Master Station

Quick Start Guide

V1.0.0
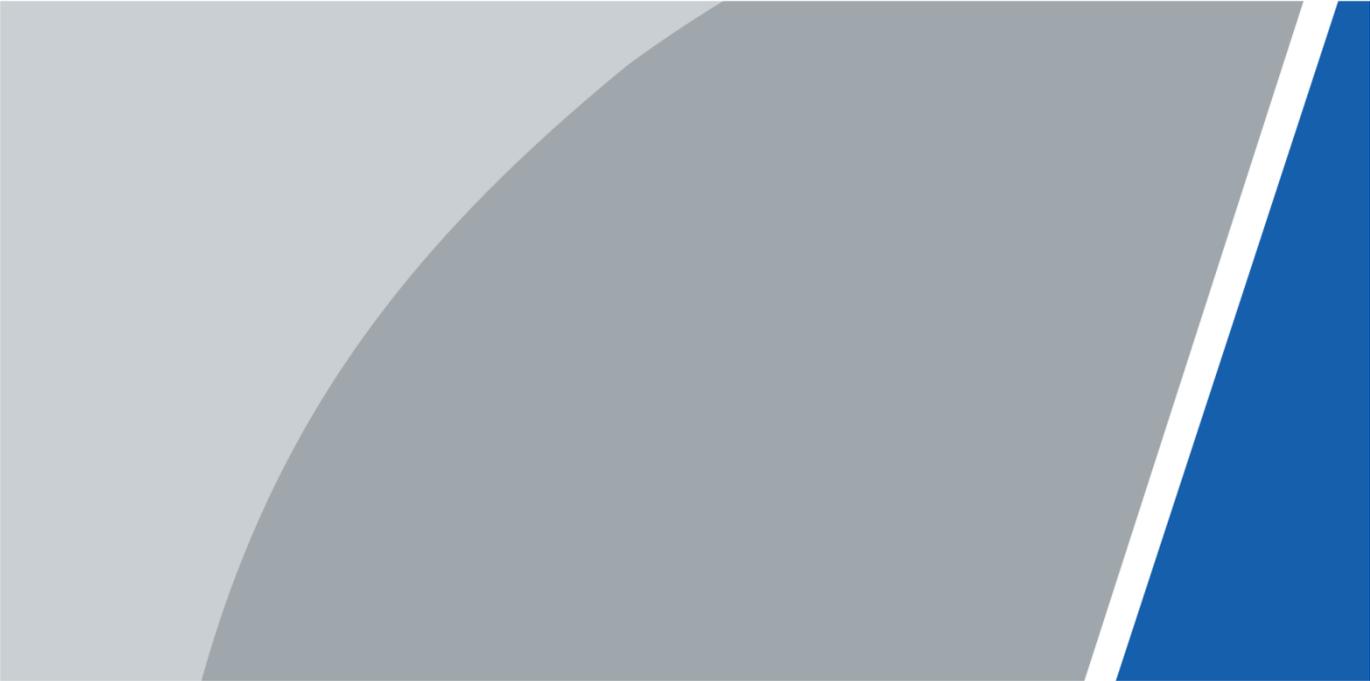
Foreword

General

This manual introduces basic operations of the master station.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
⚠️ **CAUTION**	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
📖 **Note**	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release	March 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

The following description is the correct application method of the master station. Read the Guide carefully before use, in order to prevent danger and property loss. Strictly conform to the Guide during application and keep it properly after reading.

Operating Requirement

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- The device shall be used with screened network cables.

Power Requirement

- The product shall use electric wires (power wires) required by the region where the device will be used.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.

⚠️

- Risk of explosion if the battery is replaced by an incorrect type.
- Do not throw or immerse into water, heat to more than 100℃ (212℉), repair or disassemble, leave in an extremely low air pressure environment or extremely high-temperature environment, crush, puncture, cut or incinerate.
- Dispose of the battery as required by local ordinances or regulations.

Table of Contents

1 Overview

1.1 Introduction

- You can have two-way video call with indoor monitors (VTH), door stations (VTO), and fence stations.
- You can watch videos captured by IP cameras, door stations (VTO), and fence stations on the master station.
- Unlock doors remotely.
- You can send emergency calls to the master station through indoor monitors (VTH) and door stations (VTO).

1.2 Features

- Easy operation; no need to be installed; bracket 0–45°adjustable.
- Support multiple monitoring devices; at most 4 1080P channels.
- Capacitive touch screen 10 inch LCD, human-computer interaction.
- Two calling modes: Hands-free and using handset.
- SD card expansion
- 1 HDMI output port; max resolution 1024×600.

1.3 Appearance

The VTS can be placed on the desk through the bracket. The bracket angle (0–45°) is adjustable.

Front Panel

Figure 1-1 Appearance
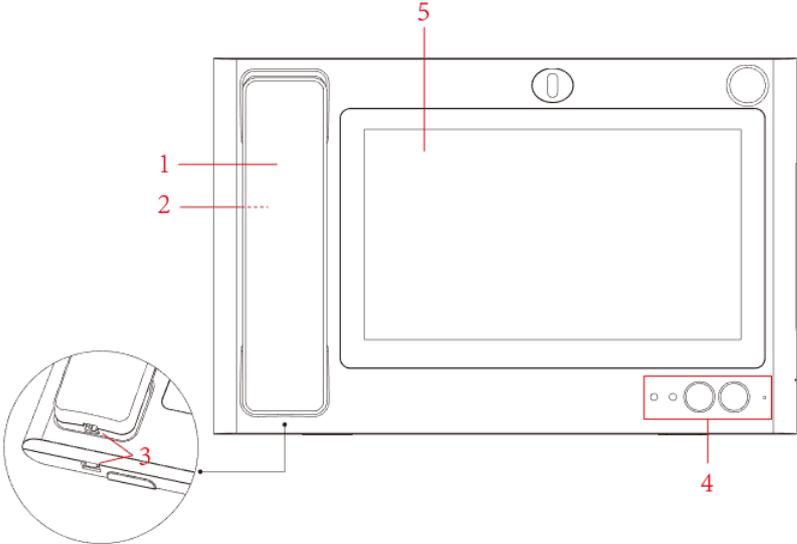
Table 1-1 Front panel description

