Digital VTH (Version 4.2)

Quick Start Guide



V1.0.0

Foreword

General

This document mainly introduces the structure, installation and commissioning 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
V1.0.0	First release.	September 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 device. Please read the manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirements

- Do not expose the device to direct sunlight or heat source.
- Do not install the device in a humid or dusty area.
- Install the device horizontally at stable places to prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids.
- Install the device at well-ventilated places and do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device by yourself.
- The device should be used with screened network cables.

Power Requirements

- Use recommended power cables in the region under their rated specification.
- 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, please refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

Device Update

Do not cut off power supply during device update. Power supply can be cut off only after the device has completed update and has restarted.

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Structure 1
1.1 Front Panel 1
1.2 Rear Panel Port 2
1.2.1 VTH5221 Series /VTH5241 Series 2
1.2.2 VTH5221E-H/VTH5221EW-H 2
1.2.3 VTH15XX-S2 Series B/CH & VTH15XX Series B/CH 2
1.2.4 VTH5222CH/VTH5222CHW-2 3
1.2.5 VTH1660CH 4
1.2.6 VTH2221A/VTH2221A-S2 4
1.2.7 VTH2421FB/VTH2421FS 5
2 Installation and Commissioning 6
2.1 Installation 6
2.1.1 Wall-mounted 6
2.1.2 Installation with 86 Box 6
2.1.3 Desktop Installation with Bracket 7
2.2 Preparations 8
2.2.1 VTO Settings 8
2.2.2 VTH Settings 12
2.3 Commissioning 17
2.3.1 VTO Calls VTH 17
2.3.2 VTH Monitors VTO 18
Appendix 1 Cybersecurity Recommendations 20

1 Structure

1.1 Front Panel

Different models of devices may have different front panel dimensions and key types, but keys or indicators with the same name or icon have the same function.

Table 1-1 Front panel description

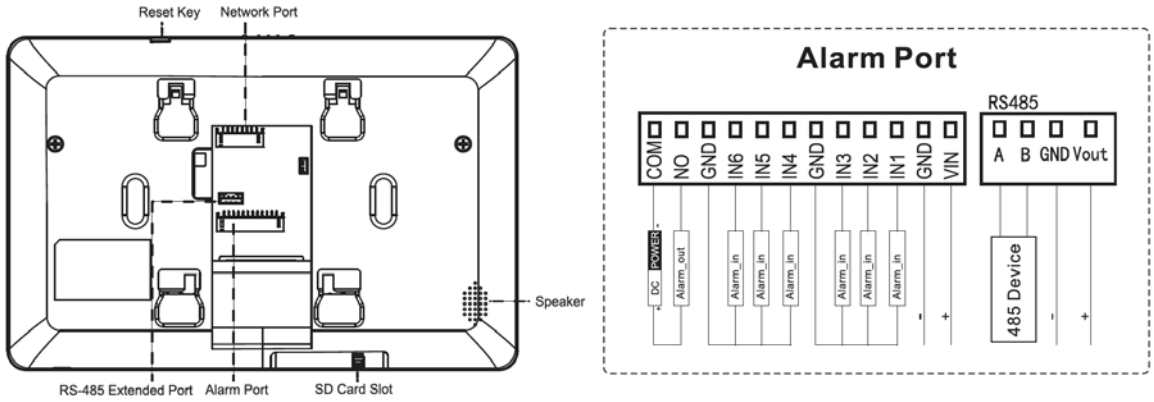
Icon	Name	Description
	SOS	Emergency call.
	Menu	Go to main menu.
	Call	• Answer call. • During call, press to hang up. • During monitoring, press to speak to unit VTO, villa VTO, fence station and verifying VTO. • During speaking, press to exit speaking.
	Monitor	• In standby mode, press to monitor the main VTO. • During monitoring, press to exit monitoring.
	Unlock	When calling, talking, monitoring and speaking to VTO, press to unlock corresponding VTO.
	Message	If it is on, there are unread messages.
	Power	If it is green, power supply is normal.
Network	Network	• If it is on, communication with VTO is normal. • If it is off, you cannot speak to VTO.
DND	DND	If it turns green, DND function is enabled.  Refer to the user manual for DND settings by scanning the QR code on the front cover.

1.2 Rear Panel Port

1.2.1 VTH5221 Series /VTH5241 Series

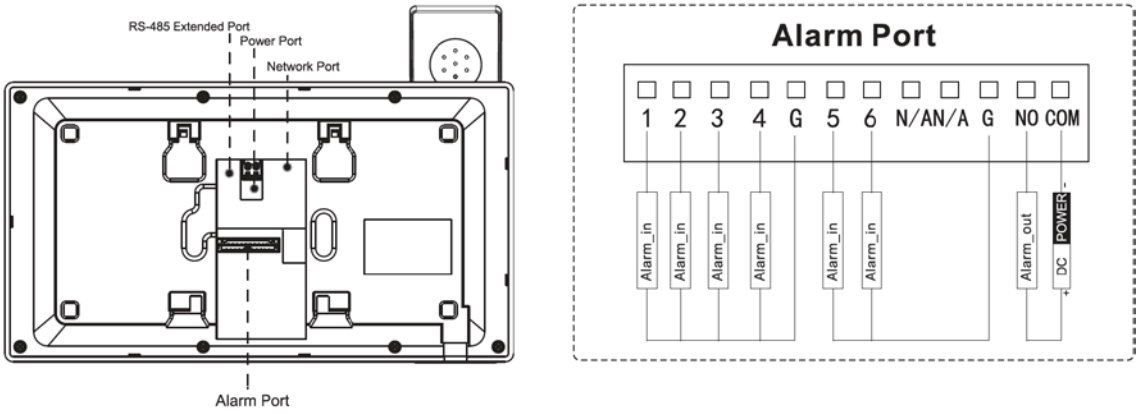
Port positions at the rear panel may differ. Take VTH5221 as an example.

Figure 1-1 Rear panel of VTH5221



1.2.2 VTH5221E-H/VTH5221EW-H

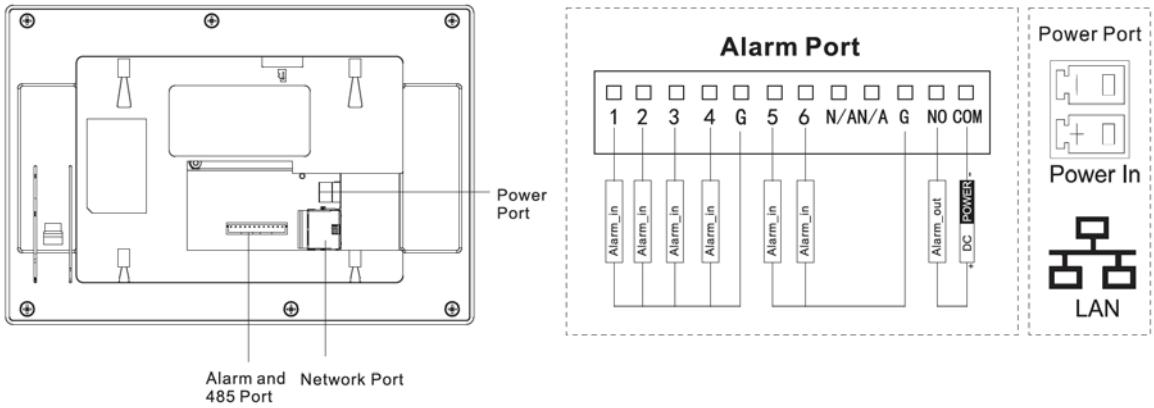
Figure 1-2 Rear panel of VTH5221E-H/VTH5221EW-H



1.2.3 VTH15XX-S2 Series B/CH & VTH15XX Series B/CH

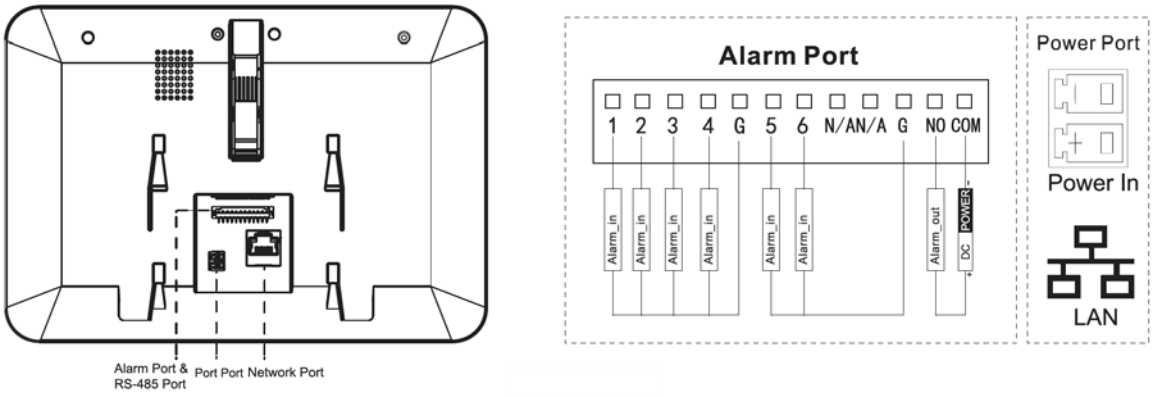
For VTH15XX-S2 CH series, port positions may differ. Take VTH1550CH-S2 as an example.

