Digital Indoor Monitor (Model G)

Quick Start Guide

Foreword

General

This manual introduces basic operations of the digital indoor monitor (hereinafter referred to as "VTH").

Models

- Non 2-wire VTH that supports both Wi-Fi and PoE.
- Non 2-wire VTH that only supports PoE.
- 2-wire VTH that supports Wi-Fi.

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	Manual optimization.	February 2022
V1.0.0	First release.	November 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

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.
- 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

⚠ WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- 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.
- Make sure the power supply meets the SELV (Safety Extra Low Voltage) requirements, and rated voltage conforms to the IEC60065, IEC60950-1 or IEC62368-1 standard. The requirements of the power supply 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.
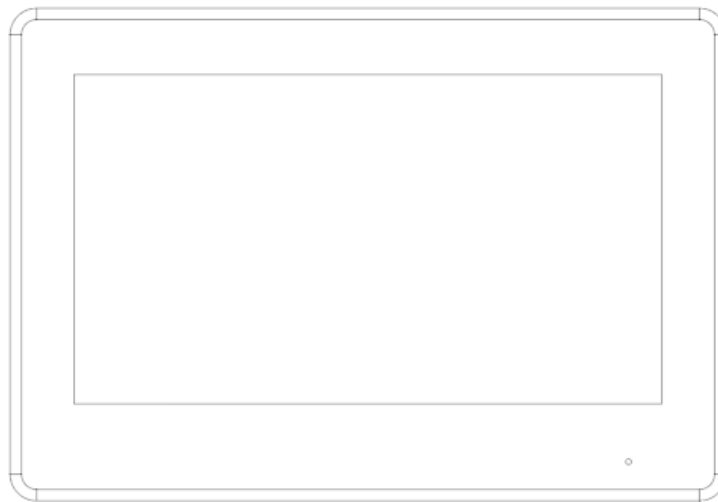
Table of Contents

1 Structure

The VTHs have the same front panel but differ in the ports in the rear panel. Some support 2-wire and others does not.

Slight differences might be found in the ports of the actual product.

1.1 Front Panel

Figure 1-1 Front panel

1.2 Rear Panel (2-wire)
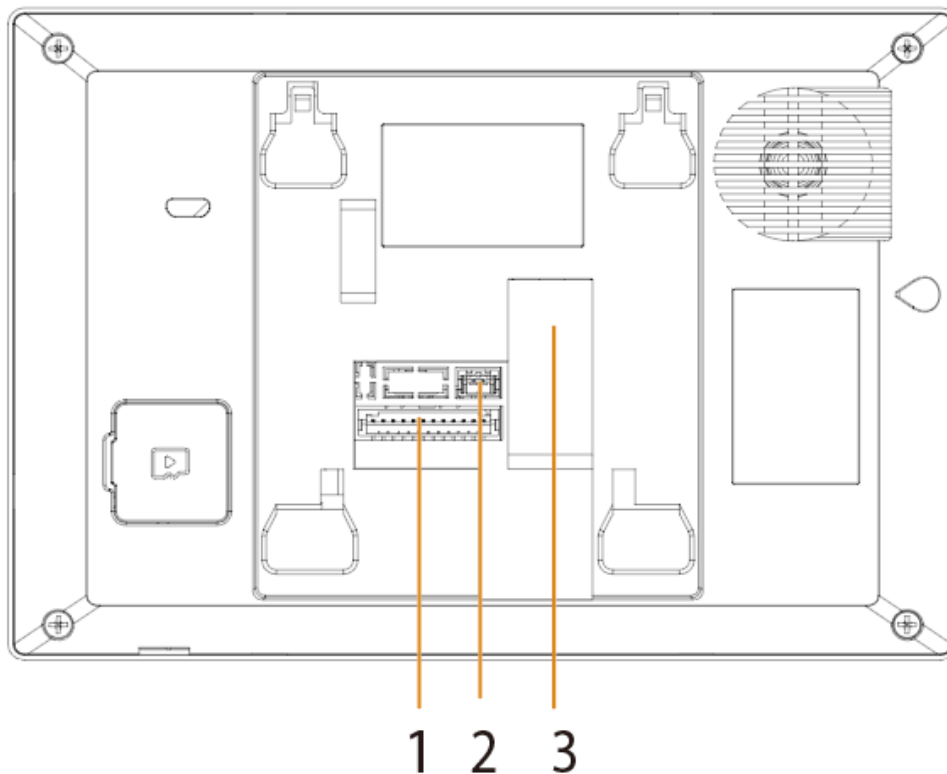
Figure 1-2 Rear panel for 2-wire model

Table 1-1 Components

No.	Name
1	Alarm port
2	2-wire port
3	Network port

1.3 Rear Panel (non 2-wire)

Figure 1-3 Rear panel for non 2-wire model
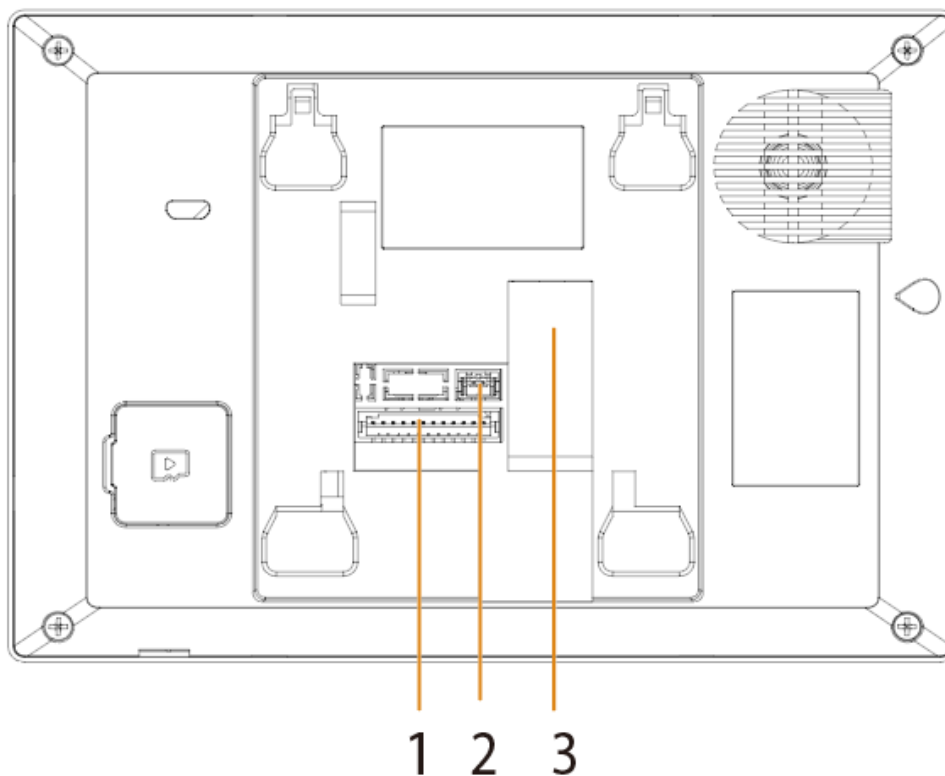
Table 1-2 Components

No.	Name
1	Alarm port
2	Power input port
3	Network port

2 Installation

2.1 Preparations

⚠️

- Do not install the VTH in harsh environment with condensation, high temperature, dust, corrosive substance and direct sunlight.
- In case of abnormality after powering on the VTH, cut off the power supply at once, and unplug the network cable. Power on after troubleshooting.
- Installation should be done by professional teams. Do not dismantle or repair the device by yourself in case of device failure. Contact after-sales service if you need any help.

2.2 Wall-mounted Installation

Directly install the VTH 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 top of the device into the top of the installation bracket, and then push in the bottom of the VTH.

