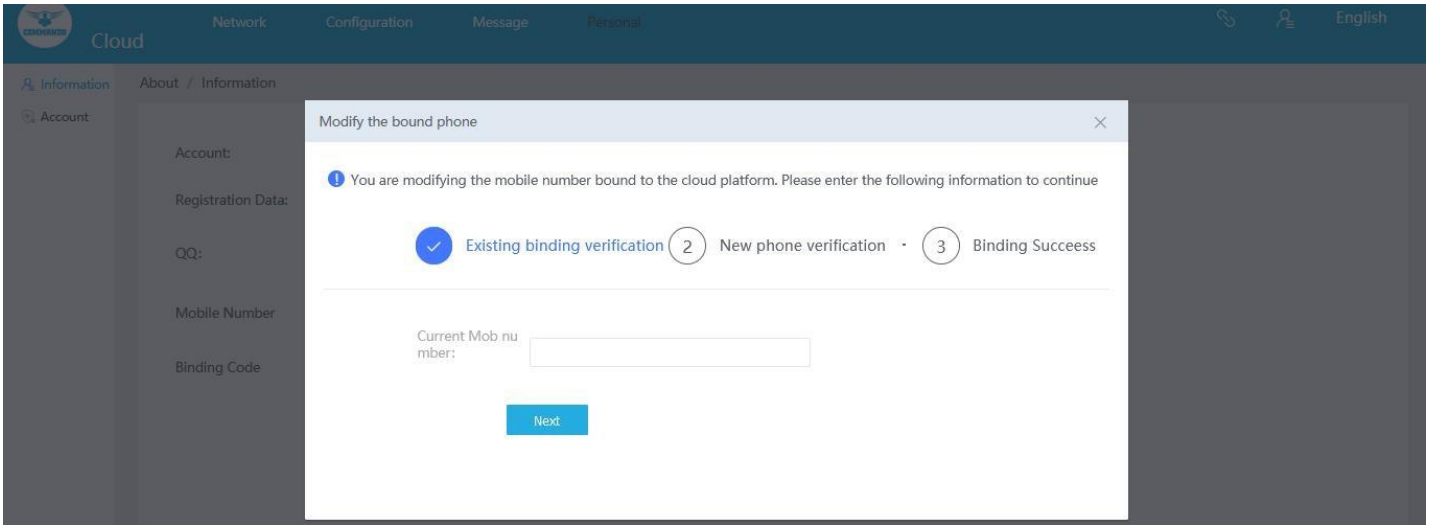


Fig 6.5.2 Modify Personal Information page

Frequently asked questions.

1. What are the differences between 802.11a/b/g/n/ac/ax/be Standards?

	HE (802.11ax) 2020	EHT (802.11be) 2024
Wi-Fi Gen. (WFA)	Wi-Fi 6E	Wi-Fi 7
Frequency	6 GHz	2.4/5/6 GHz
Channel Width	20/40/80/160 MHz	20/40/80/160/320 MHz
Spatial Streams	8	16
Data Rate	Up to 9.6 Gbps	Up to 40 Gbps
MIMO	Yes	Yes
MU-MIMO	DL & UL	DL & UL
Max Modulation	1024 QAM	4096 QAM
Subcarrier Size	78.125 kHz	78.125 kHz
Symbol Duration	12.8 µs	12.8 µs
Guard Interval	0.8, 1.6, 3.2 µs	0.8, 1.6, 3.2 µs
OFDMA	Yes	Yes

Wi-Fi 6E

- More contiguous spectrum
- Superwide channels
- Less interference
- Gigabit speeds
- Extremely low latency
- High capacity

Wi-Fi 7

- Expected launch 2024
- Coordinated multiuser MIMO
- Multilink operation
- Even wider channels
- Higher modulation
- Enhanced orthogonal frequency-division multiplexing (OFDM)