Figure 1-3 Rear panel of VTH1550CH-S2



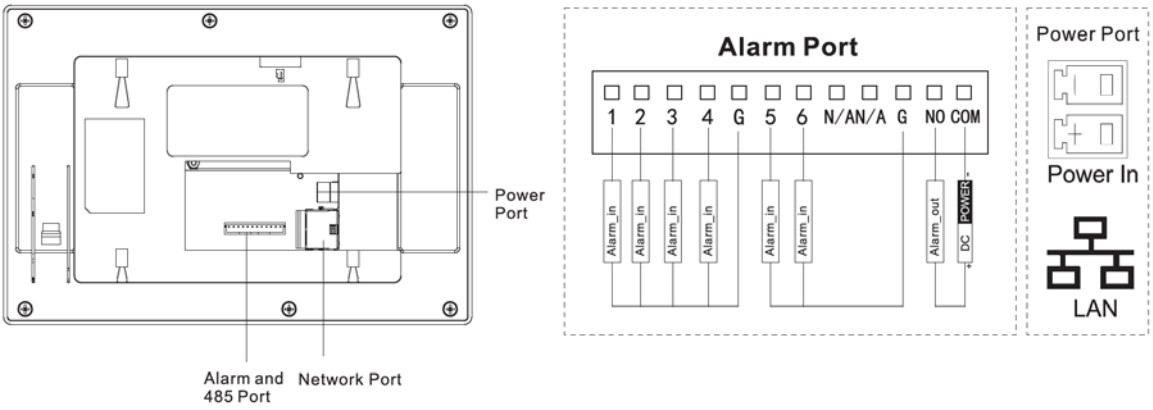
For VTH15XX-S2 B series, port positions may differ. Take VTH1560B-S2 as an example.

Figure 1-4 Rear panel of VTH1560B-S2



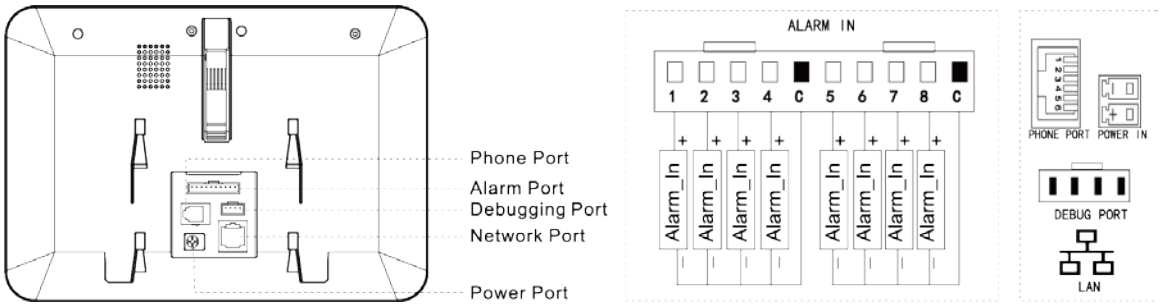
For VTH15XX CH series, port positions may differ, Take VTH1550CH as an example.

Figure 1-5 Rear panel of VTH1550CH



For VTH15XX B series, port positions may differ. Take VTH1560B as an example.

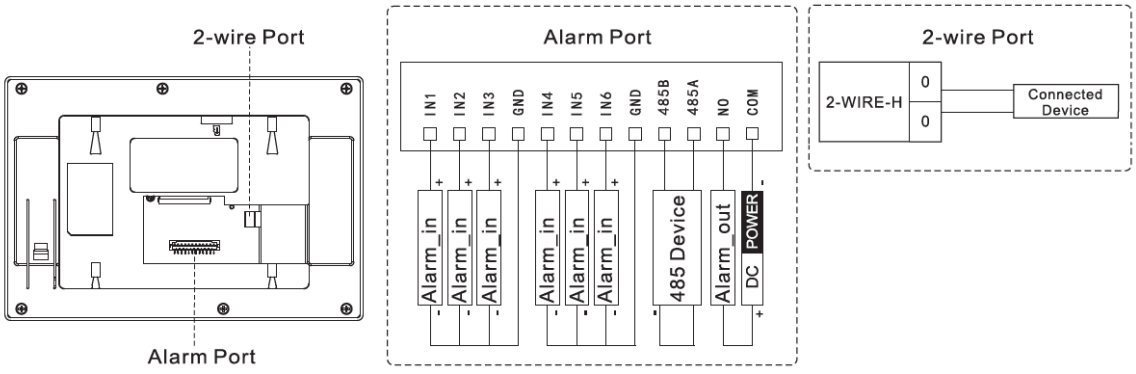
Rear panel of VTH1560B



1.2.4 VTH5222CH/VTH5222CHW-2

VTH5222CH has 1 group of 2-wire port, and VTH1550CHW-2 has 3 groups of 2-wire port.

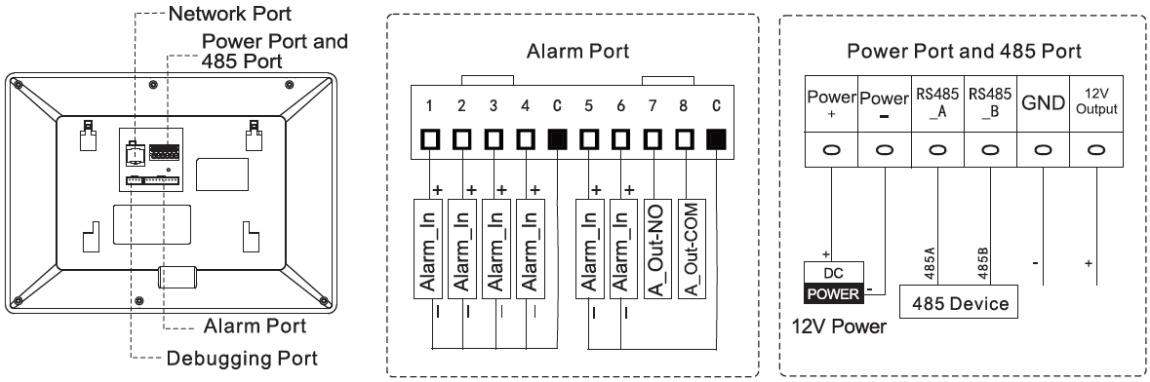
Figure 1-6 Rear panel of VTH5222CH



- Provide 1 group of 2-wire port to connect to 2-wire VTHs, VTOs, and networking control and DC power devices. Power devices are connected irrespective of positive and negative poles.
- Every group of ports can connect to multiple devices in parallel, but 3 groups support connecting to 5 devices at most.

