IP Speaker

User Manual

V1.0.0

Foreword

General

This manual introduces the installation, structure, web operations of the IP speaker (hereinafter as the “speaker”). Read this manual before you use the product and keep this manual for future reference.

Models

SH30

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 Date
V1.0.0	First release.	December 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

Store the device under allowed humidity and temperature conditions.

Installation Requirements

 **WARNING**

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Replace unwanted batteries with new batteries of the same type and model. Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion. Dispose of the old batteries as instructed.
- Do not expose the battery to extremely hot environments, such as direct sunlight and fire, to avoid the risk of fire and explosion.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 5 cm on top of the device.
- Install the device on a stable surface to prevent it from falling.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- Use the power cords that are recommended for the region and conform to the rated power specifications.

- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it.
- An easily accessible safety disconnect switch must be incorporated into the external power supply circuit during installation.

Operation Requirements

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not place an open flame on the device, such as a lit candle.
- Do not disassemble the device without professional instruction.
- Operating temperature: -20 °C to +60 °C (-4 °F to +140 °F).

Maintenance Requirements

Make sure you use the same model when replacing the battery to avoid fire or explosion. Dispose the battery strictly following the instructions.

The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

1 Product Overview

1.1 Introduction

Designed with aviation aluminum, the IP speaker is a strong network speaker that features voice talk (only VCA-SH30 IP speaker supports two-way talk), broadcasting, and storing audio files. It supports PoE, Bluetooth (only available for VCS-STW30 and VCS-STW40 IP speakers), SIP, and ONVIF protocols, and can be managed on its webpage or in batches on the platform. The IP speaker is widely used for a variety of security monitoring scenarios.

1.2 Features

VCS-SH30

- With its cone-shaped corners, it is easy to control the direction of audio broadcasts. It also supports wall mount and pole mount.
- Made of anti-corrosion aviation aluminum, it is suitable for use outdoors in most weather conditions.

  It is not suitable for corrosion-resistant environments such as seaside and chemical factories.
- With its integrated design, it has a built-in network audio decoding chip, high fidelity digital operational amplifier and horn speaker.
- Supports PoE, which is convenient for on-site installation.
- Supports device registration and intercom based on the ONVIF protocol.
- Supports the standard SIP protocol and SIP-based intercom.
- It has a 512 MB storage capacity, and supports uploading custom audios and using TF cards for expansion (the back cover must be open).
- Supports remote management over the network, facilitating operation and maintenance.
- Built-in one-click reset button.

VCS-STW30 and VCS-STW40

- Designed with a column structure, suitable for wall mount installation.
- Made of anti-corrosion aviation aluminum, it is suitable for use outdoors in most weather conditions.
- With its integrated design, it has a built-in network audio decoding chip, high fidelity digital operational amplifier and horn speaker.
- Supports PoE, which is convenient for on-site installation.
- Supports device registration and broadcast based on the ONVIF protocol.
- Supports the standard SIP protocol, connecting to SIP platforms, and SIP-based broadcasting.
- It has a 512 MB storage capacity, and supports uploading custom audios and using TF cards for expansion.
- Supports remote management over the network, facilitating operation and maintenance.
- Supports 1-channel alarm signal input and 1-channel microphone audio signal input.
- Supports Bluetooth, and playing audios through it.
- Built-in one-click reset button.

VCS-SPOE20

- With its cylindrical structure, it supports in-ceiling mount installation. The thickness of the mounting plate can also be adjusted when installing it in the ceiling.
- Made of anti-corrosion aviation aluminum.
- With its integrated design, it has a built-in network audio decoding chip, high fidelity digital operational amplifier and horn speaker.
- Supports PoE, which is convenient for on-site installation.
- Supports device registration and broadcast based on the ONVIF protocol.
- Supports the standard SIP protocol, connecting to SIP platforms, and SIP-based broadcasting.
- It has a 512 MB storage capacity, and supports uploading custom audios and using TF cards for expansion.
- Supports remote management over the network, facilitating operation and maintenance.
- Built-in one-click reset button.

