IP Indoor Monitor
(Version 4.2)

Quick Start Guide

V1.0.0

Foreword

General

This document mainly introduces structure, installation process, commissioning, and verification process of indoor monitors (VTH).

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.
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	November 2019

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.

Regulatory Information

European Directives Compliance

This product complies with the applicable CE marking directives and standards:

- Low Voltage (LVD) Directive 2014/35/EU.
- Electromagnetic Compatibility (EMC) Directive 2014/30/EU.
- Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU and its amending Directive (EU) 2015/863.

A copy of the original declaration of conformity may be obtained from Dahua Technology.

The most up to date copy of the signed EU Declaration of Conformity (DoC) can be downloaded from: www.dahuasecurity.com/support/notice/

CE-Electromagnetic Compatibility (EMC)

This digital equipment is compliant with Class B according to EN 55032.

CE-Safety

This product complies with IEC/EN/UL 60950-1 or IEC/EN/UL 62368-1, Safety of Information Technology Equipment.

Declaration of Conformity CE

(Only for the product has RF function)

Hereby, Dahua Technology declares that the radio equipment is compliant with Radio Equipment Directive (RED) 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: www.dahuasecurity.com/support/notice/

USA Regulatory Compliance

FCC

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

Attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

Note: This product has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this product does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.

FCC SDOC Statement can be downloaded from: https://us.dahuasecurity.com/support/notices/

Important Safeguards and Warnings

The following description is the correct application method of the device. Please read the Guide carefully before use 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 it horizontally installed, 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, in order to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its vent.
- 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

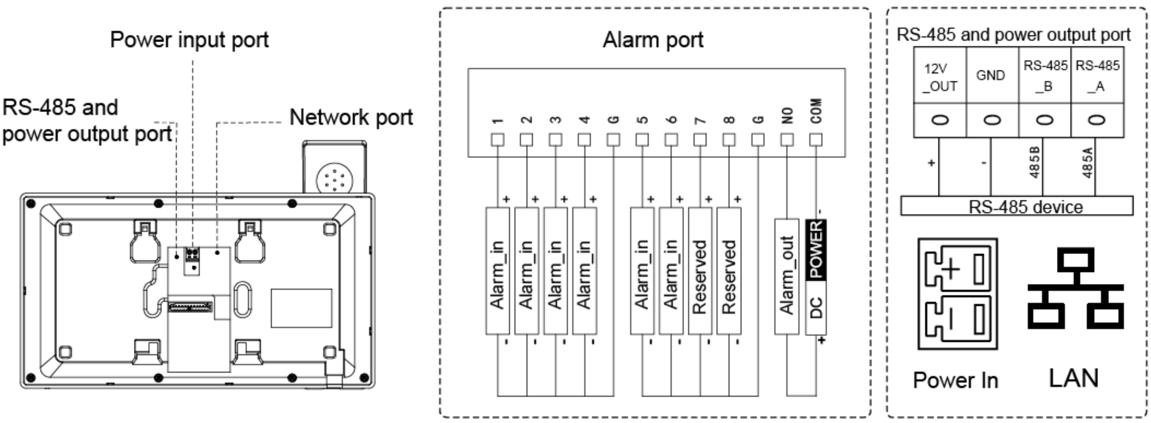
- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific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

Table of Contents

1 Rear Panel Port

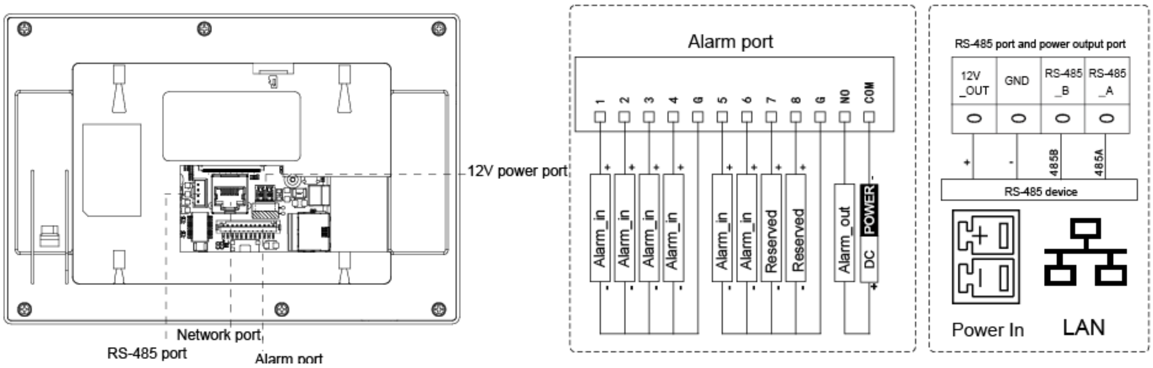
1.1 VTH5421E-H

Figure 1-1 Rear panel of VTH5421E-H



1.2 VTH5421CHM

Figure 1-2 Rear panel of VTH5421CHM



2 Installation and Cofiguration

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 power on, unplug network cable and cut off power supply at once. Power on after troubleshooting.
- Engineering installation and debugging shall be done by professional teams. Do not dismantle or repair arbitrarily in case of device failure. Contact after-sales service.
- Device central point height shall be 1.4cm–1.6cm above the ground (this equipment is only suitable for mounting at height ≤ 2m).

2.1.1 Surface Installation

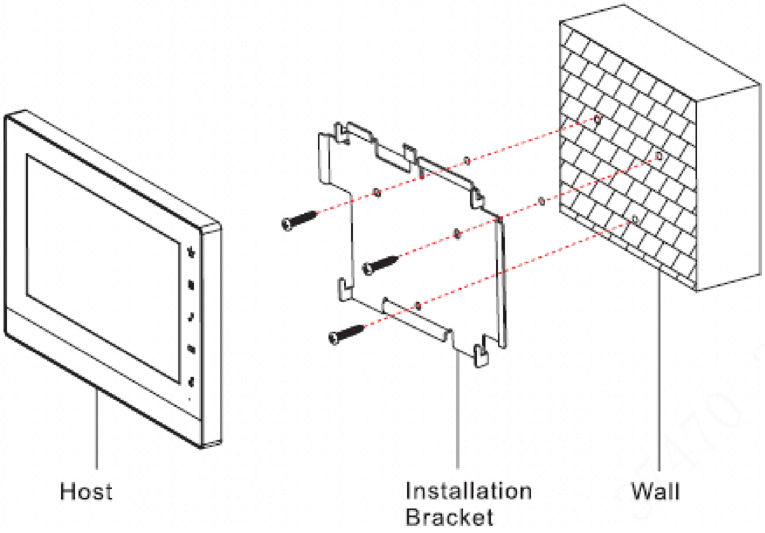
Directly install the device with a bracket onto a wall, which is suitable for all types of devices. Take VTH1550CH for example.