Protocol	Frequency Band	Compatibility	Theoretical Rate	Actual Rate
802.11a	5 GHz	N/A	54 Mbit/s	About 22 Mbit/s
802.11b	2.4 GHz	N/A	11 Mbit/s	About 5 Mbit/s
802.11g	2.4 GHz	Compatible with 802.11b	54 Mbit/s	About 22 Mbit/s
802.11n	2.4 GHz, 5 GHz	Compatible with 802.11a/b/g	450 Mbit/s (three spatial flows)	About 80 to 220 Mbit/s
802.11ac	5 GHz	Compatible with 802.11a/n	1300 Mbit/s	250 Mbit/s to 400 Mbit/s

2. What is category of copper cable?

The different categories denote the frequency at which the cable will pass or fail at a number of parameter tests. In theory, the higher the frequency, the more data (megabits per second/Mbps) you can transmit. The word Category is often abbreviated as Cat. The common network cables include Category 5 cable (Cat 5), Category 5 enhanced (Cat 5e), & Category 6 cable (Cat 6). These are twisted pair cables that use RJ45 connectors, with a maximum transmission distance of up to 250 meters. Network cables also include Category 1 cable (Cat 1), Category 2 cable (Cat 2), Category 3 cable (Cat 3), Category 4

cable (Cat 4), Category 6a (Cat 6a), and Category 7 cable (Cat 7). Generally, a higher category indicates a later version, more advanced technology, and higher bandwidth and cost.

Also, depending on whether the shield layer is available, network category of cable cables changes. There are two types of cables namely, Shielded twisted pair (STP) and unshielded twisted pair (UTP). STP cables can reduce radiation and prevent information from being intercepted and external electromagnetic interference from entering. Compared with the same type of UTP cables, STP cables boast higher transmission rate, but they are more expensive and more difficult to install. UTP cables feature low cost, light weight, and are easy to bend. They rarely cause great impact on common networks. UTP cables are more widely used. To practically implement a full-duplex transmission rate of up to 10 Gbps, recommended to use Category 7 with STP.

Category of cable	Transmission frequency	Distance Covered
Cat5e	Up to 100Mhz	Supports 1GE (Gigabit Ethernet/1000Mbps) up to 100m
Cat6	Up to 250Mhz	Supports 10GE up to 5-10m
Cat6a	Up to 500Mhz	Supports 10GE up to 30m
Cat7	Up to 600Mhz	Supports 10GE up to 100m
Cat7a	Up to 1000Mhz	Supports 10GE up to 250m

3. What is MIMO?

MIMO (Multiple-Input Multiple-Output) to multiply the capacity of radio links which consists of multiple trans and receive antennas to forward data at the simultaneously generates multiple spatial streams, The receiving antennas can take out the signal from different spatial paths and reconstruct the original signal which ultimately increases transfer rates of up to 600Mbps.

4. What Is Beamforming Technology?

Beamforming processes the signals sent by multiple antennas to generate a directional signal radiation pattern to boast signal from the transmitter helping to increase distance to receiver with improving in signal to noise ratio and ultimately increase signal coverage.

5. What Are Beacon Interval, RTS Threshold?

Beacon Interval is the time between beacon frames transmitted by an access point. The AP radio will transmit one beacon for each SSID it has enabled at each beacon interval.. Beacon Interval determines

the time interval of the beacon frames sent by the AP device. RTS Threshold is the packet size, in bytes, that requires the AP to check the transmitting frames to determine if an RTS/Clear to Send (CTS) handshake is required with the receiving client.

6. What are physical interfaces generally used in networks?

Physical interfaces exist on interface cards and transmit service data. Physical interfaces are classified into the following types:

LAN Interface: They are 10/100/1000 Mbps ports to exchange data with network devices on LANs. Following are common LAN interfaces used worldwide.

7. Fast Ethernet interface

A FE interface works at the data link layer, provides a maximum transmission rate of 100 Mbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

8. Gigabit Ethernet interface

A GE interface works at the data link layer, provides a maximum transmission rate of 1000 Mbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

9. 10 Gigabit Ethernet interface

A 10GE interface works at the data link layer, provides a maximum transmission rate of 10 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

10. MultiGE interface

It is an Ethernet electrical interface that can work at the rate of 1000 Mbps, 2500 Mbps, 5000 Mbps, or 10000 Mbps.

