



DH-EAP Series

User's Manual








Foreword

This manual mainly introduces the DH-EAP series Initialization and Web operation. (hereinafter referred to as the "AP")

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release	June 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic

version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

Foreword	I
1 Product Description	1
2 AP Initialization	2
2.1 Wired Mode.....	2
2.2 Wireless Mode.....	3
2.3 Logging in to the AP WEB.....	4
3 Fit AP Mode	5
3.1 Network Settings.....	5
3.2 Upgrading	6
3.3 Resetting.....	7
3.4 Restarting	7
4 Fat AP Mode	8
4.1 Configuration Wizard	8
4.2 Home Page.....	10
4.3 Wi-Fi Settings.....	12
4.3.1 Configuring 2.4G Wi-Fi or 5G Wi-Fi.....	12
4.3.2 Configuring MAC ACL.....	15
4.3.3 Configuring Wi-Fi Shutdown.....	16
4.4 Device Management	16
4.4.1 Configuring the Device	16
4.4.2 Restarting.....	17
4.4.3 Changing Password.....	17
4.4.4 Upgrading.....	17
4.4.5 Time Management.....	18
4.4.6 System Logs.....	19
4.4.7 Cloud Platform Config.....	19
4.5 Auth Config.....	19
Appendix 1 Security Commitment and Recommendation	21

1 Product Description

The DH-EAP series of products is a high-performance, high-speed indoor dual band AP that supports both PoE and DC power supply methods. It supports ceiling and wall mounting, and has a built-in high gain antenna, suitable for various indoor wireless coverage scenarios such as education, buildings, and catering.

The wireless ceiling AP has three working modes: Fit, Fat, and Gateway. In Fit AP mode, the AP is managed by the DH-ERC series all-in-one router, which is plug and play and easy to manage. In Fat AP mode, the AP can be used alone to provide wireless network services directly to clients. In Gateway AP mode, the AP connects to the higher-level router or optical modem through the Ethernet cable of the WAN port, assigns an IP to the devices on the LAN side, and extends the wireless network signal to the devices in the LAN area. All devices share a wide area network IP, which can be selected when there are no wired/wireless routers.

The working temperature of this series of wireless ceiling APs is -20°C to 45°C (-4°F to 113°F), the working humidity is 5%~95% (RH), and the storage temperature is -40 ° C to 70 ° C (-40°F to 158°F).

2 AP Initialization

Accessing the AP's management Web page, you can choose to connect the AP device either wired or wireless. If the device is already connected to the DH-ERC series all-in-one router, the IP address of the device depends on the DHCP server's enabled status of DH-ERC:

- When the DHCP function is enabled, log in to the ERC web interface and view the device's IP address in the AC Management ->AP list.
- When the DHCP function is turned off, the IP address of the device is set to the default value of 192.168.1.110.

2.1 Wired Mode

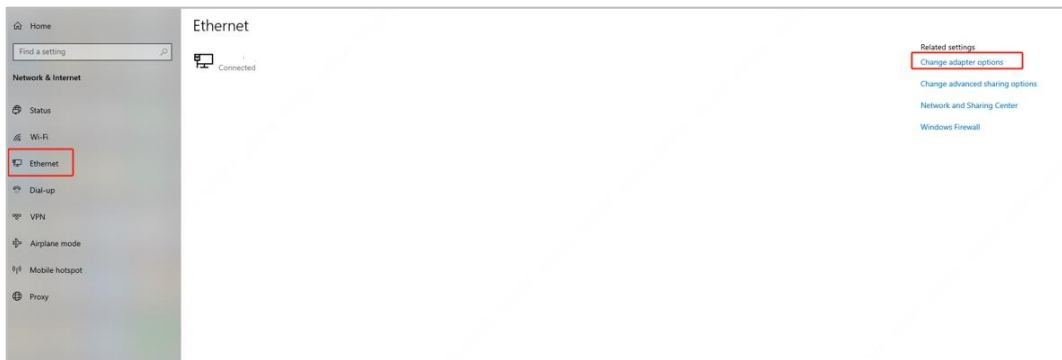
Confirm that the PC and device routing are reachable, and then set the IP address of the PC. The specific steps for setting the PC IP address are as follows:

Step 1 Connect AP LAN port to the PC.

Step 2 Right click on the network icon in the bottom right corner of the PC and select **Open Network & Internet Settings**.

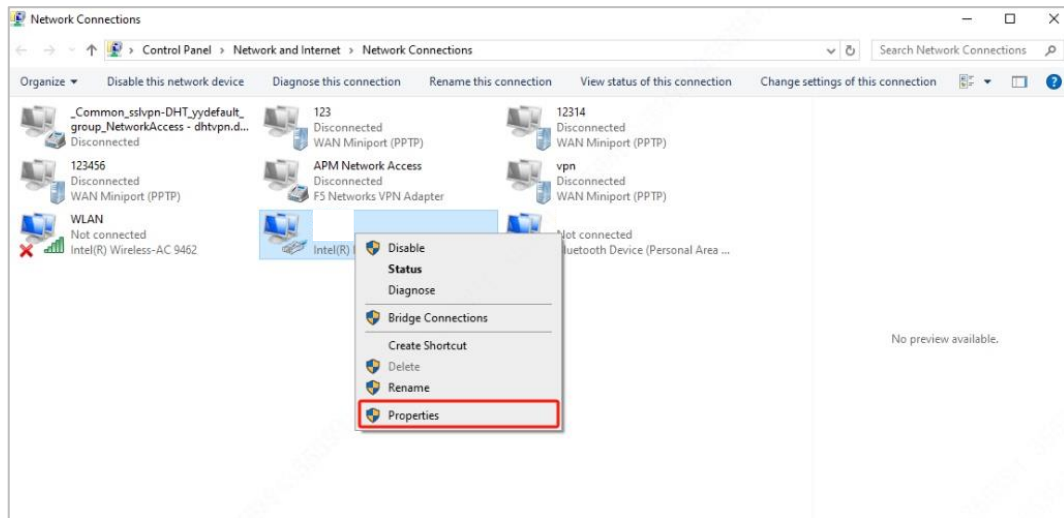
Step 3 Click **Ethernet** on the settings page and select **Change adapter options**.

Figure 2-1 Change adapter options



Step 4 Right click Ethernet and select **Properties**.