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

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

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

Figure 2-1 Surface installation



2.1.2 Installation with 86 Box

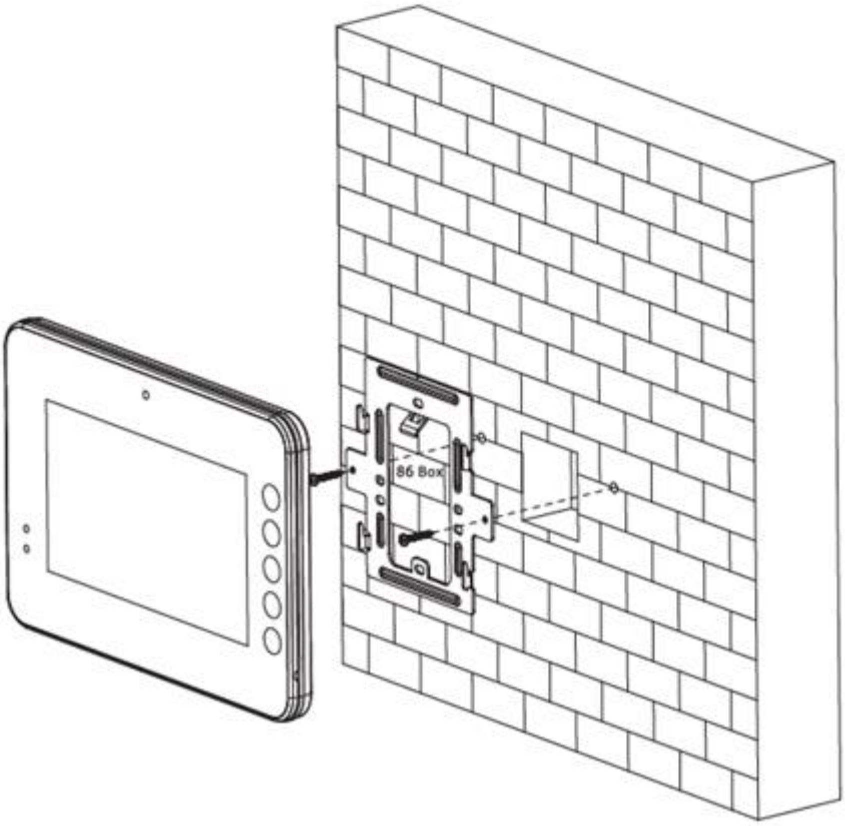
Install the device with 86 box, which is suitable for all types of devices. Take VTH1560B/BW as an example.

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

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

Step 3 Fix the device to the installation bracket.

Figure 2-2 Installation with 86 box



2.1.3 Desktop Installation

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

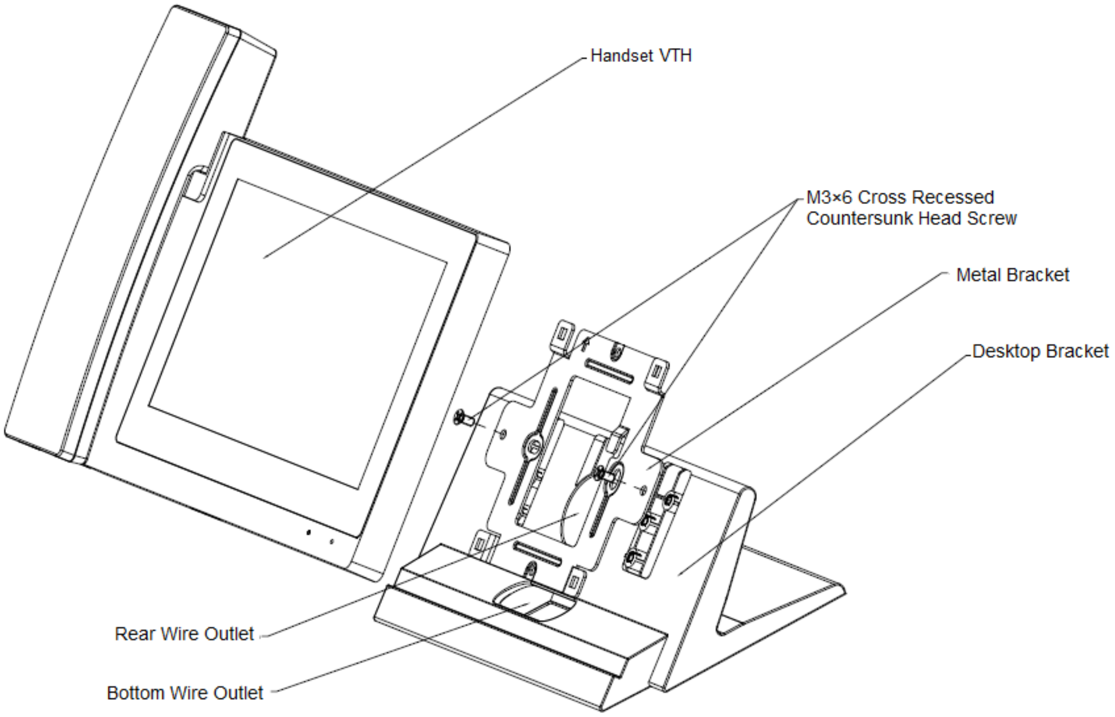
Step 1 With two M3×6 cross recessed countersunk head screws, tighten the metal bracket onto the top two nuts of desktop bracket.

Step 2 Connect cables. For details, see "1 Rear Panel Port."

Step 3 Thread the cable through wire outlet.

Step 4 Put the handset VTH along slot at the top of metal bracket, and install it into the bracket.

Figure 2-3 Desktop installation



2.2 Configuration

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

- Check whether there is short circuit or open circuit. Power on the device only after the circuit is confirmed to be normal.
- IP and No. of each VTO and VTH have been planned.
- Know location of the SIP server.
- Scan QR code on the cover for details.

Set VTO info and VTH info at Web interface of every VTO, set VTH info, network info and VTO info on every VTH, and thus realize video intercom function.

2.2.1 VTO Settings

VTO interfaces of different models might be different, and the actual interface shall prevail.

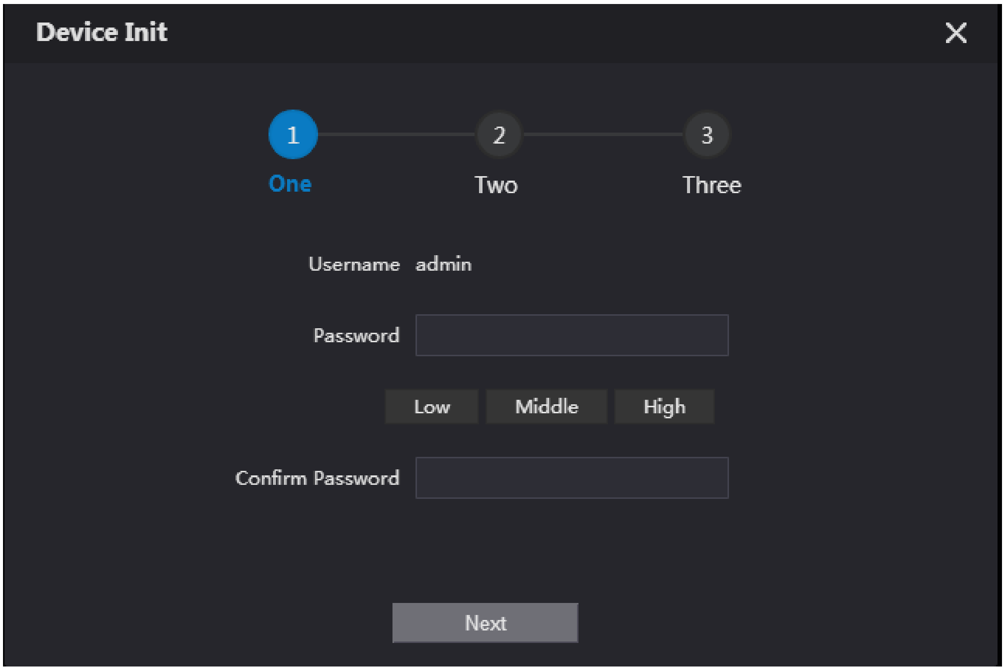
If it is the first time that you use the VTO, initialize it and modify login password.

Ensure that default IP addresses of PC and VTO are in the same network segment. Default IP address of VTO is 192.168.1.108.

Step 1 Power on the device, and enter default IP address of VTO at the address bar of PC browser.

The **Device Init** interface is displayed. See Figure 2-4.

Figure 2-4 Device initialization



Username admin

Step 2 Enter password and confirm password, and then click **Next**.

Step 3 Select **Email**, and then enter your email address.

This email address is used to reset the password

Step 4 Enter default address in the browser to log in to the web interface.