Figure 2-1 Wall-mounted installation

Host   Installation   Wall
            Bracket
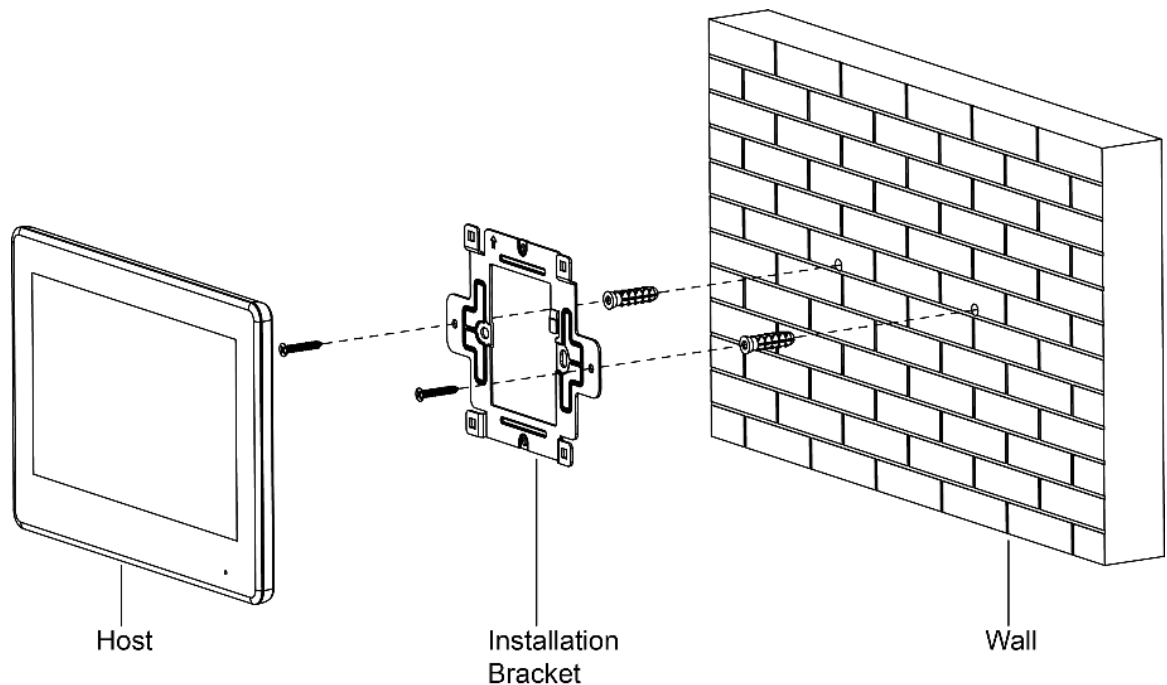
3 VTO Configuration

This chapter provides a step-by-step configuration of the VTO. Follow the instructions below to get started.

📖

The snapshots are for reference only and slight differences might be found in the actual web page of the VTO depending on your model.

3.1 Configuration Tool

You can download the configuration tool VDPConfig and use it to configure and update multiple devices. For more details, see the corresponding user's manual.

3.2 Initialization

For the first time login, you need to initialize the VTO.

Step 1 Power on the VTO.

Step 2 Go to the default IP address (192.168.1.108) of the VTO in the browser address bar, and then press the Enter key to go to the web page of the VTO.

📖

- The user name is admin by default.
- Make sure that the IP address of the PC is on the same network segment as the VTO.

Step 3 On the **Device Init** page, enter and confirm the password, and then click **Next**.

📖

The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).

Figure 3-1 Device initialization
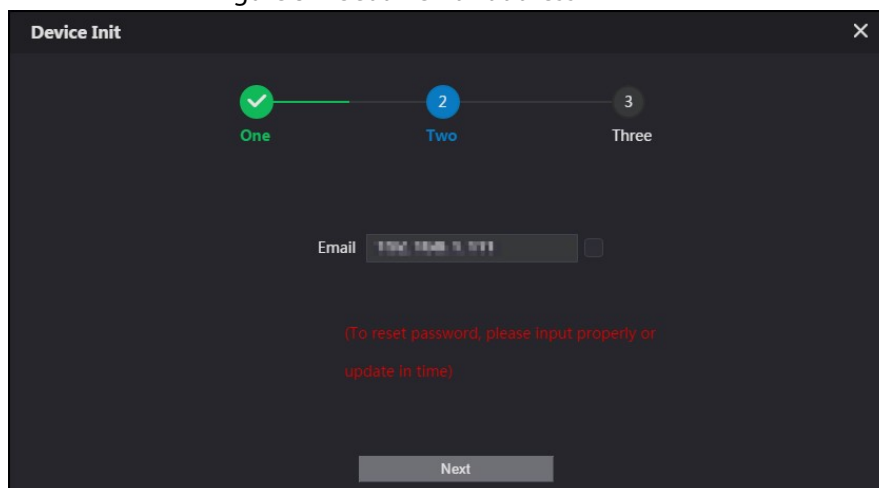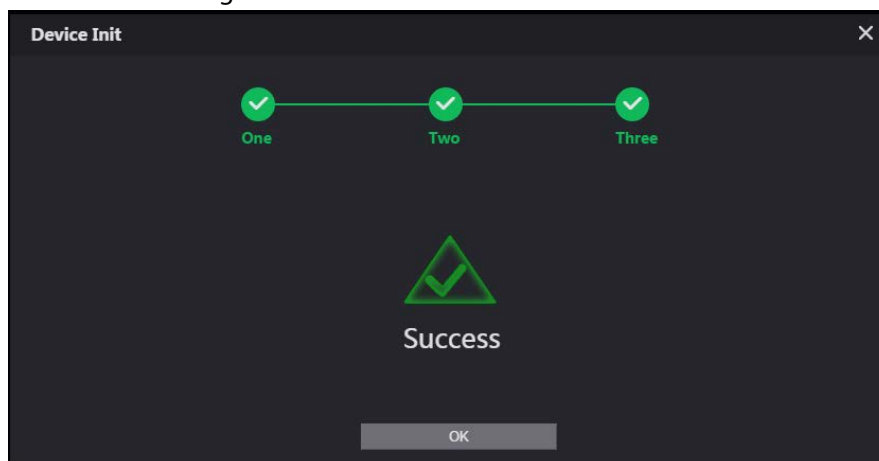
Step 4   Select the **Email** checkbox and enter email address.

This helps you to reset your password when your password is lost or forgotten.
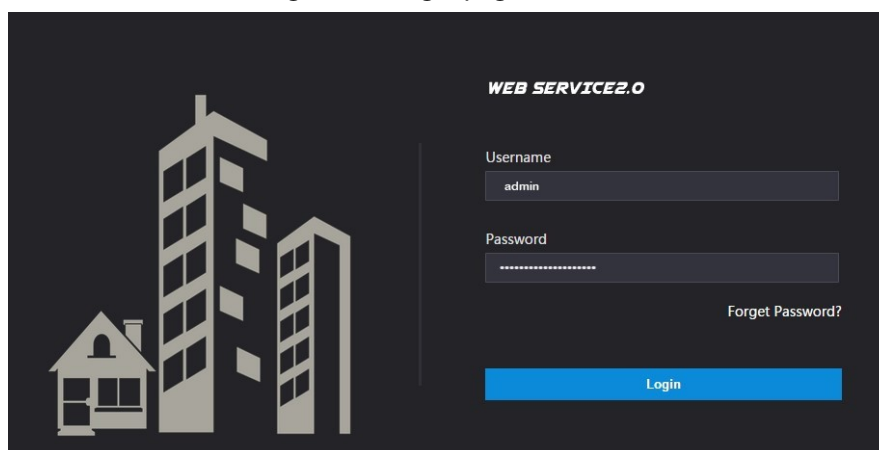
Figure 3-2 Set an email address

Step 5   Click **Next**.

Figure 3-3 Initialization successful

Step 6   Click **OK**.

Enter username (admin by default) and the new password to log in to the web page.