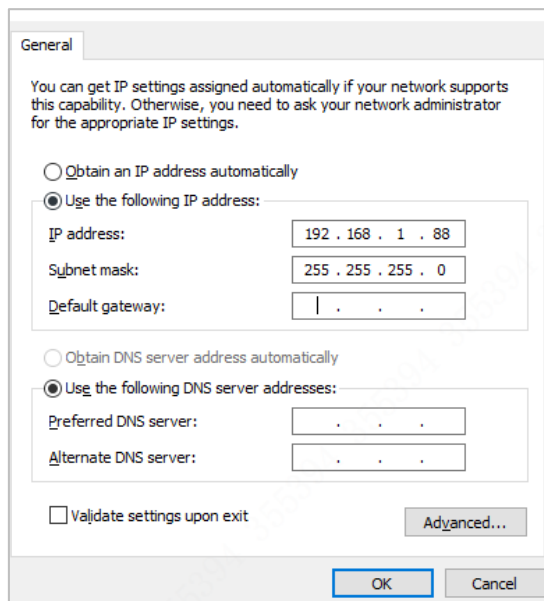
Figure 2-2 Select Properties



Step 5 Double click **Internet Protocol Version 4 (TCP/IPv4)**.

Step 6 By manually configuring the PC IP address, set the IP address and subnet mask for the same network segment as the device.

Figure 2-3 Set IP address



Step 7 Click **OK**.

2.2 Wireless Mode



- The wireless terminal needs to successfully install a wireless network card in order to connect wirelessly.
- Place the wireless terminal within the wireless range of the AP device (recommended within 10 meters).
- Search for a wireless network with the Wi-Fi name "DAHUA_Wireless_XXXXXX" through a wireless terminal (mobile phone or computer with a wireless network card, etc.) (default not encrypted, XXXXXX is the last 6 digits of the MAC address) and connect.

- Refer to wired methods and manually configure the computer IP address to maintain the same network segment as the device's IP address.

2.3 Logging in to the AP WEB

Open the browser, enter the 192.168.1.110 in the address bar, press enter, and then jump to the web management page.

Enter the password initialization page for the first time (without entering the management account), set the login password, and use the new password to access the device web.

Figure 2-4 Initialization page

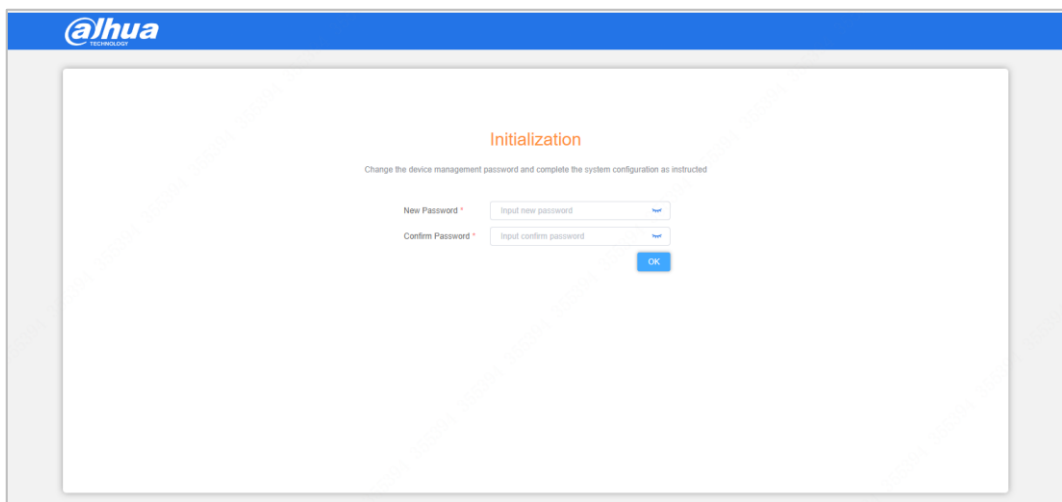
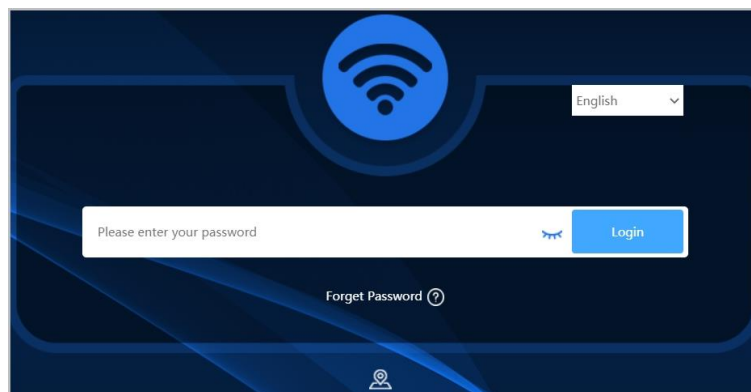



Figure 2-5 Login



First time use, Default enters fit AP mode.

Click  on the upper right corner and could switch to Fat AP mode. Switching to Fat AP mode will restart the device to apply the configuration.

3 Fit AP Mode

3.1 Network Settings

Procedure

Step 1 Login to the WEB and enter the Fit AP mode.

Step 2 Select Connect Method.

Connect Method supports DHCP and Static IP.

- DHCP: Allocate dynamic IP addresses by managing servers.
- Static IP: Manually configure IP address, default gateway, management server address, and other information.

Figure 3-1 Set Connect method (DHCP)