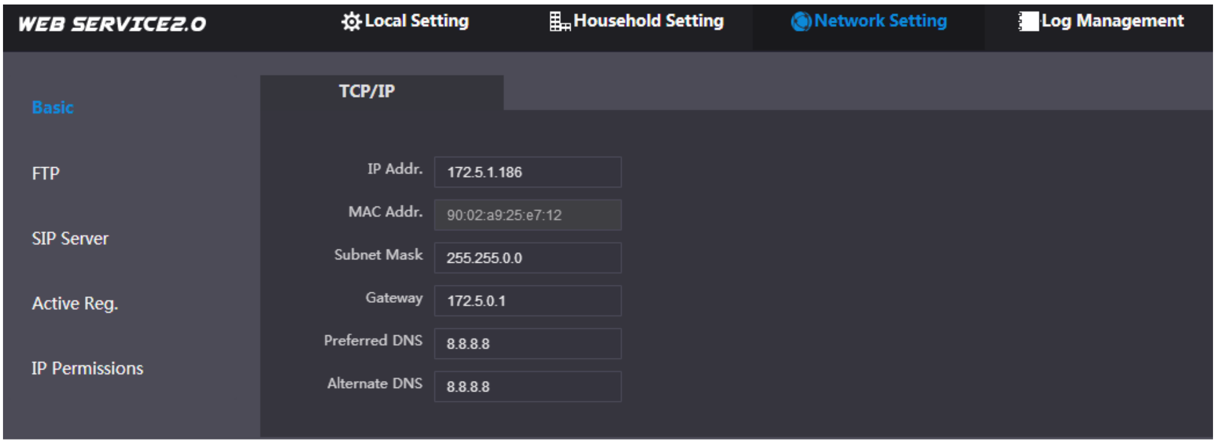
🕮

Default username is admin. Password is the new one set during initialization.

Step 5 Select **Network Setting > Basic**.

The **TCP/IP** interface is displayed, see Figure 2-5.

Figure 2-5 TCP/IP



IP Addr. 172.5.1.186

MAC Addr. 90:02:a9:25:e7:12

Subnet Mask 255.255.0.0

Gateway 172.5.0.1

Preferred DNS 8.8.8.8

Alternate DNS 8.8.8.8

Step 6 Enter the planned IP address, subnet mask and gateway, and then click **OK**.

🕮

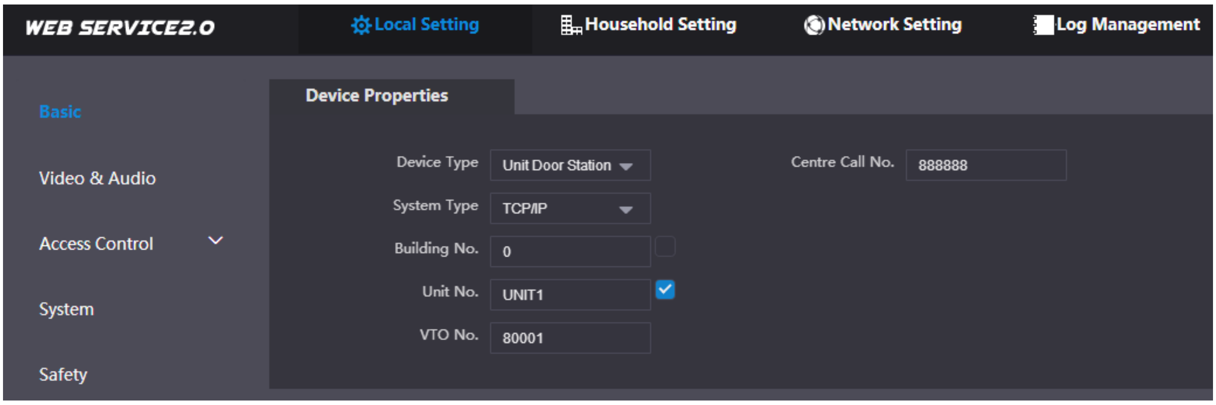
After modification, VTO will restart automatically, while the following two cases occur on the web interface.

- If PC is in the planned network segment, web interface will go to new IP login interface automatically.
- If PC is not in the planned network segment, login will fail. Add PC to the planned network segment and login to web interface again.

Step 7 Log in to web interface again, and then select **Local Setting > Basic**.

The **Device Properties** interface is displayed, see Figure 2-6.

Figure 2-6 Device properties



Device Type: Unit Door Station

System Type: TCP/IP

Building No.: 0 □

Unit No.: UNIT1 ☑

VTO No.: 80001

Centre Call No.: 888888

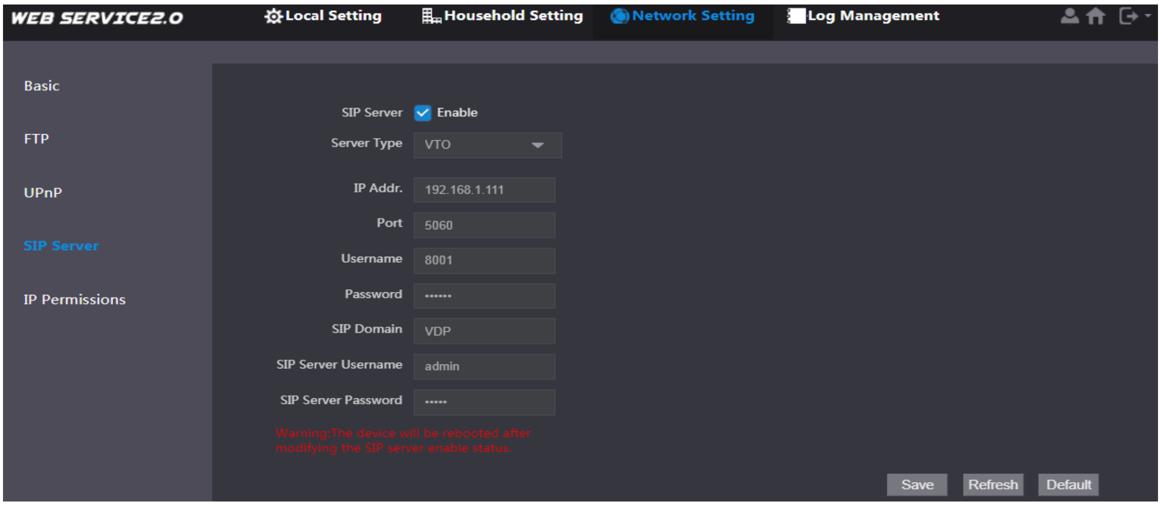
1) Select **TCP/IP** from the **System Type** drop-down list.

2) Click **OK** to save the settings.

Restart the device manually, or wait for the device to restart automatically, and then the settings can be valid.

Step 8 Log in to the web interface again, and then select **Network Setting > SIP Server**. The **SIP Server** interface is displayed, see Figure 2-7.

Figure 2-7 SIP server (1)



SIP Server: ☑ Enable

Server Type: VTO

IP Addr.: 192.168.1.111

Port: 5060

Username: 8001

Password: ······

SIP Domain: VDP

SIP Server Username: admin

SIP Server Password: ·····

Warning:The device will be rebooted after modifying the SIP server enable status.

1) Select server type.

   ◇ When this VTO or another VTO works as SIP server, select **VTO** from the **Server Type** drop-down list. It applies to a scenario where there is only one unit.

   ◇ When the platform (Express/DSS) works as SIP server, select **Express/DSS** from the **Server Type** drop-down list. It applies to a scenario where there are multiple buildings or multiple units.