| No.	Parameter	Description
1	MIC	Converts sound into an electrical signal.
2	Speaker	Outputs sound.
3	Telephone Port	Connected to master station and MIC.
4	Indicator	From left to right: ● Power indicator If the indicator is on, it indicates that the device is powered on. If the indicator is off, the device is not connected to the power supply. ● Information indicator If the indicator light is on, it indicates that the device has a missed call. If the indicator light is off, the missed call has been processed or there are no missed calls. ● Unlock button When you are making calls, watching videos, or talking to others through the VTS, press the unlock button, you can remotely open doors. ● Hands-free button You can select hands free mode or handset mode. ● Built-in MIC Input sound.
5	Display and Touch	Screen and touch area.

Rear Panel

Figure 1-2 Rear panel
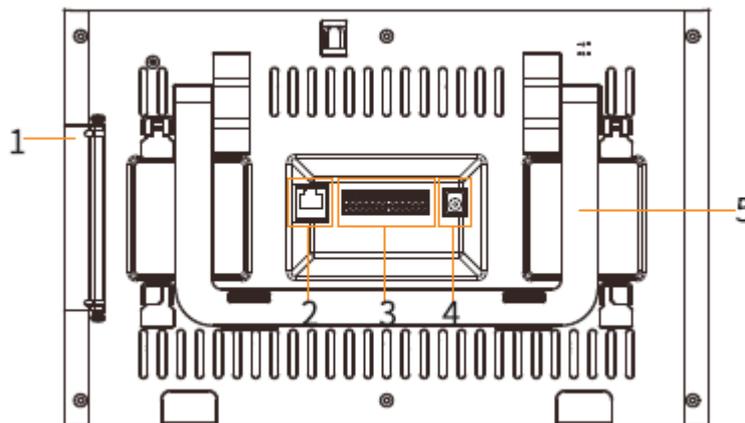
Table 1-2 Description of rear panel

No.	Parameter	Description
1	Port	● HDMI video transmission port, for video transmission only. ● USB port. ● USB port. ● SD card slot.

| No.	Parameter	Description
2	Network Port	Used to connect RJ-45 cable.
3	12-pin Port (Reserved)	Ports from left to right are: ● Power output port. ● GND. ● Alarm input port 1. ● Alarm input port 2. ● Alarm input port 3. ● Alarm input port 4. ● Power input port. ● GND. ● RS-485A port. ● RS4-85B por. ● Alarm output port NO. ● Alarm output port COM.
4	Power Port	DC 12V power.
5	Bracket	Place VTS on the desk. You can adjust the bracket angle to an appropriate position.

2 Wiring

⚠️

- Use the power adapter provided for you. Do not use other power adapters.
- Before turning on the VTS, make sure that all cables are correctly connected. If the VTS is working normally, the indicator light will be in red.

Figure 2-1 Cable connection
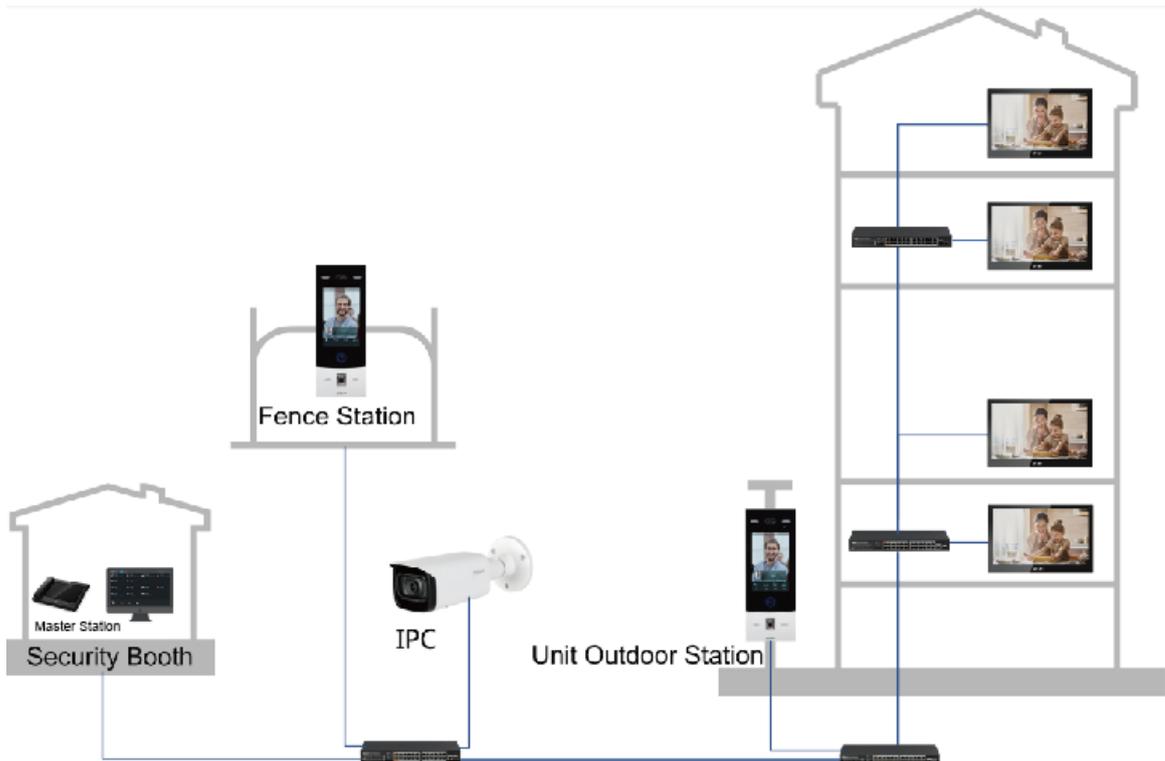
3 Operation

3.1 Initialization

For the first time use, you need to set password and email. The password is used to enter the **Advance Login** interface.