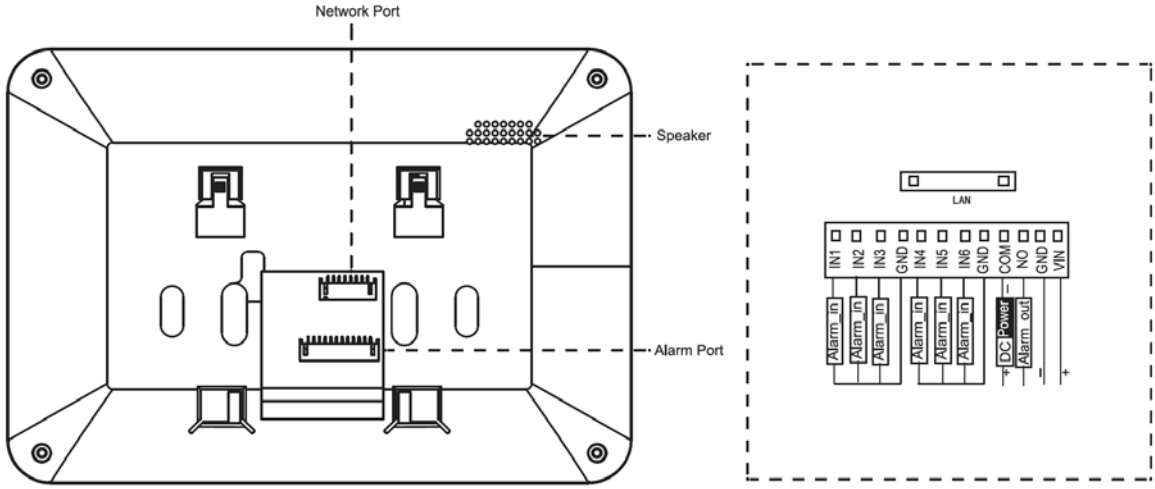
1.2.5 VTH1660CH

Figure 1-7 Rear panel of VTH1660CH



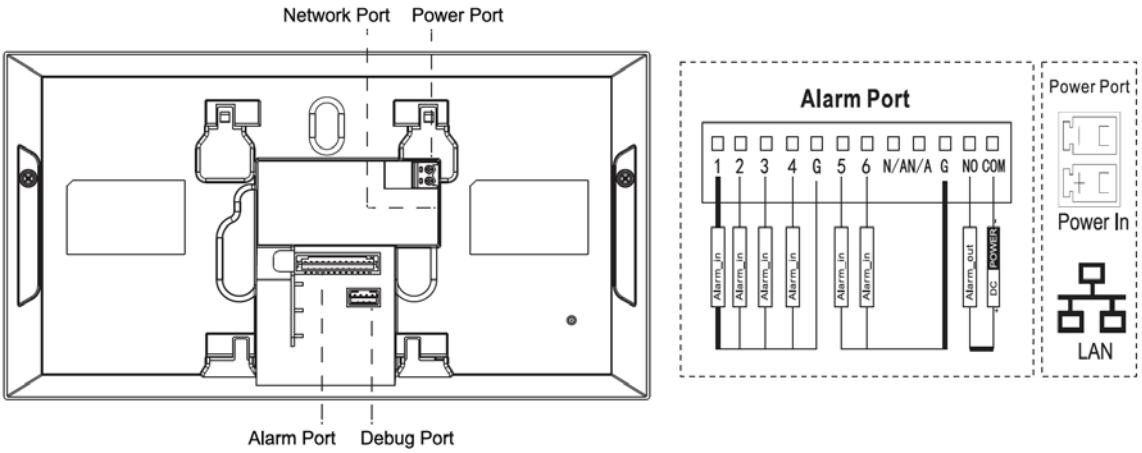
1.2.6 VTH2221A/VTH2221A-S2

Figure 1-8 Rear panel of VTH2221A/VTH2221A-S2



1.2.7 VTH2421FB/VTH2421FS

Figure 1-9 Rear panel of VTH2421FB/VTH2421FS



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 immediately. 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 technical support.
- Device central point height should be 1.4 m–1.6 m above the ground.

2.1.1 Wall-mounted

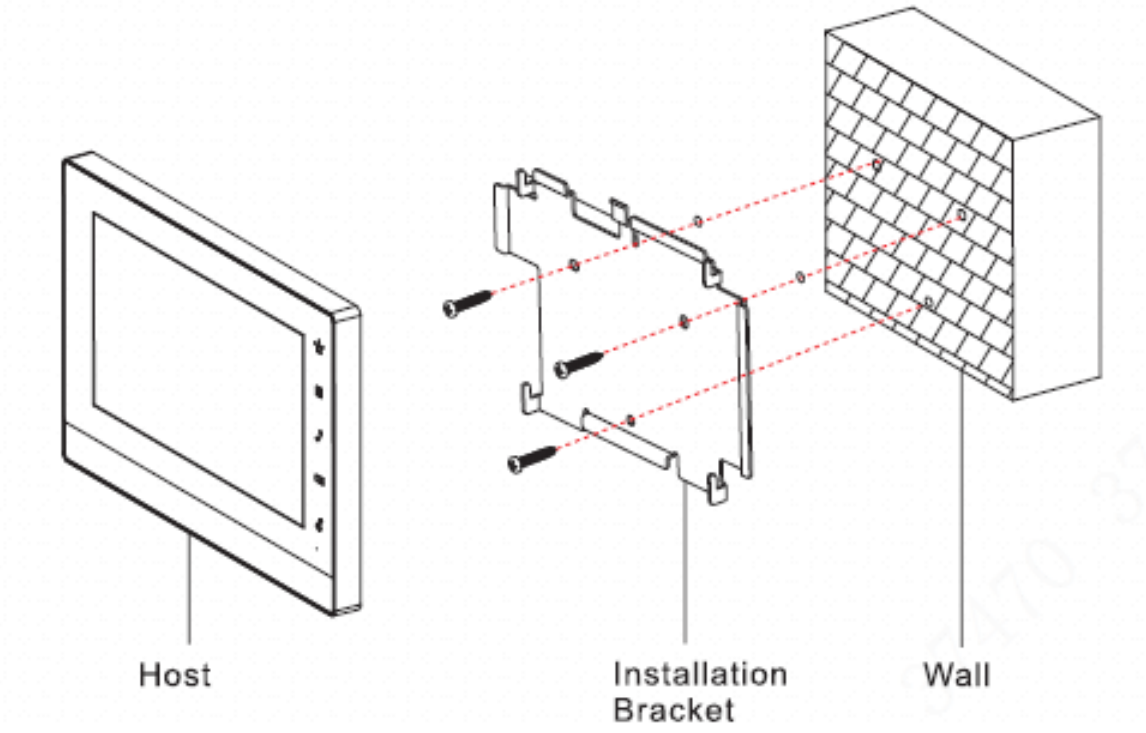
Directly install the device with a bracket on the wall, which is suitable for all types of devices. Take VTH1550CH as an example.

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

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

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

Figure 2-1 Wall-mounted installation



2.1.2 Installation with 86 Box

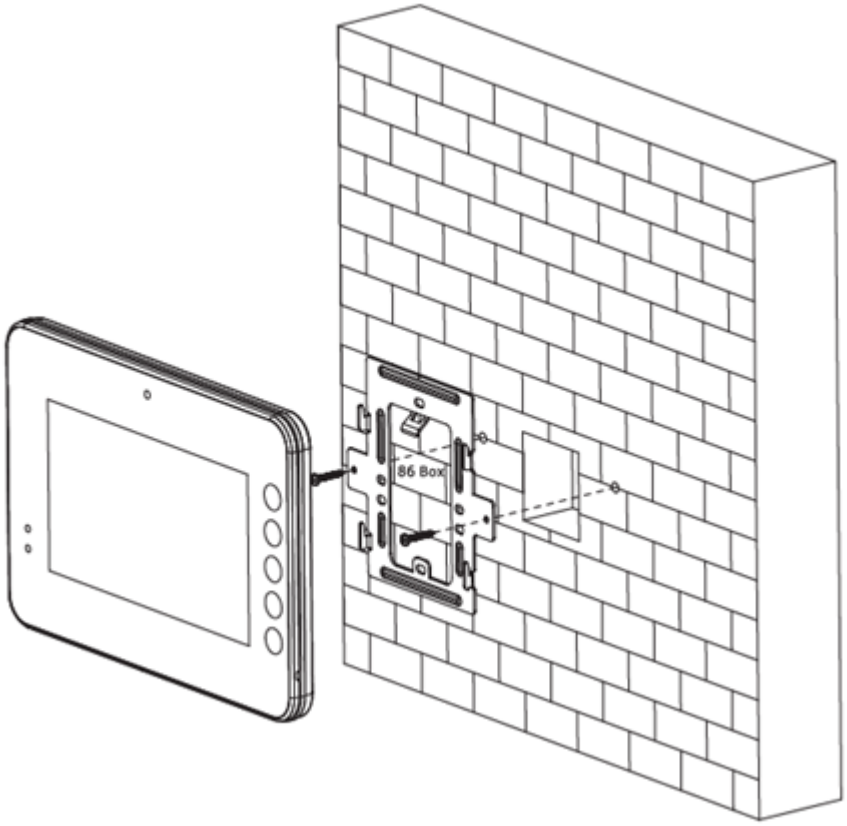
Install the device with 86 box, which is suitable for all types of devices. Take VTH1560B/BW as an example.

Step 1 Embed 86 box into the wall at a proper height.

Step 2 Fix the installation bracket on the 86 box with screws.

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

Figure 2-2 Installation with 86 box



2.1.3 Desktop Installation with Bracket

Install the device with bracket on the desktop, which only applies to handset VTH. Take VTH5221E-H as an example.