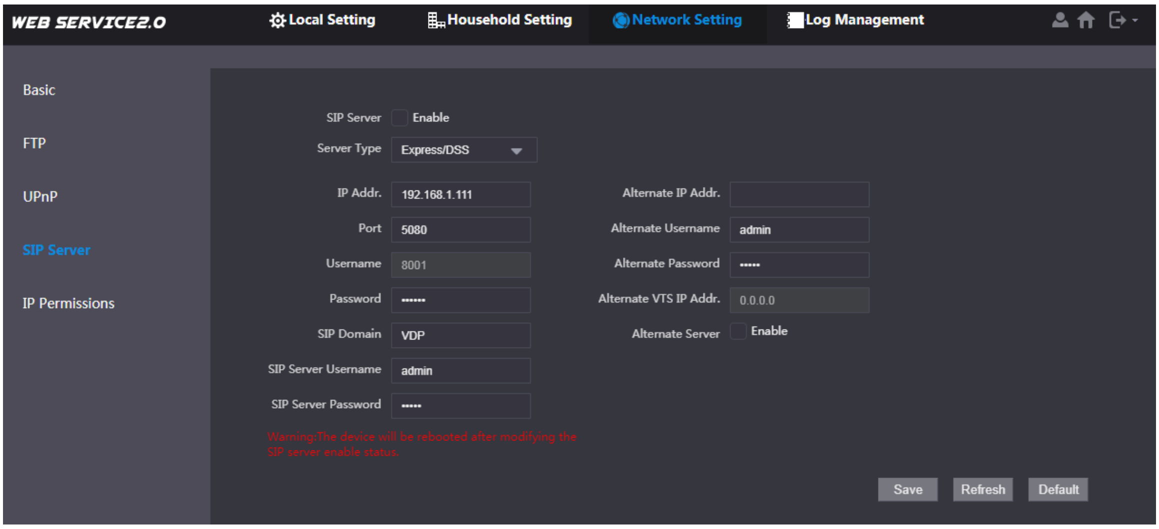
2) Set VTO number and click **OK** to save the configuration.

- When the platform works as SIP server, if it is necessary to set Building No. and Building Unit No, enable **Support Building** and **Support Unit** first.
- After VTO is set to be SIP server, group call function will appear on the interface. To realize group call, select **Enable** next to the group call.

Step 9 Select **Network Setting > SIP Server**.

The **SIP Server** interface is displayed, see Figure 2-8.

Figure 2-8 SIP server (2)



SIP Server □ Enable

Server Type Express/DSS

IP Addr. 192.168.1.111

Port 5080

Username 8001

Password ••••••

SIP Domain VDP

SIP Server Username admin

SIP Server Password •••••

Alternate IP Addr.

Alternate Username admin

Alternate Password •••••

Alternate VTS IP Addr. 0.0.0.0

Alternate Server □ Enable

Warning:The device will be rebooted after modifying the SIP server enable status.

- This VTO works as SIP server.
  Select **SIP Server Enable**, and click **OK** to save the configuration. The VTO will restart automatically.
- Another VTO or platform works as SIP server.
  Set parameters according to Table 2-1 and click **OK**. The VTO will restart automatically.

Table 2-1 SIP server parameter

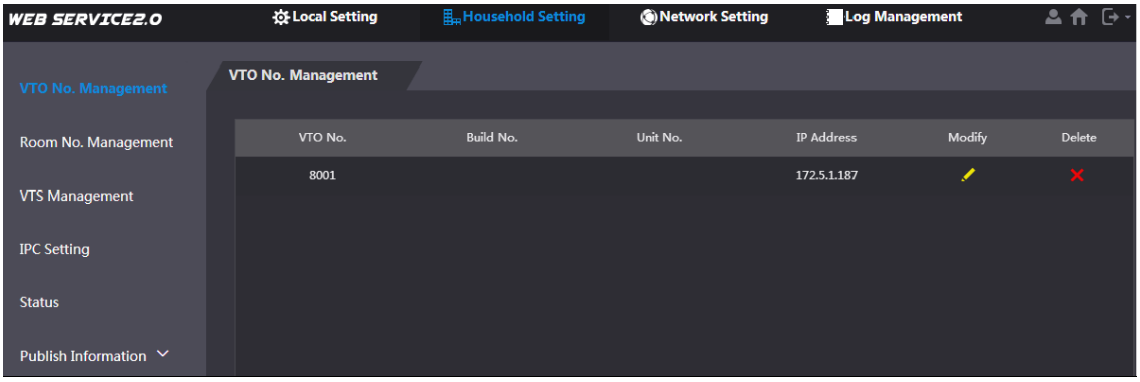
Parameter	Description
IP Address	IP address of SIP server.
Port	● It is 5060 by default when another VTO works as SIP server. ● It is 5080 by default when the platform works as SIP server.
Username/Password	Use default value.
SIP Domain	● It shall be VDP when another VTO works as SIP server. ● It can be null or keep default value when the platform works as SIP server.
Login Username/ Password	Username and password to log in to the SIP server.

- VTO settings have been completed if the platform or another VTO works as SIP server.
- If this VTO works as SIP server, VTO No. Management and Room No. Management appears in the left parameter tab. Add VTO and VTH according to Step 9 and Step 10.

Step 10 (Optional) Log in to web interface again, and then select **Household Setting > VTO No. Management**.

The **VTO No. Management** interface is displayed, see Figure 2-9.

Figure 2-9 VTO No. management



VTO No.	Build No.	Unit No.	IP Address	Modify	Delete
8001			172.5.1.187	✎	✕

Click **Add**, set outdoor station parameters according to Table 2-2 and click **OK**. Repeat this step to add other outdoor stations in the group.

Table 2-2 VTO No. management description

Parameter	Description
VTO No.	VTO number.
Register Password	Signaling interactive use in SIP system. Use default value.
Build No.	Number of the building where VTO is located.
Unit No.	Number of the unit where VTO is located.
IP Address	IP address of VTO.
Username/Password	Username and password to log in to the web interface of this VTO.

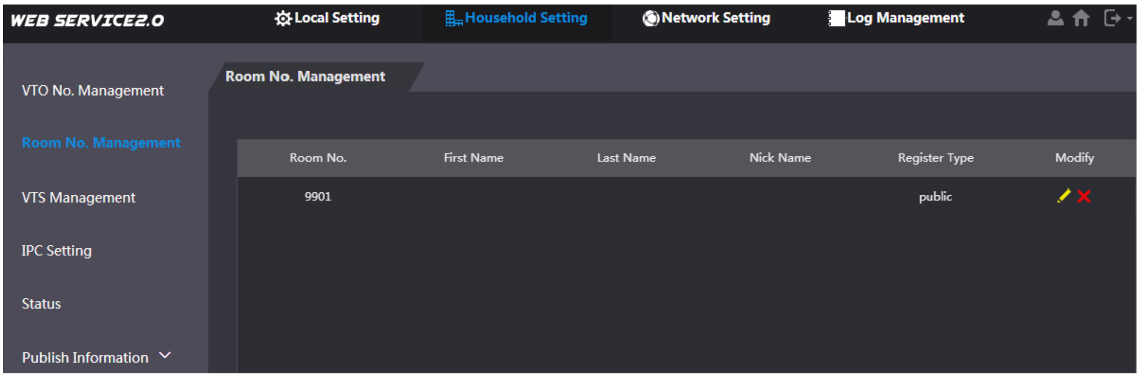
Step 11 (Optional) Select **Household Setting > Room No. Management**.

Room No. Management interface is displayed, see Figure 2-10.

🕮

When there are master VTH and extension, both shall be added.

Figure 2-10 Room No. management



Room No.	First Name	Last Name	Nick Name	Register Type	Modify
9901				public	✎ ✕

Click **Add**, set VTH parameters according to Table 2-3 and tap **OK**. Repeat these steps to add other VTH in the group.