Figure 3-4 Login page
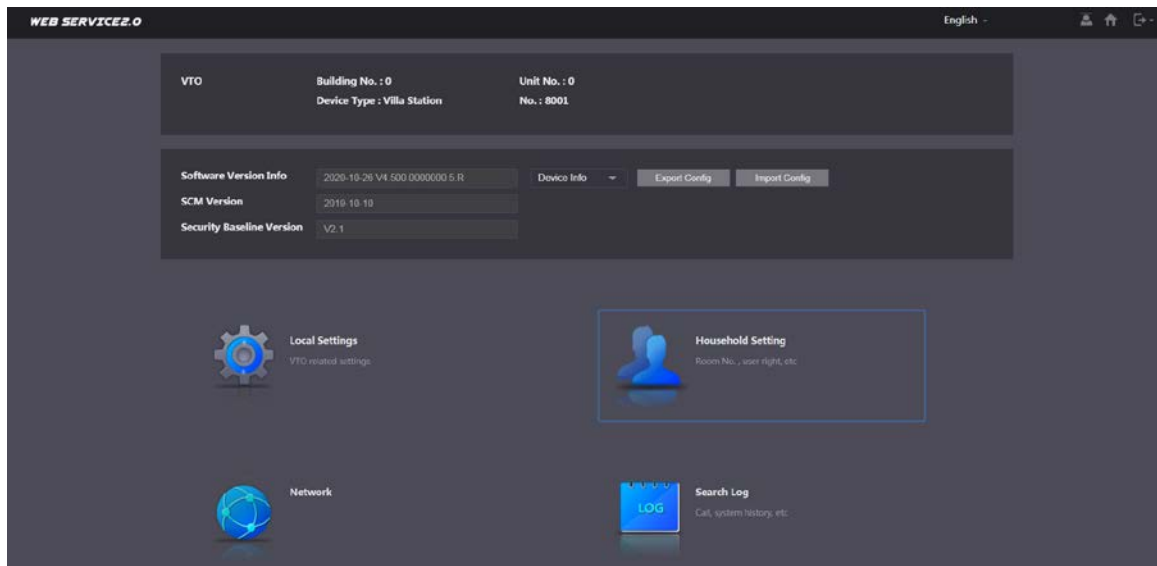
3.3 Configuring VTO Number

Numbers can be used to distinguish each VTO, and we recommend you set it according to the unit or building number.

📖
- You can change the number of a VTO when it is not working as the SIP server.
- A VTO number can contain up to 5 numbers, and it cannot be the same as any room number.
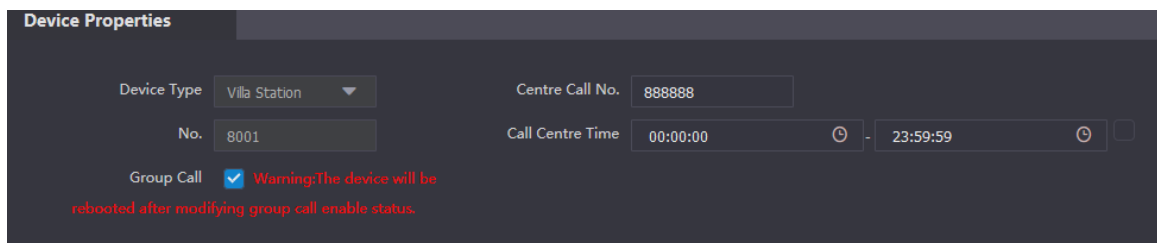
Step 1 Log in to the VTO web page.

Figure 3-5 Home page

Step 2 Select **Local Settings > Basic**.
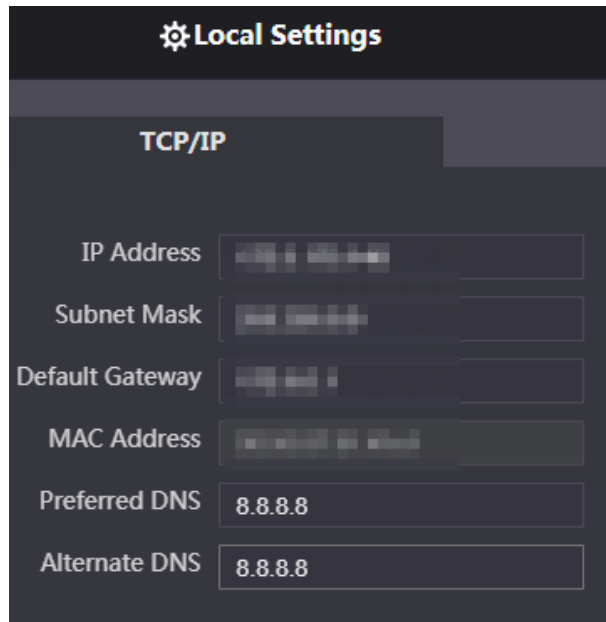
Figure 3-6 Device properties

Step 3 Enter the number in **No.**, and then click **Confirm**.

3.4 Configuring Network Parameters

Step 1 Select **Network > Basic**.

Figure 3-7 TCP/IP information

Figure 3-7 TCP/IP information

Step 2   Enter each parameter, and then click **Save**.

The VTO will automatically restart. You need to add the IP address of your PC to the same network segment as the VTO to log in again.

3.5 Configuring SIP Server

When connected to the same SIP server, all VTOs and VTHs can call each other. You can use a VTO or other servers as the SIP server.

Step 1   Select **Network > SIP Server**.

Figure 3-8 SIP server
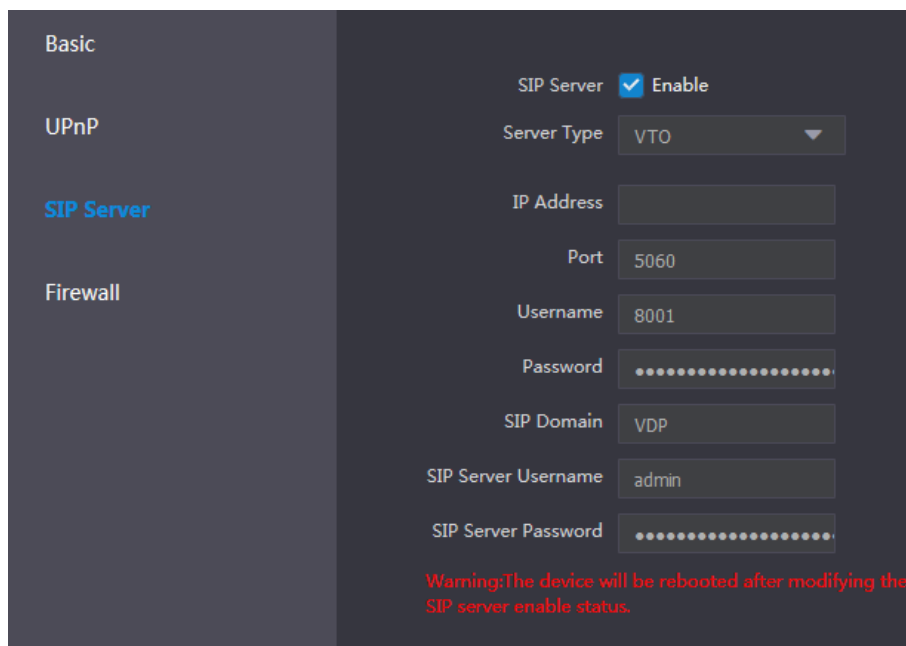
Step 2   Select the server type as needed.

- If the current VTO works as the SIP server, enable **SIP Server**, and then click **Save**.

The VTO will automatically restart, and then you can add other VTOs and VTHs to this VTO.

📖

If the current VTO does not work as the SIP server, do not enable **SIP Server**. Otherwise the connection with this VTO will fail.

- If other VTOs work as the SIP server, set **Server Type** as VTO, and then configure the parameters.

Table 3-1 SIP server configuration

Parameter	Description
IP Addr.	The IP address of the VTO that works as the SIP server.
Port	5060 by default when VTO work as SIP server. 5080 by default when the platform works as SIP server.
Username	Leave it as default.
Password	
SIP Domain	Leave it as default.
SIP Server Username	SIP server web page login username and password.
SIP Server Password	

- If other servers work as the SIP server, set **Server Type** as needed, and then see the corresponding manual for details.

3.6 Configuring Call Number and Group Call

To dial and call a VTO, you need to configure the call number on each VTO that works as the phone number.

Step 1   Select **Local Settings > Basic**.

Figure 3-9 Device properties

Step 2   In the **No.** input box, enter the room number you need to call, and then click **Confirm** to save. Repeat this operation on every villa door station (VTO) web page.

