InHand Networks Enterprise AP

EAP600 Series Product User Manual

Version：V1.1-2023.10

InHand Networks
Global Leader in Industrial IoT
www.inhandnetworks.com

Declarations

Thank you for choosing our company's product! Before use, please carefully read this user manual. By complying with the following statements, you will help maintain intellectual property rights and legal compliance, ensuring that your user experience aligns with the latest product information. If you have any questions or need written permission, please feel free to contact our technical support team.

- Copyright Statement

This user manual contains copyrighted content, and the copyright belongs to InHand Networks Technology and its licensors. Without written permission, no organization or individual may excerpt, copy any part of the content of this manual, or distribute it in any form.

- Disclaimer

Due to ongoing updates in product technology and specifications, the company cannot guarantee that the information in the user manual is entirely consistent with the actual product. Therefore, no disputes arising from any discrepancies between the actual technical parameters and the user manual are accepted. Any changes to the product will not be notified in advance, and the company reserves the right to make the final changes and interpretations.

- Copyright Information

The content of this user manual is protected by copyright laws, and the copyright belongs to InHand Networks and its licensors, reserving all rights. Without written permission, the content of this manual may not be used, copied, or distributed without authorization.

Conventions

Symbol	Indication
[ ]	Referring to function modules or menus, such as in the [Status] menu."
“ ”	Referring to a button name, such as Clicking the “Add” button.
〉	Multiple levels of menus are separated by " 〉". For example, "File 〉New 〉Folder" represents the "Folder" menu item under the "New" submenu, which is under the "File" menu.
Cautions	Please be mindful of the following points during the operation, as improper actions may result in data loss or device damage.
Note	Supplement and provide necessary explanations for the description of the operation.

Technical Support

E-mail：support@inhandnetworks.com

URL: www.inhandnetworks.com

CONTENT

1. Overview 1
2. Hardware 2
    2.1 LED Indicators 2
    2.2 Perform a factory reset using the Reset button. 3
3. Default Settings 4
4. Device Initialization Settings 5
    4.1 Environment Setup 5
    4.2 Internet Connection 5
5. Function Configuration 7
    5.1 Dashboard 7
        5.1.1 Device Information 7
        5.1.2 Traffic Statistics 8
        5.1.3 Wi-Fi Connections 8
    5.2 Status 9
        5.2.1 Link Monitoring 9
        5.2.2 Clients 9
        5.2.3 Events 10
        5.2.4 Logs 11
    5.3 Configuration 12
        5.3.1 WAN 12
        5.3.2 LAN 13
        5.3.3 Radio 13
    5.4 Wi-Fi 15
    5.5 System 16
        5.5.1 adm Management 16
        5.5.2 Cloud Management 16
        5.5.3 Remote Access Control 17
        5.5.4 Country & System Clock 18
        5.5.5 Device Option 18
        5.5.6 Configuration Management 19

5.5.7 Device Alarms 20
5.5.8 Tools 21
5.5.9 Scheduled Reboot 23
5.5.10 System Settings 23
5.5.11 Log Server 24
5.5.12 Other Settings 24
6. Security Precautions 26
7. Troubleshooting 27
7.1 Clients Cannot Connect to the Wireless Network 27
7.2 Wireless network is slow or experiencing instability 27
7.3 AP Cannot Start Properly or Frequent Crashes 28
7.4 Unable to Connect to a Specific Website or Service. 28
7.5 Unable to access the Incloud Manager 28
8. Hardware Specification 29

1. Overview

The EAP600, developed by InHand Networks, is a Wi-Fi 6 Access Point designed for the commercial sector. This product delivers secure and high-speed network access, catering to a wide range of industries. Harnessing the robust network access capabilities of Wi-Fi 6, it provides a straightforward and efficient solution for small businesses, enterprise branches, hotels, and any other settings requiring wireless coverage with high-speed network access. With a comprehensive set of security features and intelligent software services, it ensures an efficient and worry-free networking experience, delivering a secure and dependable business data connection in wireless environments.

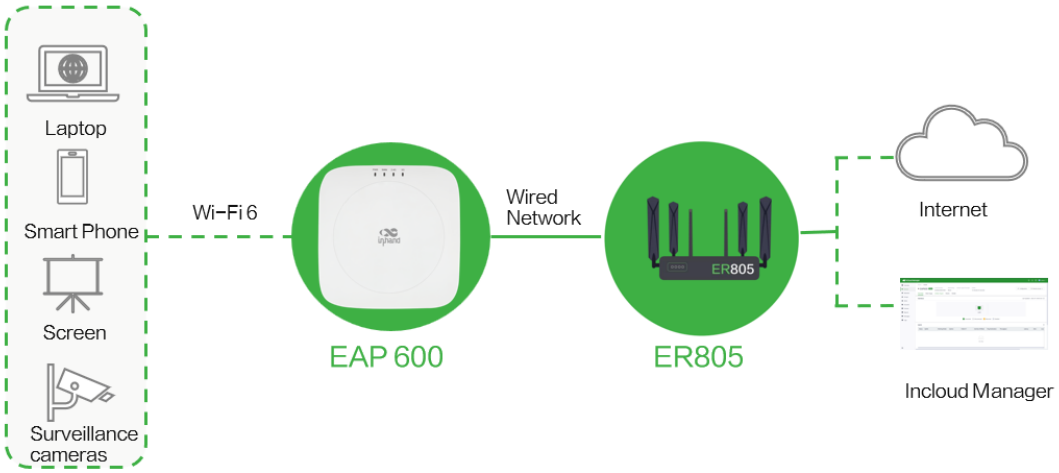

Fig. 1 EAP600 application scenario

2. Hardware

2.1 LED Indicators

LED Indicator	Status and Description
PWR	OFF --- The device is Off. Blink in green --- The system is starting. Blink in green rapidly --- The system does not work properly. Blink in green --- The system is upgrading.
WAN	OFF --- The network is disconnected. Blink in green --- The router is connecting to the wired network.
Wi-Fi 2.4G	OFF --- AP mode disabled. Always on --- Other anomalies. Blink in rapidly green --- The device functions normally as an AP.
Wi-Fi 5G	OFF --- AP mode disabled. Always on --- Other anomalies Blink in green rapidly --- The device functions normally as an AP.

Note: The rapid blinking occurs every 200ms, and the steady blinking interval is 500ms.

2.2 Perform a factory reset using the Reset button.

Step 1: Power on the device, and within 10 seconds, long-press the Reset button until the PWR indicator light rapidly blinks green with a 200ms interval.

Step 2: After the rapid blinking, release the Reset button and wait for the device to complete the factory reset process. The PWR indicator light will stay constantly lit, indicating that the factory reset is complete.

3. Default Settings

Function	Default Settings
Wi-Fi	1. The Wi-Fi 2.4 GHz access point (AP) is enabled, and its SSID is EAP600– followed by the last six digits of the wireless MAC address. 2. The Wi-Fi 5 GHz AP is enabled, and its SSID is EAP600-5G– followed by the last six digits of the wireless MAC address. 3. The authentication method is WPA2-PSK. 4. The two access points have the same password: The last eight digits of the router's SN.
Network access control	1. Local HTTPS service is enabled, using port 443. 2. The device management address is 192.168.10.1
Username and password	The username is **adm**, and the password is **123456** by default.

4. Device Initialization Settings

4.1 Environment Setup

Step 1: Connect the power cable and Ethernet cable. When using PoE (Power over Ethernet) to power the EAP600, please ensure that the upstream device has PoE functionality enabled.

Step 2: Set the PC and device management IP addresses in the same network segment. The DHCP Server function is enabled by default, and the PC and device must be in the same address segment. The PC needs to be connected to the device's Wi-Fi (SSID and password reference 3. Default Settings), and check whether the PC has obtained an address, which should belong to the 192.168.10.0 network segment.

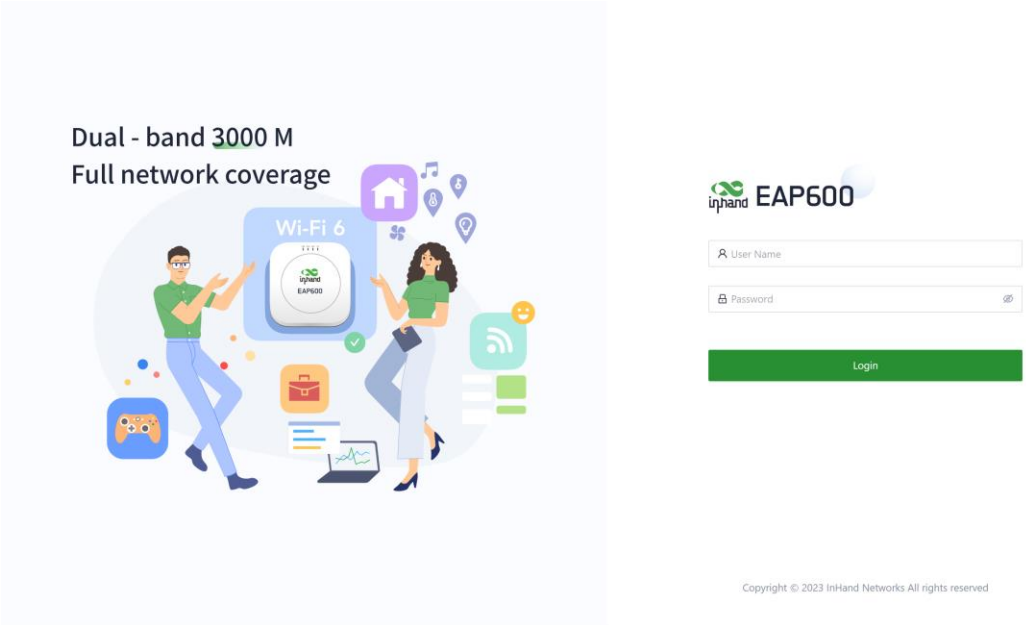

Fig. 4-1 EAP600 Web Login page

4.2 Internet Connection

The EAP600 supports single-port wired access, and users can configure it to use DHCP or static IP address assignment based on their requirements. Click on "Configuration > WAN" to select the network connection type.