Table 2-3 Room No. management

Parameter	Description
Family Name	Set VTH username and nickname, in order to distinguish.
First Name	
Nick Name	
Room No.	Set VTH room number. 🕮

Parameter	Description
	● VTH room number consists of 1–6 numbers, letters, or their combinations. It shall be consistent with room number configured at VTH. ● When there are master VTH and extensions, to realize group call function, master VTH short no. shall end with "#0", whereas extension VTH short no. shall end with #1, #2 and #3. For example, if master VTH is 101#0, extensions will be 101#1, 101#2…
Register Type	Signaling interactive use in SIP system. Keep the default value.
Modify	

2.2.2 VTH Settings

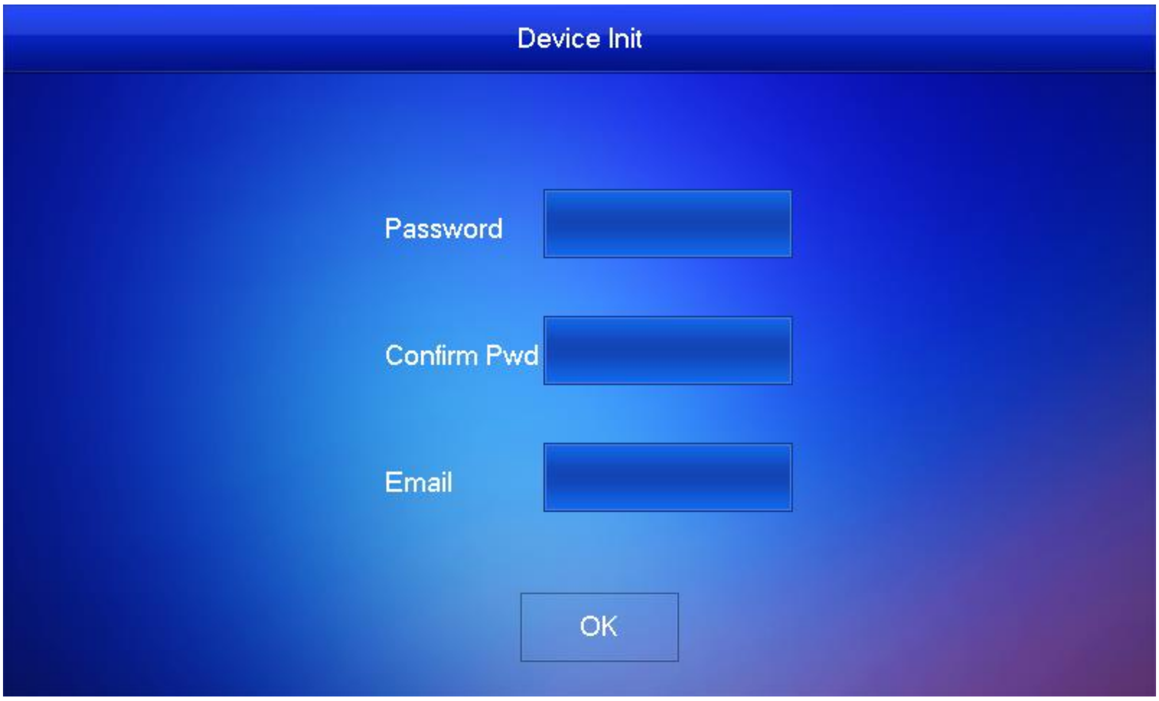
Initialization

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

Step 1 Power on the device.

The **Welcome** interface and **Initialization** interface will be displayed, see Figure 2-11.

Figure 2-11 Device initialization



Device Init

Password

Confirm Pwd

Email

OK

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

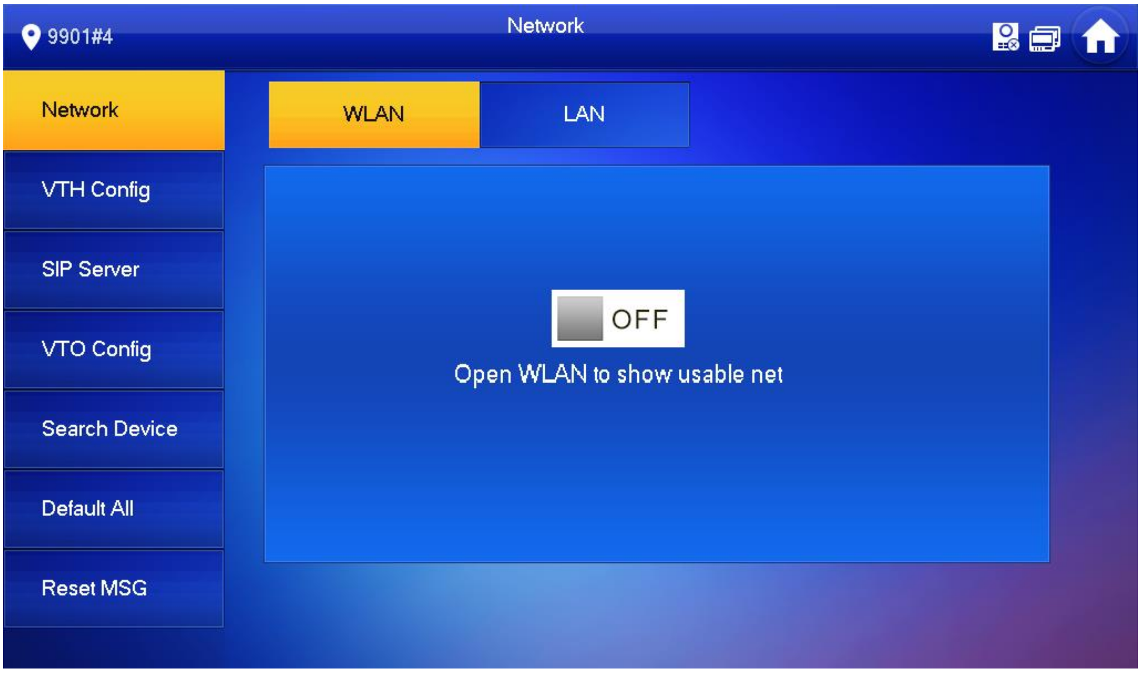
Step 3 Tap **Setting** for more than 6 seconds, enter the password set during initialization, and click **OK**.

Step 4 Tap **Network**.

The **Network** interface is displayed, see Figure 2-12 or Figure 2-13.

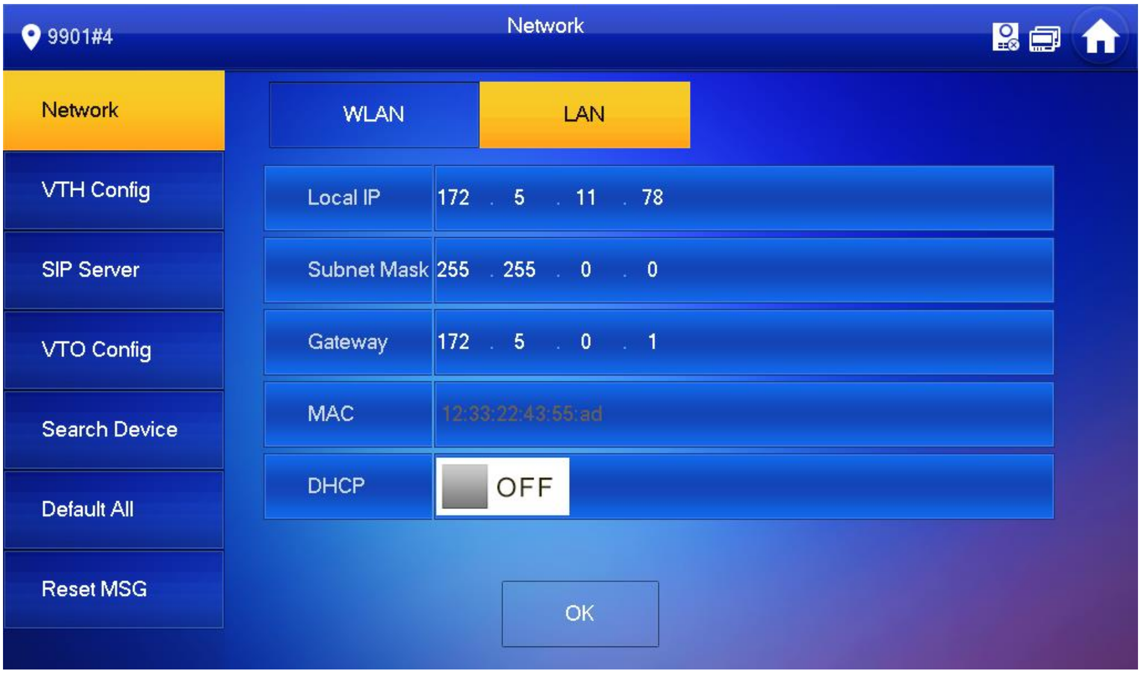
IP addresses of VTH and VTO shall be in the same network segment. Otherwise, VTH will fail to obtain VTO information after configuration.