2 Web Operations

You can view the basic information, upload MP3 files, configure system settings and more.

2.1 Initialization and Login

Procedure

Step 1 Enter the IP address of the Unit in the browser address bar (the IP address is 192.168.1.108 by default), and then press Enter key.

Step 2 Set the password for the admin user.

The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters among uppercase and lowercase letters, numbers, and special characters (excluding ', ", ;, :, and &). The confirming password must be the same as the new password.

Step 3 Click **OK**.

Step 4 Enter the username and password, and then click **Login**.

Figure 2-1 Login

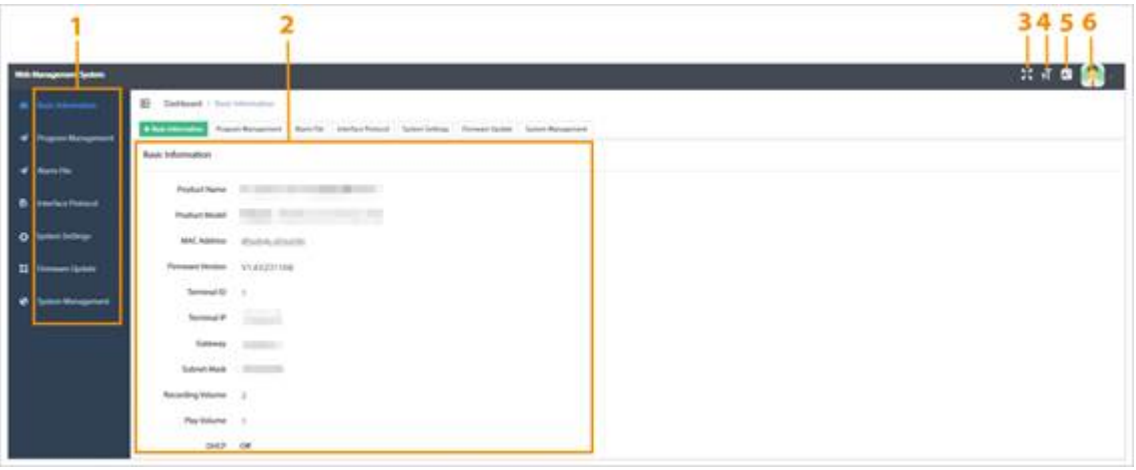


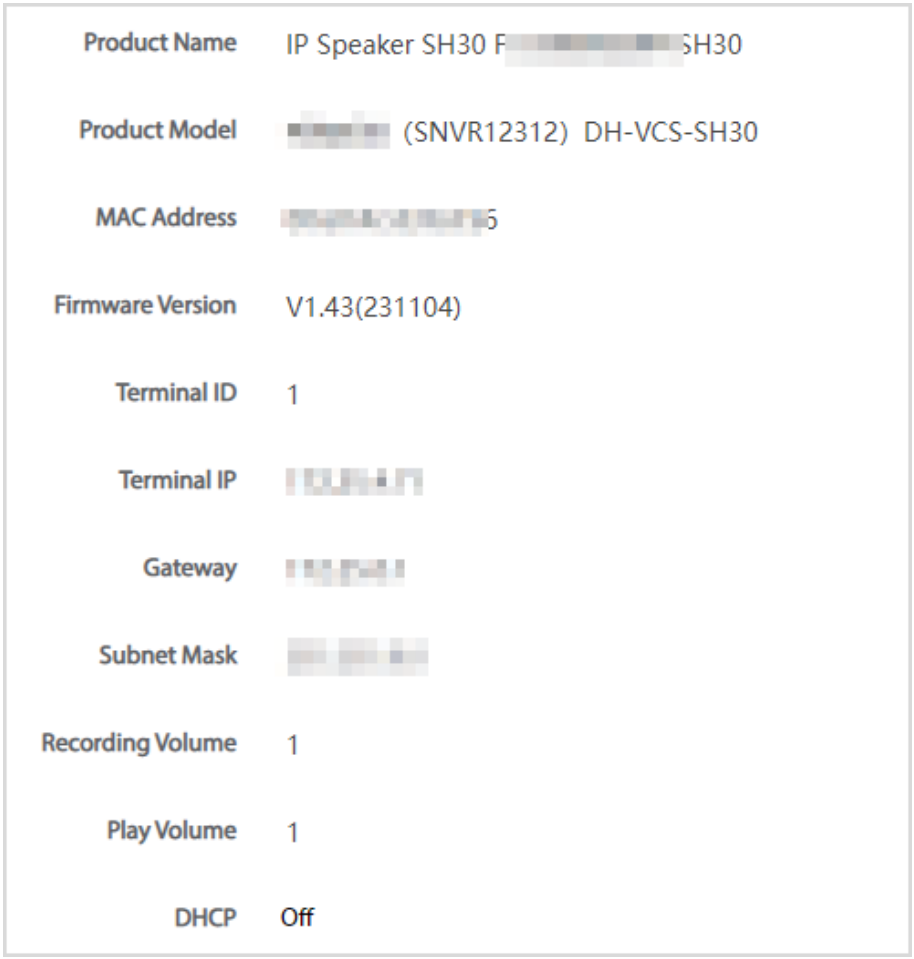
Table 2-1 Parameter description of main page