Figure 3-1 Initialization
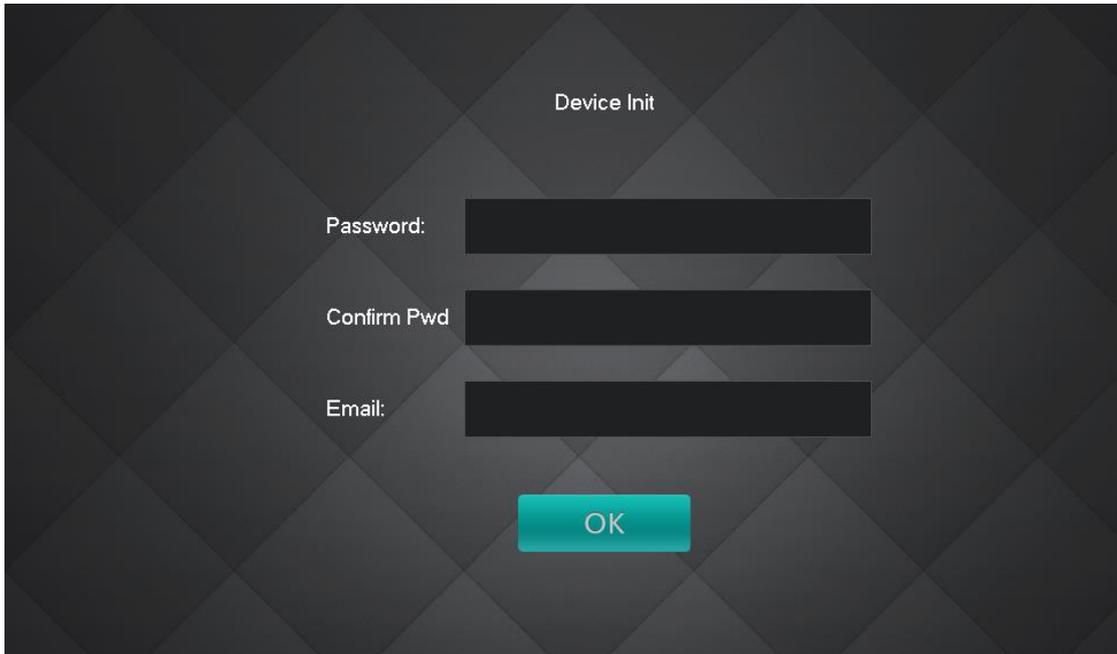
□□

- If you forget the **Advance Login** password, you can reset the password with the email you entered here.
- The password should be 6 numbers.

3.2 Login

Enter the VTS login password (123456 by default and cannot be modified), and then tap **OK**.

Figure 3-2 Login
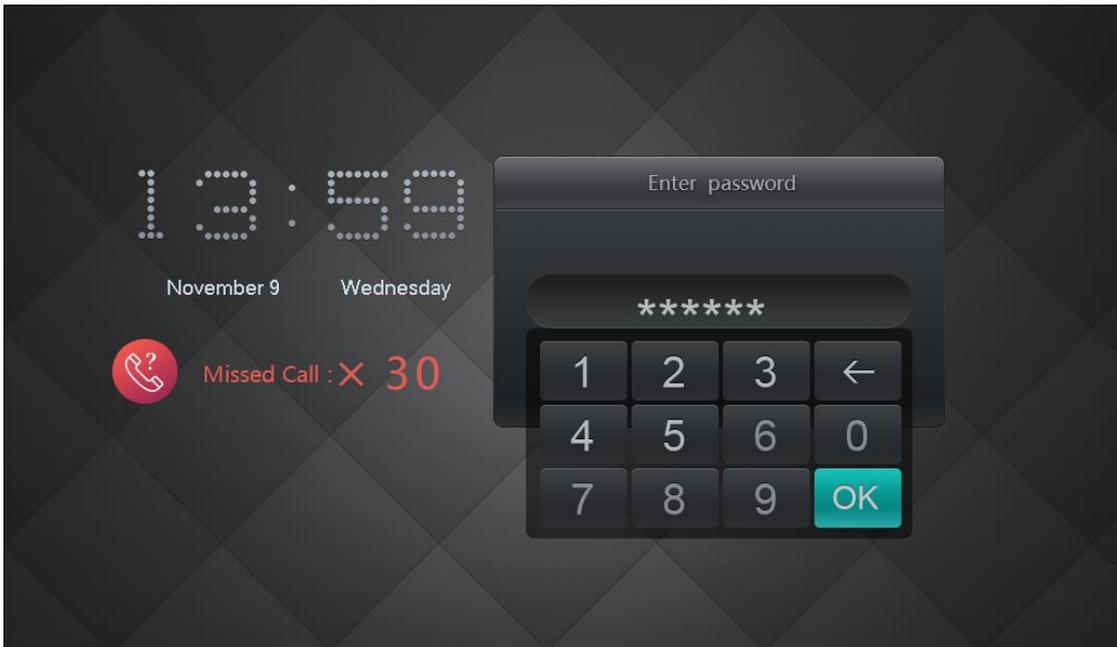

3.3 Resetting Password

If you forget the password for logging in to the **Advanced Login** interface, you can rest the password through the email address you entered on the **Initialization** interface.

You need to enable the password resetting function. See "3.8 Resetting Messages".