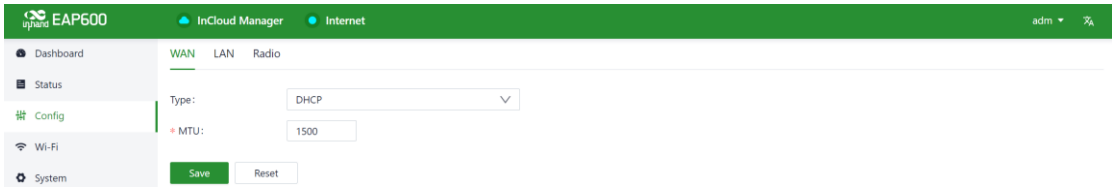

Fig. 4-2-a Access the WAN editing interface

- DHCP: The device's WAN interface is set to enable DHCP service by default. You can simply connect the WAN interface to the internet using an Ethernet cable to establish the AP's network connection.

- Static IP: Users can manually configure the address assigned by the ISP or upstream device. After the configuration is completed, the AP will connect to the network using the specified static IP.

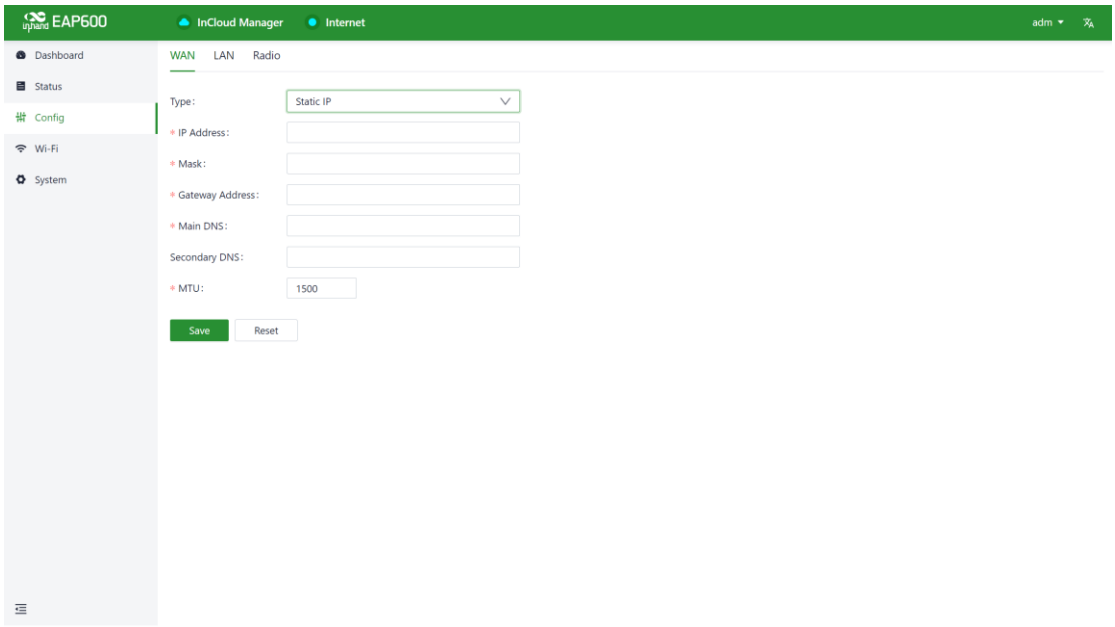

Fig. 4-2-b Configuring the AP to connect to the network via a static IP address

5. Function Configuration

5.1 Dashboard

Click on [Dashboard] in the left-hand menu to access the dashboard interface and view the device's basic information, operating mode, traffic statistics, Wi-Fi connection count, and other information.

Users can click the icon next to the "Name" field to customize the name of this device.

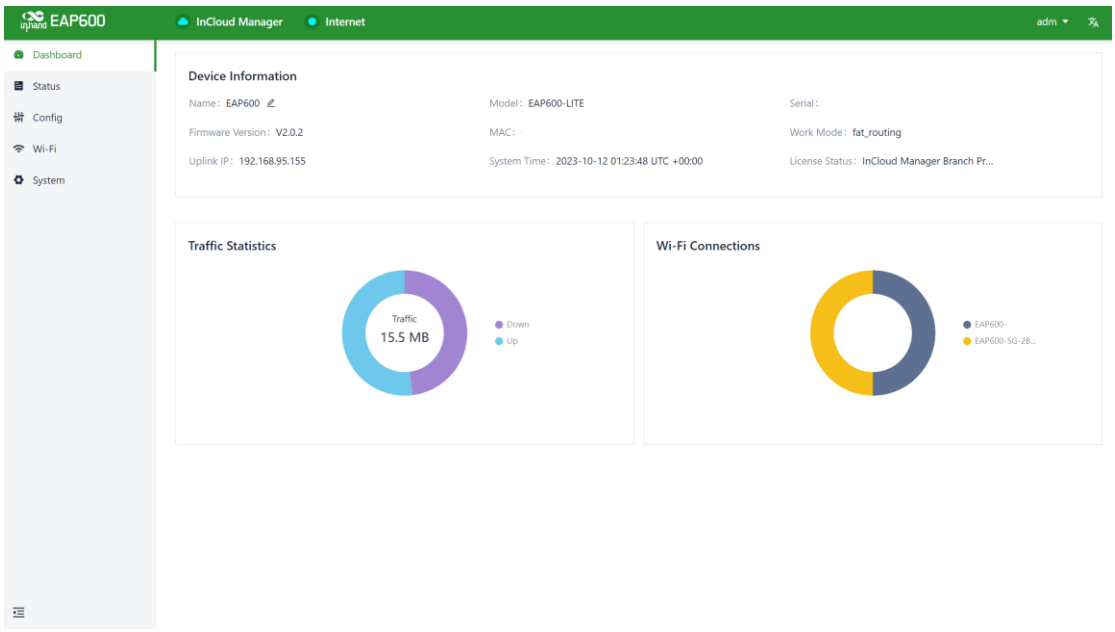

Fig. 5-1 Dashboard interface

5.1.1 Device Information

Users can view basic device information in the "Dashboard > Device Info" interface, including the device name, device model, device serial number, MAC address, online duration, upstream interface address, and other details.

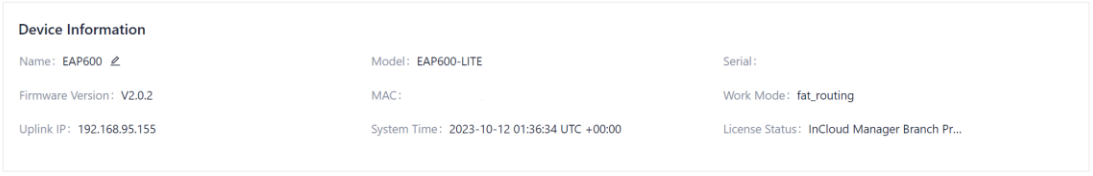

Fig. 5-1-1 Device Information interface

5.1.2 Traffic Statistics

Users can check the usage of traffic on various upstream interfaces since EAP600 was powered on through the "Dashboard > Traffic Statistics" feature. The data for traffic statistics will reset after the device is restarted. If you need to view historical traffic records, you can do so on the corresponding device's details page in the InHand Cloud Manager.