No.	Description
1	Function module.
2	Configuration area.
3	Full screen mode.
4	Font size. You can select **Default**, **Medium**, **Small** and **Mini** size of the font.
5	Set the language of the webpage. Supports Chinese and English.
6	• Profile: Select **Profile**, and then enter the old password, new password and confirm the password to update the login password. • Logout: Click **Logout** to log out.

2.2 Basic Information

Select **Basic Information** to view the basic information of the device including product name, model, Mac address, Terminal IP, and more.

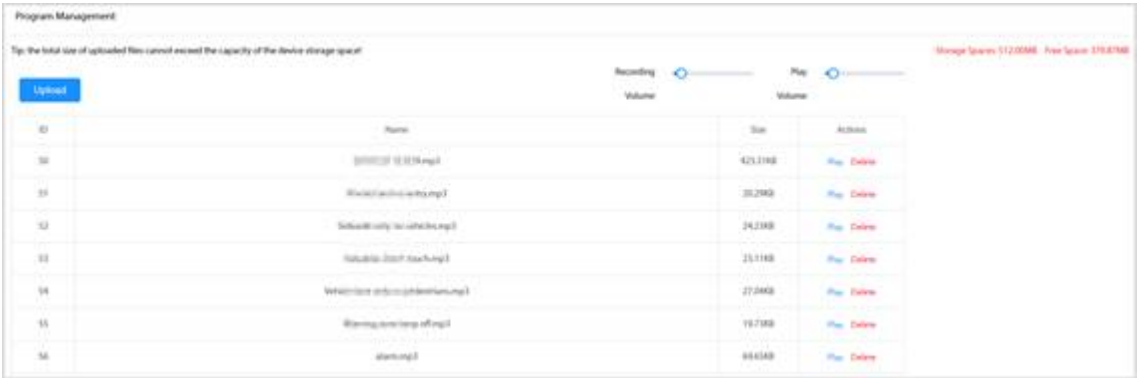
Figure 2-2 Basic information



2.3 Program Management

Select **Program Management**, and then click **Upload** to upload MP3 files.

Figure 2-3 Program management



- You can move the slider to adjust the recording volume and play volume.
- Click **Play** responding to the MP3 file to play the audio file.
- Click **Delete** responding to the MP3 file to delete the audio file.

2.4 Alarm File

You can configure the content of audio files from the drop-down list after the alarm is triggered. After that, click **Save** to save the configurations.

Figure 2-4 Alarm file

2.5 Interface Protocol

Select **Interface Protocol**, and then you can configure the parameters of UDP. SIP and ONVIF. After that click **Save** to save the configurations.