Figure 3-3 Advanced login
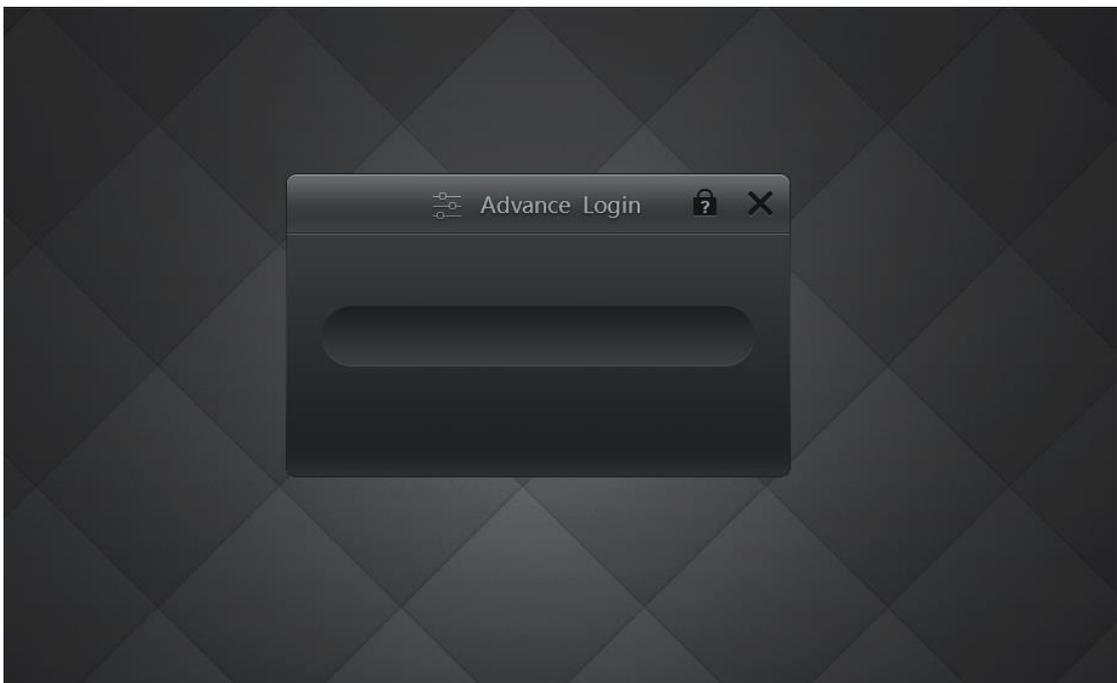
Step 1 Tap on the **Advance Login** interface.

Step 2 Tap **OK**.

Figure 3-4 Reset password
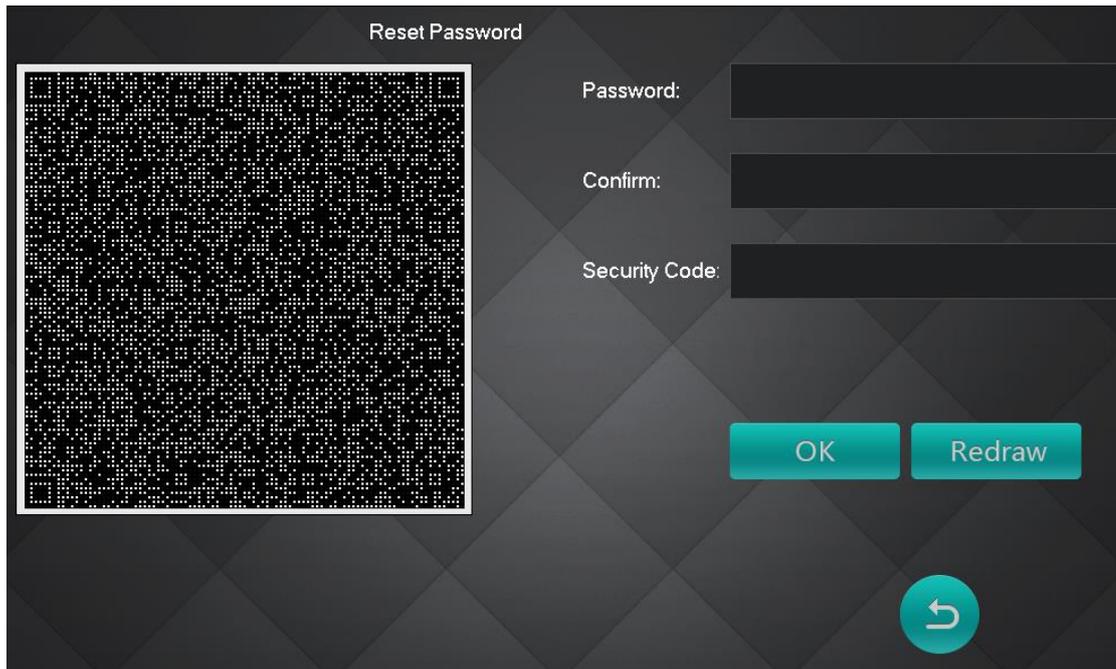
Step 3 Scan the QR code on the interface with any app that is with scanning function.
A string will be displayed.
Step 4 Send the string to support_gpwd@htmicrochip.com with your email address you set on
the **Initialization** interface.
A security code will be sent to your email address.
Step 5 Enter the new password, confirm password, and security code.
The password is reset.

3.4 Local Settings

You can set device No., IP address, subnet mask, and gateway by selecting **Setting >
Advance Config > Config**.

- The **Advance Login** password is set during initialization or can be modified on the **Reset
MSG** interface.
- Make sure that the IP address you entered is in the same network segment as door
stations and indoor monitors; otherwise the devices cannot communicate with each other.

