Digital VTH

Quick Start Guide



V1.0.1

Foreword

General

This document mainly introduces structure, installation process and configuration of the product.

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
 **TIPS**	Provides methods to help you solve a problem or save you time.
 **NOTE**	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.1	Revised "Important Safeguards and Warnings".	December 2022
V1.0.0	First release.	August 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 regions. For detailed information, see 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, please refer to our 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 occurred when using the device.
- If there is any uncertainty or controversy, please refer to our 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.

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.
- Transport, use and store the device under allowed humidity and temperature conditions.
- If the device is powered off for longer than a month, it should be placed in its original package and sealed. Make sure to keep it away from moisture, and store it 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 disassemble the device without professional instruction.

Installation Requirements



- 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.
- Improper use of the battery might result in a fire or 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.
- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- 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.

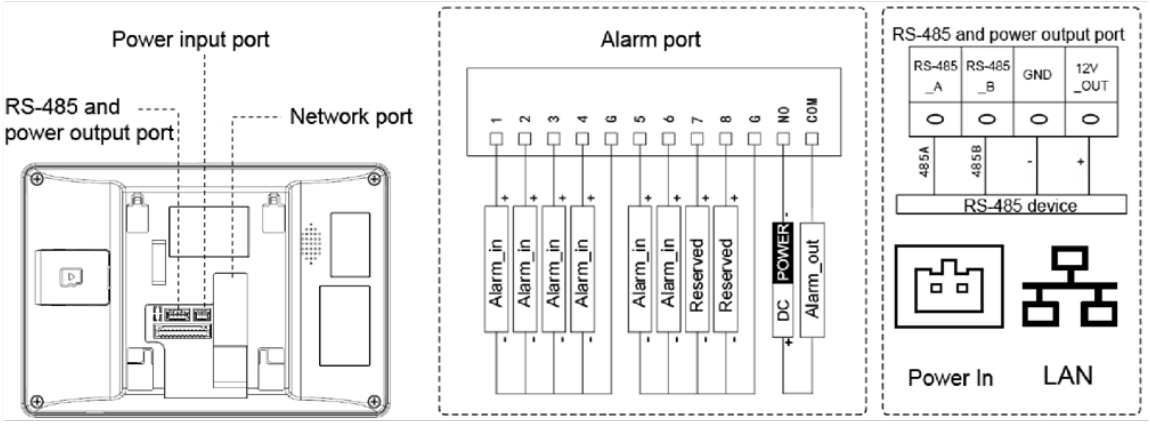
Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Rear Panel Port 1
1.1 VTH5421H 1
1.2 VTH5422H 1
2 Installation and Commissioning 2
2.1 Installation 2
2.2 Preparations 2
2.3 Commissioning 6
2.3.1 VTO Calls VTH 6
2.3.2 VTH Monitors VTO 7
Appendix 1 Cybersecurity Recommendations 9