On the SIP server, you can enable group call function. When calling a main VTH, all extension VTH will also receive the call.

📖

The VTO will restart after enabling or disabling the group call function.

Step 3   Log in to the SIP server web page, and then select **Local Settings > Basic**.

Step 4   Enable **Group Call**, click **Confirm**, and then the VTO will restart.

3.7 Adding VTOs

You can add VTOs to the SIP server, and all the VTOs connected to the same SIP server can make video call to each other. This section is applicable when a VTO works as the SIP server, and if you are using other servers as the SIP server, see the corresponding manual for the detailed configuration.

Step 1   Log in to the web page of the SIP server, and then select **Household Setting > VTO No. Management**.

Figure 3-10 VTO No. management
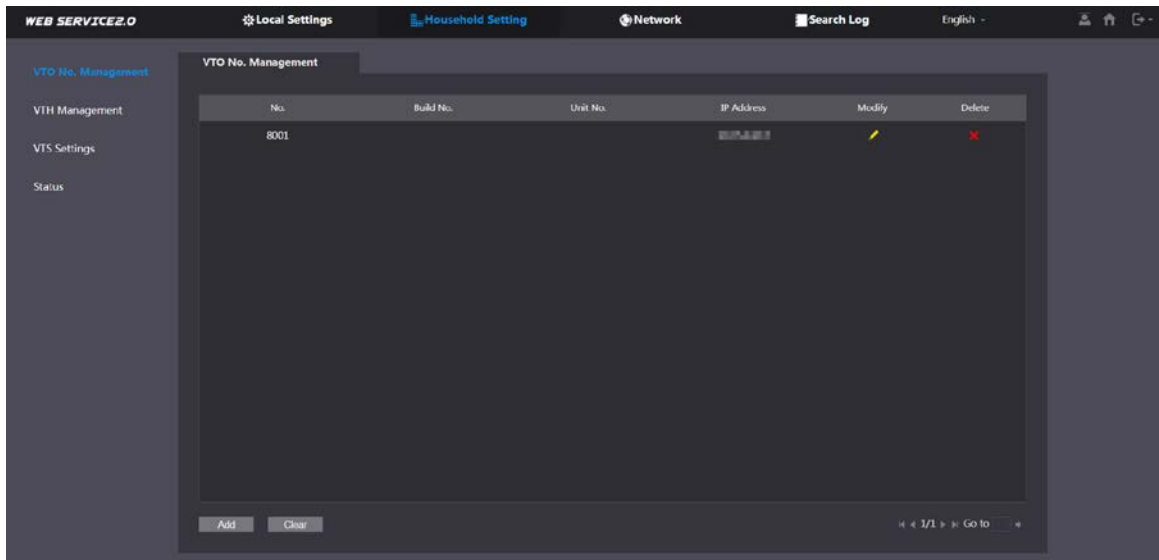
Step 2   Click **Add**.

Figure 3-11 Add VTO

Step 3   Configure the parameters.

The SIP server must be added.

Table 3-2 Add door stations (VTO)

Parameter	Description
Rec No.	VTO number.

Register Password	Keep the default value.
Build No.	Available only when other servers work as the SIP server.
Unit No.	
IP Address	VTO IP address.
Username	VTO web page login username and password.
Password	

Step 4   Click **Save**.

3.8 Adding Room Number

You can add room numbers to the SIP server, and then configure the room number on VTHs to connect them to the network. This section is applicable when a VTO works as the SIP server, and if you use other servers as the SIP server, see the corresponding manual for the detailed configuration.

📖

The room number can contain 6 digits of numbers or letters or their combination at most, and it cannot be the same as any VTO number.

Step 1   Log in to the webpage of the SIP server, and then select **Household Setting > Room No. Management**.

Figure 3-12 Room number management
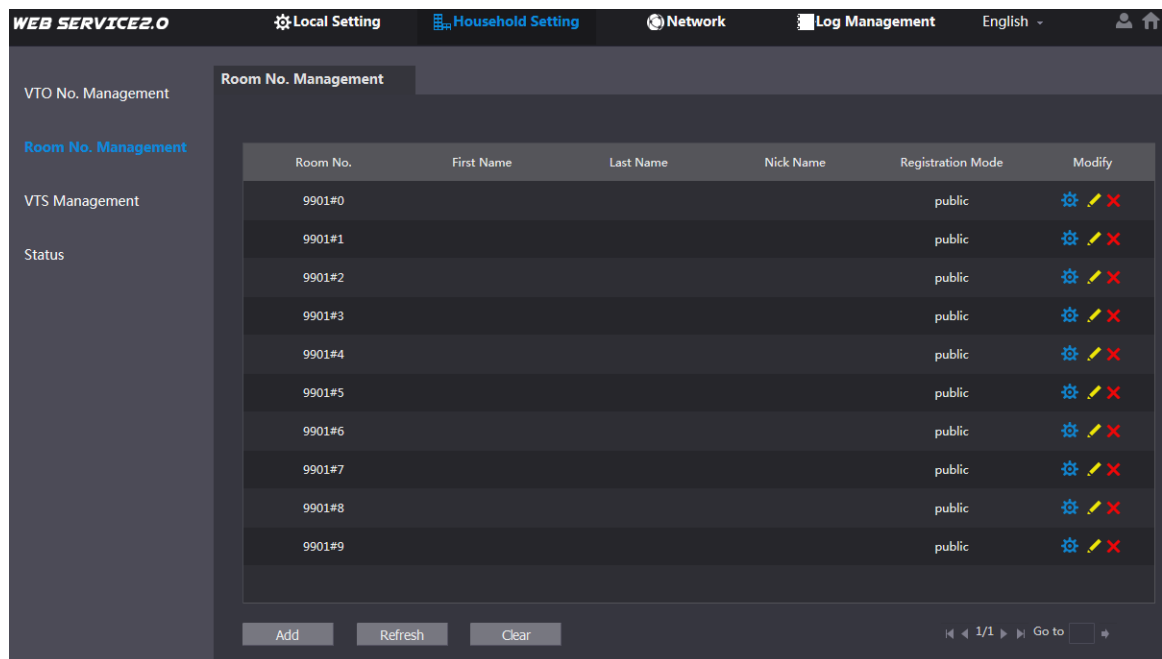
Step 2   Click **Add**.

Figure 3-13 Add a single room number

Step 3   Configure room information.

Table 3-3 Room information

Parameter	Description
First Name	Information used to differentiate each room.
Last Name	
Nick Name	
Room No.	Room number. ● When there are multiple VTHs, the room number for the main VTH should end with #0, and the room numbers for extension VTHs with #1, #2… ● You can configure up to 9 extension VTHs for one main VTH.
Registration Mode	Select **public**.
Registered Password	Keep the default value.

Step 4   Click **Save**.

Click [✏] to modify room information, and click [✖] to delete the room.

4 VTH Configuration

This chapter introduces the configuration of the VTH and how to achieve the intercom function. Follow the instructions below to get started.

4.1 Before You Begin

- Make sure that there is no short or open circuit in the VTO and VTH.
- Plan IP and number (working as a phone number) for each VTO and VTH. Make sure that the VTH and VTO are on the network segment.