Figure 3-5 Local settings
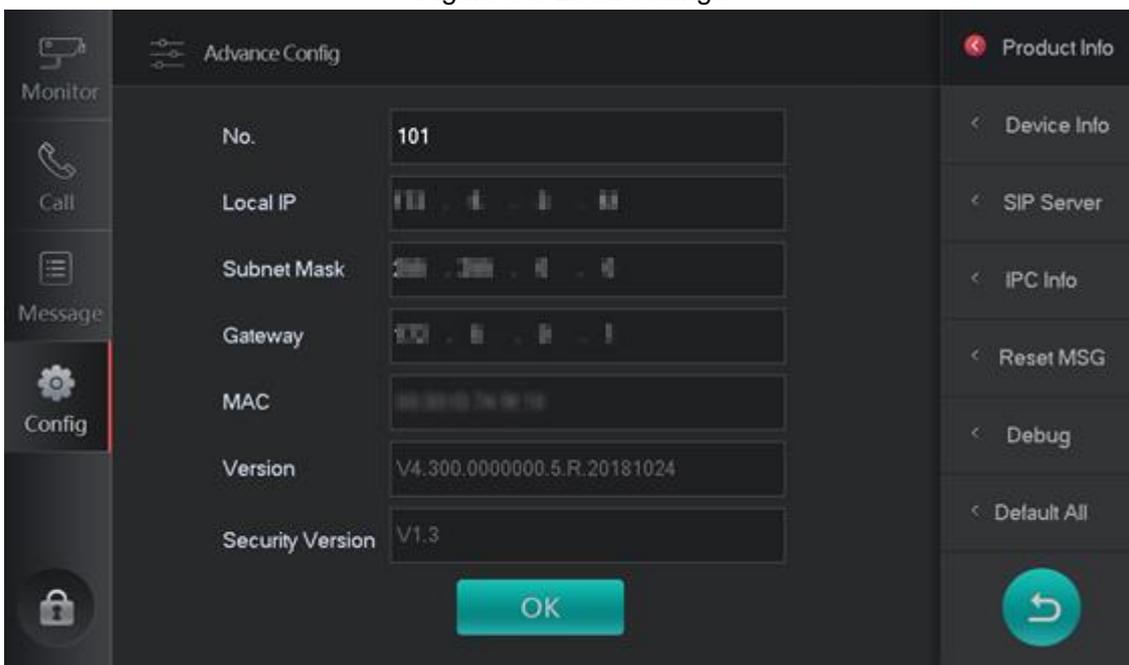
3.5 Adding Door Stations (VTO)/Fence Station

You can add door stations (VTO) and fence stations one by one or in batches by selecting **Config > Advance Config > Device Info**.

⚠️

Before adding door stations and fence stations, make sure that they are connected to the power source and are in the same network segment.

● Add one door station (VTO)

Step 1   Select **Setup > Advance Config > Device Info**.

Figure 3-6 Device information
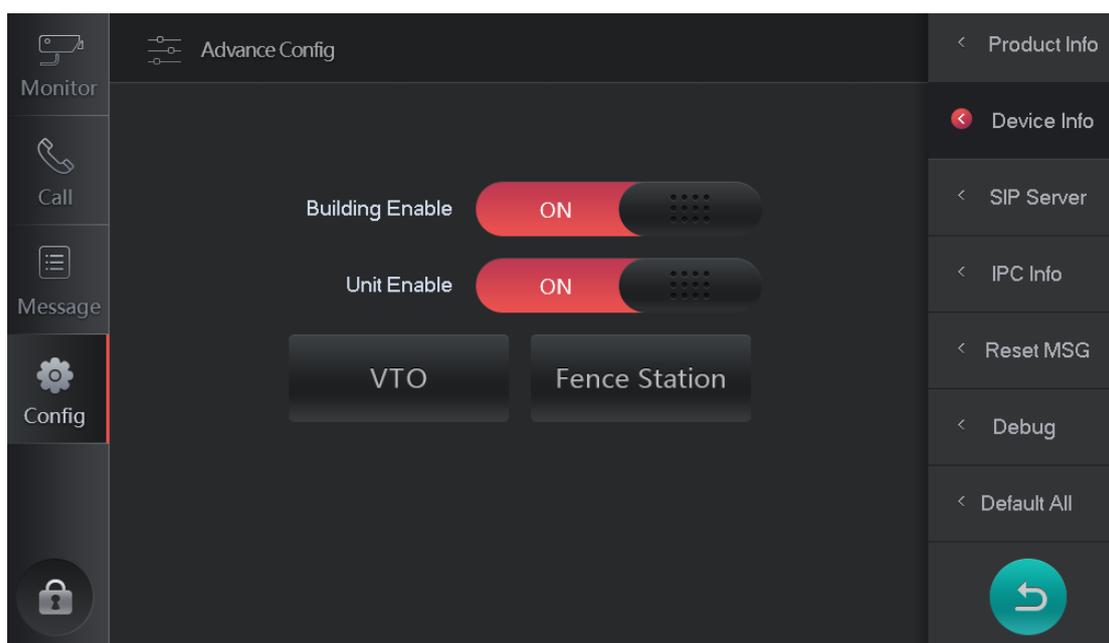
Step 2 Tap **VTO**.

Step 3 Tap **Add**.

Figure 3-7 Add one device

Step 4 Enter name, middle number, IP address, username, and password, and then turn on the **Enable Status**.

Step 5 Tap **OK**.

"**Please wait**" is displayed. Tap **OK** to continue adding door stations (VTO). The added door stations (VTO) can be seen by selecting **Monitor > VTO**.

●   Add door stations (VTO) in batches

Step 1 Select **Config > Advance Condig > Device Info**.

Step 2 Tap **VTO**.

Step 3 Tap **Add**.

Step 4 Tap **Batch Add**.