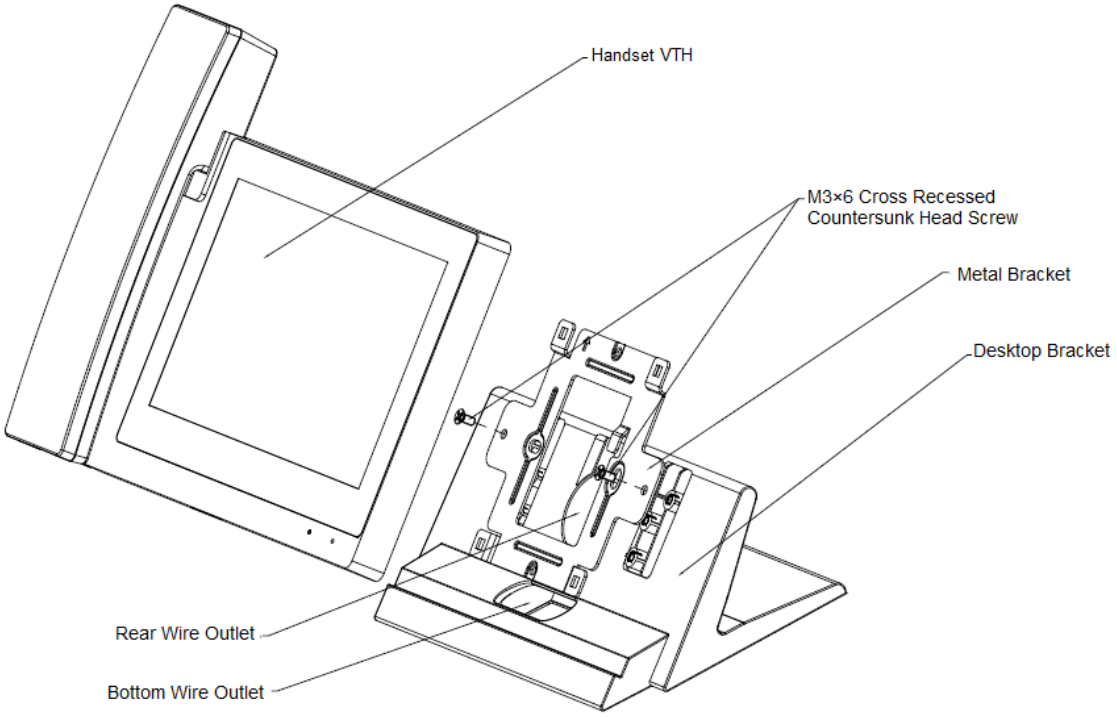
Step 1 With two M3 × 6 cross recessed countersunk head screws, tighten the metal bracket on the top two nuts of the desktop bracket.

Step 2 Connect the wires.

Step 3 Run the wires through outlet in the rear or at the bottom of the desktop bracket.

Step 4 Install the handset VTH in the slot at the top of the metal bracket.

Figure 2-3 Desktop installation with brackets



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.

2.2.1 VTO Settings

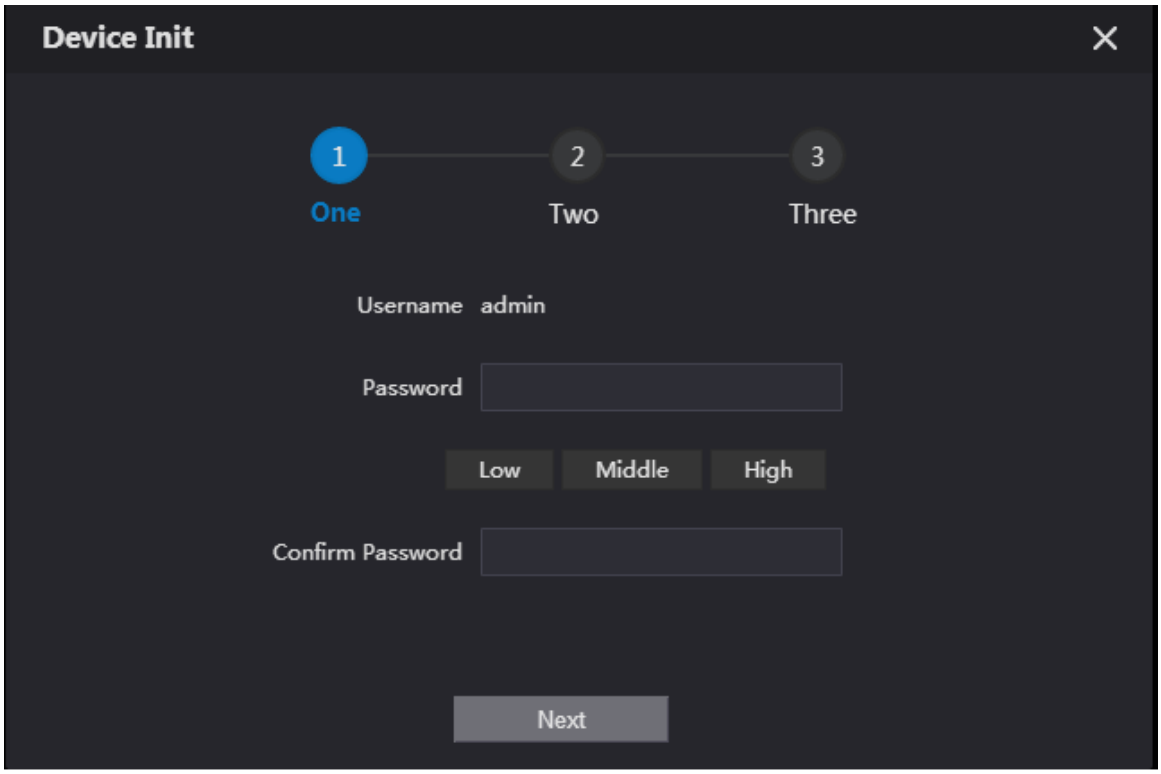
VTO interface may differ for different models and the actual interface shall prevail.

For first time use, initialize and change login password.

Make sure that the default IP addresses of PC and VTO are in the same network segment. The default IP address of VTO is 192.168.1.110.

Step 1 Power on the device, and then go to the default IP address of VTO in the browser.

Figure 2-4 Device initialization



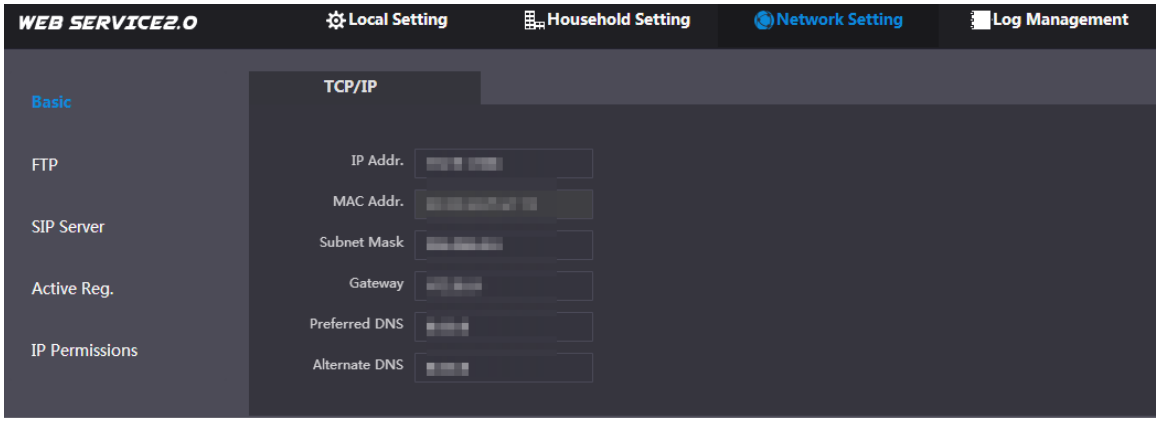
Step 2 Enter password and confirm it, and then click **Next**. Select **Email** and enter email address for resetting password.

Step 3 Enter the default address in the browser to log in to WEB interface.

The default username is admin, and the password is the one set just now.

Step 4 Select **Network Setting > Basic**.