1 Rear Panel Port

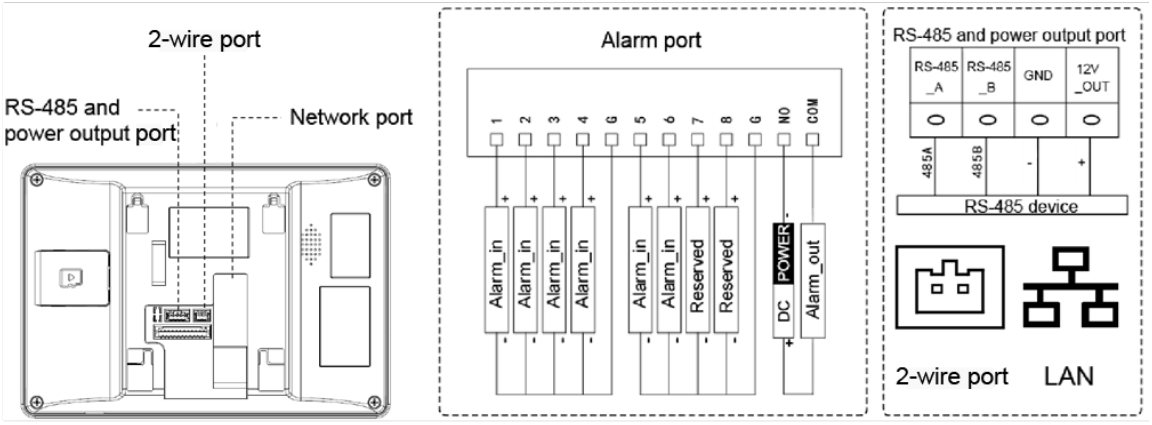
1.1 VTH5421H

Figure 1-1 Rear panel of VTH5421H



1.2 VTH5422H

Figure 1-2 Rear panel of VTH5422H



2 Installation and Commissioning

2.1 Installation

⚠

- Do not install VTH in harsh environment with condensation, high temperature, dust, corrosive substance and direct sunlight.
- In case of abnormality after powering on, unplug network cable and cut off power supply at once. Power on after troubleshooting.
- Installation and debugging should be done by professional teams. Do not dismantle or repair by yourself in case of device failure. Contact after-sales service.
- Device central point height should be 1.4 m–1.6 m above the ground (this device is only suitable for mounting at height ≤ 2 m).

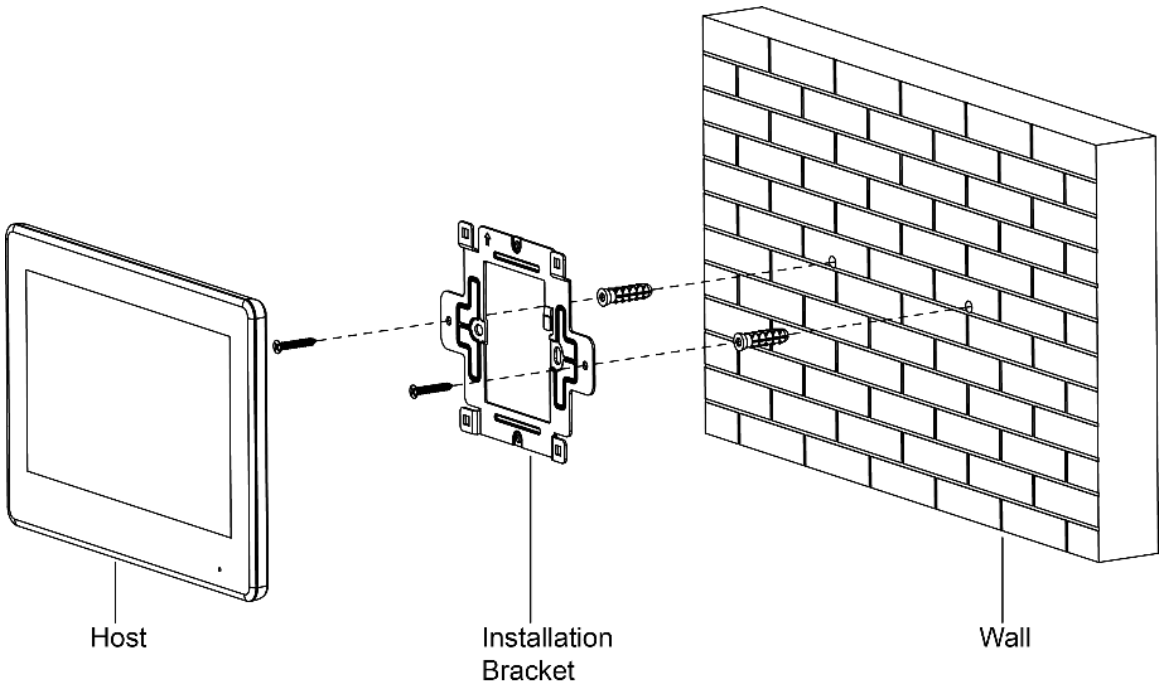
Directly install the device with a bracket onto a wall, which is suitable for all types of devices.

Step 1 Drill holes in the wall according to hole positions of the installation bracket.

Step 2 Fix the installation bracket on the wall with screws.

Step 3 Put the device into installation bracket from top down.

Figure 2-1 Surface installation



2.2 Preparations

Before commissioning, check whether the following work has been completed.