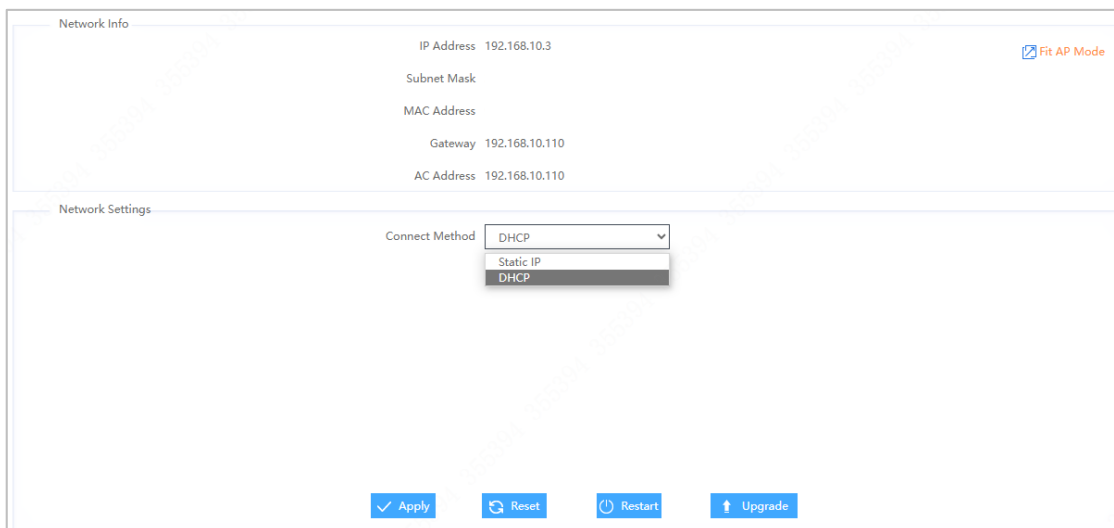
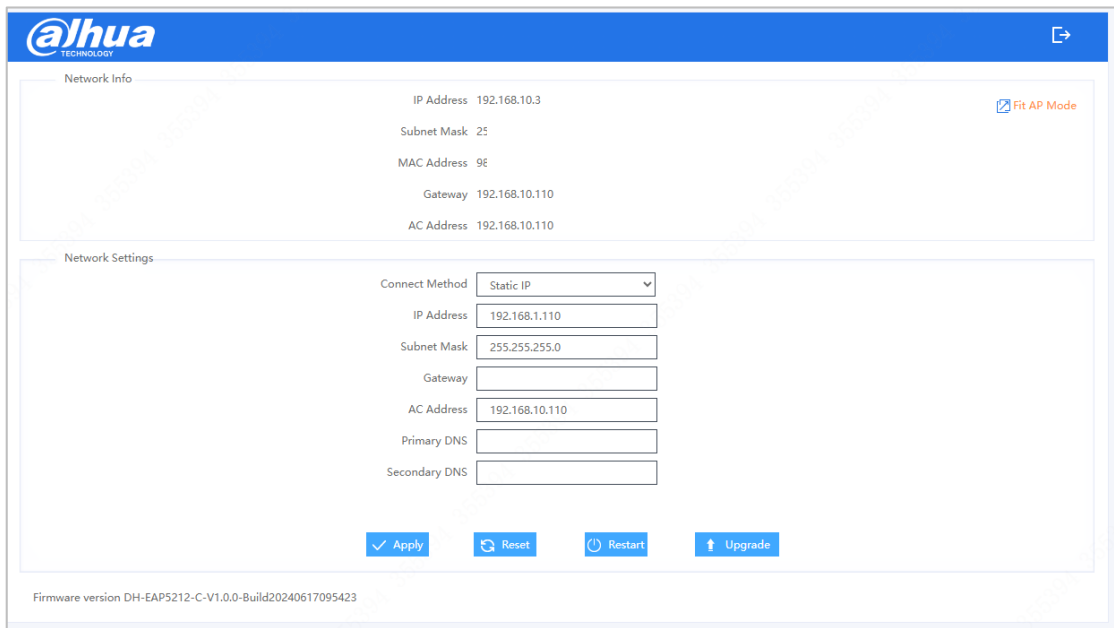


Figure 3-2 Set connect method (Static IP)



Step 3 Click **Apply**.

3.2 Upgrading

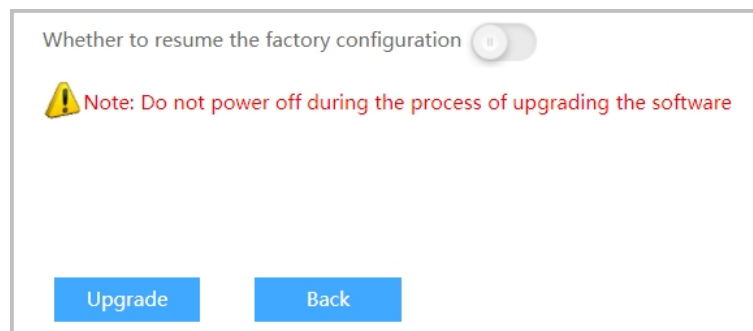
Procedure

- Step 1 Login to the WEB and enter the fit AP mode.
- Step 2 Click **Upgrade** on the bottom right corner.
- Step 3 Click **Select File** and select firmware upgrade package in on-premises.
- Step 4 Click **Upgrade** and wait for the upgrade to complete.



Click . If you enable factory reset after upgrading, all configurations will be reset to the factory default state after the upgrade is completed.

Figure 3-3 Upgrade



3.3 Resetting

Login to the WEB and enter the fit AP mode. Click **Reset** below the screen and click **OK** on the pop-up dialog box. The Device recovery default configuration.

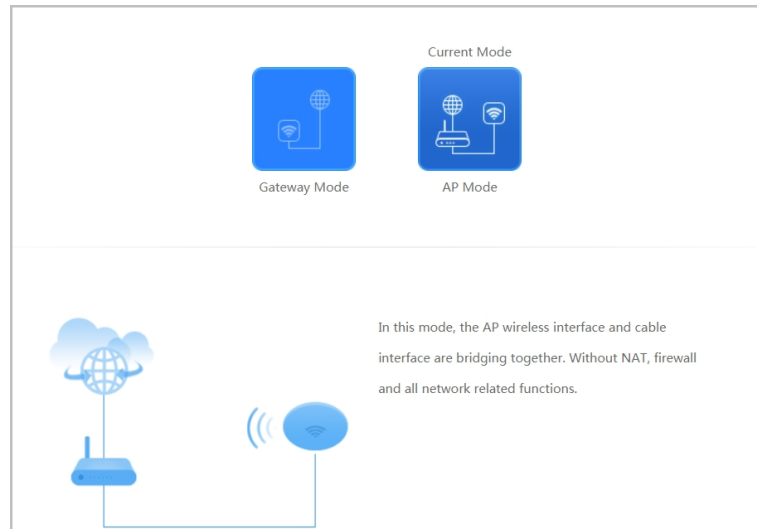
3.4 Restarting

Login to the WEB and enter the fit AP mode. Click **Restart** below the screen and click **OK** on the pop-up dialog box. The Device is restarting.