Figure 2-12 WLAN



Open WLAN to show usable net

Figure 2-13 LAN



Local IP	172 . 5 . 11 . 78
Subnet Mask	255 . 255 . 0 . 0
Gateway	172 . 5 . 0 . 1
MAC	12:33:22:43:55:ad
DHCP	OFF

- LAN

Enter local IP, subnet mask, and gateway, and then tap **OK**. Or tap OFF to enable DHCP function and obtain IP info automatically.

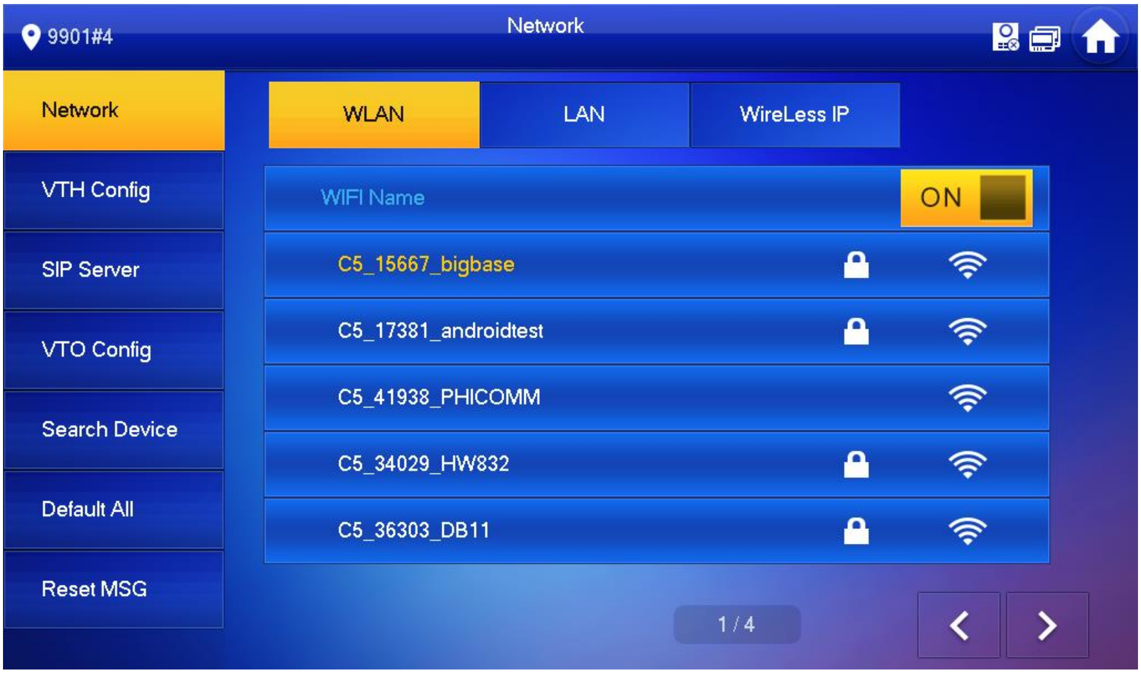
If the device has WLAN function, tap **WLAN** to set it.

- WLAN

1) Tap OFF to enable Wi-Fi function.

   Available Wi-Fi list will be displayed, see Figure 2-14.

Figure 2-14 Wi-Fi list



WIFI Name ON

C5_15667_bigbase

C5_17381_androidtest

C5_41938_PHICOMM

C5_34029_HW832

C5_36303_DB11

2) Connect Wi-Fi.

The system has 2 access ways.

◇ On **WLAN** interface, select Wi-Fi, tap **Wireless IP** to enter local IP, subnet mask, and gateway, and then tap **OK**.

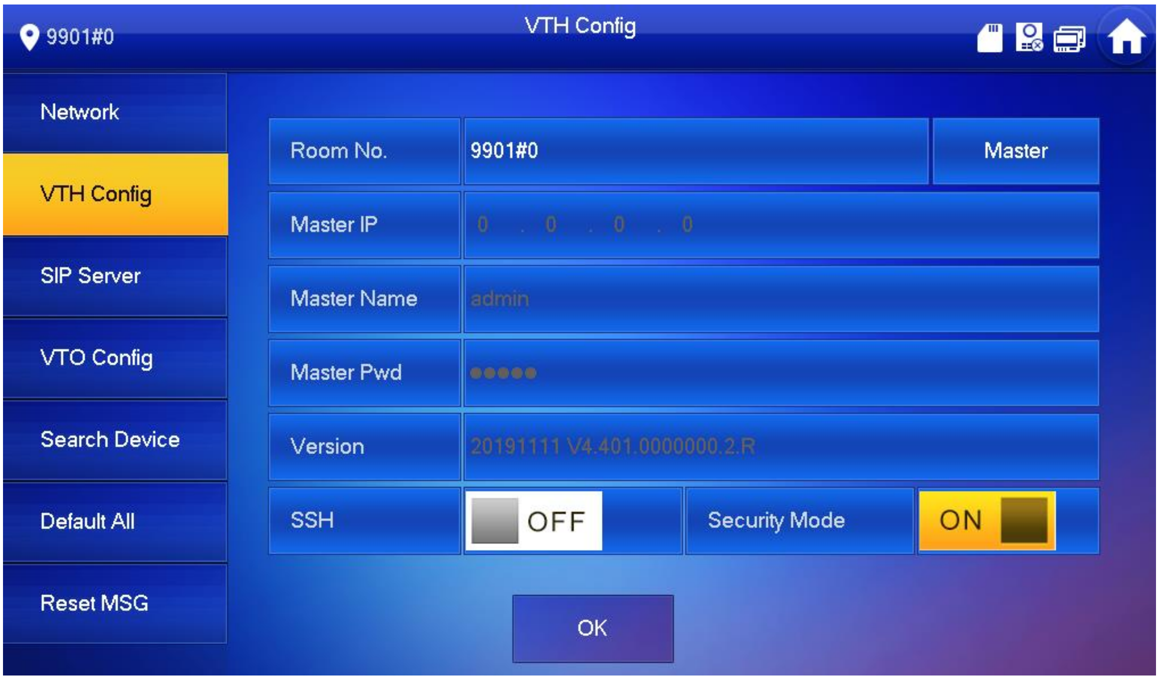
◇ At **WLAN** interface, select Wi-Fi, tap **Wireless IP**, tap OFF to enable DHCP function and obtain IP info automatically.

To obtain IP info with DHCP function, use a router with DHCP function.

Step 5 Tap **VTH Config**.

The **VTH Config** interface is displayed, see Figure 2-15.

Figure 2-15 VTH configuration



Room No.	9901#0
Master IP	0 . 0 . 0 . 0
Master Name	admin
Master Pwd	●●●●●
Version	20191111 V4.401.0000000.2.R
SSH	OFF
Security Mode	ON

- Be used as a master VTH.

