Face Recognition Apartment Outdoor Station

Quick Start Guide

V1.0.0

Cybersecurity Recommendations

Important

The following functions are for reference only. Some series products may not support all the functions listed below.

Mandatory actions to be taken towards cybersecurity

● Change Passwords and Use Strong Passwords:

The number one reason systems get "hacked" is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

● Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

"Nice to have" recommendations to improve your network security

● Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

● Change Default HTTP and TCP Ports:

◇ Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

◇ These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

● Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

● Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

● Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

● Forward Only Ports You Need:

◇ Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

◇ You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

● Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

● Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

● Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

● UPnP:

◇ ● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.

◇ ● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

● SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

● Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

● Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

● Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

● Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

● Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

Cybersecurity Recommendations   III

Regulatory Information

The regulatory information herein might vary according to the model you purchased. Some information is only applicable for the country or region where the product is sold.

FCC Information

⚠ CAUTION

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC conditions:

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

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC compliance:

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication.

- For class A device, these limits are designed to provide reasonable protection against harmful interference in a commercial environment. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
- For class B device, these limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment 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.

Table of Contents

Foreword

General

This Guide introduces the structure, mounting process, and basic configuration of the Face Recognition Apartment Outdoor Station.

Safety Instructions

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

Signal Words	Meaning
⚠ 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.
📖 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Date
1	V1.0.0	First release	2018.09

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide 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 Guide.
- The Guide 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 Guide. 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 Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

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.

Electrical safety

- All installation and operation should conform to your local electrical safety codes.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with voltage rated by DC 12 V or AC 24 V according to the Limited power Source requirement of IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Make sure the power supply is correct before operating the device.
- A readily accessible disconnect device shall be incorporated in the building installation wiring
- Prevent the power cable from being trampled or pressed, especially the plug, power socket and the junction extruded from the device.
- We assume no liability or responsibility for all the fires or electrical shock caused by improper handling or installation.

Environment

- Do not aim the device at strong light to focus, such as lamp light and sun light, otherwise it might cause over brightness or light marks, which are not the device malfunction, and affect the longevity of Charge Coupled Device (CCD) or Complementary Metal-Oxide Semiconductor (CMOS).
- Do not place the device in a damp or dusty environment, extremely hot or cold temperatures, or the locations with strong electromagnetic radiation or unstable lighting.
- Keep the camera away from water or other liquid to avoid damages to the internal components.
- Keep the indoor device away from rain or damp to avoid fire or lightning.
- Keep sound ventilation to avoid heat accumulation.
- Transport, use and store the device within the range of allowed humidity and temperature.
- Heavy stress, violent vibration or water splash are not allowed during transportation, storage and installation.
- Pack the device with standard factory packaging or the equivalent material when transporting the device.

1 Introduction

This face recognition apartment outdoor station (hereinafter referred to be "the VTO") can be connected to the video intercom home station (VTH), video intercom master station (VTS), and servers to constitute a video intercom system, which supports video call between visitors and residents. The VTO supports unlocking by face recognition and fingerprint recognition. It also supports security functions, including emergency call, information publishing, and history viewing. The VTO is applicable in residence communities and villa areas; together with a management server, it can provide overall burglar proof, disaster prevention, and security surveillance.

2 Appearance

2.1 Dimension

See Figure 2-1 for the dimension.