4.2 Quick Configuration

For the first-time login, you could initialize and configure the VTH through quick configuration.
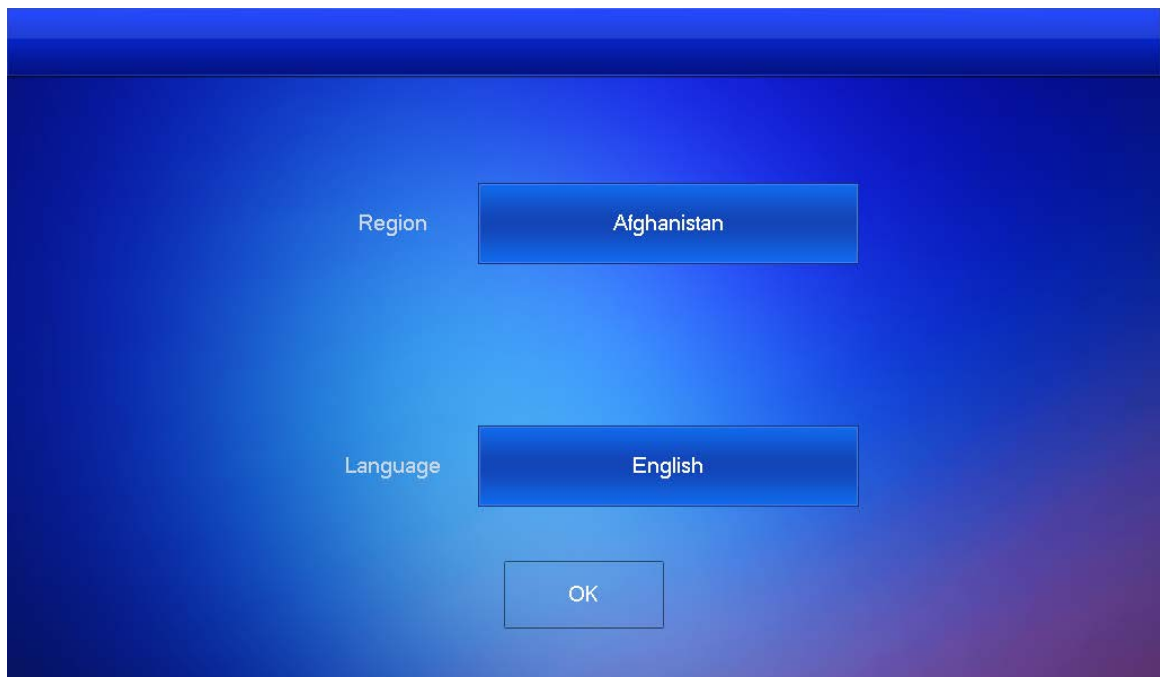
📖

The quick configuration enables you to configure the parameters of the VTO, VTH and the SIP server at once. If you want to modify the parameters, see "4.3 Manual Configuration ".

Step 1   Power on the VTH.

Step 2   Select a region and language, and then tap **OK**.

Figure 4-1 Region and language

Step 3   Set the quick configuration type as **Villa**, and then tap **OK**.

Figure 4-2 Quick configuration
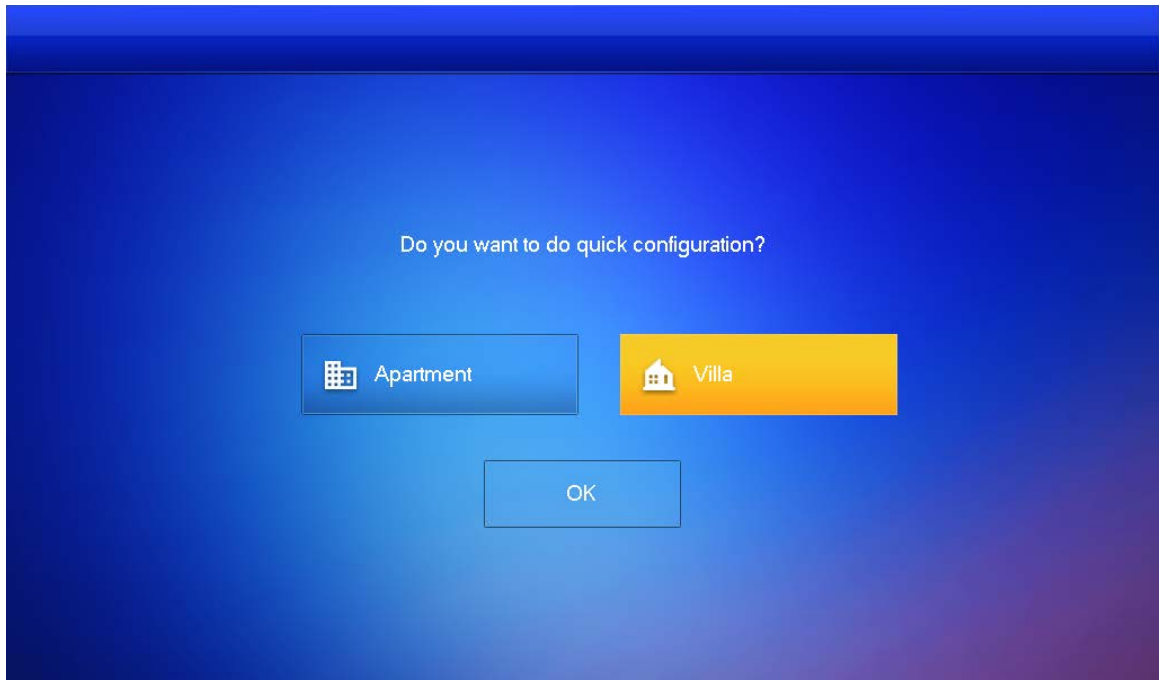
Step 4   Select **First-time Config**, and then tap **OK**.

Figure 4-3 Config mode

Step 5   Select **Static IP**, enter your planned VTH IP, net mask and gateway, and then tap **Next**.
Step 6   On the **Set VTH Password** screen, enter and confirm the password, and enter the email address, and then tap **Next**.

Figure 4-4 Set password for VTH

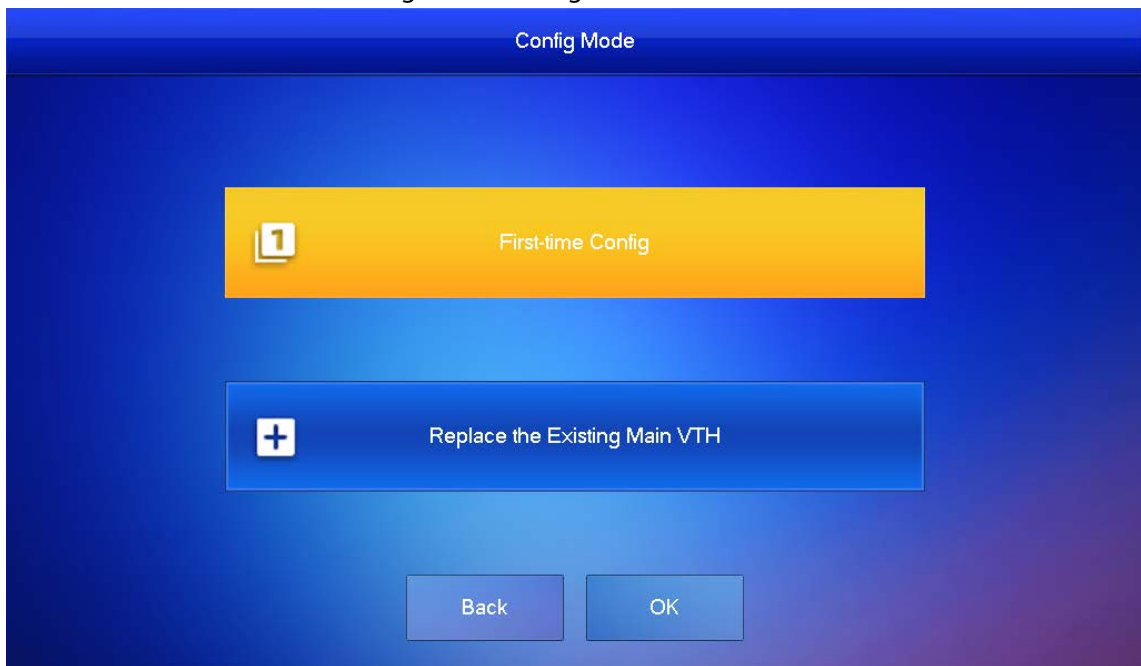Step 7 On the **Set VTO Password** screen, enter the password of VTO and confirm it, and then tap **Next**.

Figure 4-5 Set password for VTO

Step 8 Tap **Initialize** to complete the initialization of the VTO and the main VTH, and then tap **Next**. You need to make sure that the IP addresses of the VTH and VTO on the same network segment. Otherwise, VTH cannot obtain the information of VTO after configuration.