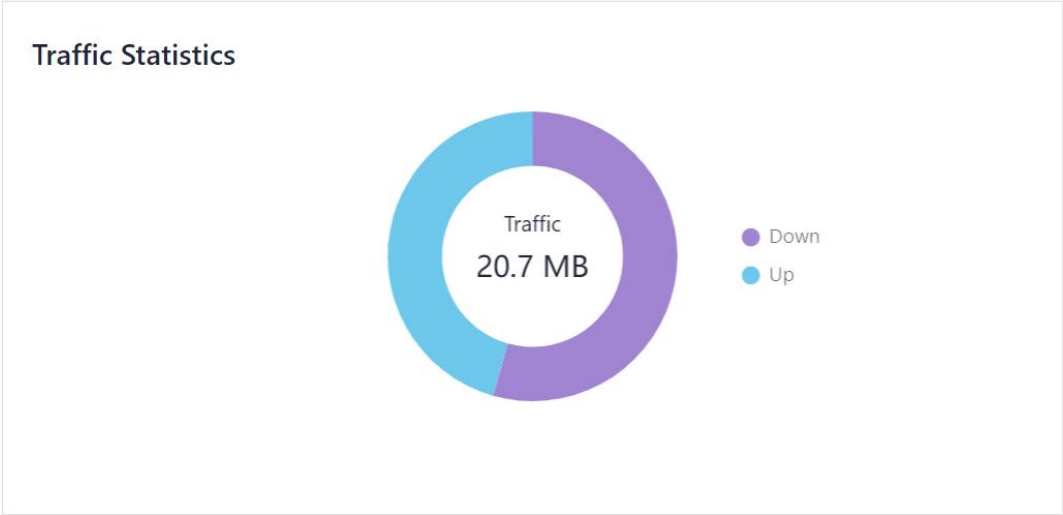

Fig. 5-1-2 Traffic statistics

5.1.3 Wi-Fi Connections

Users can view the number of active SSIDs and the client count for each SSID that is connected to the EAP600 through the "Dashboard > Wi-Fi Connections" feature.

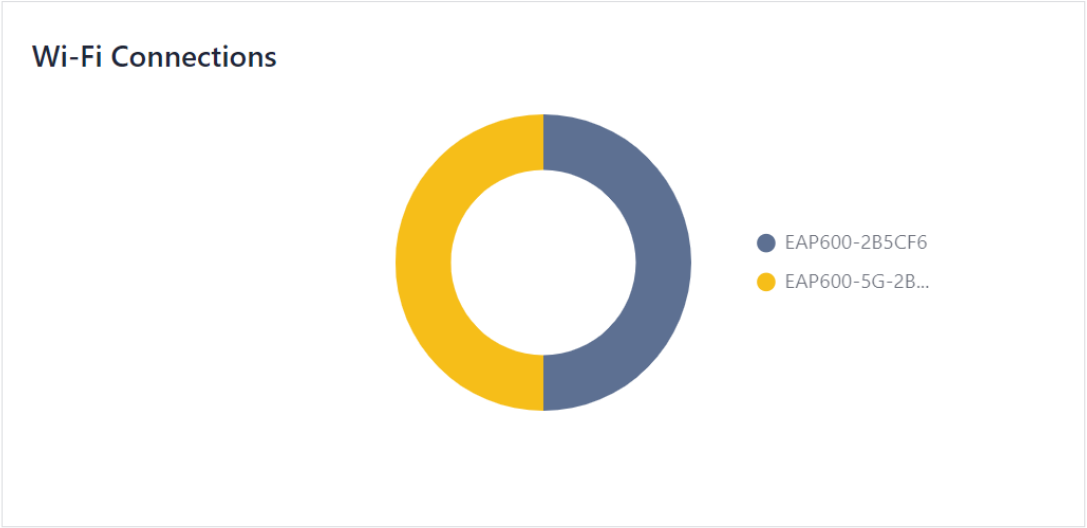

Fig. 5-1-3 view the Wi-Fi connection status

5.2 Status

Click on the [Status] option in the left menu to enter the status page, where you can check the device's link status, clients, events, logs, and other information.

5.2.1 Link Monitoring

Link monitoring is used to track and evaluate the real-time performance, availability, and stability of network connections. Users can use the "Status > Link Monitoring" function to view the health status of upstream links and information such as throughput, latency, and packet loss for each interface.

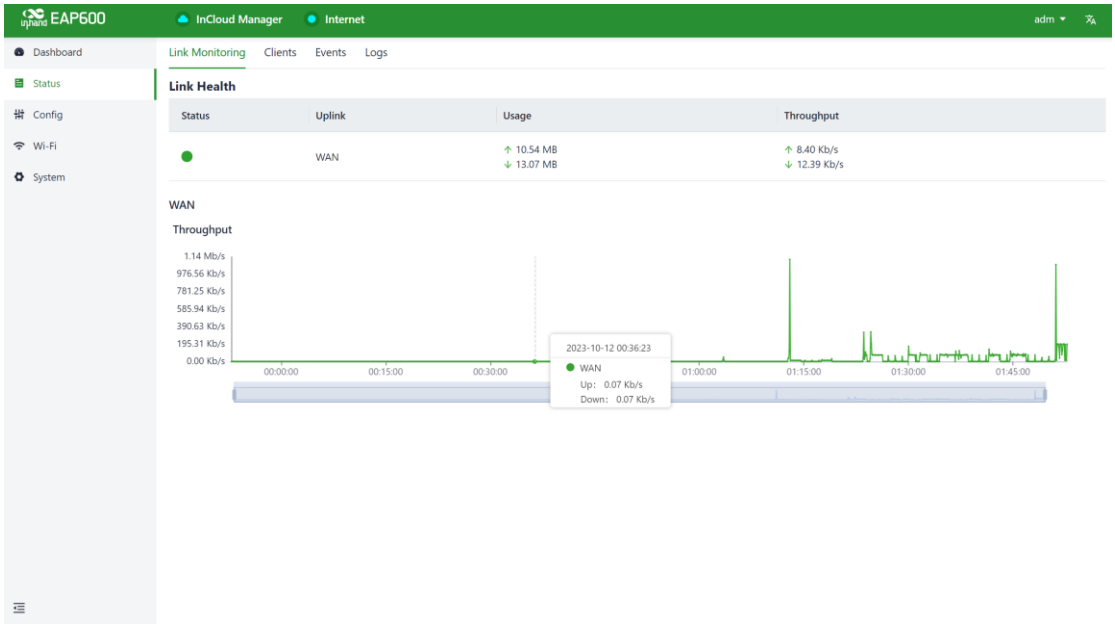

Fig. 5-2-1 Link Monitor Data

5.2.2 Clients

Clients typically refer to wireless devices connected to an access point (AP), such as laptops, smartphones, tablets, and other similar devices.

Users can access detailed client information connected to the EAP600 via the "Status > Clients" feature. This information includes client names, IP addresses, MAC addresses, VLAN, connected SSID, RSSI, operating channels, Wi-Fi standards, traffic usage, online duration, and more.

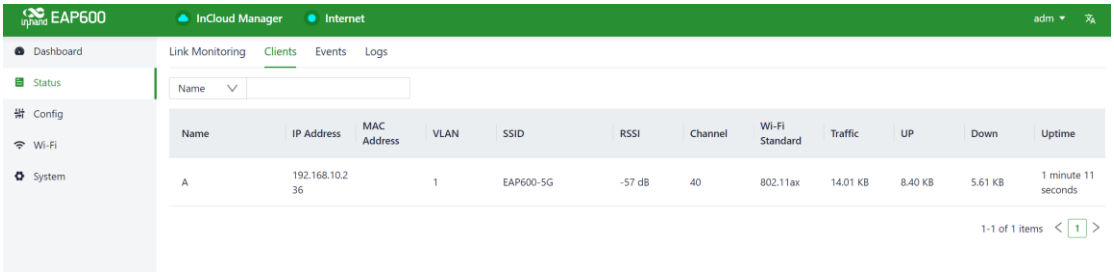

Fig. 5-2-2 Wireless Client Connection Information

5.2.3 Events

[Event] is used to record information related to the device's status, performance, and user-triggered operations. This helps IT personnel understand the network's operational status, detect problems promptly, and take necessary measures. It is a valuable tool for network monitoring and troubleshooting.

Users can access event information generated during the device's operation via the "Status > Events" function. This helps users understand the device's operational status and can be useful for troubleshooting issues. New events will be updated at the beginning of the table.