- Power on the device only after there is no short or open circuit.
- Plan IP and number (works as a phone number) for each VTO and VTH.
- Confirm the location of the SIP server.
- Scan QR code on the cover for details.
- Set VTO info and VTH info on the web interface for every VTO, and set VTH info, network info and VTO info on every VTH.

VTH Settings

For first-time use, set up password and bind Email. Password is used to enter project setting interface, while email address is used to retrieve your password when you forget it.

Step 1 Power on the device, Select region and language, and tap **OK**.

Figure 2-2 Select region and language

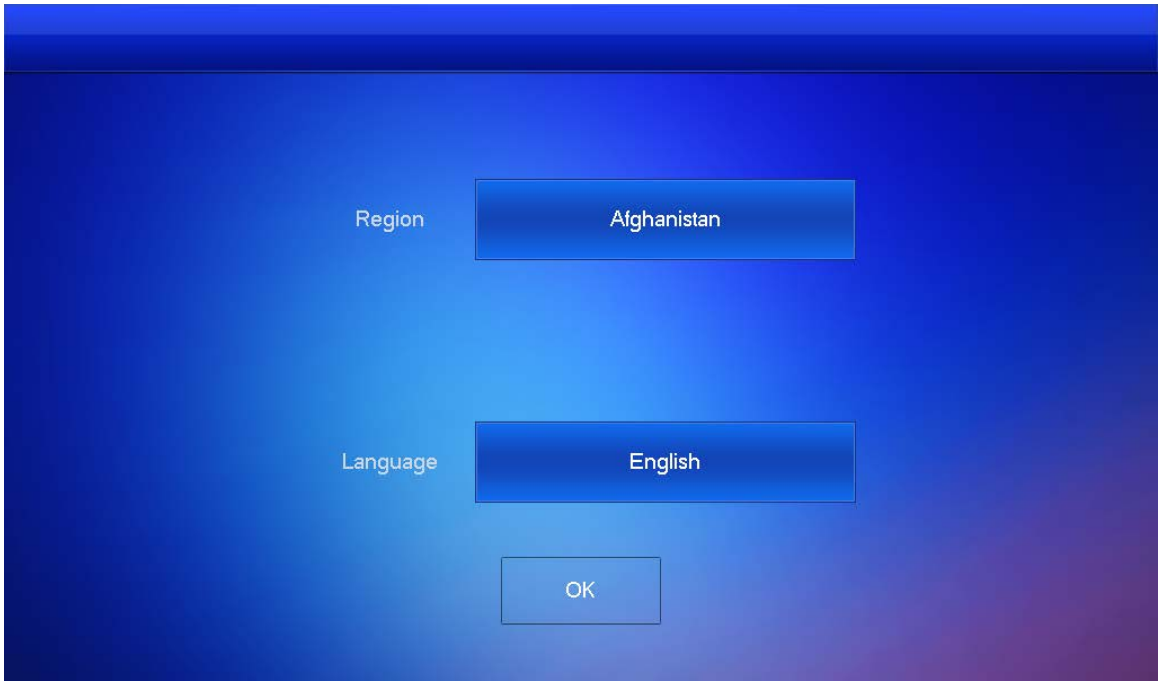
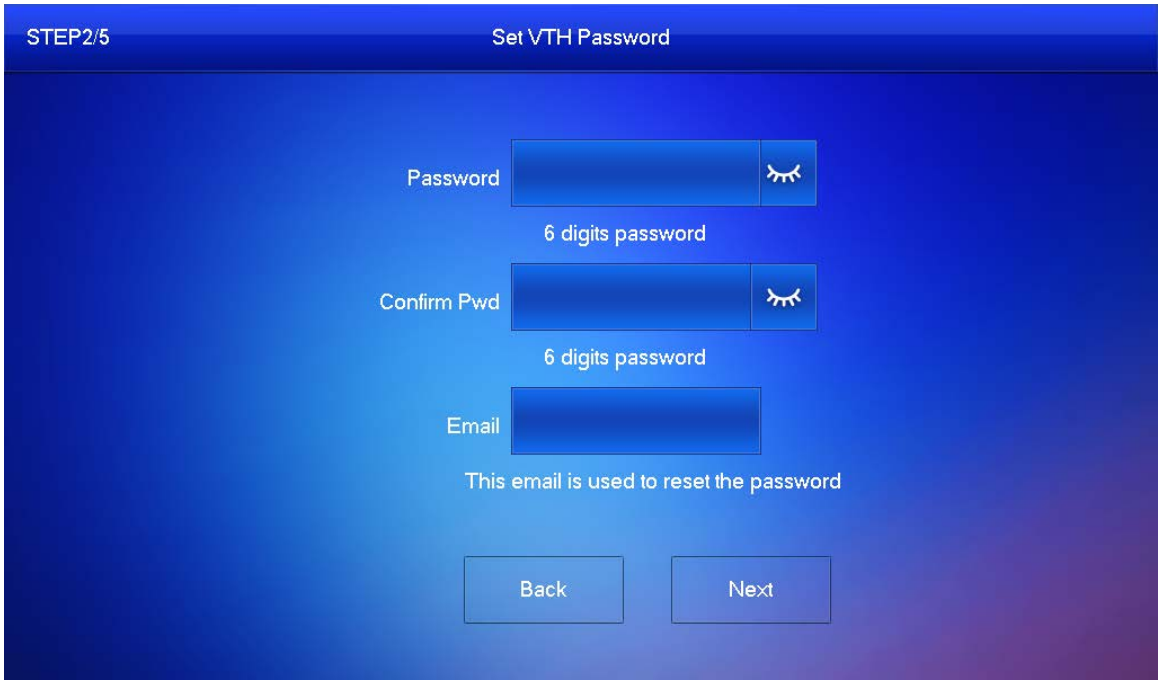