4 Fat AP Mode

Login to the WEB and select **AP Mode**. Start configuration wizard.

Figure 4-1 AP mode



4.1 Configuration Wizard

First time using Device, please follow the prompts in the wizard to complete the basic setup.

Procedure

Step 1 Login to the WEB and select **AP Mode**.

Step 2 Configure the network and click **Next**.

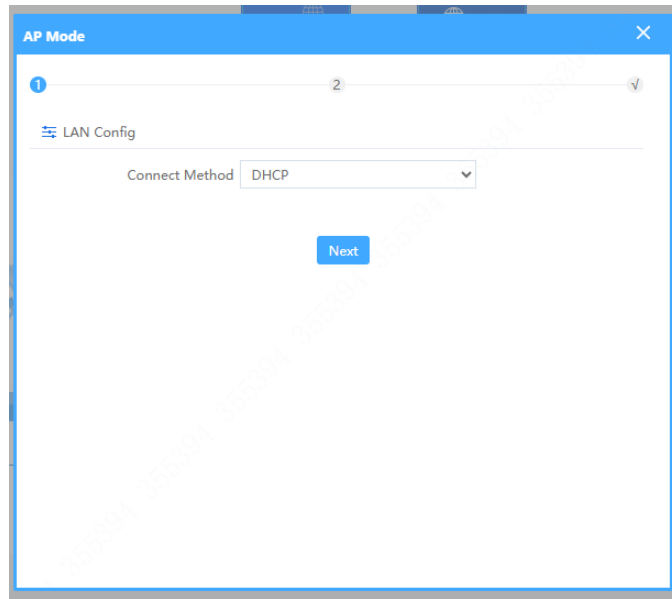
Connection mode supports DHCP and Static IP.

- DHCP: Allocate dynamic IP addresses by managing servers.
- Static IP: Manually configure IP address, default gateway, management server address, and other information.



Complete the configuration wizard, you can modify the intranet parameters on the **Network** tab.

Figure 4-2 Network configure



Step 3 Enter the Wi-Fi Settings page, set the Country/Region, SSID, Encryption Type and whether to Hide SSID.

Figure 4-3 Wi-Fi setting

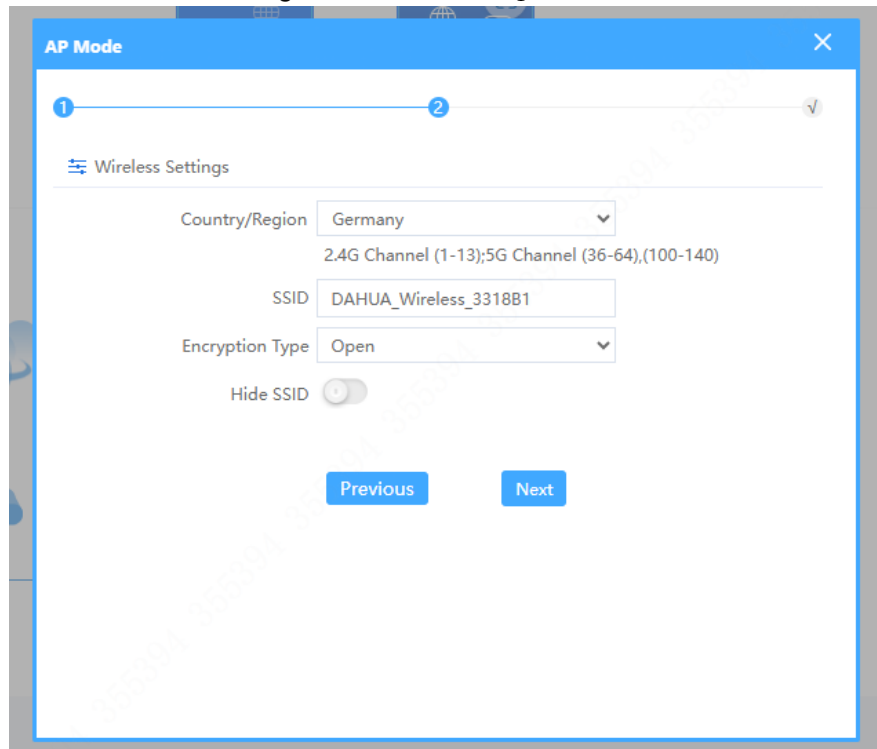


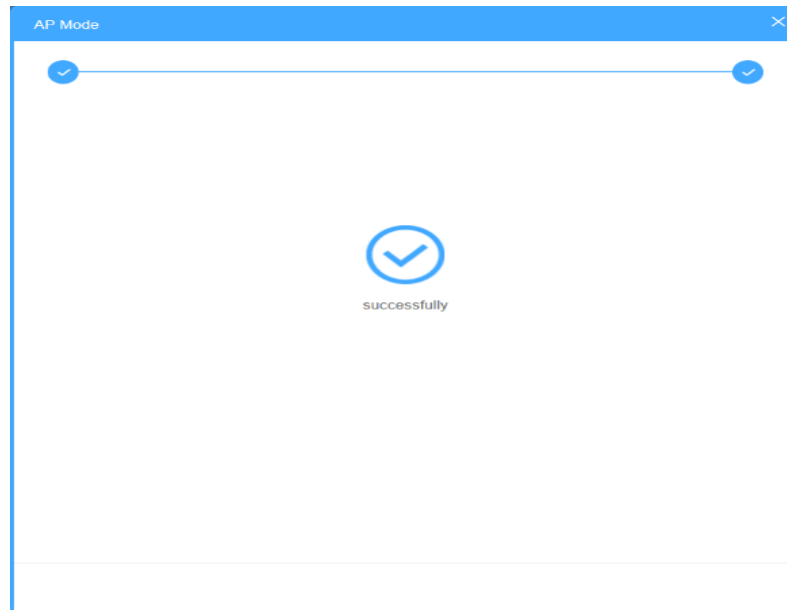
Table 4-1 Wireless parameter description

Parameter	Description
Country/Region	Select based on actual country or region, if not in the list, you can choose similar.
SSID	Customize the wireless name to distinguish different wireless signals.

Parameter	Description
Encrypt Type	Including Open , WPA/WPA2-PSK and WPA2/WPA3-PSK . WPA2/WPA3-PSK provides higher security. Please choose according to the actual support situation.
Hide SSID	Default is off, if you choose hide, the Wi-Fi will not be searched by the terminal.