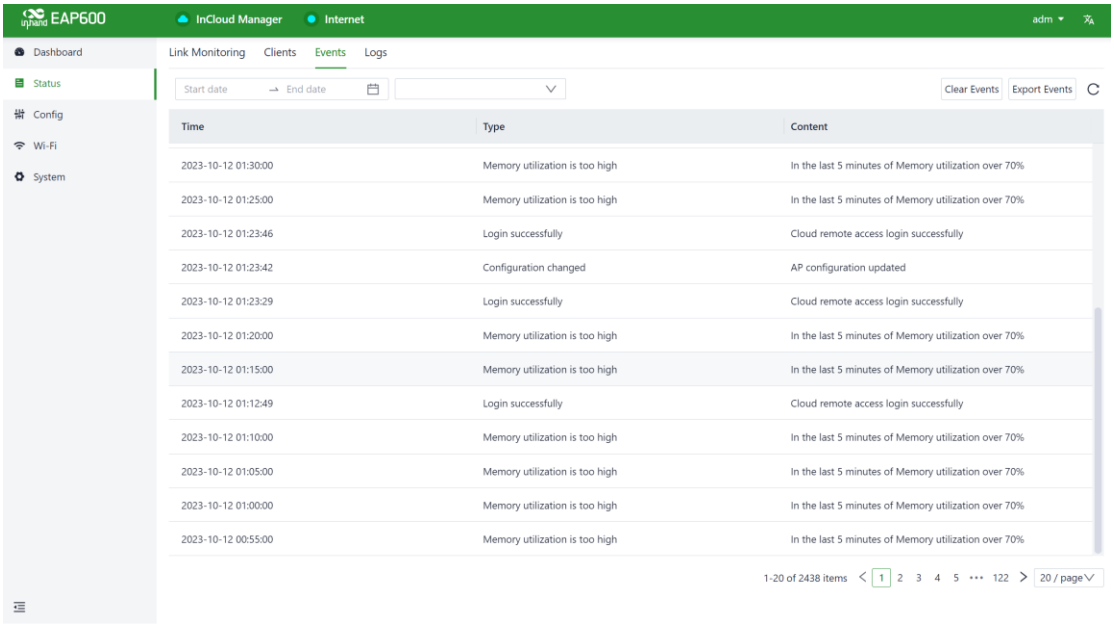

Fig. 5-2-3 Check the recorded events

At the top of the event list, you can filter the displayed content by setting the time and selecting the event level. You can also export or clear recorded events using the "Clear Events" and "Export Events" buttons. In addition, you can set the number of events displayed per page and use the fast page navigation at the bottom right of the page. The currently supported event types that can be recorded include:

- Successful User Login
- Failed User Login
- Configuration Changes
- High CPU Utilization
- High Memory Utilization
- Device Reboot
- Firmware Upgrade
- Client Status Changes
- Connection Status Changes
- These events are recorded to help you monitor and manage the device's operation and network activity.

5.2.4 Logs

The log function is used to record the raw return information of the device's operation under various circumstances. It is typically employed by IT or research and development personnel for the analysis and troubleshooting of issues.

Users can access the device's system logs by navigating to the "Status > Logs" section. System logs provide detailed information about the device's operation, and they are invaluable for troubleshooting when issues arise. Users have the option to download and clear logs as needed.

You can filter the displayed log entries based on log level or by entering keywords.

New log entries are added to the end of the log, keeping the most recent events at the bottom of the log.

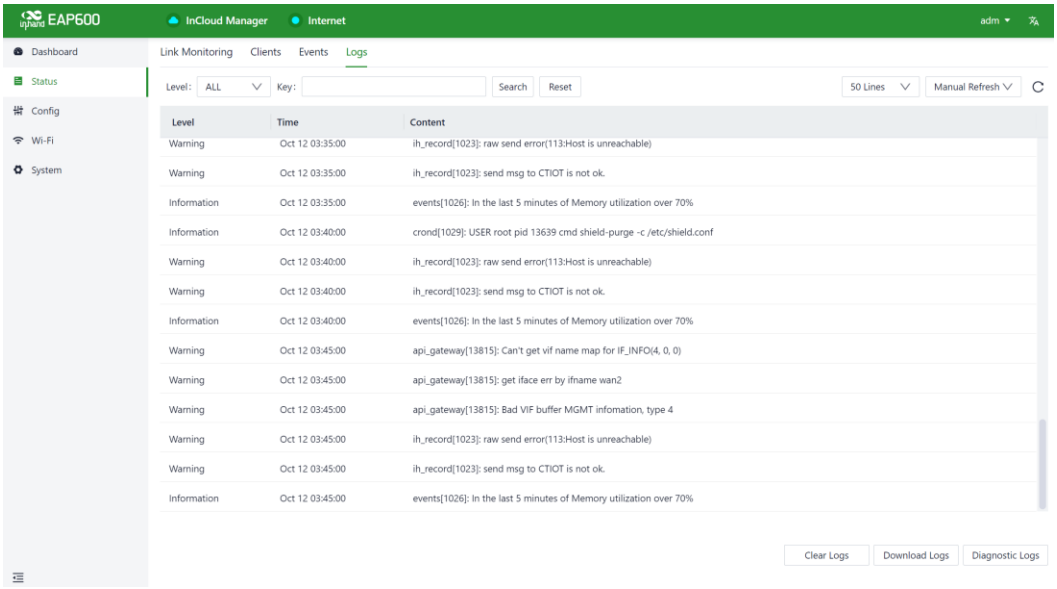

Fig. 5-2-4 Check the recorded logs

5.3 Configuration

Click on the "Config" button in the left-side navigation menu to access the configuration page. On this page, you can set up the device's WAN/LAN interface settings and RF parameters.

5.3.1 WAN

The EAP600 supports single-port wired access, and users can configure it to use DHCP or static IP address assignment based on their requirements. Click on “Configuration > WAN” to select the network connection type.

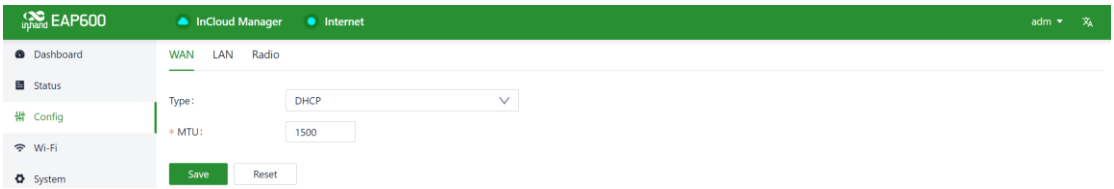

Fig. 5-3-1 Access the WAN editing interface

- DHCP: The EAP600 can dynamically obtain an internet IP address by using the DHCP server of the upstream router.
- Static IP: Users can manually configure the address assigned by the ISP or upstream device. After the configuration is complete, the AP will connect to the network using the specified static IP.
- The default MTU value is 1500, and the valid input range is from 128 to 1500.

5.3.2 LAN

This page is only visible when the device is operating in FAT-Router mode. For more details, please refer to *5.5.10 System Settings*.

When the device operates in FAT-Routing mode, users can create subnets and VLANs for different network segments in "Config > LAN" and configure subnet properties.

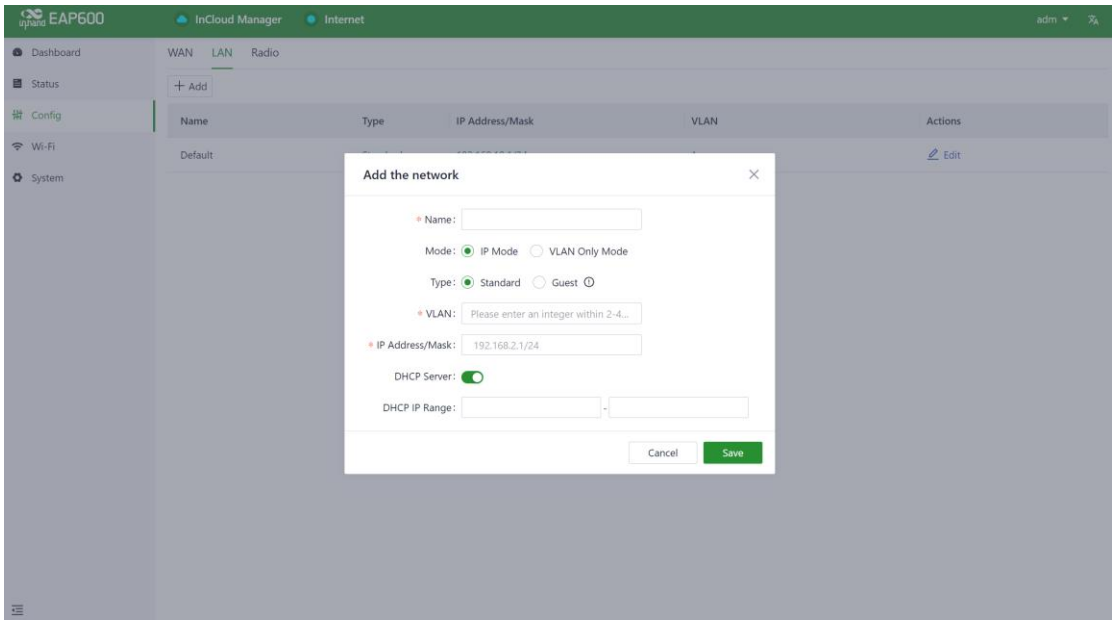

Fig. 5-3-2 Add a local network

The "Network Type" field provides two available modes:

- Standard: Clients connected to the standard mode network can access the Internet and the device's web interface.
- Guest: Clients connected to the guest mode network can only access the Internet and cannot log in to the device's web interface.

Edit Local Network: You can adjust the parameters of an existing local network, and the configuration fields are the same as when creating a new network.

5.3.3 Radio

Radio Frequency (RF) refers to the wireless communication technology used by access points (APs) in a wireless local area network. It primarily involves the configuration and adjustment of AP RF parameters to ensure optimal wireless coverage and performance.