Figure 2-3 Set password for VTH



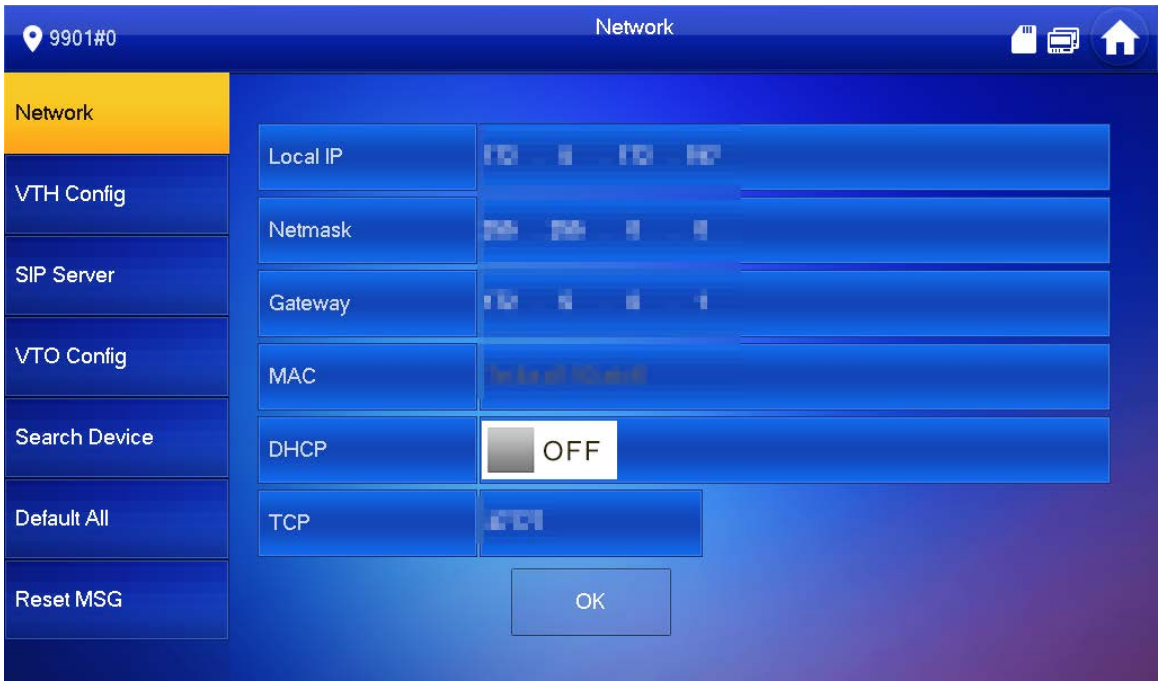
Step 2 Enter password and confirm it, enter email, and tap **Next**.