Figure 2-1 Dimension(unit: mm)
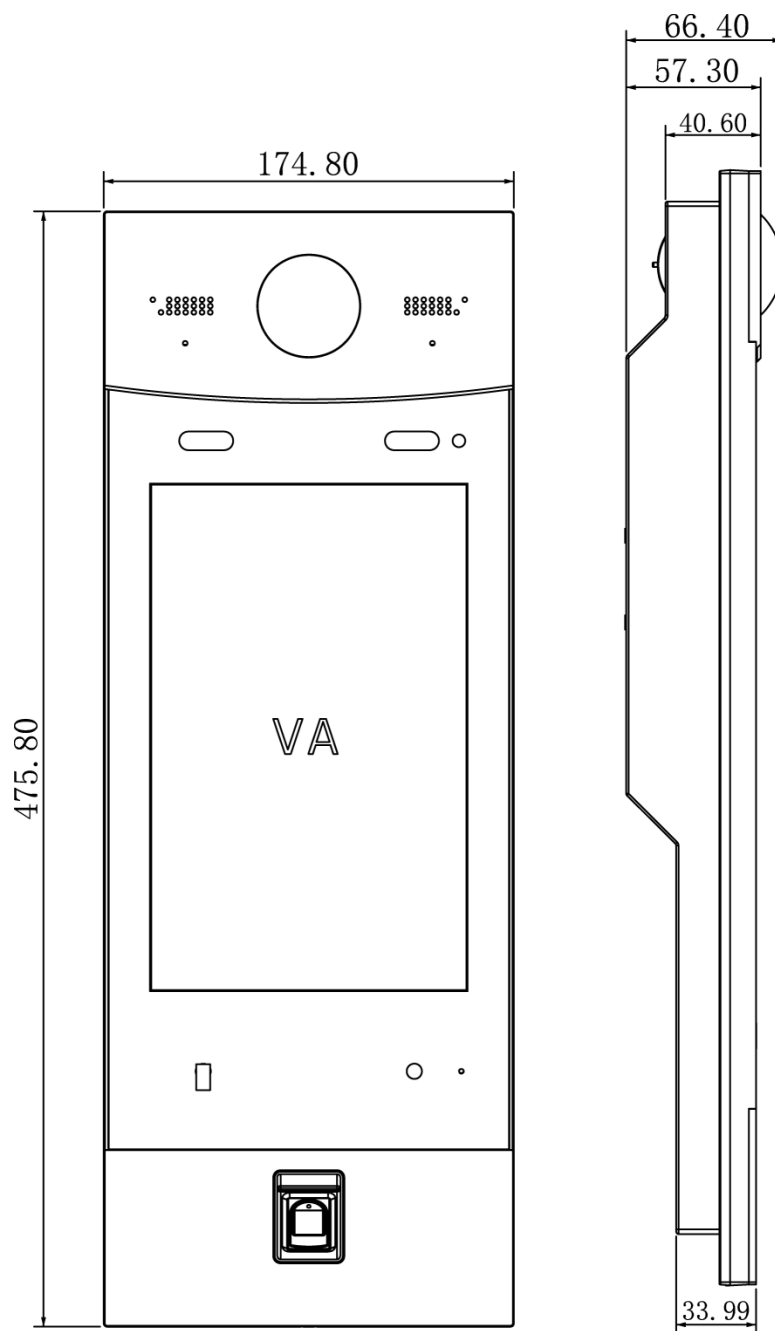
2.2 Front Panel

See Figure 2-2 for the front panel, and for the detailed description, see Table 2-1.
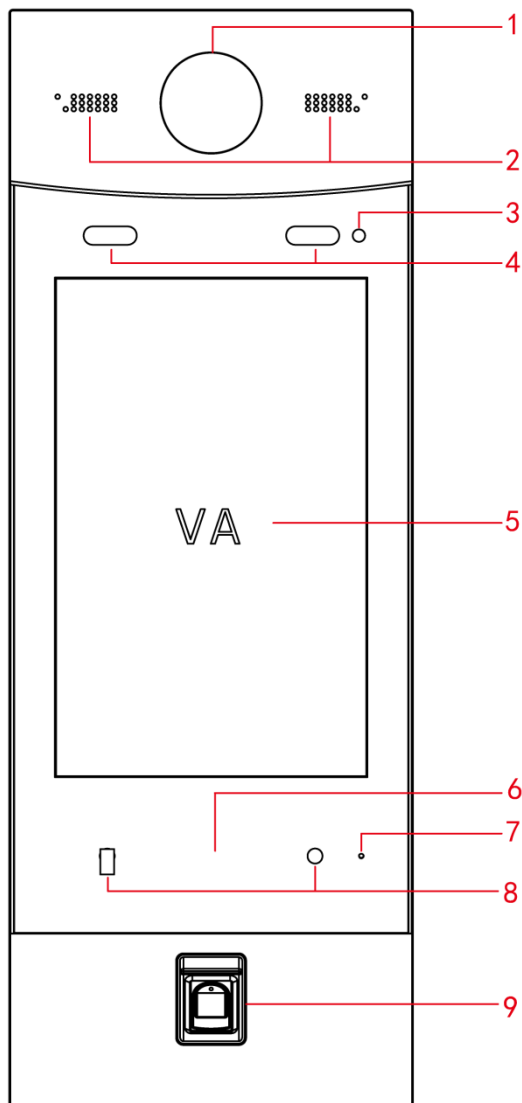
Figure 2-2 Front panel