Users can configure the device's Wi-Fi radio settings, such as the operating channels, radio power, and wireless mesh features, under "Config > Radio" in the device settings.

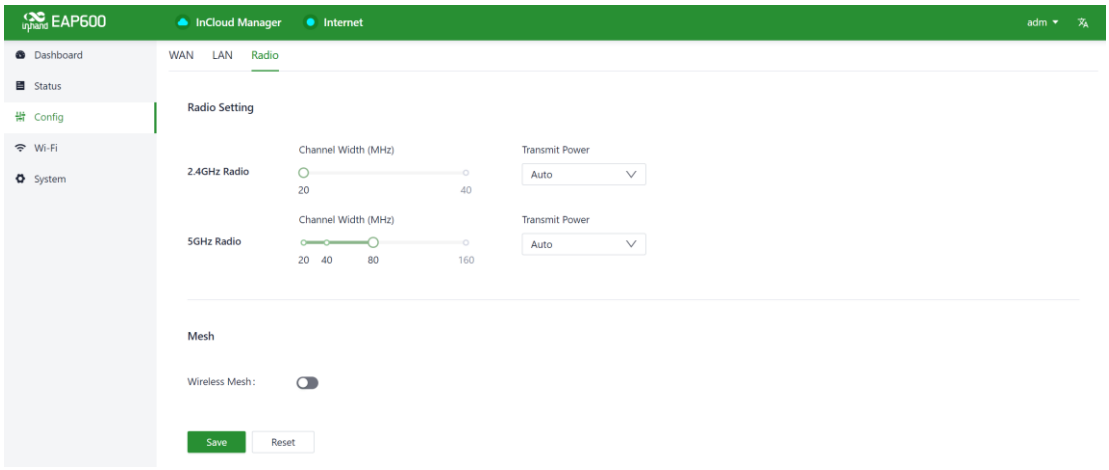

Fig. 5-3-3-a Edit the radio's parameters

You can configure the frequency width and transmit power for 2.4GHz and 5GHz radio frequencies under "Configuration > Radio > Radio Settings." When you set the "Transmit Power" to "Custom," you must manually enter the power value. The valid input range for power is between 1 and 20, with the default value being 20.

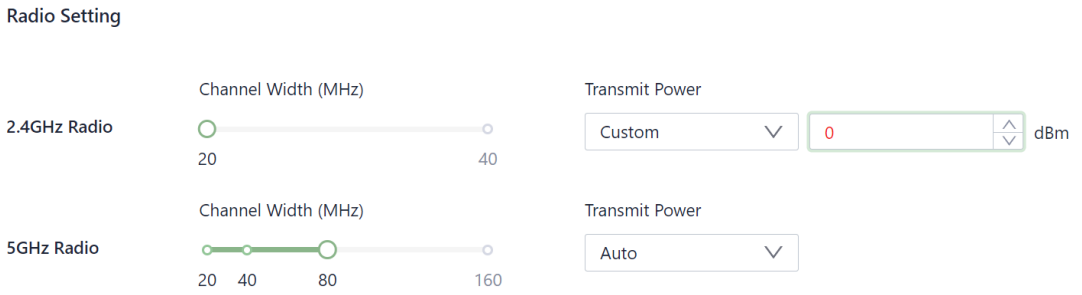

Fig.5-3-3-b Set the Transmit Power manually

The wireless Mesh network feature is disabled by default. When enabled in "config > radio > mesh," devices of the same model can quickly form a network through Mesh.

Fig.5-3-3-c Enable the Wireless Mesh

5.4 Wi-Fi

Wi-Fi functionality provides wireless local area network (LAN) connectivity for devices such as computers, smartphones, tablets, and more. It allows these devices to connect to a network wirelessly, providing internet access and communication capabilities.

EAP600 offers the ability to provide multiple SSIDs for wireless network access. Users can customize and configure different SSIDs for various purposes in the [Wi-Fi] interface.

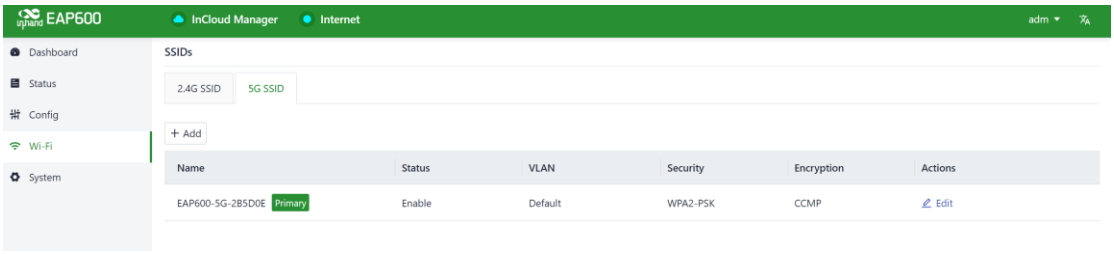

Fig. 5-4-a SSID List

By clicking on the "Wi-Fi > SSIDs" section and then the "Add/Edit" button, you can add a new SSID or edit an existing one. You can choose to hide the SSID. In this case, users will need to manually enter the SSID name and password on their client devices, and the SSID won't be visible in the list of available Wi-Fi networks.

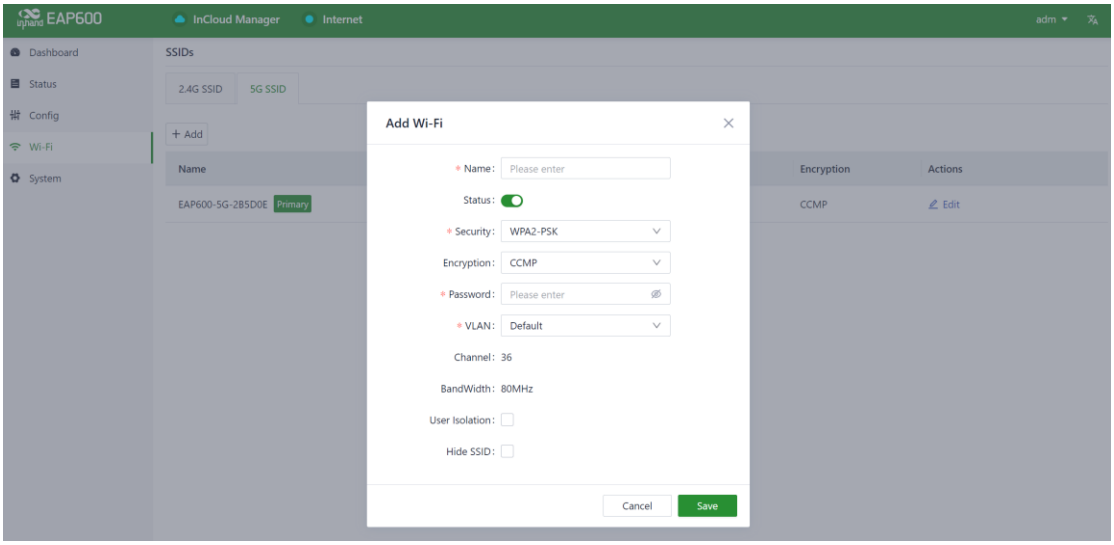

Fig. 5-4-b Add a new SSID

Cautions:

- The device comes with two default main SSIDs for the 2.4GHz and 5GHz bands, and these main SSIDs cannot be modified or deleted.

- Once you've added an SSID, you cannot change its frequency band. The channel will automatically match the channel of the corresponding main SSID.

5.5 System

Under the "System" menu, users can configure various settings and features, including cloud management, remote access control, clock settings, device options, configuration management, device alerts, tools, and log server configurations.

5.5.1 adm Management

The initial username and password for the device are "adm" and "123456." To enhance security, it is recommended to change this password. You can do this by clicking on "adm" in the top navigation bar, and then selecting "Change Password" from the dropdown menu.