Step 3 Tap **Setting** for more than 6 seconds, enter the password set just now, and then tap **OK**.

Step 4 Tap **Network**. Enter local IP, netmask, and gateway, and then tap **OK**, Or tap OFF to enable DHCP function to obtain IP info automatically.

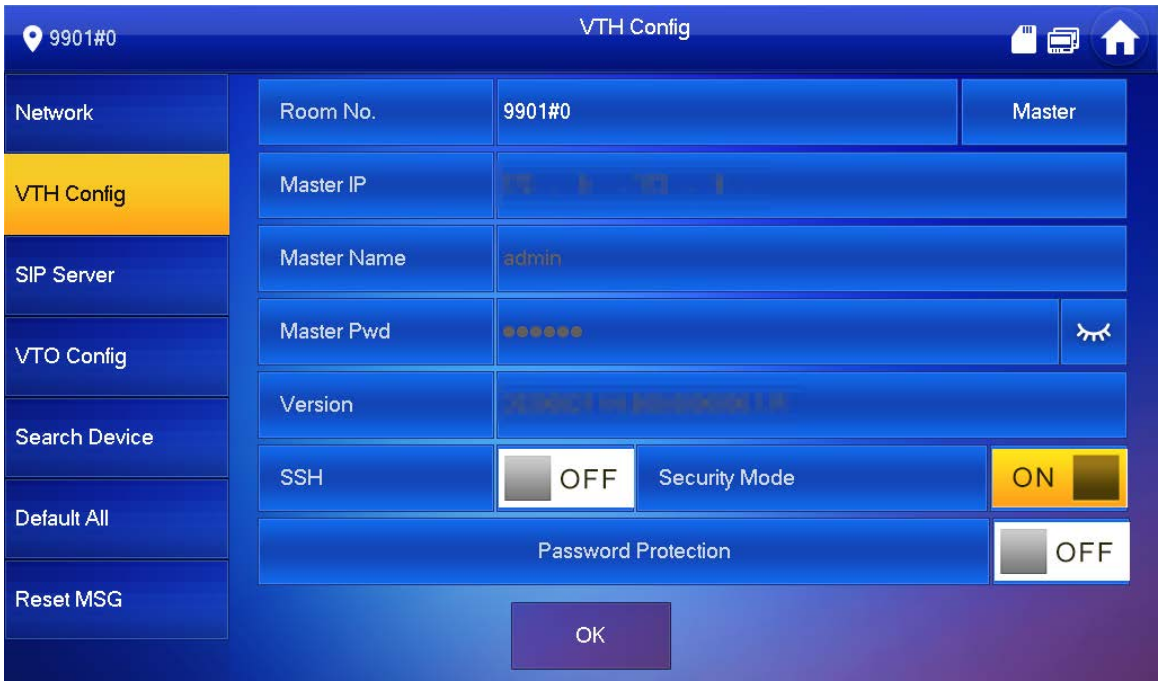
IP addresses of VTH and VTO should be in the same network segment. Otherwise, VTH cannot obtain VTO information after configuration.

Figure 2-4 Network



Step 5 Tap **VTH Config**.

Figure 2-5 VTH configuration



- Use as a main VTH.

Enter Room No. (such as 9901 or 101#0) and tap **OK**.

Room No. should be the same as VTH Short No., which is set when adding VTH on the web interface. Otherwise, it will fail to connect to VTO.

If there is extension VTH, room No. should end with #0. Otherwise, it will fail to connect to VTO.