Figure 3-8 Add door stations (VTO) in batches
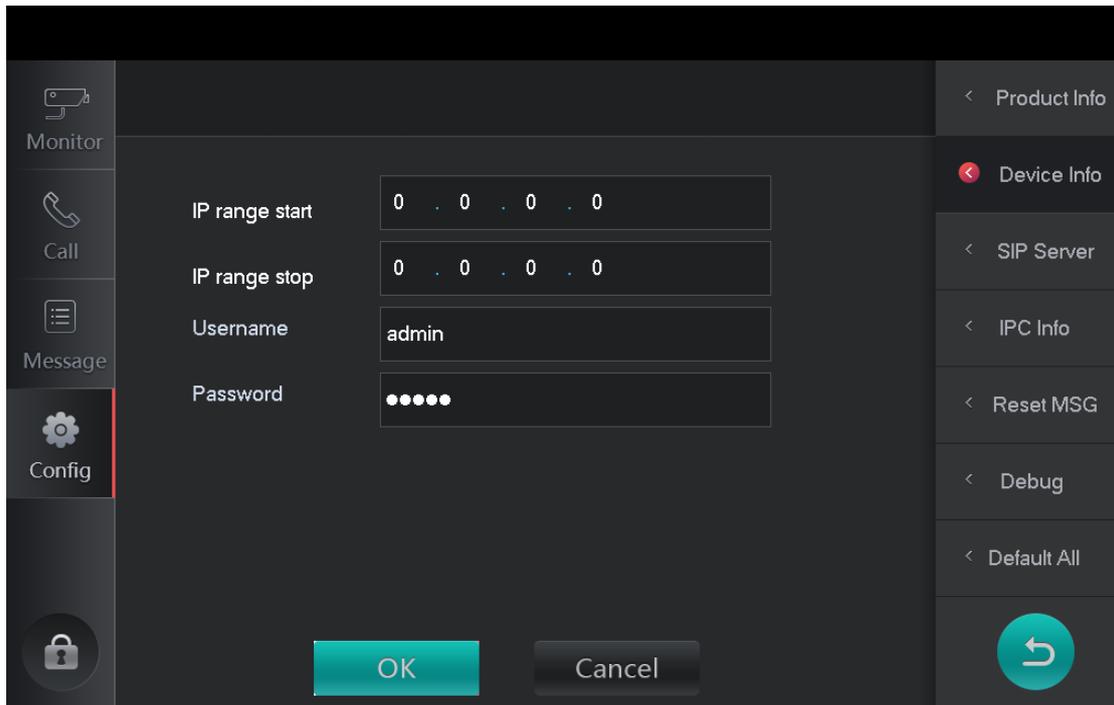
Step 5 Enter starting IP, ending IP, username, and password.
Step 6 Tap **OK**.
"**Please wait**" is displayed. Tap **OK** to continue adding door stations (VTO). The added door stations (VTO) can be seen by selecting **Monitor > VTO**.

3.6 Setting SIP Server

Step 1 Select **Config > Advance Config > SIP Server**.

Figure 3-9 Setting SIP server
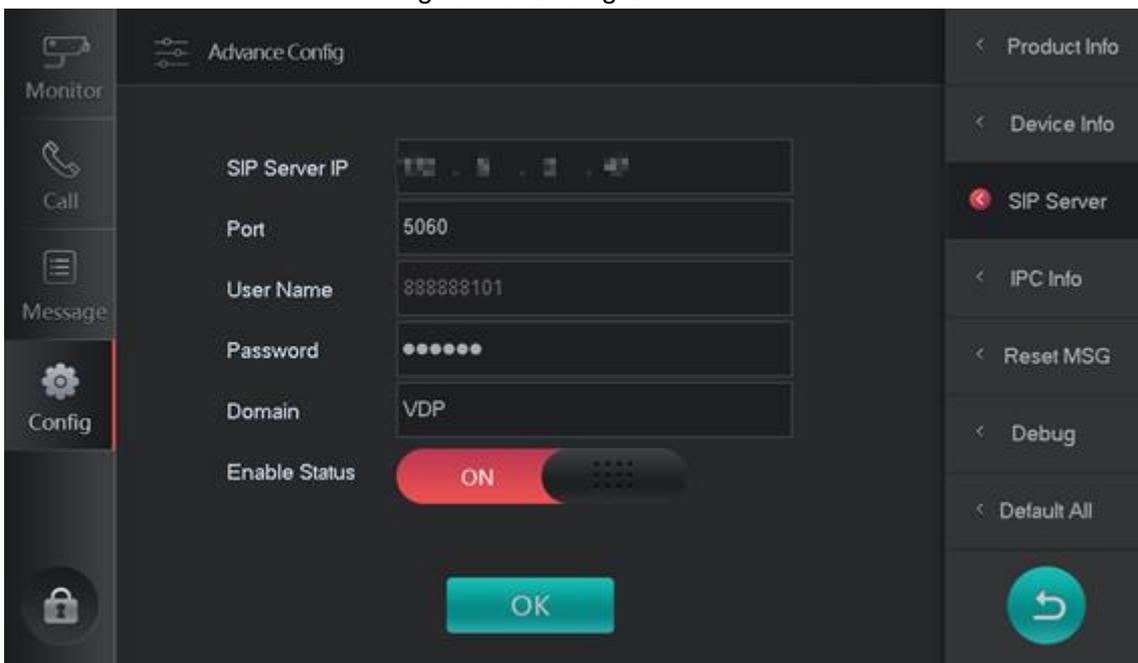
Step 2 Set parameters.

Table 3-1 Setting SIP server.

Parameter	Description
SIP Server IP	Enter the SIP server IP address.
Port	● When the platform works as SIP server, network port is 5080. ● When VTO works as SIP server, network port is 5060.
User Name	No need to modify this. Keep the default value.
Password	123456 by default.
Domain	Keep the default value.

Step 3 Select **ON** for the **Enable Status**.

Step 4 Tap **OK**.

3.7 Adding IP Cameras

You can add up to 32 IP cameras. You can watch monitoring videos captured by the IP cameras.

Step 1 Select **Config > Advance Config > IPC Info**.