Fig.5-5-a Modify the password

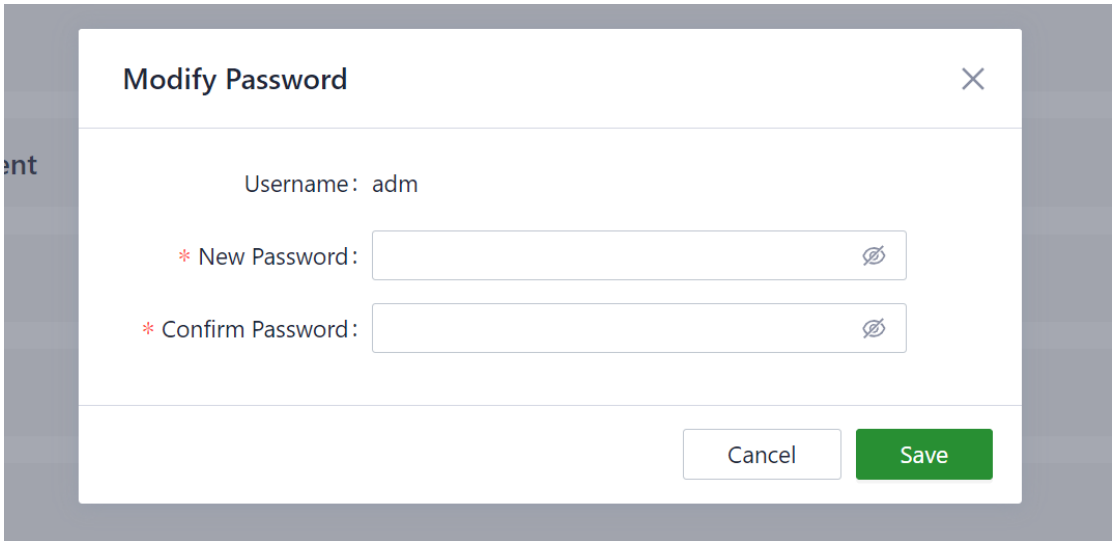

Fig.5-5-b Set a new password

5.5.2 Cloud Management

The Incloud Manager` (star.inhandcloud.com) is a cloud platform developed by InHand Networks to address the challenges faced by enterprise networks, such as slow deployment, complex operations, and poor user experiences. This platform prioritizes user needs and combines features like zero-touch deployment, intelligent operations

and maintenance, security protection, and exceptional business experience capabilities. Once devices are connected to the cloud platform, users can perform remote management, batch configuration, and traffic monitoring, making network device management more convenient and efficient.

The EAP600, by default, automatically connects to the Small Star Nebula Manager once it's online. If you prefer not to use the cloud management functionality, you can manually disable this service in the "System > Cloud Management" section.

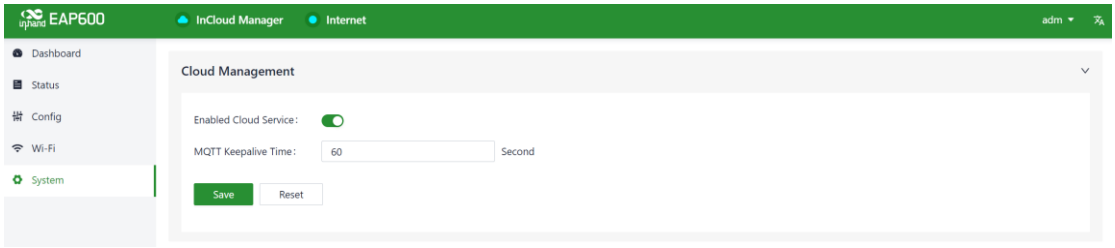

Fig. 5.-5-2 Enable the Incloud Manager service

5.5.3 Remote Access Control

You can manage the accessibility of the router's web configuration interface from external sources via the Internet by using the "System > Remote Access Control" feature. This feature enables you to control and configure remote access to the router's web interface.

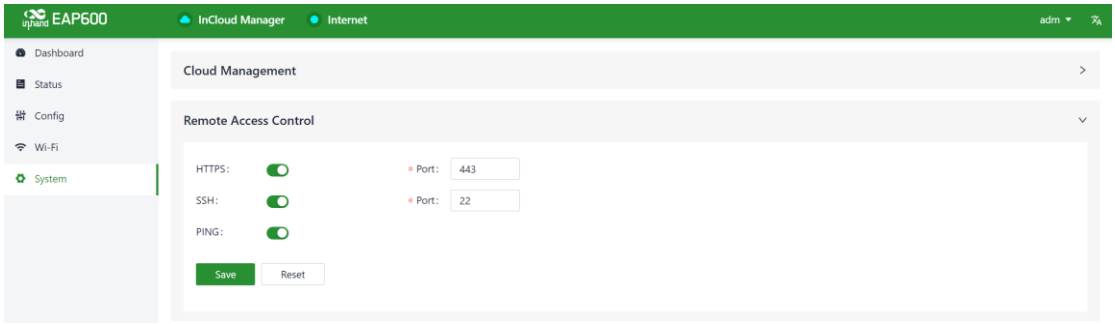

Fig. 5.-5-3 Configure the remote access

When you enable remote access to the router's web configuration interface through the "System > Remote Access Control" feature, you have the following options:

- HTTPS: Once enabled, you can access the router's web interface remotely through a web browser by entering the public IP address and port number associated with the upstream interface.
- SSH: When enabled, you can remotely log in to the router's backend using a remote tool like CRT. Enter the public IP address and port number of the

upstream interface, along with the username and password to establish remote access.

- 3. Ping: Enabling this option allows external networks to initiate Ping requests to the IP address of the upstream interface.

5.5.4 Country & System Clock

In network functionality, the clock function refers to the capability used to coordinate and synchronize time between network devices. Clock functionality within a network is crucial for data transmission, log recording, security, coordination, and troubleshooting. It ensures that various devices in the network are operating at synchronized times, which is essential for efficient and secure network operations.

In the "System > Clock" function, users can perform the following actions:

- Select your country to configure the device with the appropriate time zone.
- Set the time and date to align with your local time. This will become the device's system time.
- Configure at least one valid NTP (Network Time Protocol) Server address. This allows the device to synchronize its system time with the selected NTP server, ensuring accurate timekeeping.

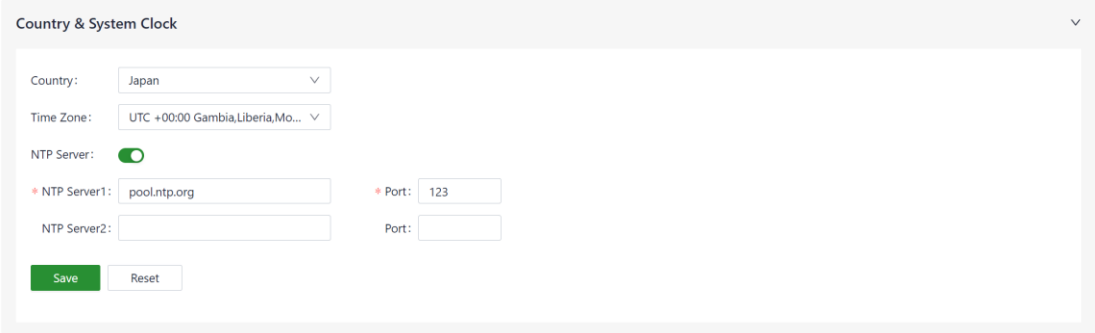

Fig.5-5-4 Choose the Country and configure the NTP server address

5.5.5 Device Option

In "System > Device Options," you can perform actions on the device, such as rebooting, firmware upgrades, and restoring to factory settings.

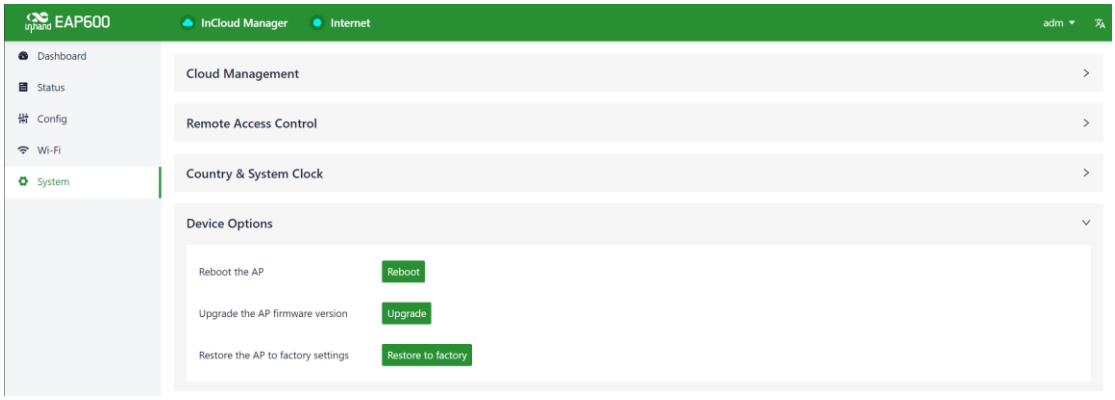

Fig. 5-5-5 Device Option interface

Cautions:

- When upgrading firmware locally, ensure that you obtain the firmware from legitimate sources to prevent the device from becoming unusable due to incorrect firmware installation.
- When the device is connected to the cloud platform, due to the cloud-based configuration synchronization mechanism, the platform will reapply the configuration that was in place before the factory reset, with the device only clearing historical data.

5.5.6 Configuration Management

Configuring backups and backup recovery are critical tasks in network management and maintenance. They involve the process of preserving configuration information for network devices so that they can be quickly restored or migrated when needed. This practice ensures the resilience and reliability of network operations and simplifies the recovery process in case of system failures or configuration changes.

In the “System > Configuration Management” section, users have the option to export the device configuration for local storage. This exported configuration can be saved on the local system and can be utilized to restore the device's configurations if they are lost or need to be replaced.