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

- Room No. shall be the same with VTH Short No., which is set when adding VTH at web interface. Otherwise, it will fail to connect VTO.
- If there is extension VTH, room No. shall end with #0. Otherwise, it will fail to connect VTO.

- Be used as an extension VTH.

1) Tap **Master** and the icon switches to **Extension**.

2) Enter room No. (such as 101#1) and master IP (IP address of master VTH). Master name and master password are the user name and password of master VTH. Default user name is admin, and the password is the one set during device initialization.

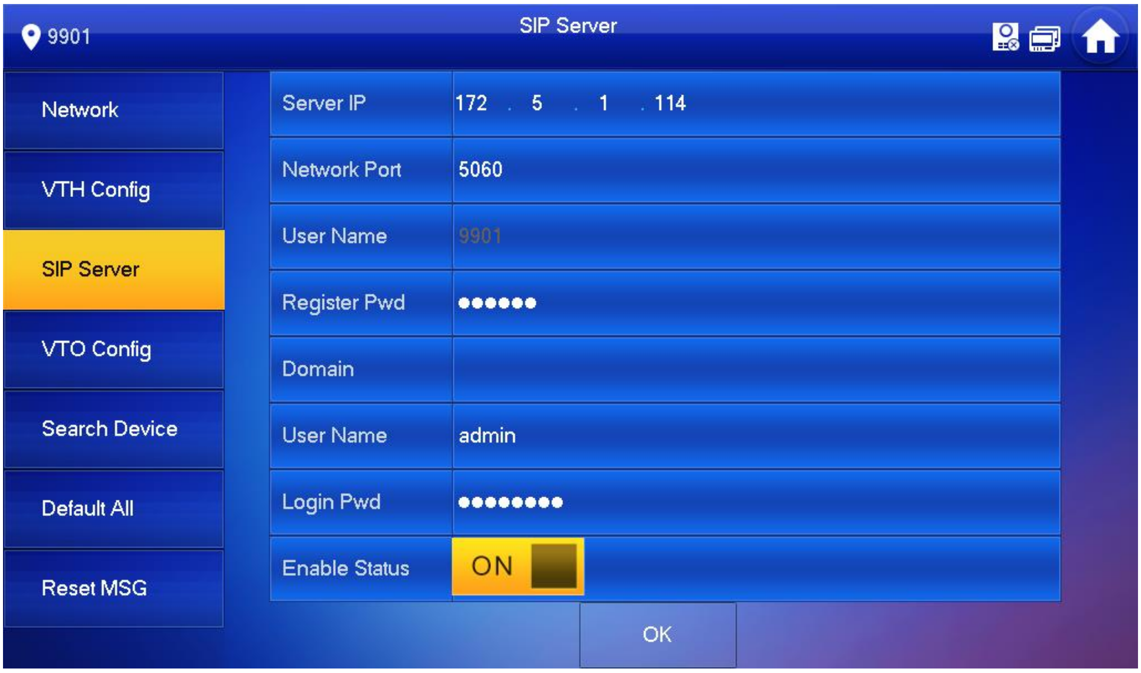
Security module is **On** by default, keep the default status.

3) Tap **OK** to save settings.

Step 6 Tap **SIP Server**.

The **SIP Server** interface is displayed, see Figure 2-16.

Figure 2-16 SIP server



Server IP: 172 . 5 . 1 . 114
Network Port: 5060
User Name: 9901
Register Pwd: ●●●●●●
Domain:
User Name: admin
Login Pwd: ●●●●●●●●
Enable Status: ON

1) Set parameters of SIP server by reference to Table 2-4.

Table 2-4 SIP server

Parameter	Description
Server IP	● When the platform works as SIP server, server IP is IP address of the platform. ● When VTO works as SIP server, server IP is 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	

Parameter	Description
Domain	Registration domain of SIP server, which can be null. When VTO works as SIP server, registration domain of SIP server shall be VDP.
User Name	User name and password to log in to SIP server.
Login Pwd	

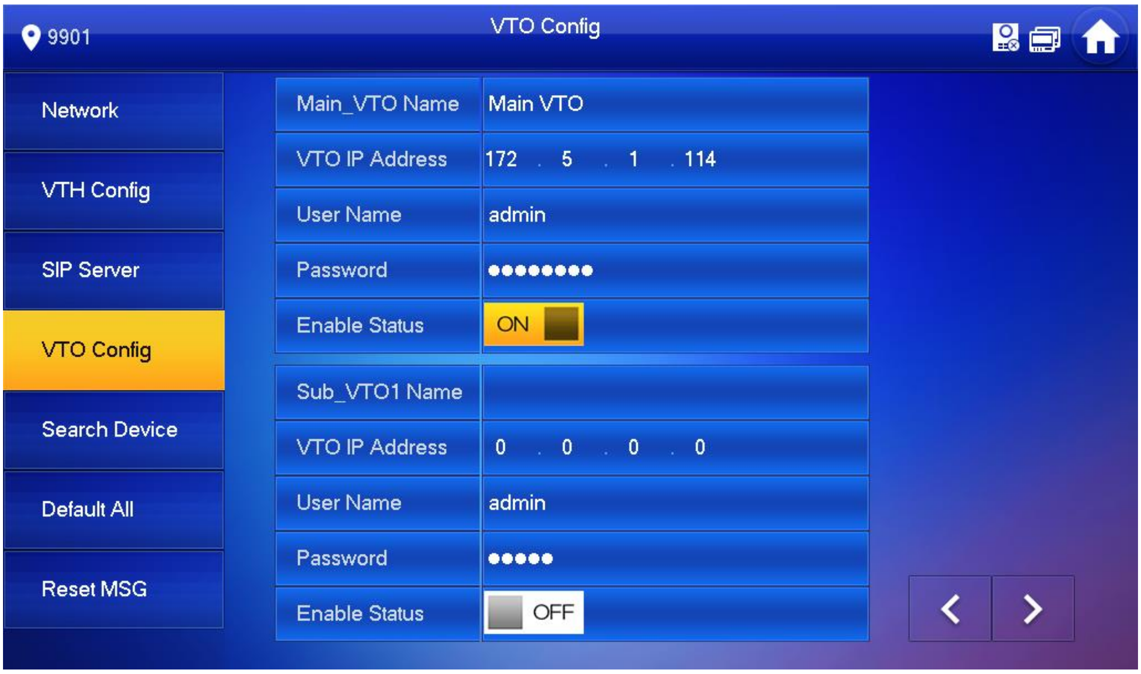
2) Set **Enable Status** to be ON.

3) Tap **OK** to save settings.

Step 7 Tap **VTO Config**.

The **VTO Config** interface is displayed, see Figure 2-17.

Figure 2-17 VTO configuration



Main_VTO Name	Main VTO
VTO IP Address	172 . 5 . 1 . 114
User Name	admin
Password	••••••••
Enable Status	ON
Sub_VTO1 Name	
VTO IP Address	0 . 0 . 0 . 0
User Name	admin
Password	•••••
Enable Status	OFF

Step 8 Add VTO or fence station.

- Add main VTO.

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

2) Switch the **Enable Status** to be ON.

User Name and Password shall the same as web login user name and password of VTO. Otherwise, it will fail to connect.

- Add sub VTO or fence station.

1) Enter sub VTO/fence station name, sub VTO/fence station IP address, user name, and password.

2) Switch the enable status to be ON.

Tap </> to turn page and add more sub VTO/fence stations.