Figure 2-5 UDP

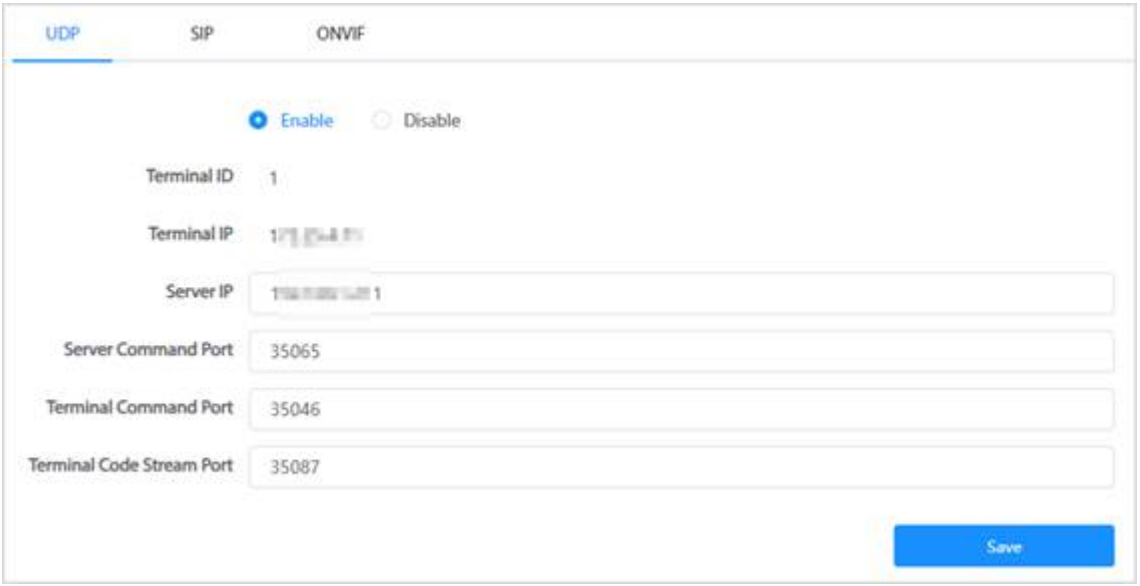


Figure 2-6 SIP

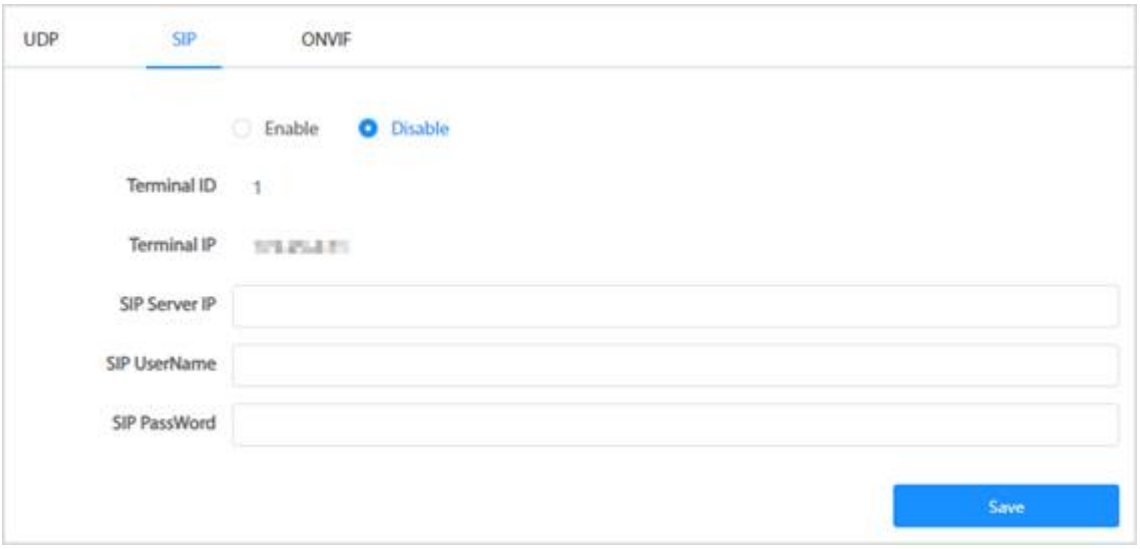
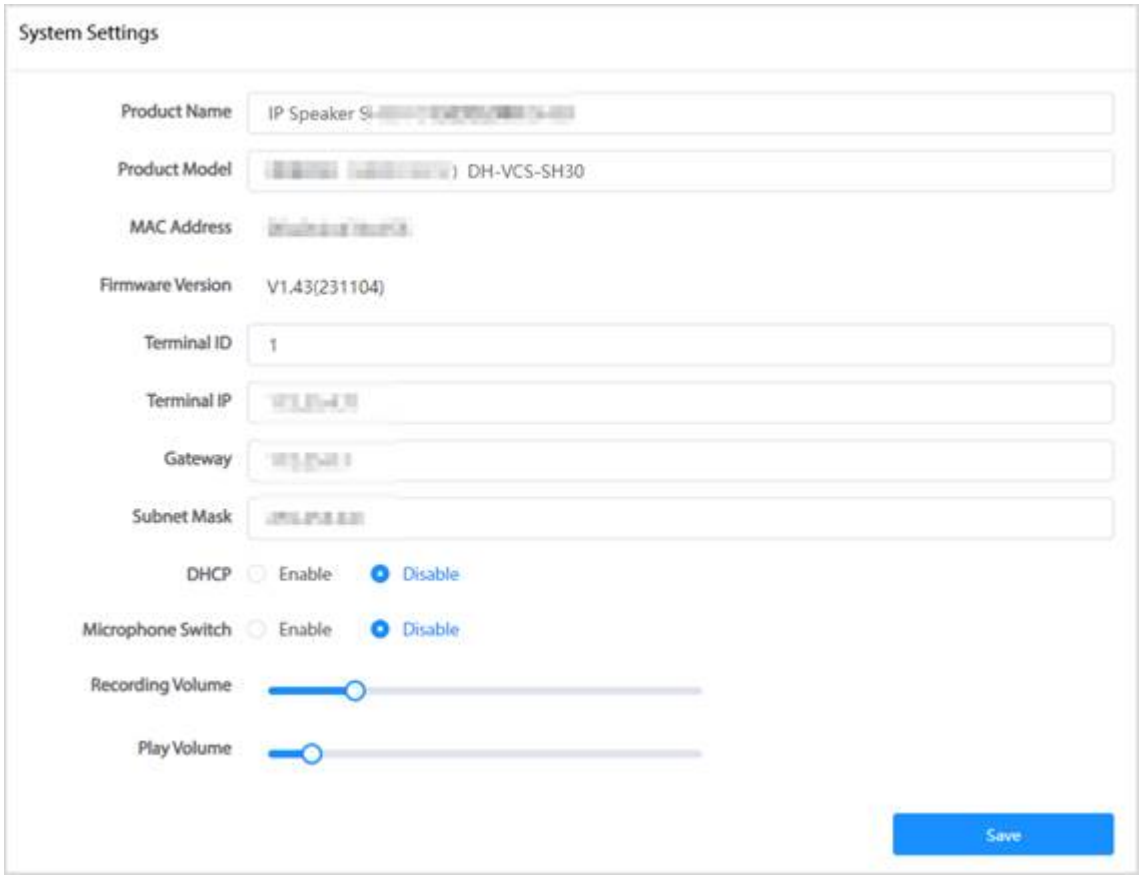


Figure 2-7 ONVIF

2.6 System Settings

Select **System Settings**, and then you can configure the parameters of the system. After that, click **Save** to save the configurations.

Figure 2-8 System settings



2.7 Firmware Update

Firmware upgrade can improve the performance and functions of the speaker.

Procedure

Step 1 Select **Firmware Update**.

Step 2 Click **Choice** to select update file.

Figure 2-9 Select update file

The firmware version must be matched with the device. Otherwise, the device might not be able to work, please be advised.

Step 3 Click **Update**.

2.8 System Management

Select **System Management**, and then you can reboot the speaker or restore factory settings.

Figure 2-10 System management

Appendix 1 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: 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 repeating characters, such as 111, aaa, etc.

2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.

2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.

4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

   It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).