Step 4 Configure successfully as follows:

Figure 4-4 Configure successfully



Step 5 All configurations are completed, the system will restart, and after restarting, it will enter the management page normally.

4.2 Home Page

Login to the WEB and default goes to the home page.



The interfaces of different model products may vary. Please refer to the actual product for details.

Figure 4-5 Home page

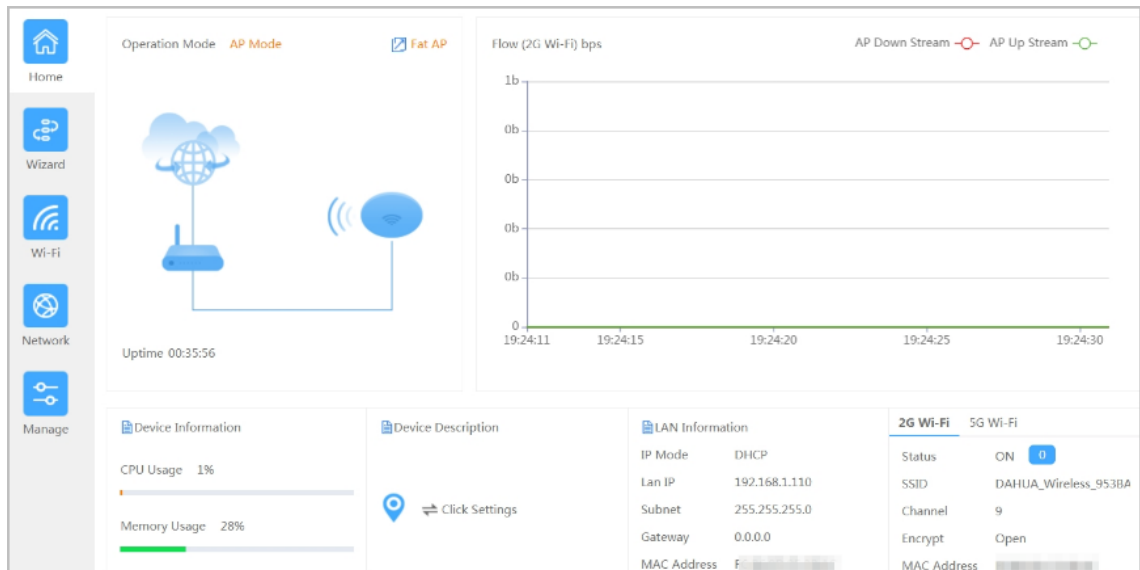




Table 4-2 Home page description

Module	Description
Working Mode	Displays the current AP mode. Click  and switch to fit AP mode.
Traffic Monitoring	Displays real-time Wireless Access Point download speed and upload speed. Click AP Down Stream or AP Up Stream on the upper right corner to cancel the display of the corresponding information.
Device Info	Displays CPU and memory usage.
Device Description	Click Click Settings and modify device name.
LAN Info	Displays device connection methods, IP address, MAC address and other information.
2.4G Wi-Fi	Displays wireless status, wireless name, encryption, and other information. Click on the number on the right side of the status. For example  , and then view detailed information about the user currently connected to the AP.
5G Wi-Fi	

4.3 Wi-Fi Settings

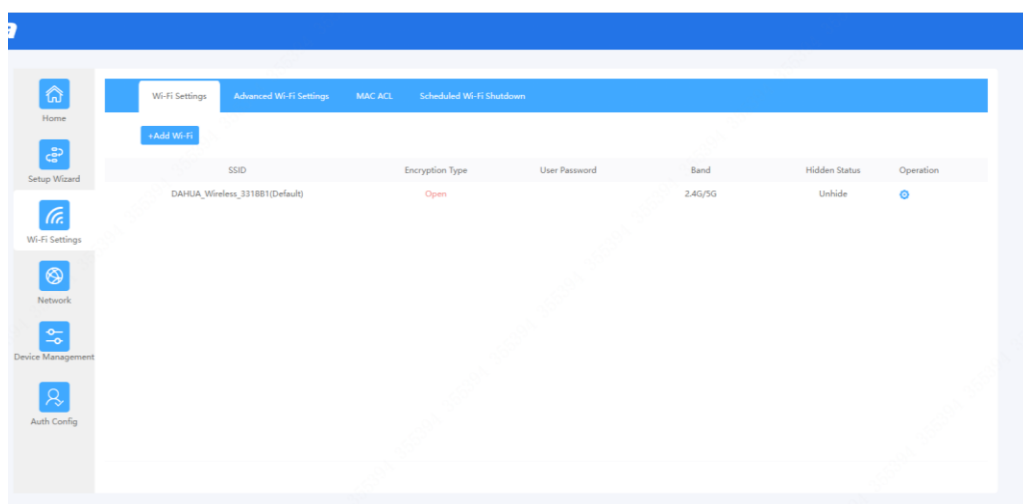
4.3.1 Configuring 2.4G Wi-Fi or 5G Wi-Fi

In Wi-Fi settings, you can add SSID, set SSID name, Encryption Type, Wi-Fi Password, Band and VLAN ID. The Advanced Wi-Fi Settings in Wi-Fi Settings can set the Country/Region, Prioritize 5G, 2.4G and 5G RF parameters, etc.

Procedure

Step 1 Login to the WEB and select **Wi-Fi Settings**, the system has default dual band Wi-Fi, DAHUA_Wireless_XXXXXX (XXXXXX is the last six digits of MAC address).

Figure 4-6 Wi-Fi Settings



Step 2 Click **+Add Wi-Fi**, you can add a new Wi-Fi for your AP.