Figure 2-5 TCP/IP



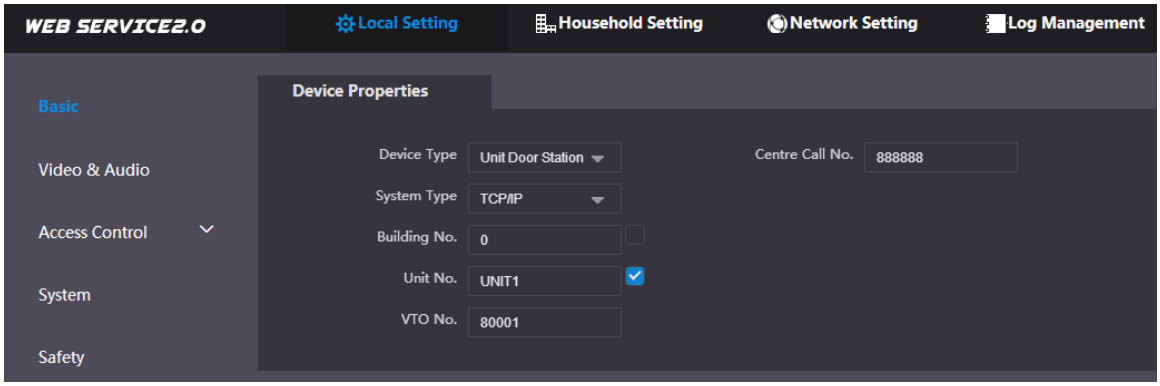
Step 5 Enter IP address, subnet mask and gateway, and then click **OK**.

The VTO will restart automatically, and:

- If PC is in the same network segment, WEB interface jumps to the login interface.
- If PC is not in the same network segment, you cannot access the new IP address. Add PC to the same network segment and try again.

Step 6 Log in to WEB interface again and select **Local Setting > Basic**.

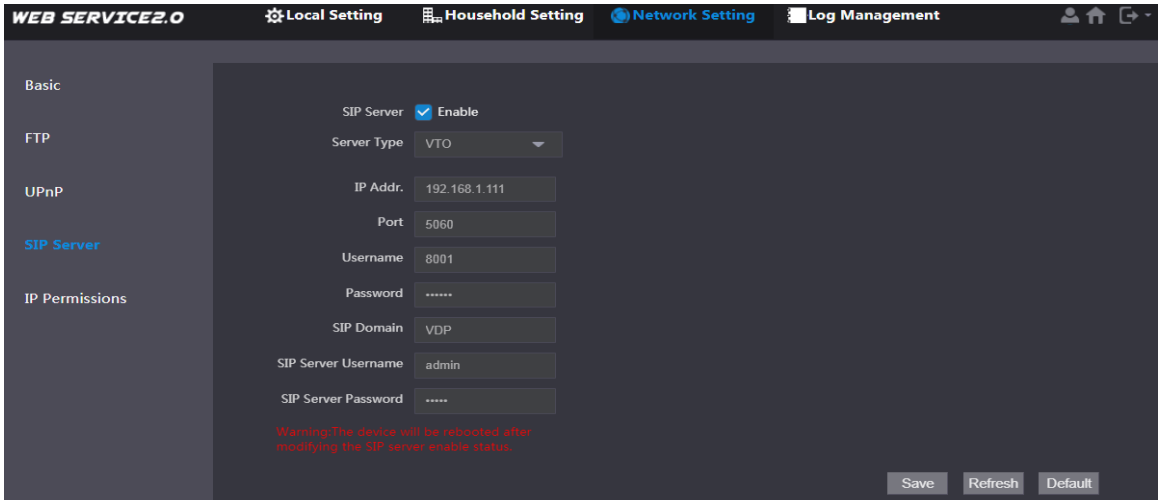
Figure 2-6 Device properties



1) Select **System Type** as TCP/IP.
2) Click **OK**.
3) Restart the device manually or wait for it to automatically restart.

Step 7 Log in to WEB interface, and then select **Network Setting > SIP Server**.

Figure 2-7 SIP server (1)

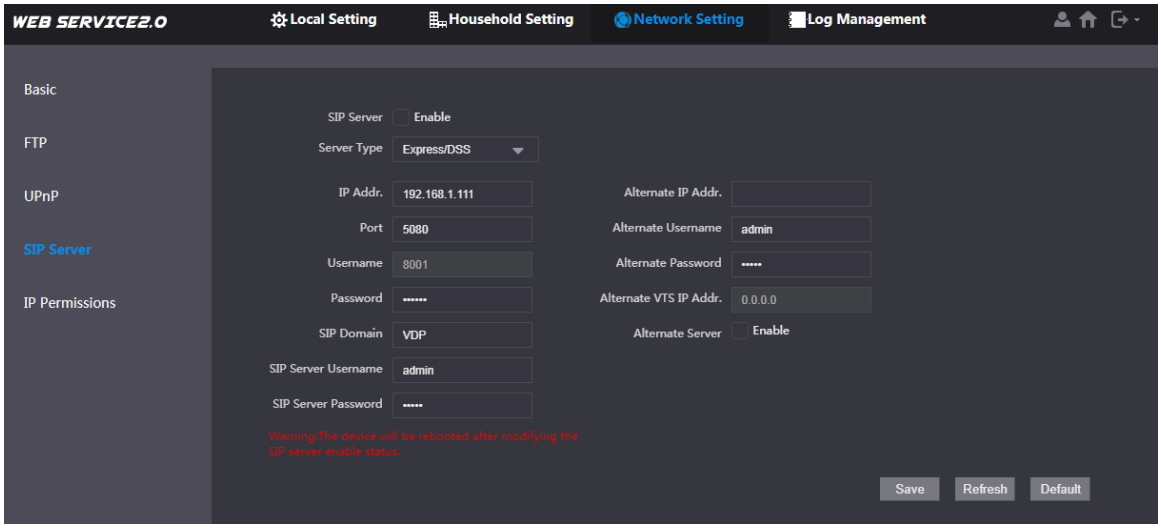


1) Select server type.
   - When VTO works as the SIP server, select **Server Type** as **VTO**. It applies to one building or unit.
   - When the platform (Express/DSS) works as the SIP server, select **Server Type** as **Express/DSS**. It applies to multiple buildings or units.
2) Set VTO number and click **Save**.

   - When the platform works as the SIP server, enable **Support Building** and **Support Unit** as needed and configure accordingly.
   - After VTO is set as the SIP server, group call function will appear at the interface. Enable it as needed.

Step 8 Select **Network Setting > SIP Server**.

Figure 2-8 SIP server (2)



- The current VTO works as the SIP server.
  Enable **SIP Server** and click **Save**. The VTO will automatically restart.
- Another VTO or platform works as the SIP server.
  Configure the parameters and click **Save**. The VTO will automatically restart.

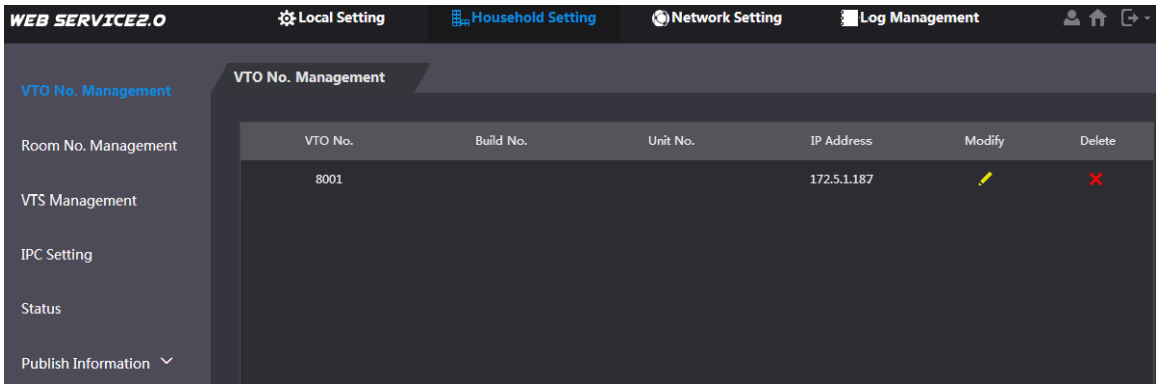
Table 2-1 Parameter description

Parameter	Description
IP Addr.	SIP server IP address.
Port	● 5060 by default when another VTO works as SIP server. ● 5080 by default when platform works as SIP server.
Username/Password	Keep default value.
SIP Domain	● Enter VDP when another VTO works as SIP server. ● Keep empty or use default value when platform works as SIP server.
Login Username/ Password	Username and password to log in to SIP server.

- VTO settings have been completed when the platform or another VTO works as the SIP server.
- If the current VTO works as the SIP server, go through Step 9 and 10.

Step 9 (Optional) Log in to WEB interface, and then select **Household Setting > VTO No. Management**.

Figure 2-9 VTO No. management



Click **Add**, configure the parameters and click **OK**. Repeat this step to add other VTOs.