Table 2-1 Front panel description

No.	Name	Description
1	Camera	Monitors door area, and recognizes face information.
2	Speaker	Outputs audio.
3	Light sensor	Detects ambient lighting condition.
4	Fill light	- Provides extra light when recognizing faces. - Provides extra light to the camera during dark condition.
5	Screen	10-Inch IPS HD screen.
6	Access card area	- Issues access card, which is giving an access card the unlocking authority. - Recognizes access card and unlock.
7	Microphone	Inputs audio.
8	Motion sensor	The sensor is triggered when people or object approaching.
9	Fingerprint sensor	Adds fingerprint data or unlock by fingerprint.

2.3 Rear Panel

See Figure 2-3 for the rear panel, and for the detailed description, see Table 2-2.
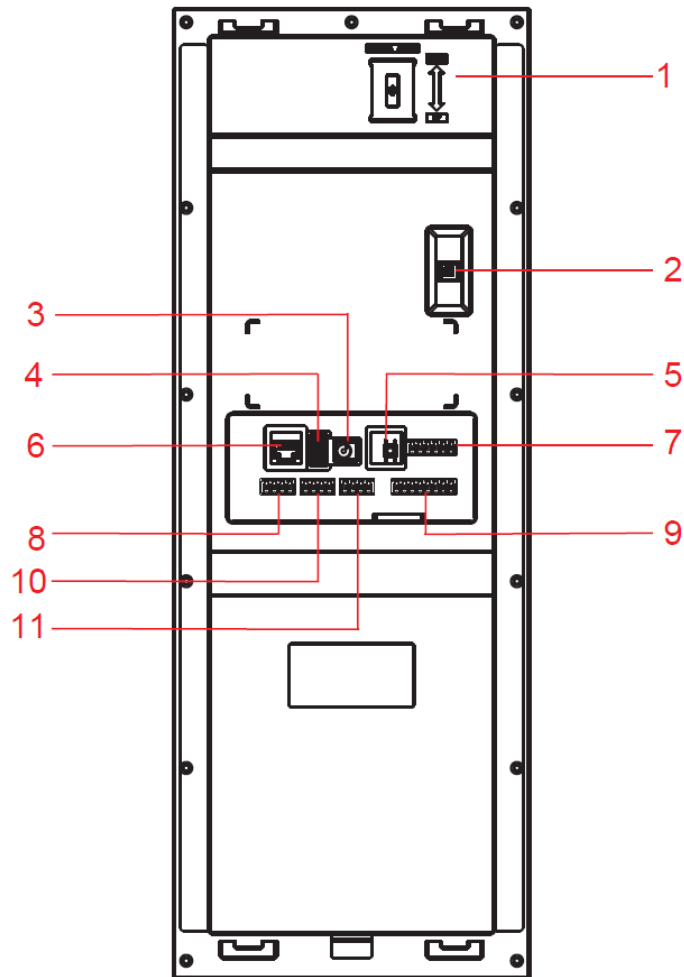
Figure 2-3 Rear panel