Figure 3-10 Adding IP cameras
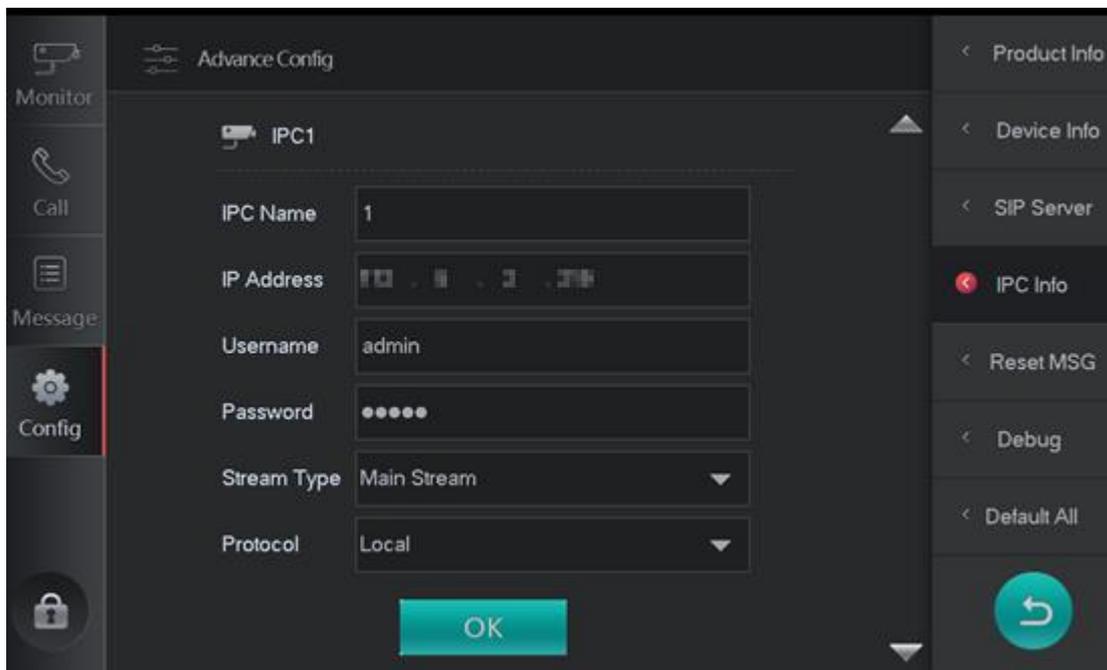
Step 2 Configure parameters.

Table 3-2 Adding IP cameras

Parameter	Description
IPC Name	Enter the name of the IP camera.
IP Address	Enter IP address of the IP camera.
User Name	Username and password used to login IPC web interface.
Password	
Stream Type	● Main Stream: Large stream, high definition, occupies high bandwidth, suitable for local storage. ● Sub Stream: Fluent videos, occupies low bandwidth, suitable for low bandwidth network transmission.

Parameter	Description
Protocol	Two options: Local protocol and Onvif protocol. Select as needed.

Step 3 Tap **OK**.

The IP cameras added can be seen by selecting **Monitor > IPC**.

📖

You can tap ✉ to continue adding IP cameras.

3.8 Resetting Messages

You can modify the email address that you entered during initialization to reset password.

Step 1 Select **Config > Advance Config > Reset MSG**.

Step 2 Enter a new email.

Step 3 Tap the **OFF** button to enable the password resetting function.

Figure 3-11 Resetting password
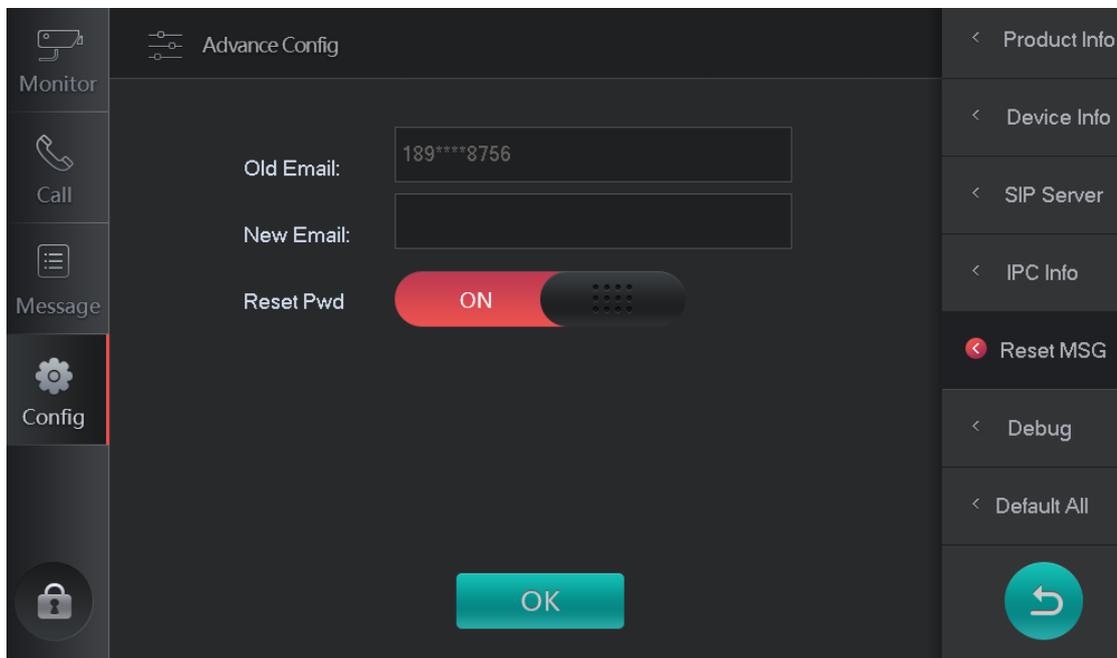
Step 4 Tap **OK**.