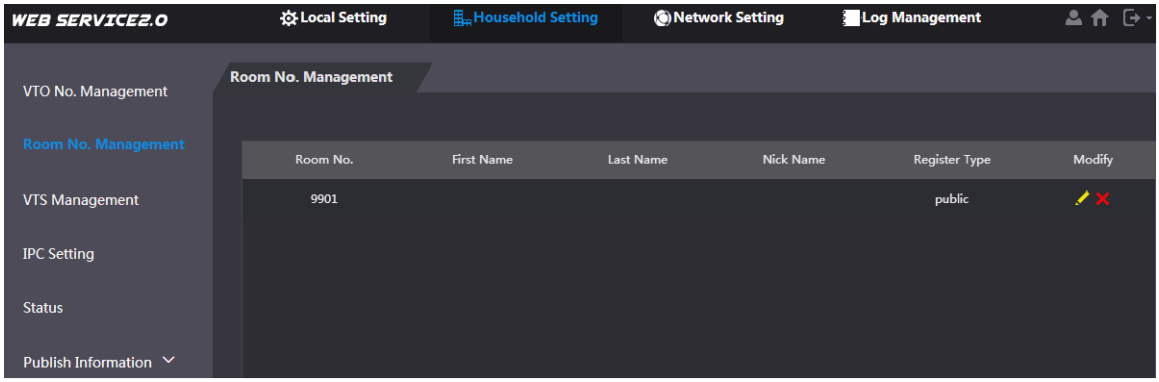
Table 2-2 VTO No. management

Parameter	Description
VTO No.	VTO number.
Build No.	Number of building where VTO is located.
Unit No.	Number of unit where VTO is located.
IP Address	IP address of VTO.

Step 10 (Optional) Select **Household Setting > Room No. Management**.

Add both when there are master VTH and extension.

Figure 2-10 Room No. management



Click **Add**, configure the parameters and click **OK**. Repeat this step to add other VTHs.

Table 2-3 Room No. management

Parameter	Description
Room No.	Set VTH room number. ● VTH room number consists of 1–6 numbers, letters, or their combinations. It should the same with room number configured on VTH. See Figure 2-15. ● When there are master VTH and extensions, end master VTH short no. with #0, and extension VTH short no. with #1, #2 and #3, to achieve group call function. For example, if master VTH is 101#0, extensions should be 101#1, 101#2…
First Name	Set username and nickname for each VTH.
Last Name	
Nick Name	
Register Type	Signaling interactive use in SIP system. Keep the default value.

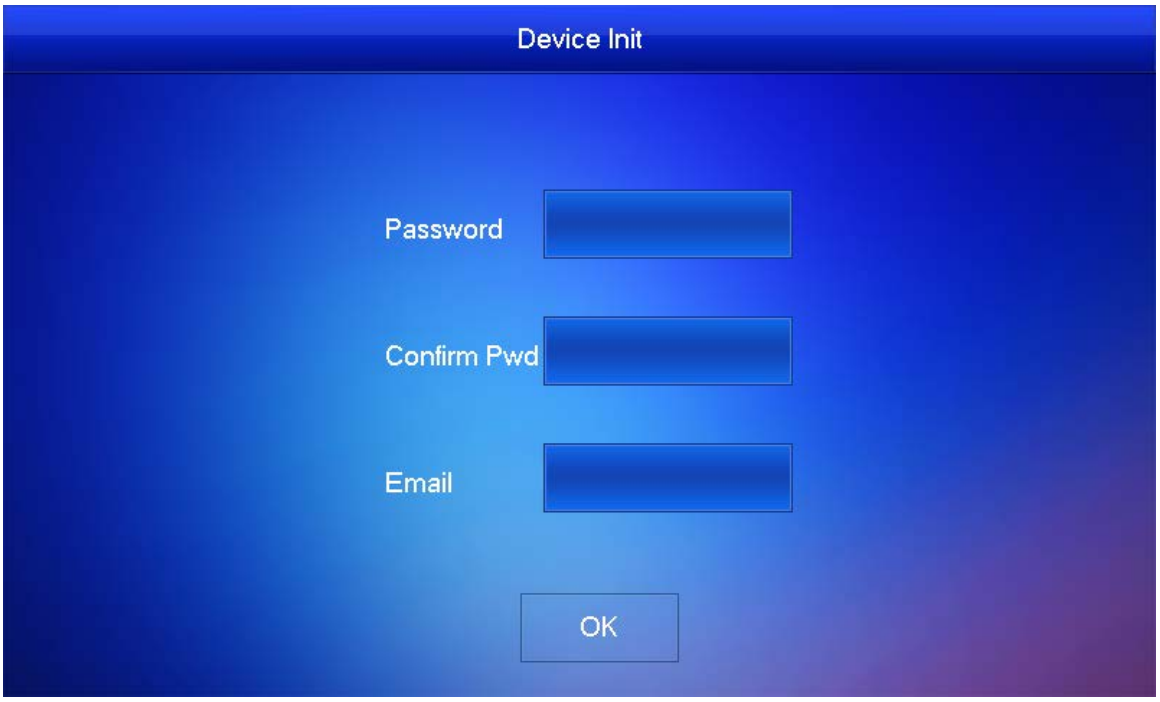
2.2.2 VTH Settings

2.2.2.1 Initialization

For first-time use, set up password and bind email address. 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.

Figure 2-11 Set up password and bind email address



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

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

Step 4 Tap **Network**.

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

Figure 2-12 Network

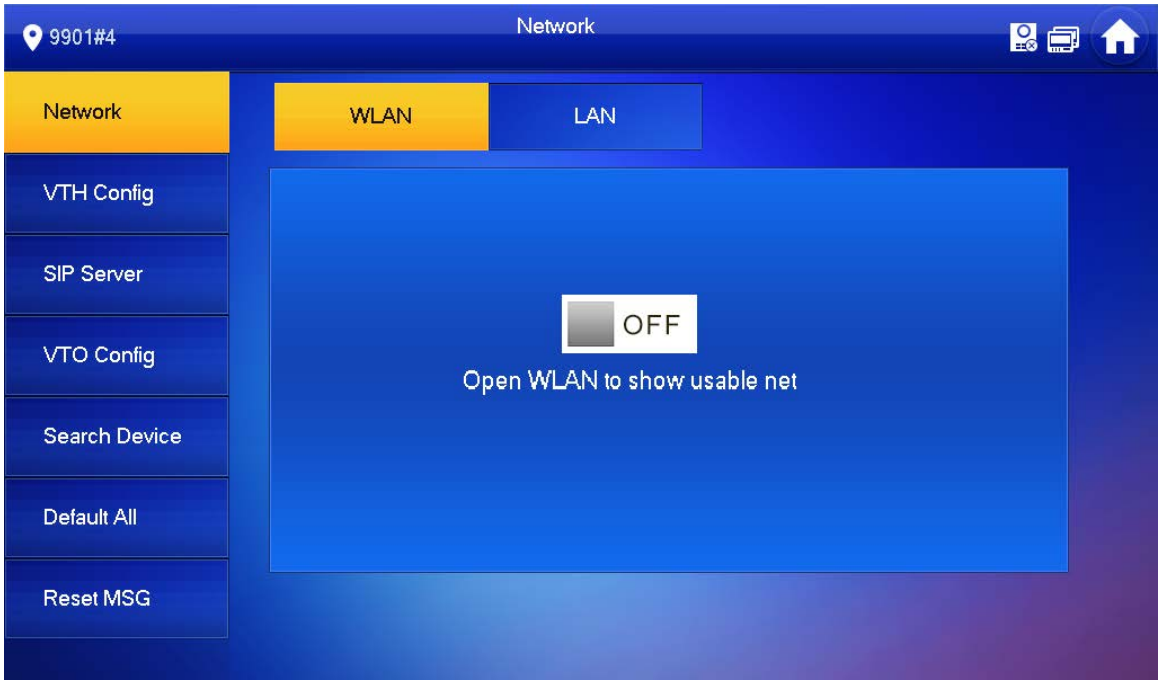
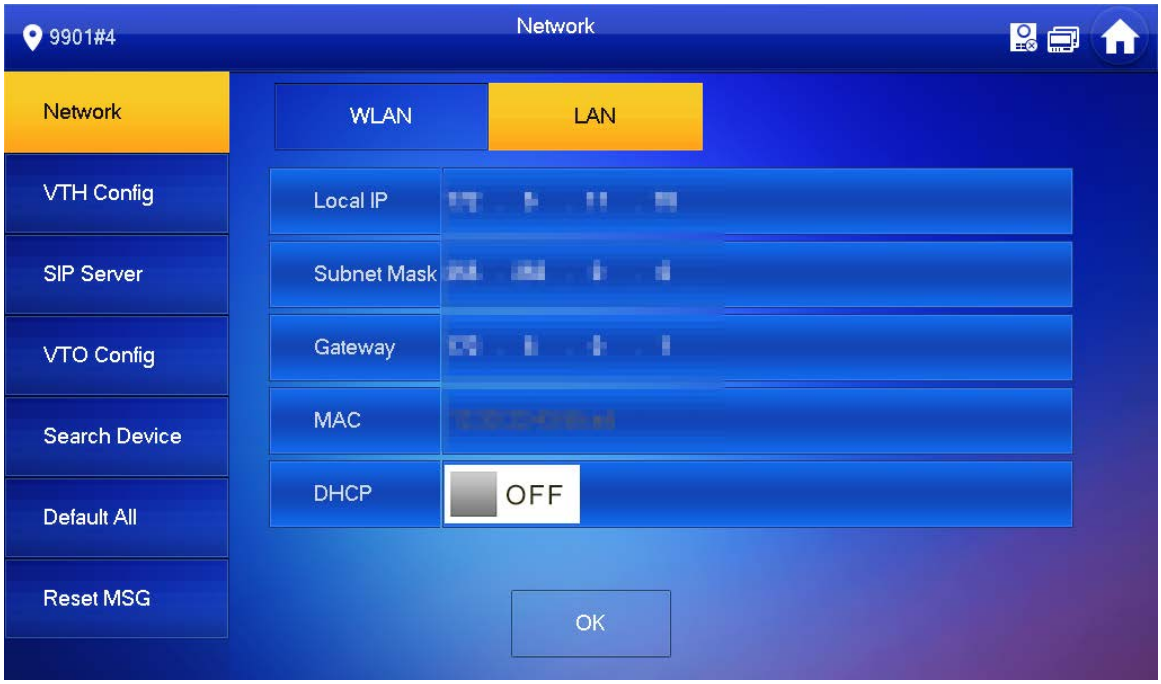