Figure 4-6 Initialize the devices
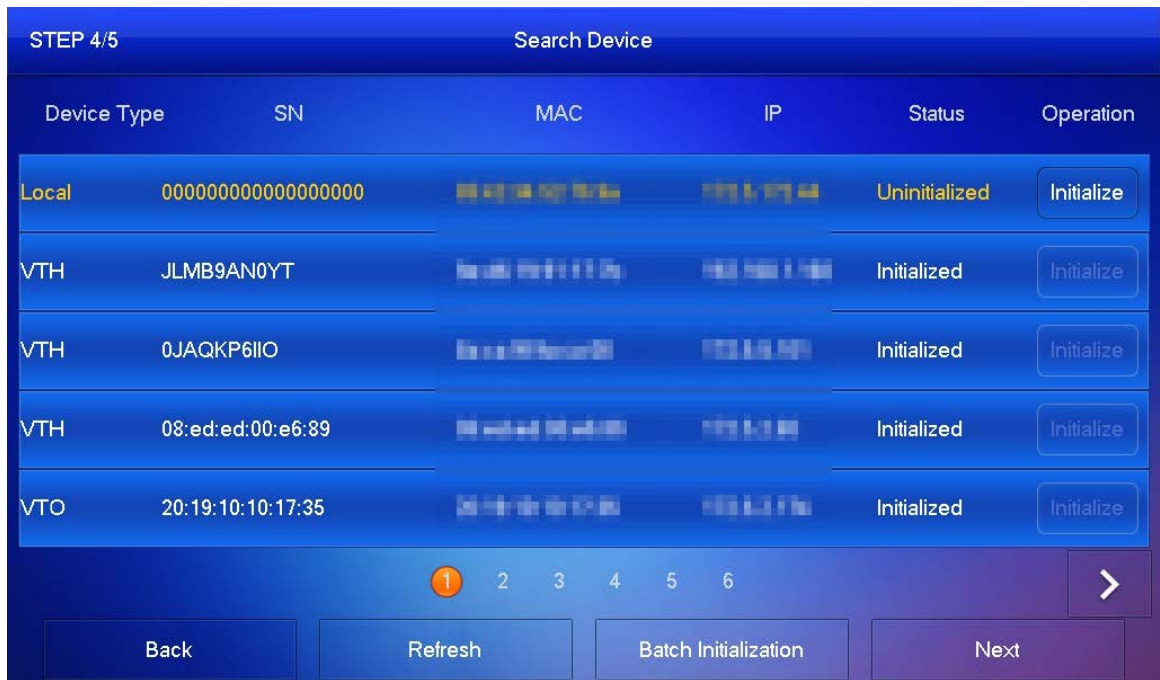
Step 9   Tap **One-key Config** to finish the configuration of the VTO and VTH, as well as the SIP server. The status bar will suggest whether your configuration is successful.

4.3 Manual Configuration

You could manually configure the parameters you want to modify.

4.3.1 Configuring Network Parameters

You can choose to connect the VTH to the network either through WLAN or LAN.

4.3.1.1 WLAN

Step 1   Tap and hold **Setting** for about 3 seconds, and enter the password that you set for the VTH.
Step 2   Tap **Network > WLAN**.
Step 3   Enable [OFF] to see all the usable networks.
Step 4   Before connecting to a Wi-Fi network, do either of the following first.
● Tap **WireLessIP**, enter local IP, subnet mask and gateway that you plan for the VTH, and then tap **OK**.
● Tap **WireLessIP**, tap [OFF] to enable the DHCP function to obtain IP information automatically.

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

Step 5   On the **WLAN** screen, tap the Wi-Fi name, and then enter password to connect to the network.

Figure 4-7 WLAN
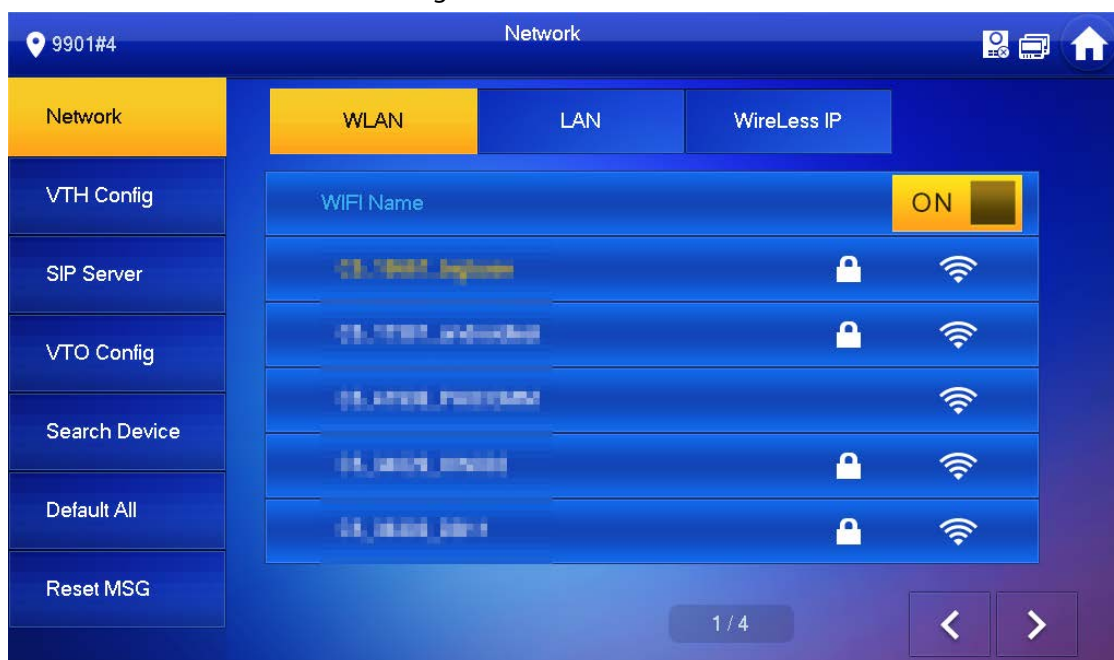
4.3.1.2 LAN

Step 1   Tap and hold **Setting** for about 3 seconds, and enter the password that you set for the VTH.

Step 2   Tap **Network > LAN**.

Step 3   Enter local IP subnet mask and gateway that you plan for the VTH.

You can also tap [OFF] to enable the DHCP function to obtain IP information automatically.

Figure 4-8 LAN

Step 4   Tap **OK**.

4.3.2 Configuring SIP Server

Step 1   Tap and hold **Setting** for about 3 seconds, and enter the password that you set for the VTH.

Step 2   Tap **SIP Server.**

Figure 4-9 SIP server

Step 3   Configure the SIP server parameters.
Step 4   Set **Enable Status** to [ON].
Step 5   Tap **OK**.