11. 40 Gigabit Ethernet interface

A 40GE interface works at the data link layer, provides a maximum transmission rate of 40 Gbps, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

Management interface: Management interfaces are used to log in to switches for configuration and management purposes.

USB interface: It is a generally data transmission interface. You can perform USB based deployment on a switch through this interface.

Mini USB interface: It is a data transmission interface as well as management interface. You can perform basic configuration and management on a switch through this interface.

Monitoring Interface: Monitoring interfaces are used to monitor a switch's components, including the cabinet door, power supply, and backup power supply.

Console interface: The console interface is connected to the COM serial interface of a configuration terminal to set up an on-site configuration environment. This interface can be connected to a network interface of a configuration terminal or network management workstation to set up an on site or remote configuration environment.

Out of band Eth interface: This interface can be connected to a network interface with RJ45 cable of a configuration terminal or network management workstation to set up an on site or remote configuration environment.

Optical Interfaces: In a fiber optic communications link, a point at which an optical signal is passed from one equipment or medium to another without conversion to an electrical signal. Depending on transmission rates, optical modules are classified into 100G, 40G, 10G, and 1G optical modules.

12. What are logical interfaces generally used in networks?

Logical interfaces do not physically exist. They are manually configured and can be used to exchange data and transmit service data.

Trunk Interface: An Trunk has Layer 2 and Layer 3 features and is formed by binding multiple Ethernet interfaces to provide more bandwidth and higher transmission reliability.

Tunnel interface: A tunnel interface has Layer 3 features, transmits packets, & identifies and processes packets transmitted over a tunnel.

VLAN interface: A VLAN interface has Layer 3 features and enables VLANs to have gateway IP.

Ethernet Sub interface: An Ethernet sub nterface is configured on a main interface to allow the local L3 device to communicate with multiple L2 devices.

Loopback interface: A loopback interface is always UP and can be configured with a 32 bit subnet mask.

NULL interface: A null interface is used to filter routes because any data packets received by the null interface are discarded

NVE interface: An NVE interface is the logical interface to establish VXLAN tunnels with other NVE devices.
VBD interface: A VBD interface is the virtual interface based on a BD to support Layer 3 features and implement communication between different BDs, between BD and non- BD networks, and between BDs and Layer 3 networks.

Virtual Ethernet (VE) interface: A VE interface is used when other data link layer protocols need to be carried by the Ethernet protocol. A VE sub interface can be created to allow an L2VPN to access to an L3VPN.

Layer 2 Interface: A L2 interface can act a switchport decides how to forward data based on the MAC address. They can only forward the received packets in Layer 2 switching mode, or join VLANs to forward the packets in Layer 3 routing mode through VLAN interfaces.

Layer 3 Interface: Layer 3 interfaces forward packets to another device using static or dynamic routing protocols. You can use Layer 3 interfaces for IP routing and inter VLAN routing of Layer 2 traffic. IP addresses can be configured for these interfaces. They can forward the received packets in Layer 3 routing mode. That is, they can send and receive the packets whose source and destination IP addresses are located in different segments.

13. What are different types of VLAN within a private VLAN?

Primary VLAN: It can forwards the traffic from the promiscuous ports to isolated ports, community ports and other promiscuous ports in the same private VLAN.
Community VLAN: It is a secondary VLAN. It forwards traffic between ports which belong to the same community and to the promiscuous ports. There can be multiple community VLANs per private VLAN.
Isolated VLAN: It is a secondary VLAN. It carries traffic from isolated ports to promiscuous ports.

14. What is ARP & how it works?

The basic purpose of the Address Resolution Protocol (ARP) is to resolve IP addresses to Ethernet mac addresses. It is the method by which any node or interface on a LAN can dynamically learn the MAC address of another IP host or router on the same LAN. The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

ARP Request, is a message that makes the simple request "if this is your IP address, please reply with your MAC address." ARP also defines the ARP Reply message, which indeed lists both the original IP address and the matching MAC address. It is used to dynamically map layer-3 network addresses to data-link addresses. The ARP cache is vulnerable to ARP cache poisoning and ARP spoofing attacks. ARP table for all devices connected to it. The ARP table to obtain the MAC address of the device. The ARP table contains both static and dynamic addresses. Static addresses are manually configured and do not age out. The device creates dynamic addresses from the ARP packets it receives.