Fig. 5-5-6 Manage the device configuration

5.5.7 Device Alarms

Users can choose to focus on specific events that may occur on the device by selecting the corresponding alarm events and configuring the email address for receiving alerts. When an alarm event occurs, the device will automatically send an email notification. It's important to note that even if a user doesn't select certain alarm options, related alarm events will still be recorded in the device's local logs.

You can set alarm event types and configure the email address for alerts in the "System > Device Alarms" function.

The currently supported alarm events for the device are as follows:

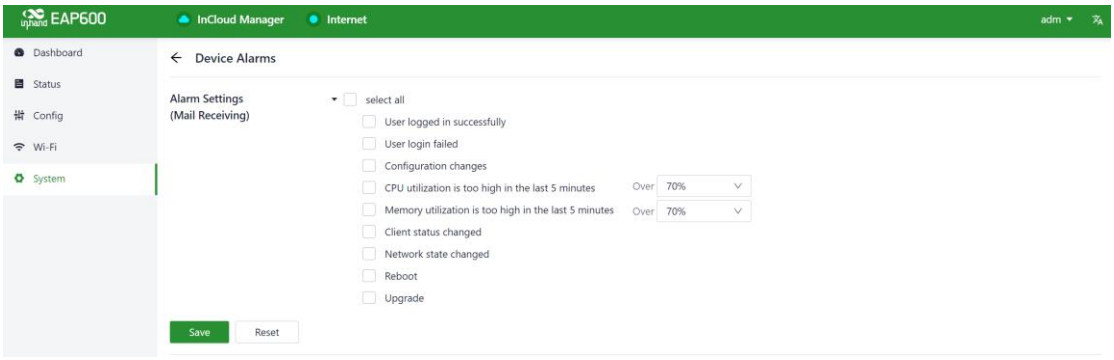

Fig. 5-5-7-a Configure the alarm events

Once you've configured the outgoing email server address, port, username, and password for the sender's email, the device will use this email account to send alarm notifications. To verify the configuration of the sender's email, you can use the "Send Test Email" option. This feature allows you to check if the sender's email settings are correctly configured and that the device can successfully send test emails.

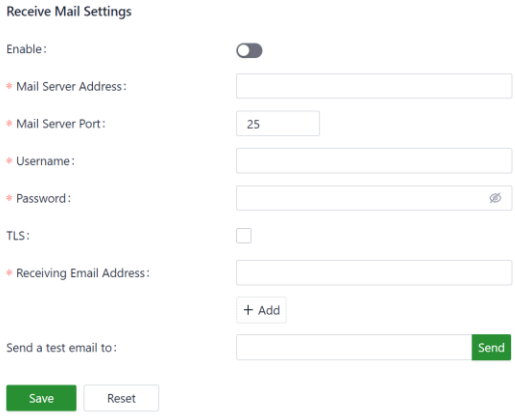

Fig. 5-5-7-b Set the alarm email receiving address

5.5.8 Tools

Users can use the provided tools for initial troubleshooting or issue localization.

5.5.8.1 Ping

To check the external network connectivity of the device using ICMP protocol, you can go to "System > Tools > Ping" and input any domain name or IP address in the "Target" field. Then, click "Start" to test the device's network connectivity with the specified target.

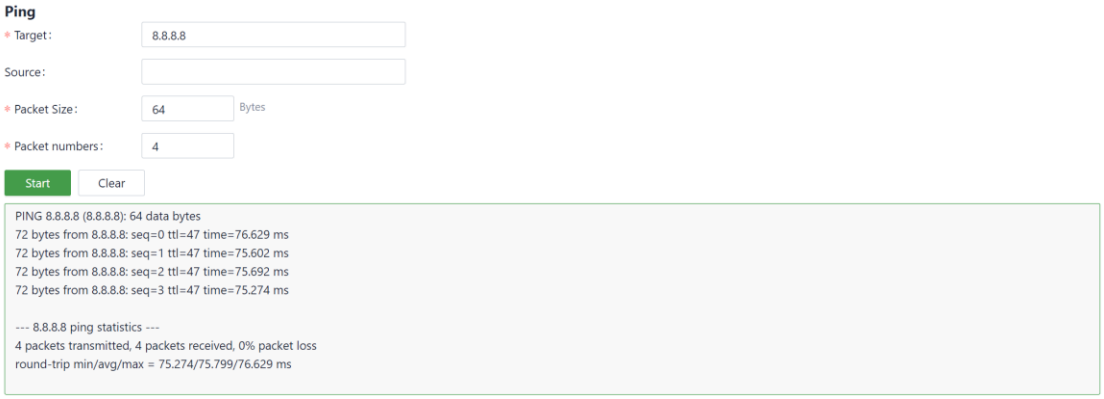

Fig. 5-5-8-1 Ping

5.5.8.2 Traceroute

Users can check the route connectivity between the device and the target IP address by entering the target host's IP address in "System > Tools > Traceroute." Select the interface, click "Start," and it will trace the route from the device to the specified target IP, displaying the connectivity information.

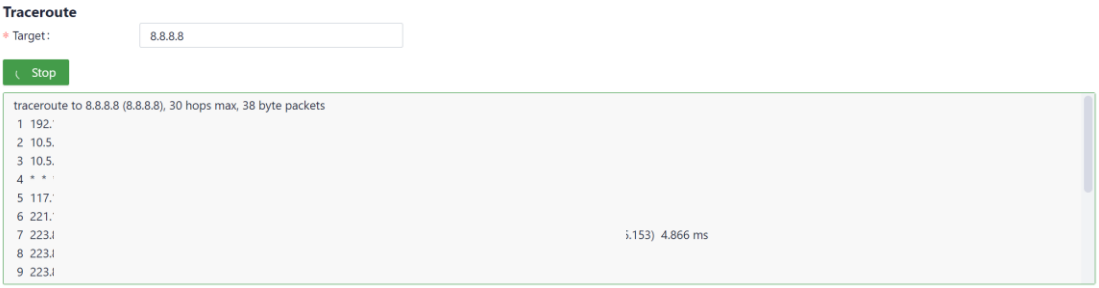

Fig. 5-5-8-2 Traceroute

5.5.8.3 Capture

Users can capture packets passing through a specific interface using the "System > Tools > Capture" feature. Select the "Output" option, and you can choose to either display the captured packets in the interface or export them locally for analysis or further examination.

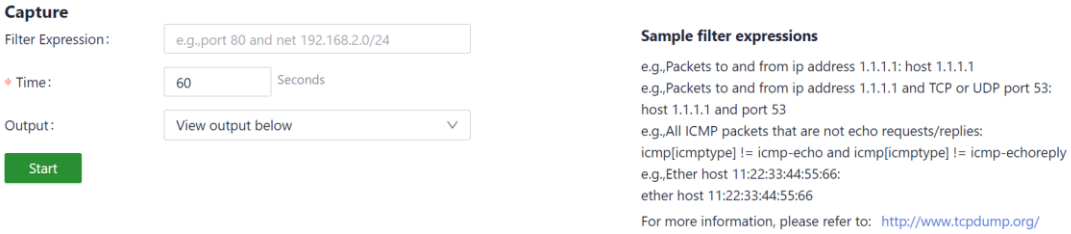

Fig. 5-5-8-3 Packet Capture

5.5.9 Scheduled Reboot

Users can set up an automatic reboot schedule in "System > Scheduled Reboot." You can choose the reboot frequency, such as daily, weekly, or monthly, and specify the exact time for each scheduled reboot.

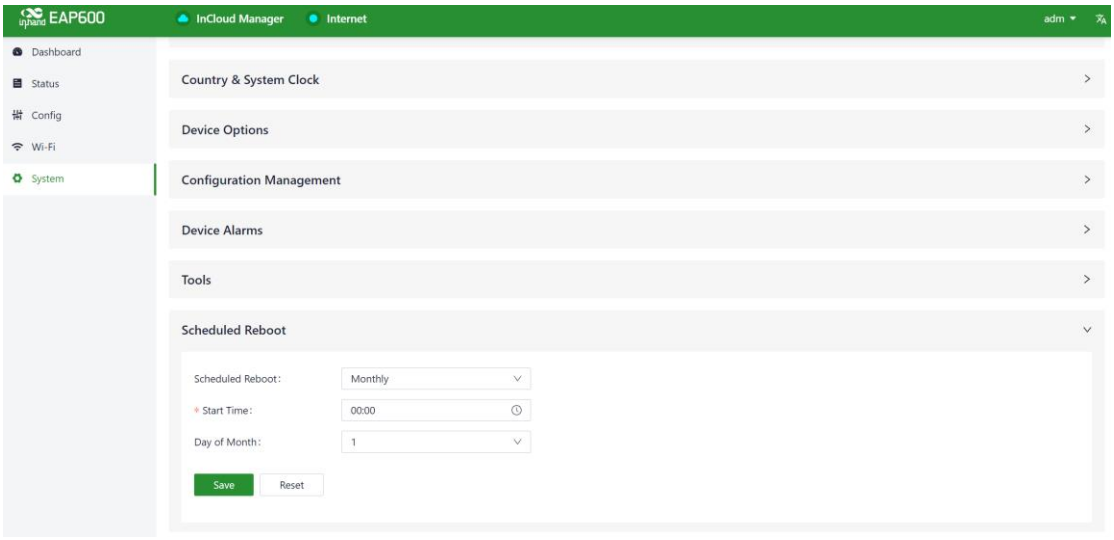

Fig. 5-5-9 Set the reboot plan

When selecting "Monthly Reboot," if the chosen reboot day is greater than the actual number of days in that month, the device will perform the scheduled reboot at the specified time on the last day of that month.