3.9 Debug

The debug function is only for engineers.

Step 1 Select **Config > Advance Config > Reset MSG**.

Step 2 Tap **OFF** to enable the SSH function.

3.10 DefaultAll

You can restore the VTS to factory settings by selecting **Config > Advance Config > DefaultAll**. After the master station is restored to default settings, the VTS will restart.

Figure 3-12 Default
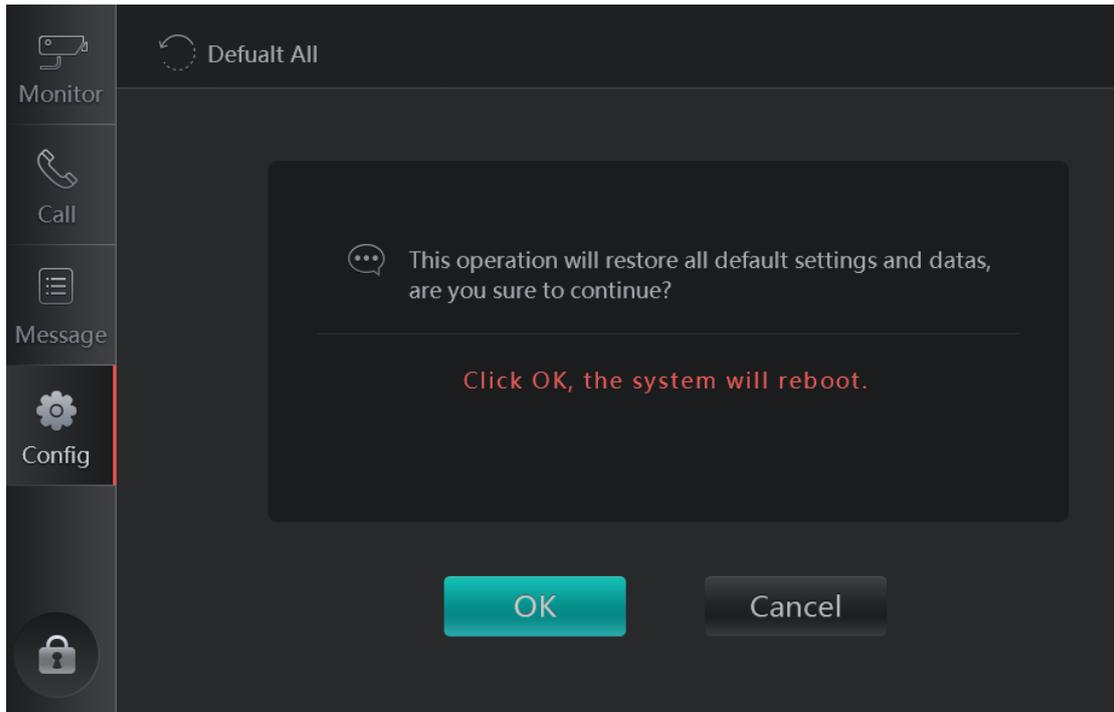
4 Making Calls

You can call indoor monitors (VTH) through the VTS.

Figure 4-1 Call indoor monitors
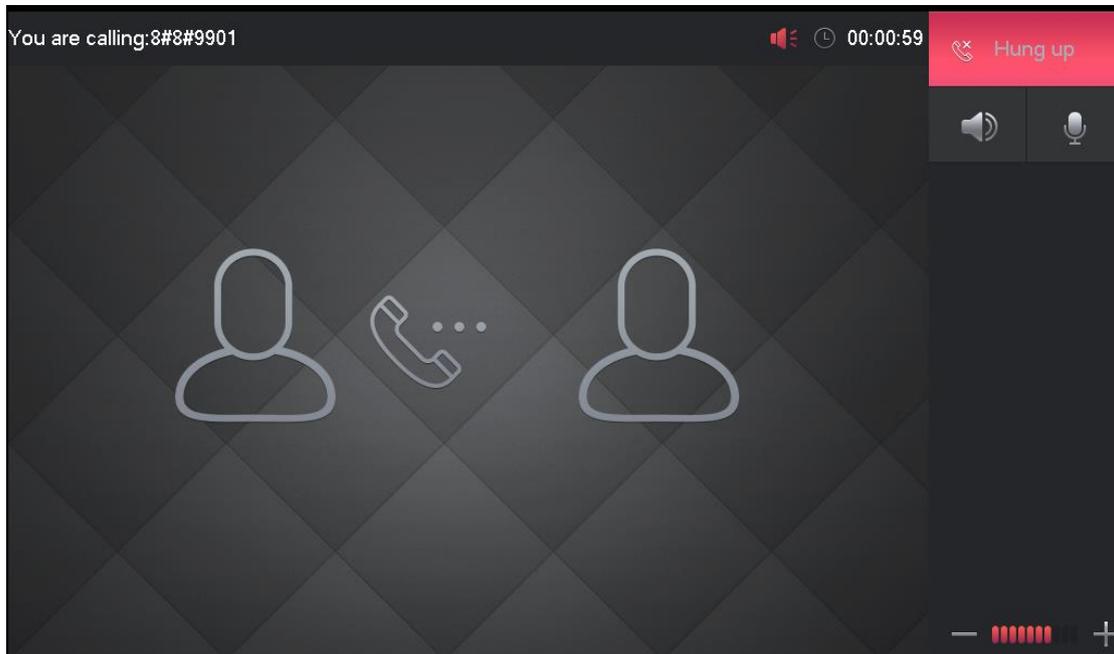
Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong 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; 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.;

2. **Update Firmware and Client Software in Time**
   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

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

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. 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.

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.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers

between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

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

7. **Enable Whitelist**

   We suggest you to enable whitelist 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 whitelist.

8. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. **Disable Unnecessary Services and Choose Secure Modes**

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

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

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

11. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. **Network Log**

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

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network,

so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.