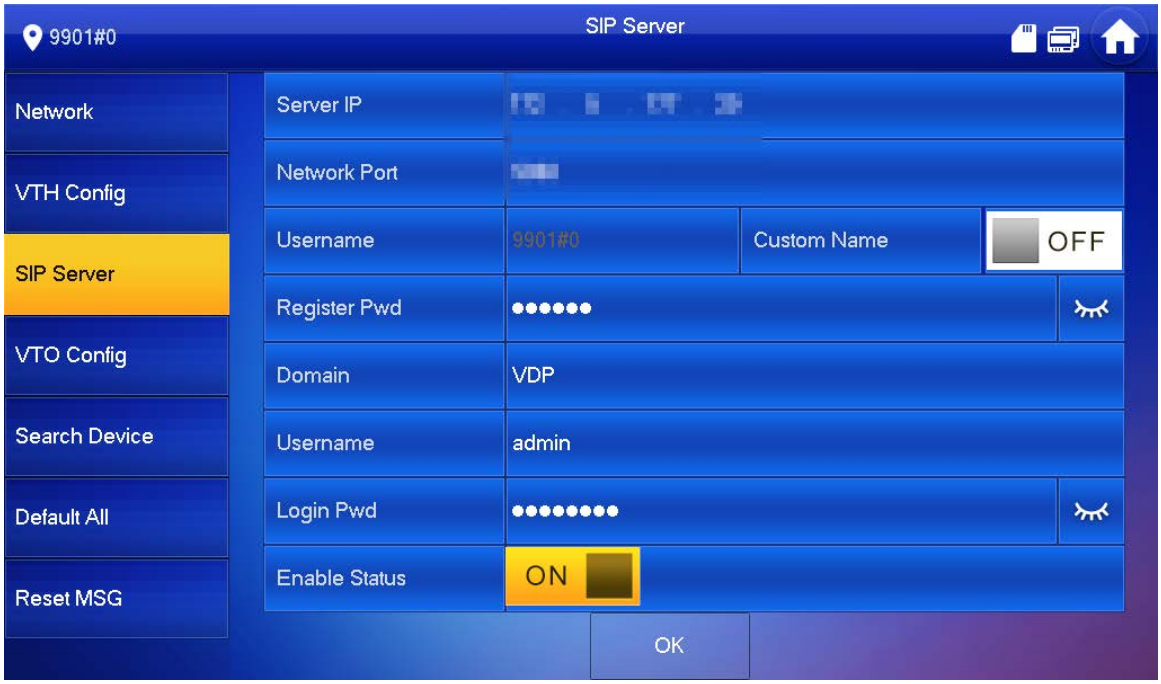
- Use as an extension VTH.

1) Tap **Master** and the icon switches to **Extension**.
2) Enter room No. (such as 101#1) and the IP address of main VTH.
   Default username is **admin**, and the password is the one set from previous step.

   Security mode is **On** by default, and you can keep the default status.
3) Tap **OK** to save the settings.

Step 6 Tap **SIP Server**.

Figure 2-6 SIP server



1) Set parameters of **SIP Server** by reference to Table 2-1.