Figure 4-7 Wi-Fi setting

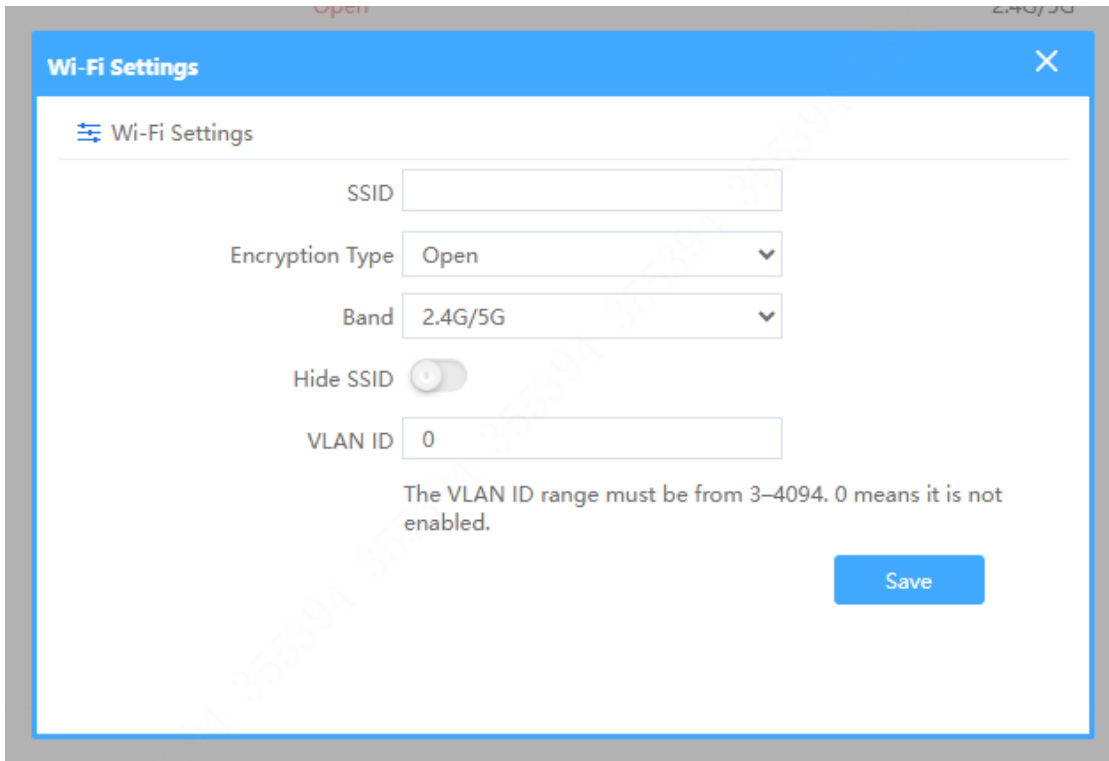


Table 4-3 Wireless parameter description

Parameter	Description
SSID	Customize the wireless name to distinguish different wireless signals.
Encrypt Type	Including Open, WPA/WPA2-PSK and WPA2/WPA3-PSK. WPA2/WPA3-PSK provides higher security. Please choose according to the actual support situation.
Band	Including 2.4G、5G、2.4G/5G.
Hide SSID	Default is off, if you choose hide, the Wi-Fi will not be searched by the terminal.
VLAN ID	Set according to the actual situation.

Step 3 Click **Save**.

Step 4 In **Advanced Wi-Fi Settings**, you can set Country/Region , Prioritize 5G , and 2.4G/5G radio frequency parameters settings.

Figure 4-8 Advanced Wi-Fi Settings

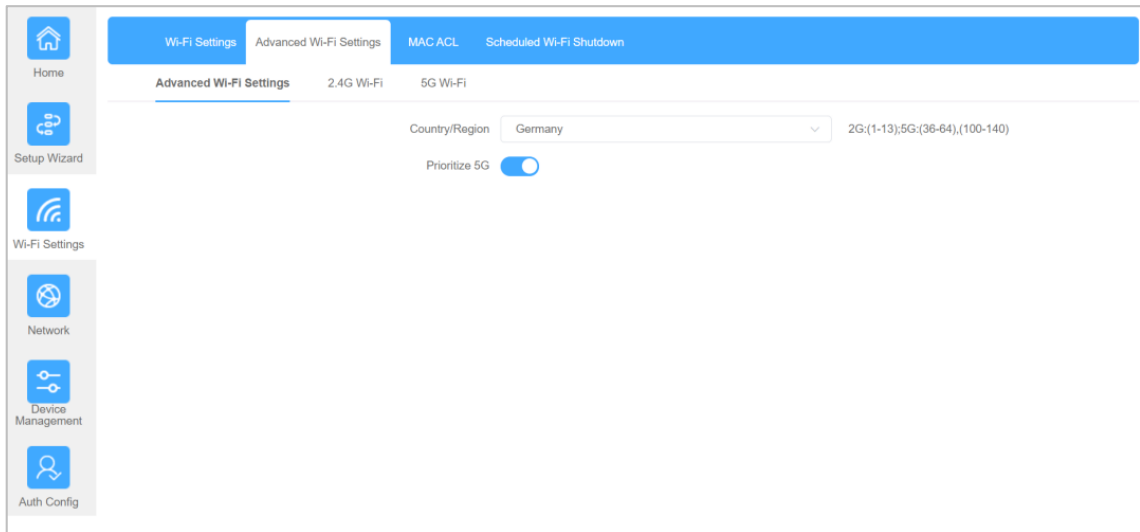


Figure 4-9 2.4G/5G radio frequency parameters settings



Table 4-4 Wireless parameter description

Parameter	Description
Country Region	Choose the correct country code based on the actual situation. The country code determines the available frequency band, channels, and power, etc.
Prioritize 5G	Enable 5G priority, the Device prioritizes sending 5G wireless data.
Channel Bandwidth	Bandwidth refers to the bandwidth occupied by wireless signals in the spectrum. It determines the data transmission rate and stability of Wi Fi networks. There are generally options such as 20MHz, 40MHz, 80MHz, 160MHz, etc. Devices with different speeds will have different options.

Parameter	Description
Channel	Channel list includes automatic and other channel numbers. Select Auto indicates the Device will evaluate the channel mass and select the best channel.
Transmit power	Support High, Medium and Low
Wireless Mode	Wireless protocol can be selected
User Isolate	When User Isolate is enabled, all wireless users connected to the same AP cannot communicate directly with each other.
Limit Users that can Access	Enable user access restriction and set the maximum number of users that can connect to each AP. When the number of users connected to an AP reaches the preset value, other users will not be able to connect to the AP.
AP Coverage Limit	Set the signal strength range that the AP can validly cover.
Short GI	Enable short GI to reduce interference between data blocks and improve network transmission efficiency.

Step 5 Click **Apply**.

4.3.2 Configuring MAC ACL

Block access or data transmission for a device by specifying its specific MAC address.

Procedure

Step 1 Login to the WEB and select **Wi-Fi Settings > MAC ACL**.