Table 4-1 SIP server

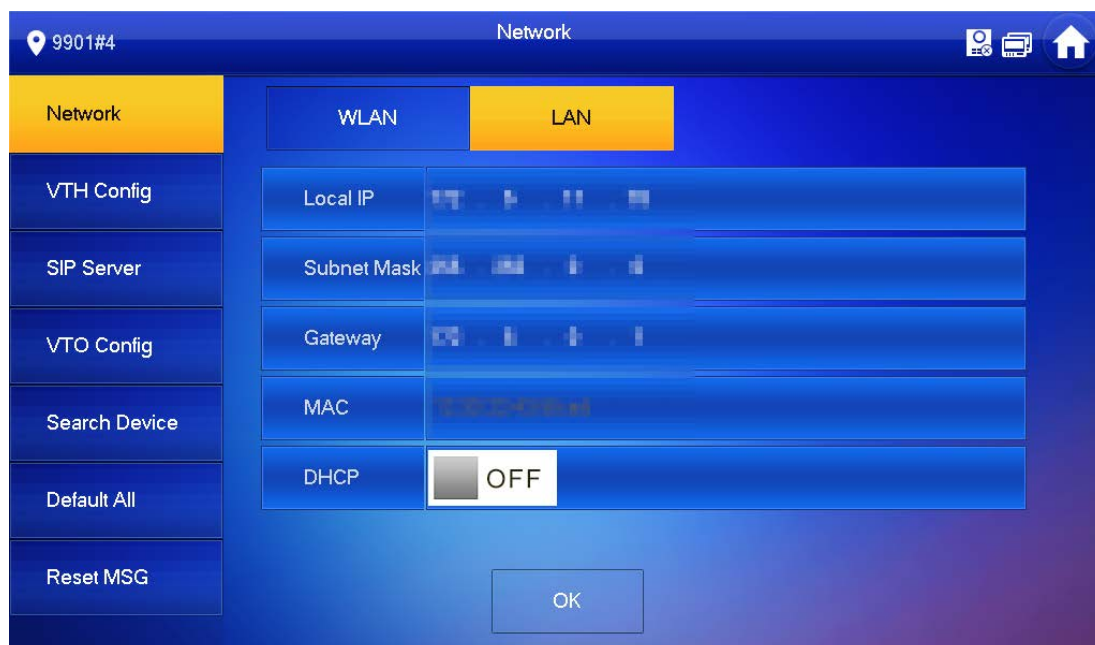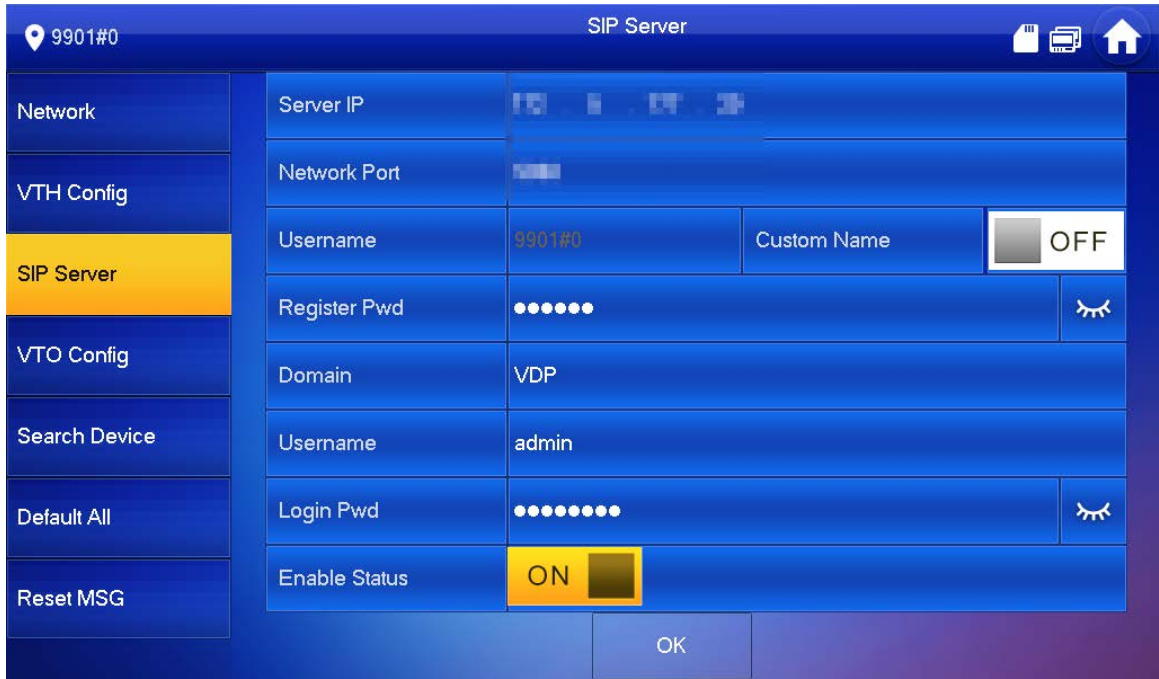| Parameter	Description
Server IP	- When the platform works as SIP server, server IP is the IP address of the platform. - When VTO works as SIP server, server IP is the IP address of the VTO.
Network Port	- When the platform works as SIP server, the network port is 5080. - When VTO works as SIP server, the network port is 5060.
Username	Leave it as default.
Register Pwd	
Domain	Registration domain of SIP server, which can be null. When VTO works as SIP server, registration domain of SIP server is VDP.
Username	Username and password to log in to SIP server.
Login Pwd	

4.3.3 Configuring VTH

Step 1   Tap and hold **Setting** for about 3 seconds, and enter the password that you set for the VTH.
Step 2   Tap **VTH Config.**

Figure 4-10 VTH configuration
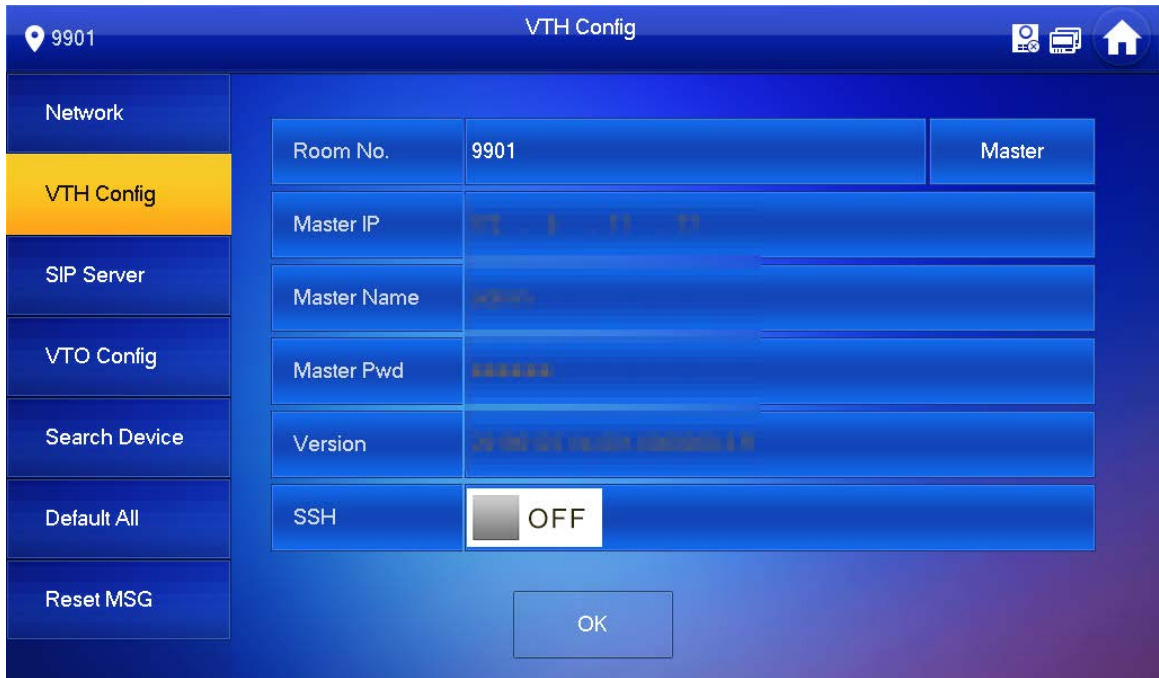
Step 3   Enter room number (such as 9901 or 101#0).
         If there is an extension VTH, room number must end with #0. Otherwise, it will fail to connect to VTO.
Step 4   Tap **OK**.