Figure 2-13 LAN



- LAN

Tap **Network > LAN**. Enter local IP, subnet mask and gateway, and then tap **OK**. Or tap 

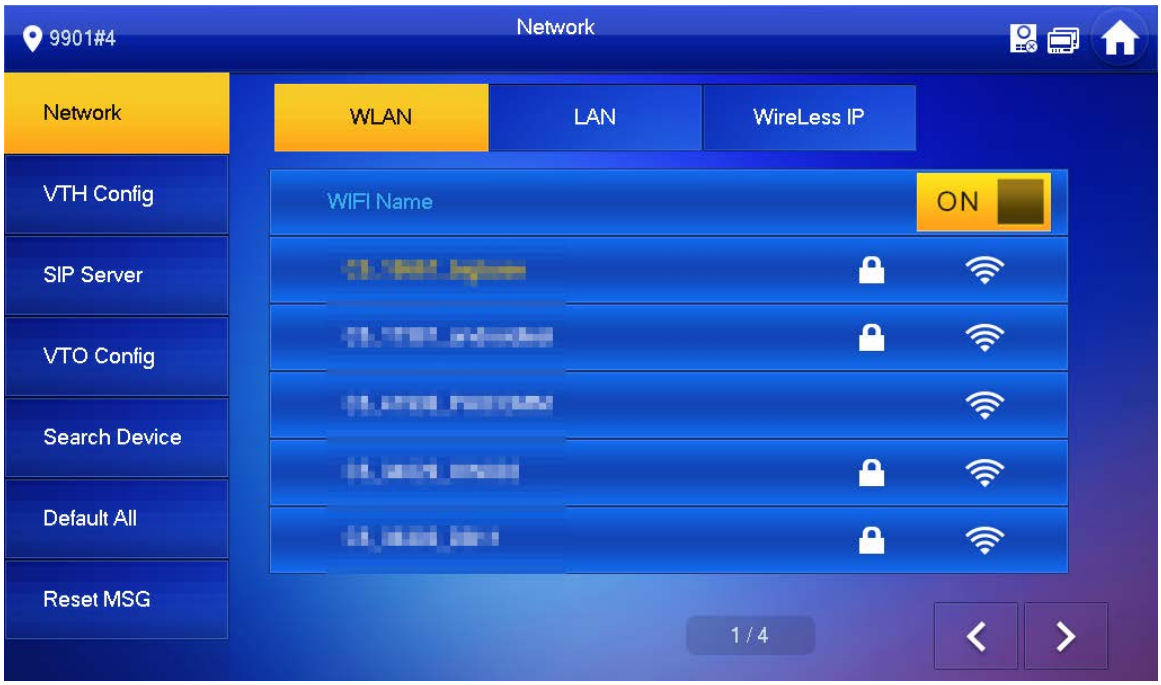
to enable DHCP function to obtain IP info automatically.

- WLAN

1) Tap **Network > WLAN**, and then tap 

.

Figure 2-14 WLAN



2) Before connecting to a WIFI network, do either of the following first.
   - Tap **WireLessIP**, enter local IP, subnet mask and gateway, and then tap **OK**.
   - Tap **WireLessIP**, tap 

to enable DHCP function to obtain IP info automatically.

To enable DHCP function, use a router with DHCP function.

3) Connect to a WIFI network.

Step 5 Tap **VTH Config**.

Figure 2-15 VTH configuration



- Use as a master VTH.

Enter room number (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.

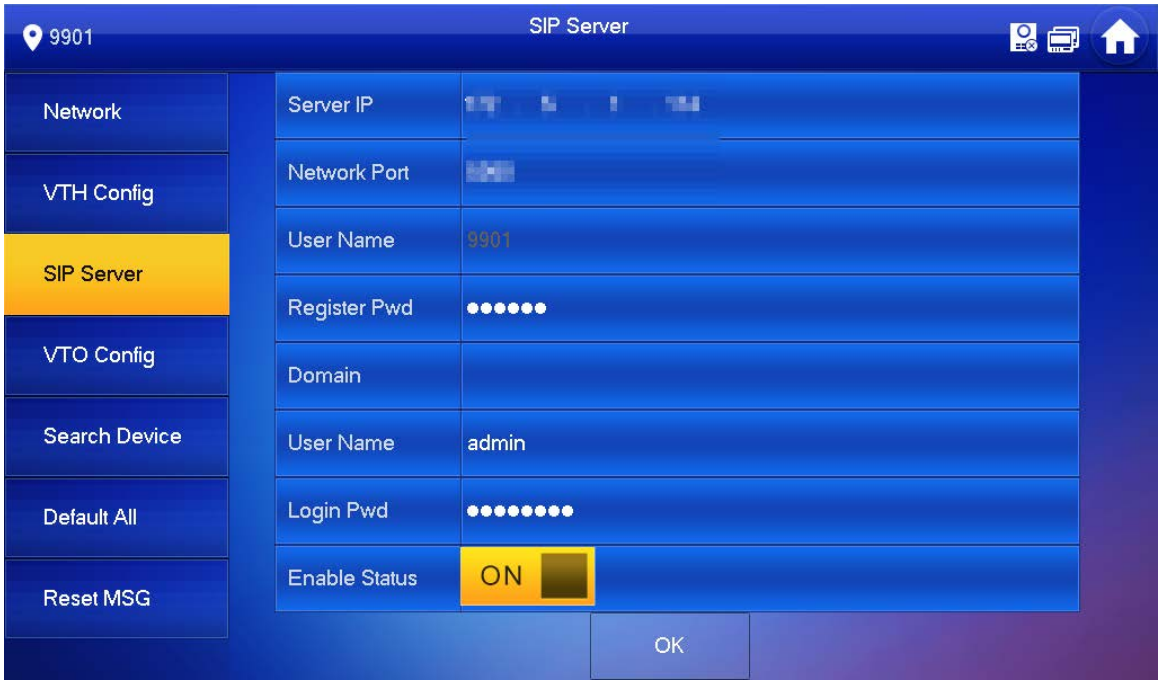
If there is extension VTH, room No. should end with #0. Otherwise, it will fail to connect to VTO.

- Use as an extension VTH.

1) Tap **Master** and the icon switches to **Extension**.
2) Enter room number (such as 101#1) and the IP address of master VTH.
   Master name and password are the username and password of master VTH. Default username is **admin**, and the password is the one set from previous step.
3) Tap **OK** to save the settings.

Step 6 Tap **SIP Server**.

Figure 2-16 SIP server



1) Configure parameters of **SIP Server**.