Step 2 Click **Add** and enter the MAC address and remarks information on the popped up box.



- MAC address separated by semicolons, for example FF:FF:FF:FF:FF:FF.
- Click **Scan** and quickly find the currently connected device.


Step 3 Click **Save**.

Figure 4-10 MAC ACL

Step 4 Select control type and click **Apply**.

Control type including **Disable** and **Prohibited rules within the device through**.

Related Operations

- Click  and modify the added MAC address information.
- Select one or multiple configurations that have been added and click **Delete**. Then you can delete the MAC address information.

4.3.3 Configuring Wi-Fi Shutdown

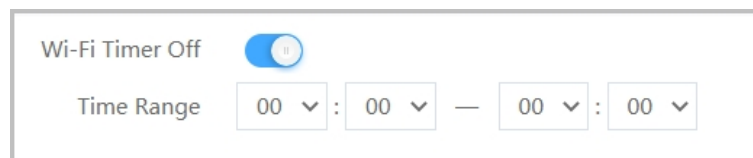
Shut Down wireless network within the specified scheduled time.

Procedure

Step 1 Login to the WEB and select Wi-Fi Settings > Schedule Wi-Fi shutdown.

Step 2 Click  and set time range.

Figure 4-11 Wi-Fi shutdown



Step 3 Click **Apply**.

4.4 Device Management

Device management supports operations such as backup configuration, factory reset, device reboot, modify password, firmware upgrade, and download system log.

4.4.1 Configuring the Device

Login to the WEB and select **Device Management** > **Configuration Management**. Perform backup, recovery configuration or reset operation.

Backup

Click **Backup** and download backup file (.bin format) to PC.

Restore

Click **Select File** and select profile on your PC, and then restore configuration.

Reset Default

Click **Reset Default** and click **OK** in the pop-up dialog box to restore the device to factory settings.

4.4.2 Restarting

Supports immediate reboot or scheduled reboot.

Procedure

Step 1 Login to the WEB and select **Device Management > Restart**.

Step 2 Choose to reboot immediately or set a scheduled reboot based on actual needs.

- Restart Now: Click **Restart Now** and perform reboot operation once.
- Scheduled Restart: Enable **Scheduled Restart** and set reboot time. Click **Apply** and the Device will be scheduled to reboot.

Reboot time supports every day or specific days of the week, such as Monday.

Figure 4-12 Restart



The screenshot displays a web interface for device restart settings. It includes a 'Restart Now' button, a 'Scheduled Restart' toggle switch (currently turned on), and a 'Restart Time' section with a dropdown menu set to 'Every Day' and a time field set to '3:00'. An 'Apply' button is located at the bottom right.

4.4.3 Changing Password

Login to the WEB and select **Device Management > Change Password**. Enter the old password and set the new password, and then click **Apply**.

4.4.4 Upgrading

Procedure

Step 3 Login to the WEB and select **Device Management > Upgrade**.

Step 4 Click **Select File** and select firmware upgrade package in on-premises.




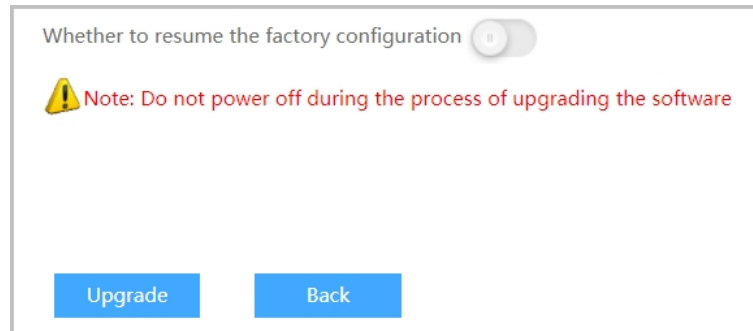
Click . If you enable factory reset after upgrading, all configurations will be reset to the factory default state after the upgrade is completed.

Figure 4-13 Upgrade



4.4.5 Time Management

The Device supports synchronizing time from the PC main server or network server.

Procedure

Step 1 Login to the WEB and select **Device Management > Time**.

Step 2 Choose to synchronize from the main server or network server based on actual needs.

Network Time Synchronization(NTP): Enable **NTP Enable** and set the time zone. Manually set the time server or choose an existing network server and click **Apply**.


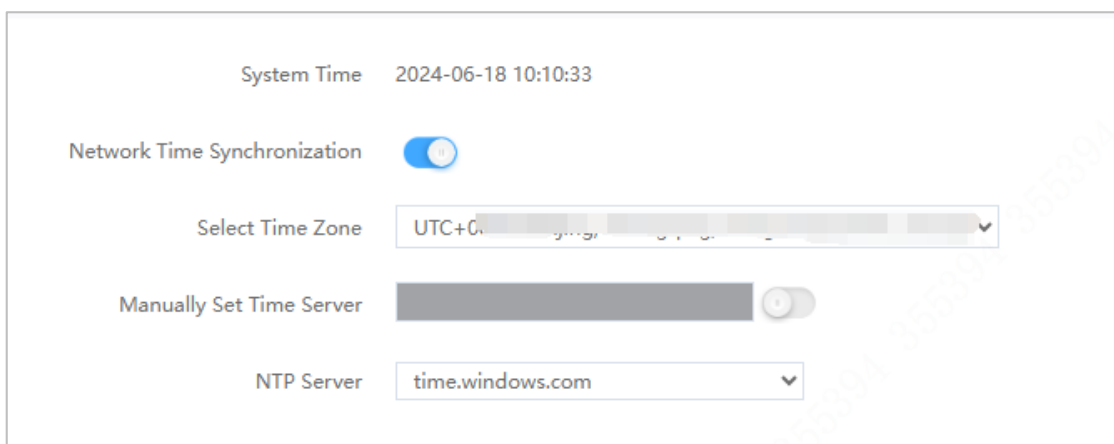
- Manually Set Time Server: Click  on the right side of the Manually Set Time Server and enter IP server address.
- NTP Server: Shut down **Manual Set time Server** and select a server from the dropdown menu.

Figure 4-14 NTP



4.4.6 System Logs

Login to the WEB and select **Device Management > System Logs > Export logs**. Export the log (.bin format) to PC on-premises.

4.4.7 Cloud Platform Config

After enabling cloud management, it is possible to achieve remote management through DoLink Care App and Web.