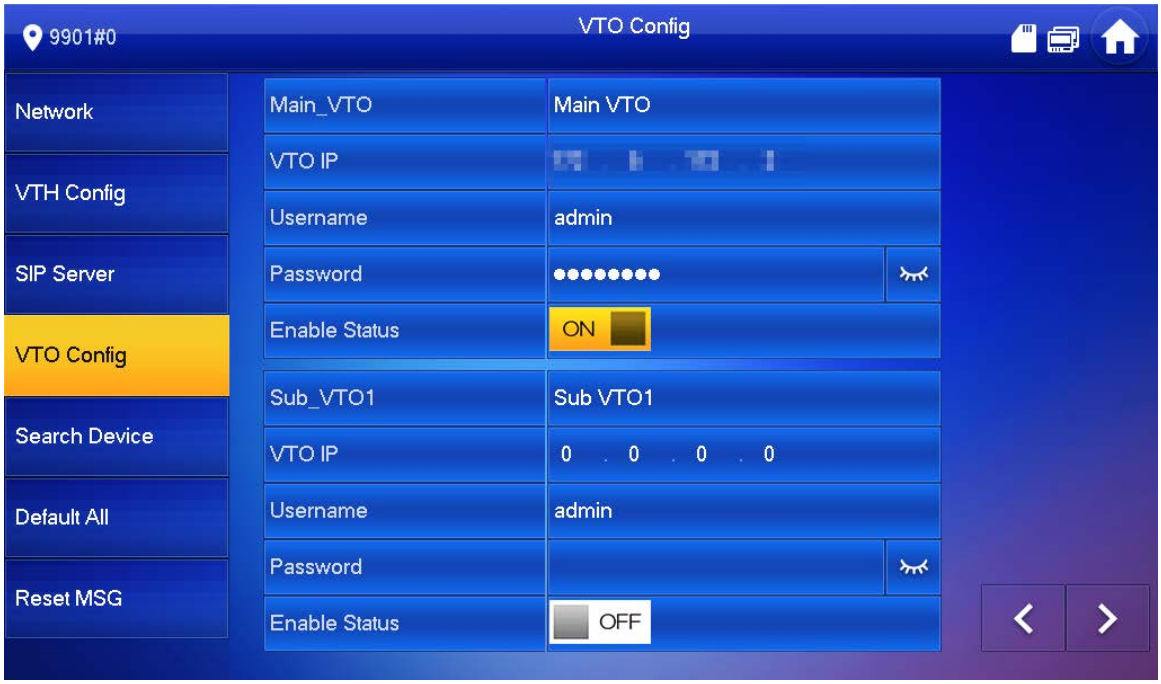
Table 2-1 SIP server

Parameter	Description
Server IP	• When the platform works as SIP server, server IP is the IP address of the platform. • When VTO works as SIP server, server IP is the IP address of the VTO.
Network Port	• When the platform works as SIP server, network port is 5080. • When VTO works as SIP server, network port is 5060.
User Name	Use default value.
Register Pwd	
Domain	Registration domain of SIP server, which can be empty. When VTO works as SIP server, registration domain of SIP server should be VDP.
Username	Username and password to log in to SIP server.
Login Pwd	

2) Set **Enable Status** to ON.
3) Tap **OK**.

Step 7 Tap **VTO Config**.

Figure 2-7 VTO configuration



Step 8 Add VTO.

- Add main VTO.

1) Enter main VTO name, VTO IP address, username and password.

2) Set **Enable Status** to ON.

Username and **Password** should the same as web login username and password of VTO. Otherwise, it will fail to connect.

- Add sub VTO.

1) Enter sub VTO name, sub VTO IP address, username, and password.

2) Set **Enable Status** to ON.

Tap / to turn page and add more sub VTOs.

2.3 Commissioning

2.3.1 VTO Calls VTH

Dial VTH room No. (such as 101) at VTO to call VTH. VTH pops up monitoring video and operating icons. See Figure 2-8.

The following figure means that SD card has been inserted into VTH. If SD card is not inserted, recording and snapshot icons are gray.

Figure 2-8 Call VTH from VTO



2.3.2 VTH Monitors VTO

VTH is able to monitor VTO or IPC. Take VTO as an example.

Select **Monitor > Door**. See Figure 2-9. Select the VTO to enter monitoring video. See Figure 2-10.

The following figure means that SD card has been inserted into VTH. If SD card is not inserted, recording and snapshot icons are gray.