15. How DHCP Server works?

DHCP Server is used to dynamically assign IP addresses, default gateway and other parameters to DHCP clients. DHCP (dynamic host configuration protocol) allows a server to assign an IP address to a computer from a preselected range of numbers configured for a particular network. Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring IP address, gateways and other IP related things automatically to connected hosts. DHCP Host/client generally require four IPv4 settings namely IP address, Subnet mask, Default Gateway IP and optional DNS server IP addresses. You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. DHCP allows both the permanent assignment of host addresses, but more commonly, DHCP assigns a temporary lease of IP addresses. With these leases, the DHCP server can reclaim IP addresses when a device is removed from the network, making better use of the available addresses. DHCP also enables mobility by mac to IP binding.

GLOSSARY

ACL: Access Control List can limit network traffic and restrict access to certain users, ports or mac by by allowing and disallowing based on L2/L3/L4 information.

ALG: Application Level Gateway (ALG) is application specific translation agent that allows an application on a host in one address domain to connect to its receiver port running on a host in different address domain. It allows client applications to use dynamic TCP/UDP ports to communicate with known ports used by server applications.

AH: Authentication Header provides data origin authentication, data integrity, and replay protection. However, AH does not provide data confidentiality.

ARP: Address Resolution Protocol used to map an IP address to a MAC address in short converts between IP addresses and MAC addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP: Boot Protocol is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CFM: Connectivity Fault Management provides fault monitoring for end-to-end connections within a designated service area by using continuity check messages which can detect faults in maintenance points, fault verification through loop back messages, and fault isolation with link trace messages.

COS: Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DDNS: DDNS (Dynamic Domain Name Server) is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DDNS

configuration of its configured hostnames, addresses capability of assigning a fixed host and domain name to a dynamic Internet IP address.

DHCP: Dynamic Host Control Protocol provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP SNOOPING: It is used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

DIFFSERV: Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

DNS: Domain Name Service used for translating host names for network nodes into IP addresses.

DMZ: DMZ(Demilitarized Zone) allows local hosts exposed to the Internet (untrusted Networks) additional protection and adds an extra layer of security to an organization's internal local-area network from untrusted traffic. The main goal of a DMZ is to allow an organization to access untrusted networks, such as the internet, while ensuring its private network or LAN remains secure.

DSCP: Differentiated Services Code Point Service uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and

then into the output queues.

DSL: Digital Subscriber Line that allows data to be sent or received over existing traditional phone lines that uses existing telephone lines to transport high-bandwidth data, Voice and video, to service subscribers. DSL provides dedicated, point-to-point, public network access.

EAPOL: Extensible Authentication Protocol over LAN is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

ERPS: Ethernet Ring Protection Switching can be used to increase the availability and robustness of Ethernet rings, such as those used in Metropolitan Area Networks (MAN). ERPS provides Layer 2 loop avoidance and fast reconvergence in Layer 2 ring topologies, supporting up to 255 nodes in the ring structure. It can also function with IEEE 802.1ag to support link monitoring when non-participating devices exist within the Ethernet ring.

ESP: Encapsulating Security Payload provides data privacy services, optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

EUI: Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.

FTP: File Transfer Protocol is a application layer protocol, is a way to download, upload, and transfer

files on the internet or privet networks between computer systems. It allows transfer of files back and forth between VPN's, cloud or public networks. .

GARP: Generic Attribute Registration Protocol is a protocol that can be used by end stations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered end stations.

GMRP: Generic Multicast Registration Protocol allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

GMT: Greenwich Mean Time also World Time, UTC nominally reflects the mean solar time along the Earth's prime meridian. Network Time Protocol (NTP) is a protocol that allows the synchronization of system clocks which is very convenient for log and troubleshooting purpose for events in networks.

GVRP: GARP VLAN Registration Protocol is a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

H.323: H.323 allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. It defines a common set of CODECs, call setup, negotiating procedures, and basic data transport methods.