Table 2-4 SIP server

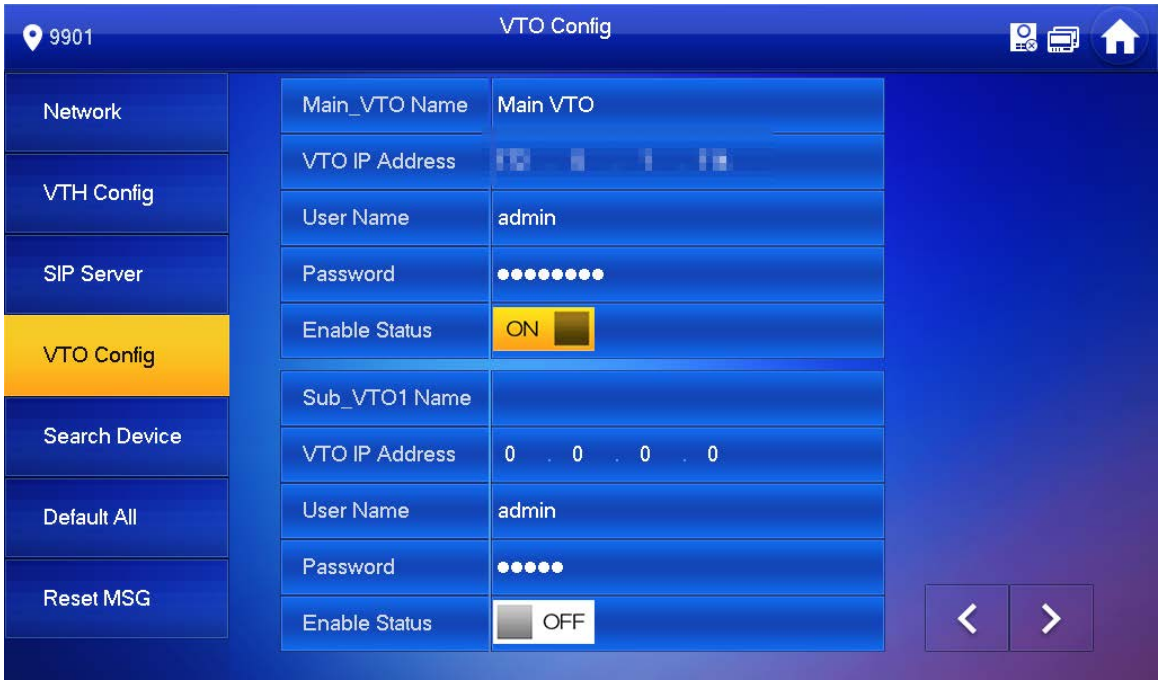
Parameter	Description
Server IP	● When the platform works as SIP server, server IP is the IP address of the platform. ● When VTO works as SIP server, server IP is the IP address of the VTO.
Network Port	● When the platform works as SIP server, network port is 5080. ● When VTO works as SIP server, network port is 5060.
User Name	Use default value.
Register Pwd	
Domain	● Registration domain of SIP server, which can be empty. ● Enter VDP when VTO works as SIP server.
User Name	SIP server login username and password.
Login Pwd	

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

3) Tap **OK**.

Step 7 Tap **VTO Config**.

Figure 2-17 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 interface 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.

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 2-18 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**, and select the VTO to enter monitoring image.

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 2-19 Door

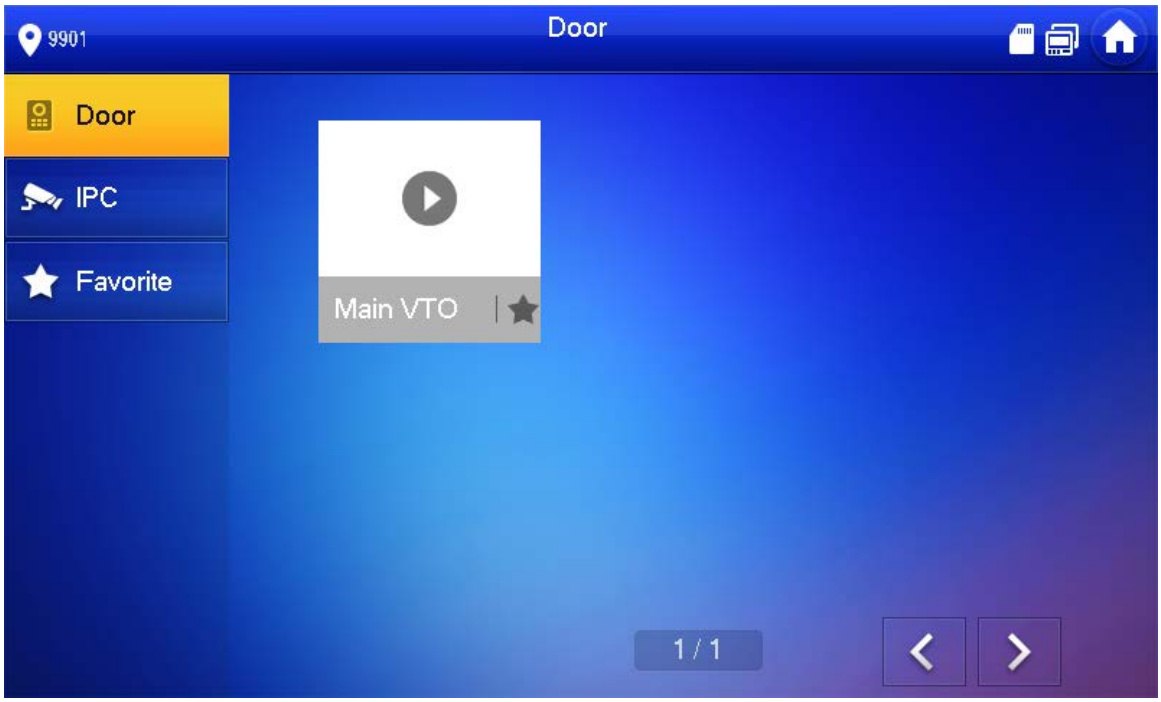
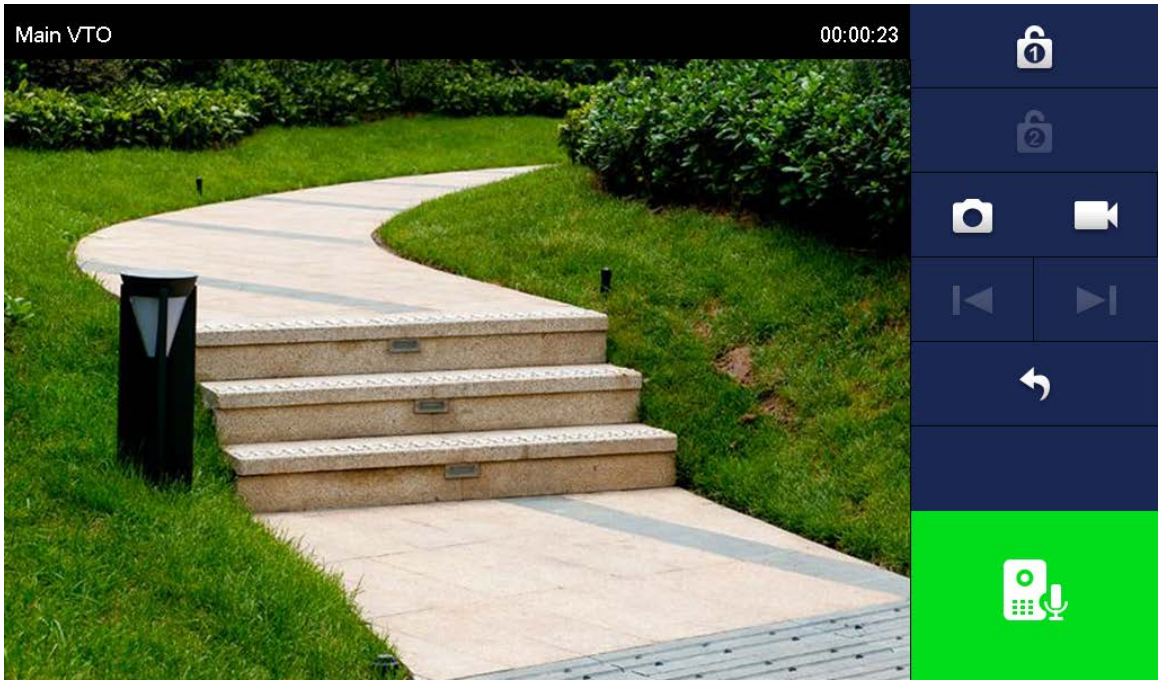


Figure 2-20 Monitoring video



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.