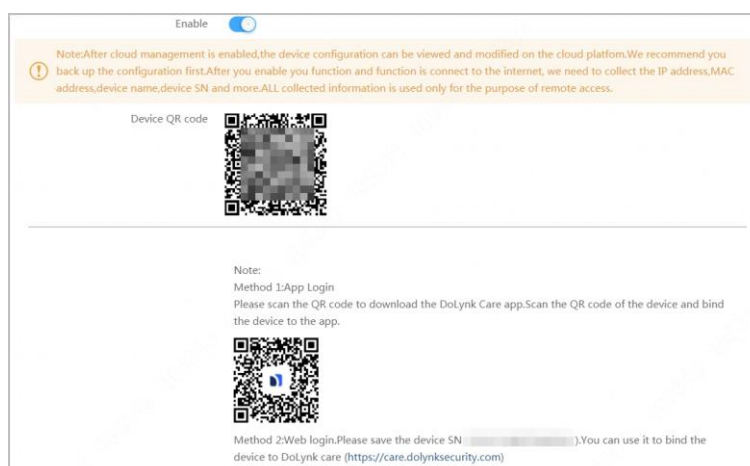
Procedure

Step 1 Login to the WEB and select Device Management > Cloud Platform Config.

Step 2 Click  on the right side of the **Enable**.

Step 3 Download and login to the App. Use your mobile phone to scan the Device QR code and add the Device to the App.

Figure 4-15 Cloud platform config



4.5 Auth Config

Configure portal authentication, support cloud authentication.

When the function is enabled, the user connects to AP and portal authentication will pop up. Only the authenticated user can normally use Wi-Fi.

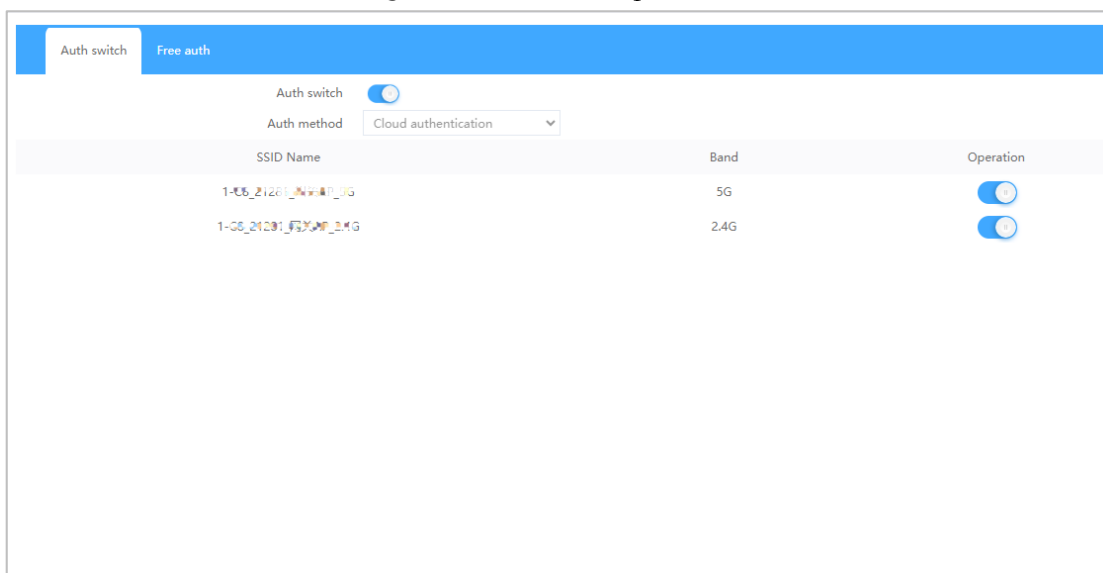
Cloud authentication must be used in conjunction with DoLink Care Web. Create portal configuration on the web end and send it to the AP device.

If it is account password authentication, create portal authentication account and bind it to the AP device; The cloud portal can also be opened and closed locally for SSID (Wi-Fi) after successful issuance.

Procedure

- Step 1** Login to the WEB and select **Auth Config> Auth Switch**.
- Step 2** Cloud authentication must be used in conjunction with **DoLynk Care Web**. Create portal configuration on the web end and send it to the AP device. If it is account password authentication, create portal authentication account and bind it to the AP device
- Step 3** The cloud portal can be opened and closed locally for SSID (Wi-Fi).

Figure 4-16 Auth Config



For the AP gateway mode, most functions are the same as Fat AP mode. You can refer to the configuration steps of Fat AP.

Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") places great emphasis on cybersecurity and privacy protection. We continuously allocate special funds to enhance employees' awareness and capabilities in security, and ensure sufficient security protection for our products. Dahua has established a professional security team to provide comprehensive security empowerment and control throughout the entire product lifecycle, including design, development, testing, production, delivery, and maintenance. Dahua products adhere to the principle of minimum necessary data collection, service minimization, strict prohibition of backdoors, and the disabling of unnecessary and insecure services (such as Telnet). We continuously introduce innovative security technologies to bolster the security capabilities of our products. Additionally, we go above and beyond by providing global users with security alarm and 24/7 security emergency response services. This approach ensures that we are better safeguarding their security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report potential risks or vulnerabilities to the Dahua PSIRT. They can do so by visiting the cybersecurity section on the Dahua website.

The security of software platforms not only relies on the continuous attention and efforts from manufacturers throughout R & D, production, and delivery, but also requires active participation from users. Users should remain attentive to the environment and methods to ensure its secure operation. To this end, we suggest users to safely use the software platform, including but not limited to:

1. Account Management

1.1 Use Strong Passwords

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

1.2 Change Password Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

1.3 Assign Accounts and Permissions Reasonably

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

1.4 Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

1.5 Set and Update Passwords Reset Information Timely

The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

1.6 Enable Account Binding IP/MAC

It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

2. Service Configuration

2.1 Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

2.2 Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.

3. Network Configuration

3.1 Enable Firewall Allowlist

We suggest you to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.

3.2 Network Isolation

The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

4. Security Auditing

4.1 Check Online Users

It is recommended to check online users irregularly to identify whether there are illegal users logging in.

4.2 View the Platform Log

By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

5. Physical Protection

We suggest that you perform physical protection to the device that has installed the platform. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware.

6. Perimeter Security

We suggest that you deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188