HTTP: Hypertext Transfer Protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

ICMP: Internet Control Message Protocol is a network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feedback information about better routing choices.

IEEE 802.1D: Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q: VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1P: An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1S: An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1W: An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard now incorporated in IEEE 802.1D-2004.

IEEE 802.1X: Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3AC: Defines frame extensions for VLAN tagging.

IEEE 802.3X: Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

IGMP: Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.

IGMP QUERY: On each subnetwork, one IGMP-capable device will act as the querier that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP PROXY: Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in an simple tree that uses IGMP Proxy.

IGMP SNOOPING: Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IN-BAND MANAGEMENT: Management of the network from a station attached directly to the network.

Internet: INTERNET stands for Interconnected Network systems that connects millions of web servers which provides a variety of information and communication facilities with standardized communication protocols.

IP MULTICAST FILTERING: A process whereby this switch can pass multicast traffic along to participating hosts.

IP PRECEDENCE: The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

ISP: Internet Service Provider provides individuals or organizations access to the internet and other telecom related services. An ISP has the equipments to have a point of presence on the internet for the geographic area served.

LACP: Link Aggregation Control Protocol allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

LAYER 2: Data Link layer in the ISO OSI 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC

addresses.

LAN: Local Area Network is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

LINK AGGREGATION: Link aggregation increases bandwidth, provides graceful degradation as failure occurs, and increases availability. It provides network redundancy by load-balancing traffic across all available trunk links.

LLDP: Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

MAC address: Media Access Control address is a hardware identifier that uniquely identifies each device on a network.

MD5: Message-Digest 5 is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB: Management Information Base is an acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MSTP: Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

MRD: Multicast Router Discovery is used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled

devices to determine where to send multicast source and group membership messages.

Multicast Switching: A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

MVR: Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as such as television channels or video-on- demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard or private VLAN groups.

MTU: Maximum Transmission Unit is the largest size frame or packet. MTU is the largest packet or frame size, specified in octets, Standard Ethernet supports an MTU of 1500 bytes and Ethernet implementation supporting jumbo frames, allow for an MTU up to 10000 bytes.

NAT: Network Address Translator conserves IP addresses that are legally registered and prevents their depletion and provides security to access the internet with privacy by hiding the device IP address from the public network, even when sending and receiving traffic. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.

NTP: Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical master slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio. NTP Server NTP Server is used for synchronize the time across computer networks.

OAM: Operation, Administration, and Maintenance provides remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment). This section describes functions including enabling OAM for selected ports, loopback testing, and displaying remote device information.

OSPF: Open Shortest Path First (OSPF) is an open link state routing protocol. OSPF routers learn the entire network topology for their “area” (the portion of the network they maintain routes for, usually the entire network for small networks). OSPF routers send event driven updates. If a network is converged for a week, the OSPF routers will send no updates. OSPF has far faster convergence than distance vector protocols such as RIP.

OUT-OF-BAND Management: The device can be accessed from a station not attached to the network.

PORT MIRRORING: A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be monitored.

PORT TRUNK: Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower speed physical links.

PRIVATE VLANS: Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

QINQ QinQ tunneling: It is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs.
QOS: Quality of Service refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS: Remote Authentication Dial-in User Service is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RIP: Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a

distance vector routing protocol that has an AD value of 120 uses port number 520.

RMON: Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

RSTP: Rapid Spanning Tree Protocol reduces the convergence time for network topology changes.

SMTP: Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

SNMP: Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

SNTP: Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

SSH: Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

STA: Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance & efficiency of the network.

TACACS+: Terminal Access Controller Access Control System Plus is a logon authentication protocol that uses software running on a central server to control access to TACACS compliant devices on the network.

TCP/IP: Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the

primary transport protocol, and IP as the network layer protocol.

TELNET: It is a remote communication facility for interfacing to a terminal device over TCP/IP.

TFTP: Trivial File Transfer Protocol used for software/firmware downloads.

UDP: User Datagram Protocol provides a datagram mode for packet switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC: Universal Time Coordinate is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN: Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XMODEM: A protocol used to transfer files between devices. Data is grouped in 128- byte blocks and error-corrected.