Figure 2-9 Door

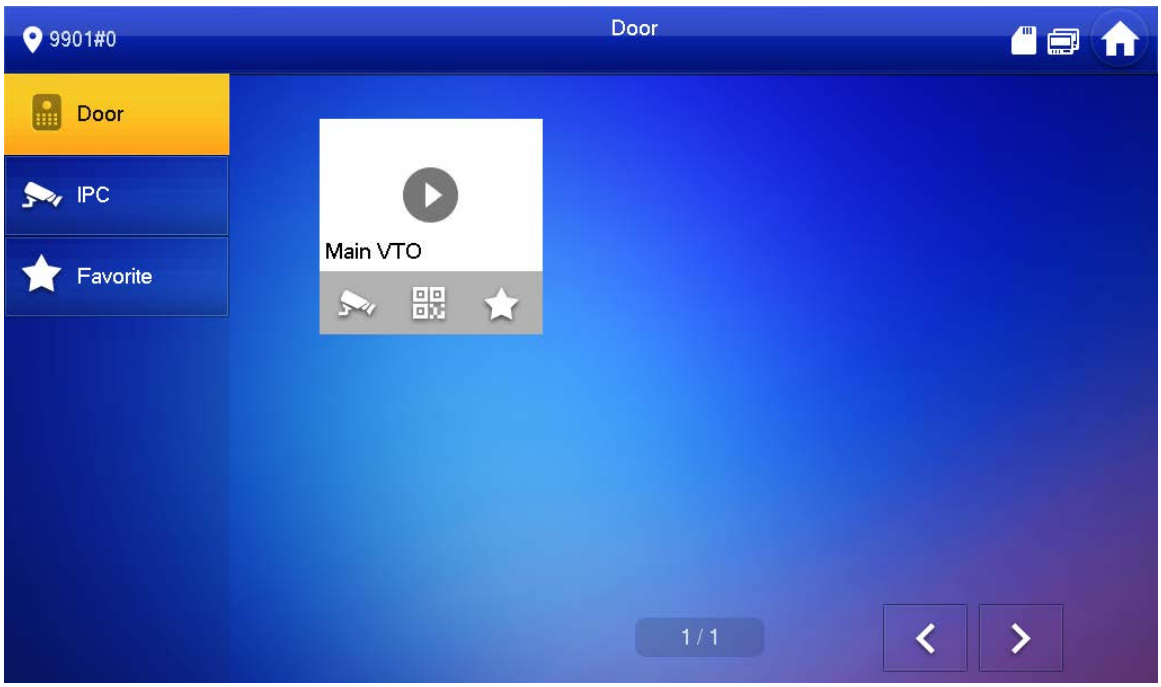
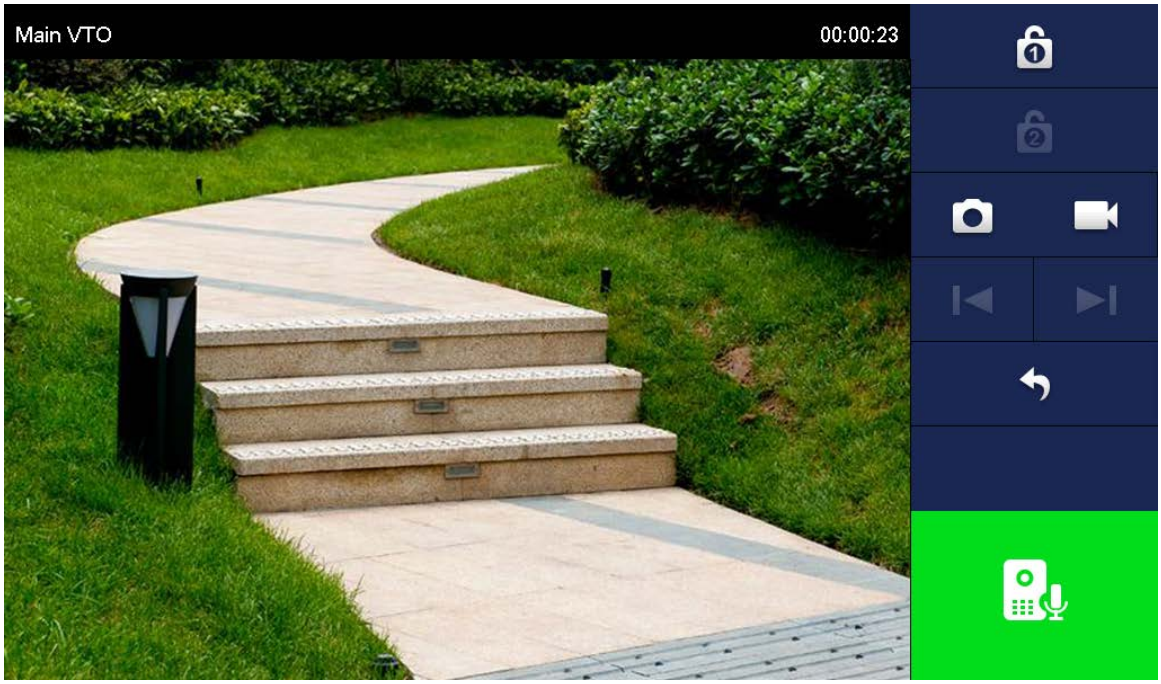


Figure 2-10 Monitoring video



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 device 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 device (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 device 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 device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. 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, unauthorized connection of removable device (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 device 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. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

9. **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.

10. **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.

11. **Secure Auditing**

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

12. **Network Log**

    Due to the limited storage capacity of the device, 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.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device 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.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.