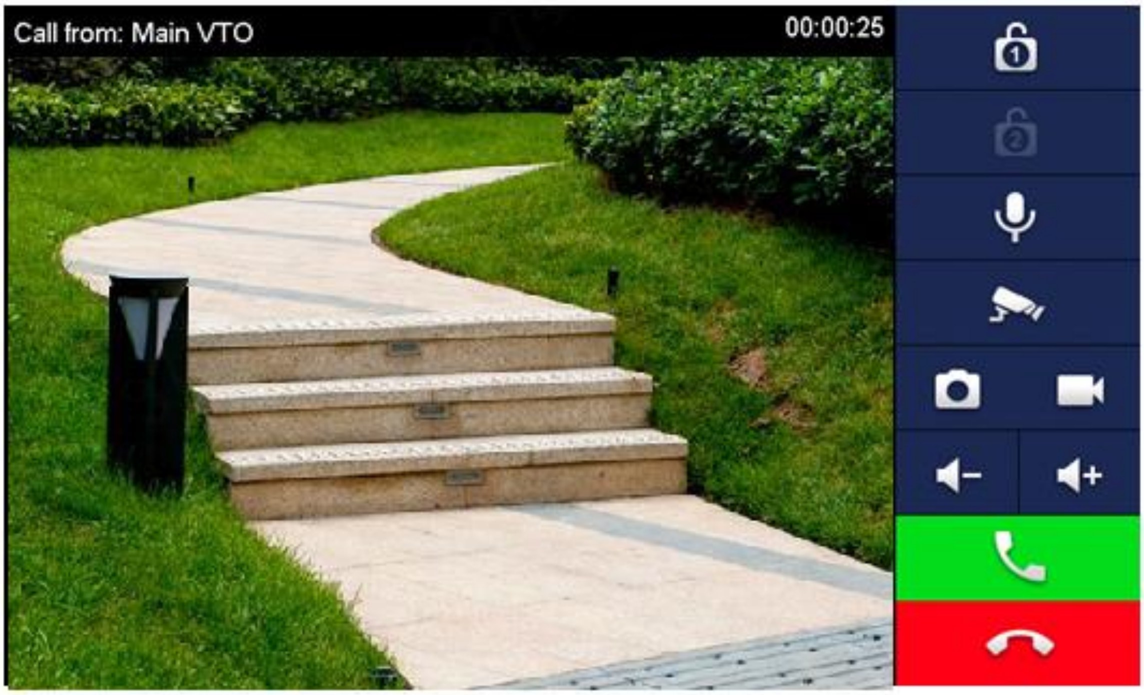
2.3 Debugging

2.3.1 VTO Calls VTH

Dial VTH room No. (such as 101) at VTO to call VTH. VTH pops up monitoring image and operating icon, see Figure 2-18.

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, fence station or IPC. Take VTO for example.

Select **Monitor > Door**, see Figure 2-19. Select the VTO to enter monitoring image, see Figure 2-20.

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

2.3.3 Device Upgrade

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

Figure 2-19 Door

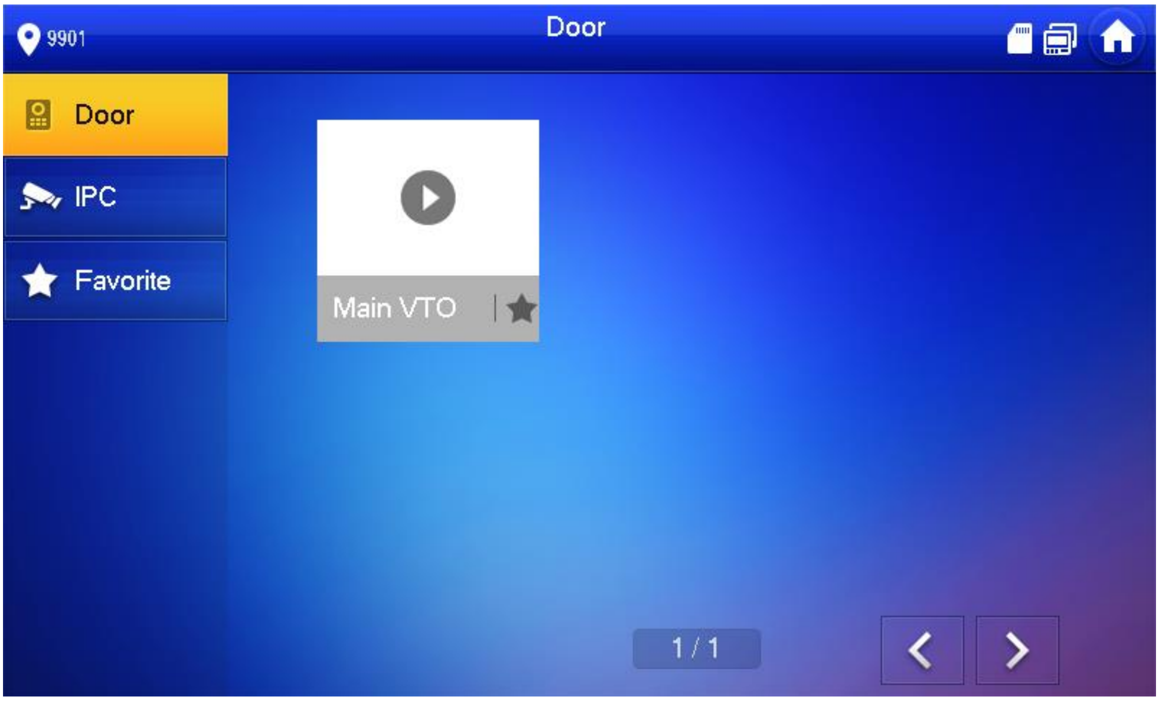
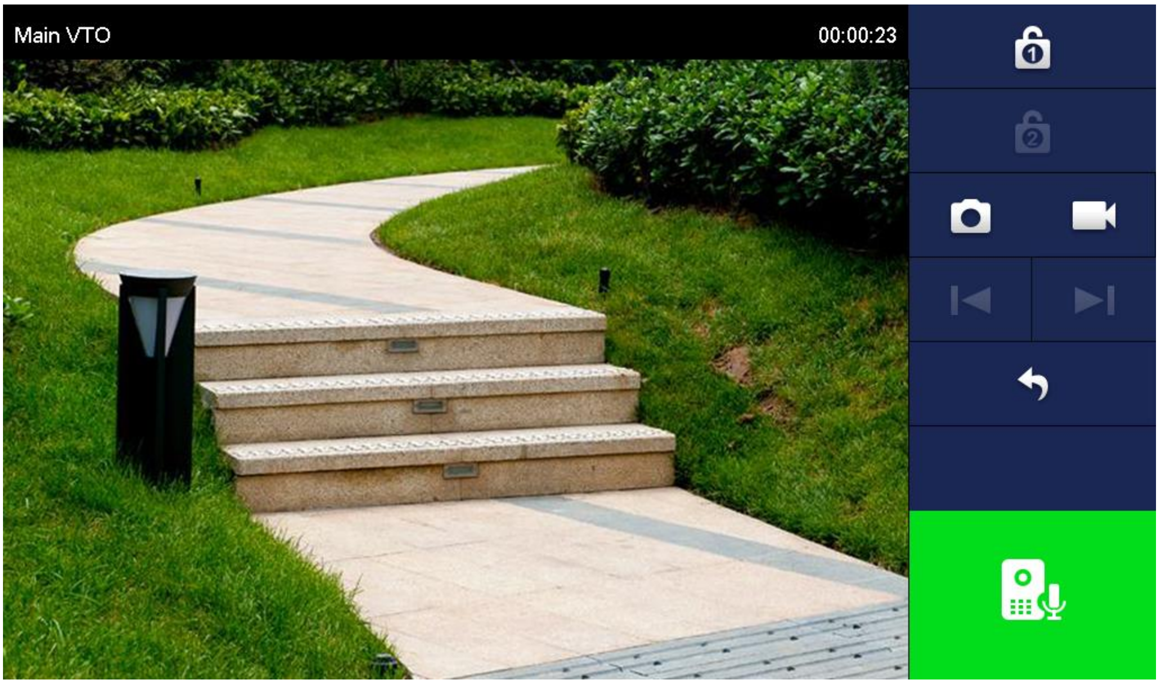


Figure 2-20 Monitoring image



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.