4.3.4 Configuring VTO

Step 1   Tap and hold **Setting** for about 3 seconds, and enter the password that you set for the VTH.
Step 2   Tap **VTO Config.**

Figure 4-11 VTO configuration
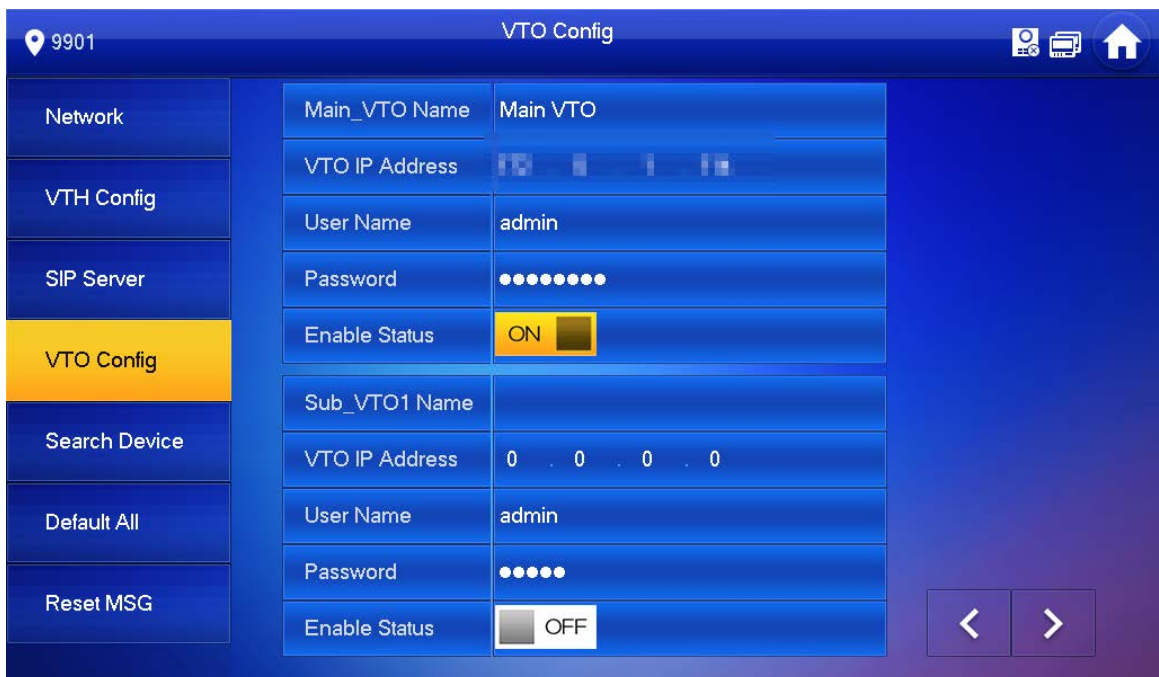
Step 3   Add VTO.

4.3.4.2 Adding Main VTO

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

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

Step 3 Check whether the configuration is successful by checking the status bar at the top right corner.

4.3.4.3 Adding Sub VTO

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

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

Step 3 Check whether the configuration is successful by checking the status bar at the top right corner.

5 Commissioning

After the basic configuration is complete, check whether the intercom function can work.

5.1 VTO Calling VTH

Step 1   Dial a room number on the VTO (for example, 9901).

Step 2   Tap [icon] on the VTH to answer the call.

Figure 5-1 Call VTH from VTO

5.2 VTH Monitoring VTO

A VTH can monitor VTO.

Step 1   On the home screen, select **Monitor > Door.**

Step 2   Set the VTO to go to the monitoring page.

Step 3   Tap the icon to view the VTO video.

[icon]

The following figure means that SD card has been inserted into VTH. If SD card is not inserted, recording and snapshot icons are gray.
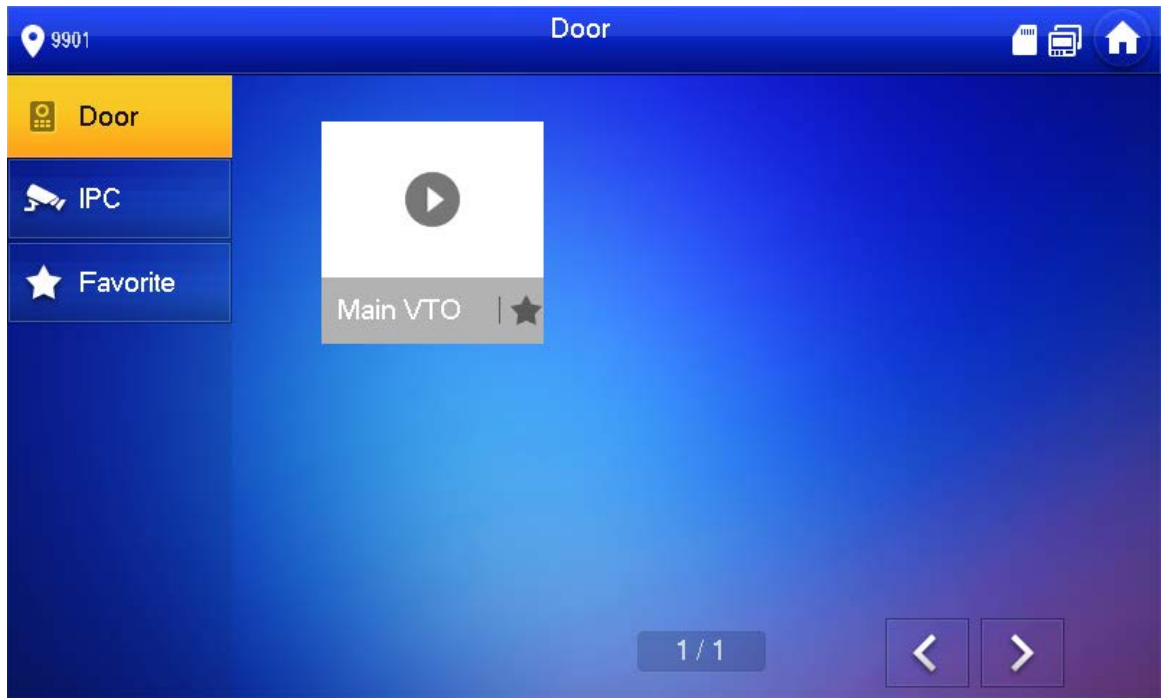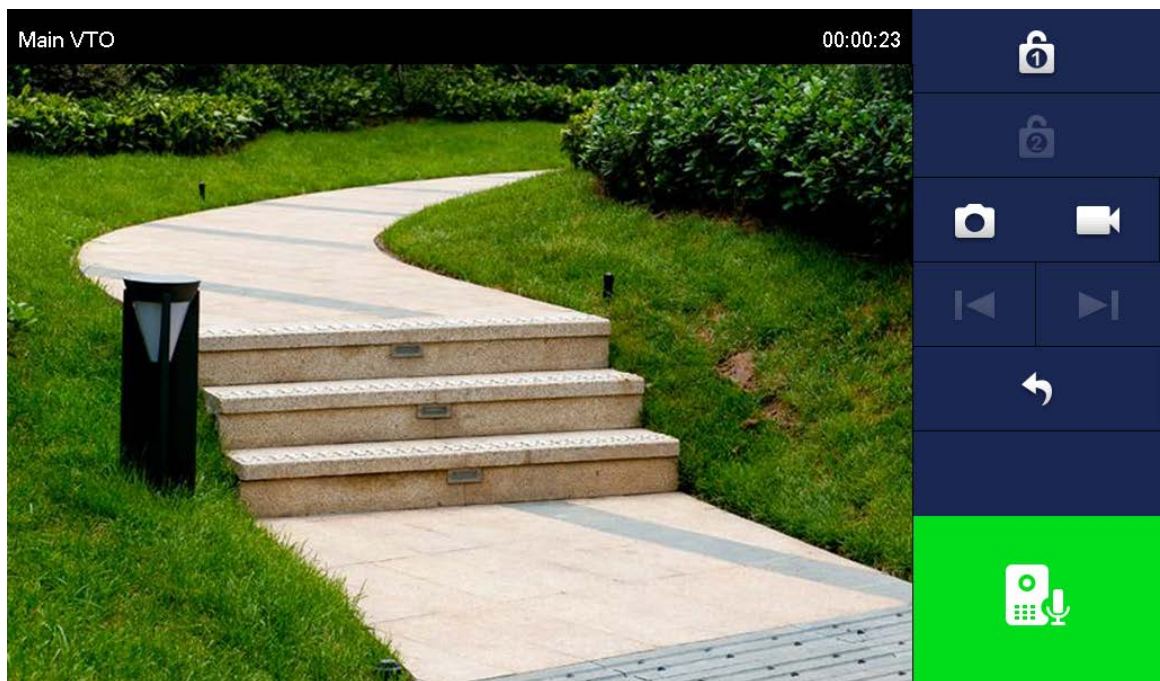
Figure 5-2 Door

Figure 5-3 Monitoring device

Appendix 1 Cybersecurity Recommendations

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.