5.5.10 System Settings

In the "System > System Settings" function, you can set the operating mode of EAP600.

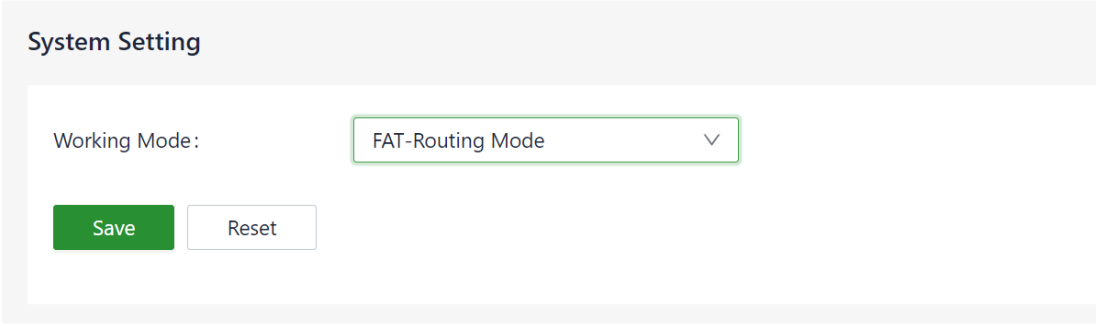

Fig. 5-5-10 Set the reboot plan

- FAT (Firmware-Defined Access Point) Router Mode: In this mode, the AP operates in a FAT mode and uses the configuration set on the AP itself, including SSID, password, and other settings. In router mode, the WAN and LAN ports are

isolated from each other, and client devices connected to the AP are assigned addresses from the AP's local address pool.

- FAT Bridge Mode: In this mode, the AP operates in FAT mode and uses the AP's configured SSID, password, and other settings. In bridge mode, the WAN and LAN ports are in the same Layer 2 network, and client devices connected to the AP obtain addresses from the DHCP server of the upstream router connected to the AP.

5.5.11 Log Server

When users enable the log file server function in the "System > Log Server" feature, the device will periodically upload log files to the specified server.

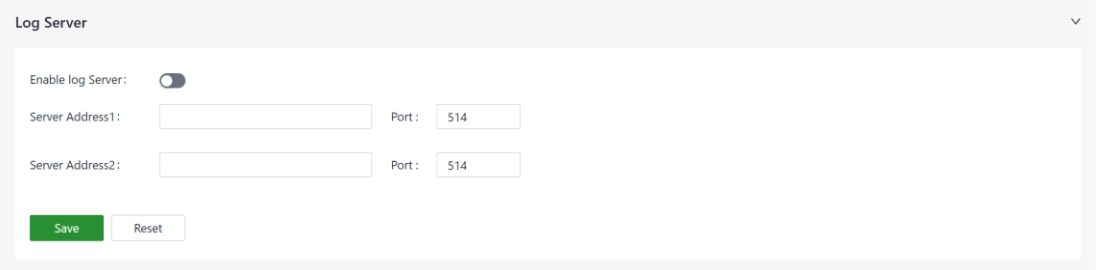

Fig. 5-5-11 Enable the log server service

5.5.12 Other Settings

5.5.12.1 Web Login Management

Users can set the logout time in "System > Other Settings > Web Login Management." Once the online time for a single login session on the device's web page exceeds the set time, the system will automatically log out of the user, requiring them to log in again to continue their operations.

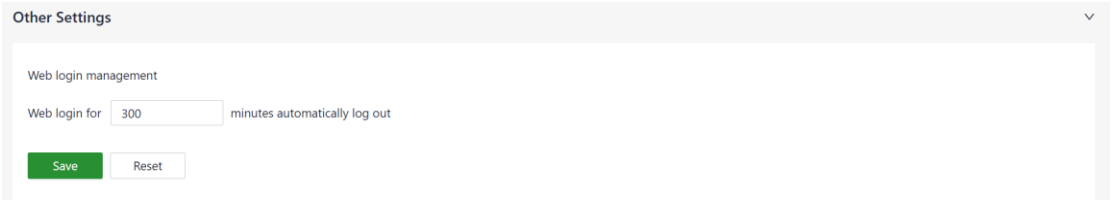

Fig. 5-5-12-1 Setting the automatic log-out time

5.5.12.2 Automatically Restart

When users enable this feature in "System > Other Settings > Automatically Restart," the device will automatically reboot if it cannot connect to the network and, after one hour of retrying, remains unable to access the network.

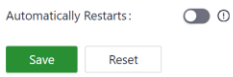

Fig. 5-5-12-2 Enable the Automatically Restart

6. Security Precautions

1. Please use PoE (Power over Ethernet) equipment that complies with the IEEE 802.3af/at standards to power the AP. If you are not using PoE for powering the device, make sure to use the original power adapter to avoid damaging the device.

2. Do not install the device in environments with strong electromagnetic interference and keep it away from high-power equipment. After installation, ensure that the device is securely fixed to prevent damage or potential harm due to the device falling.

3. Verify that the operating environment meets the specified temperature and humidity conditions for the device.

4. Regularly inspect the device cables, keeping them clean, and promptly replace any damaged cables.

5. When cleaning the device, avoid spraying chemical agents directly on the device's surface to prevent damage to the casing or internal components. Use a soft cloth for cleaning.

6. Do not attempt to disassemble or modify the device on your own, as this can pose safety risks and void the warranty for the device.

7. Troubleshooting

7.1 Clients Cannot Connect to the Wireless Network

1. Verify that the Access Point (AP) is operational and online. If any issues are detected, try restarting the AP or restoring it to a backup configuration.
2. Refer to the *2.1 LED Indicators* to check the AP's LED indicators for any abnormal signals.
3. Ensure that the AP's firmware is up to date. Obtain the latest firmware version from the official source.
4. Double-check that the AP's SSID and encryption settings match the configurations on your client devices.
5. Examine the AP's wireless channel settings to ensure there is no interference from neighbouring channels.
6. Review the AP's wireless configuration, including transmit power and frequency band settings.
7. If the issue persists, attempt to overwrite the current configuration with a backup or restart the device.

7.2 Wireless network is slow or experiencing instability

1. Check the signal strength and interference level of the Access Point (AP).
2. Verify that the number of clients connected to the AP does not exceed its capacity.
3. Review the AP's channel settings and transmit power parameters to ensure they are configured appropriately.
4. Inspect the vicinity for other electronic devices or high-power equipment, such as microwave ovens or Bluetooth devices. Ensure that the AP is not located too close to such devices.
5. If the problem persists, try overwriting the current configuration with a backup or reboot the AP.

7.3 AP Cannot Start Properly or Frequent Crashes

1. Check if the AP's power adapter is properly connected or if the PoE power supply device is functioning correctly.
2. Refer to the "2.1 LED Indicator Description" to check the AP's LED indicators for any abnormal indications.
3. Inspect the AP's temperature to ensure it is not overheating and verify that the environmental humidity meets the device's requirements.
4. If the issue persists, consider updating or reinstalling the AP's firmware.

7.4 Unable to Connect to a Specific Website or Service.

1. Check if other devices can access the website or service.
2. Clear your browser's cache and cookies.
3. Verify if the DNS server addresses are configured correctly and consider trying different DNS server addresses.

7.5 Unable to access the Incloud Manager

1. Check if the device's cloud service is enabled. You can verify this on the device's local web page under *5.5.2 Cloud Management.*
2. To confirm that the device can access the network, you can perform a network check using the tools referring to *5.5.8 Tools*.
3. Verify that your cloud platform account has correctly added the device and issued a license. Afterwards, check the license status in the "Dashboard > Device Information" section of the device's local web page.

If you are unable to resolve the issue using the steps mentioned above or encounter any other problems, please contact InHand Network for technical support. You can visit www.inhandnetworks.com to obtain more information.

8. Hardware Specification

EAP600	
Wireless Network	Maximum 2974Mbps
Coverage radius	15m
Recommended Users	150
ETH Port	1*Gigabit Ethernet Port
Reset	1*Reset Button
LED Indicators	PWR/WAN/2.4G/5G
Antenna Gain	2.4GHz/5GHz:3dBi
Protocol	802.11 a/b/g/n/ac/ax
Power Supply	12V 1A / 802.3 af（PD）
Power Consumption	12W
Weight	400g
Dimensions	158*158*28mm
Installation	Desk-top; Ceiling
Operating Temperature	0℃~45℃
Storage Temperature	-40℃~70℃
Humidity	95%RH @ 40℃