Table 2-2 Rear panel description

No.	Name	Description
1	Camera angle adjusting knob	Pull up or down to adjust camera angle.
2	Tamper alarm switch	The VTO would make alarm sound if it is being removed from the wall by force, and the alarm will also be sent to the management center.
3	Power port	Inputs power to the VTO.
4	USB debugging port	Connects to debugging devices.
5	Reset button	Press and hold the button for 8 s to reset the VTO.
6	Ethernet port	Connects to the network with Ethernet cable.
7	Door lock port	See "2.3.1 Door Lock Port."
8	RS485 port	See "2.3.2 RS485 Port."
9	Wiegand port	See "2.3.3 Wiegand Port."
10	Alarm-in port	See "2.3.4 Alarm-in Port."
11	Alarm-out port	See "2.3.5 Alarm-out Port."

2.3.1 Door Lock Port

This port can be used to connect to door locks, and the connection method varies with different locks. For the detailed information, see Figure 2-4, Figure 2-5, and Figure 2-6.
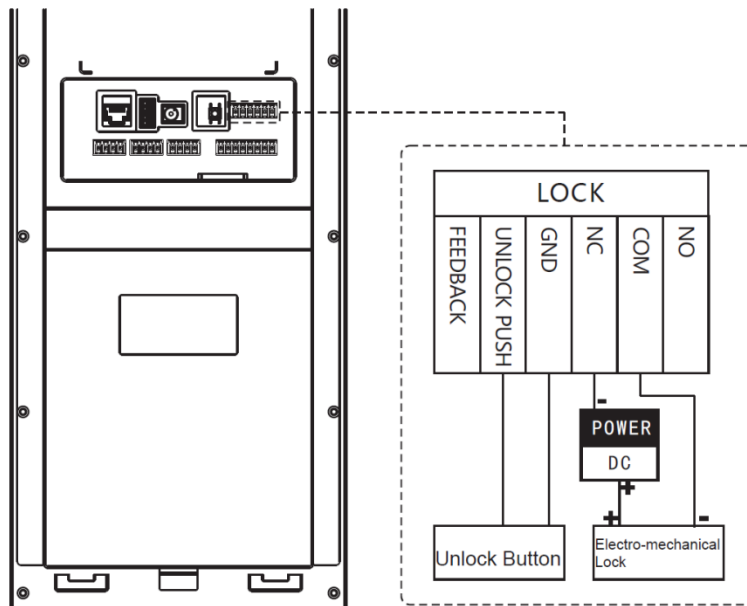
Figure 2-4 Electro-mechanical lock connection

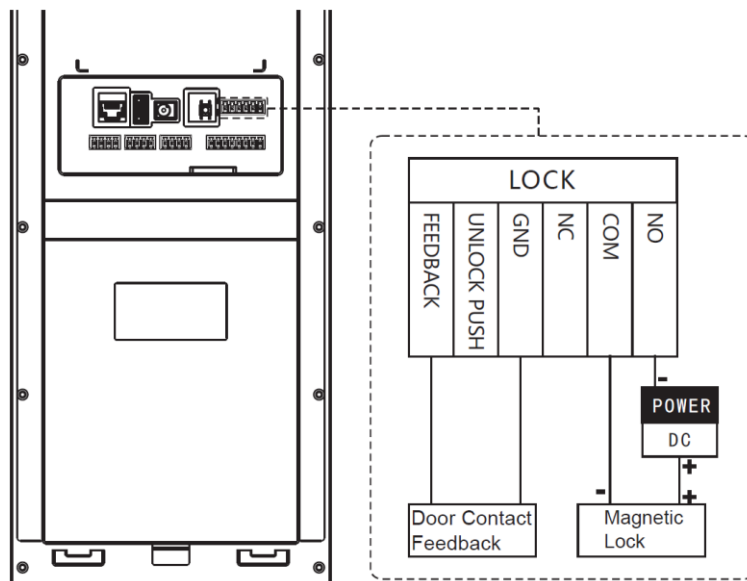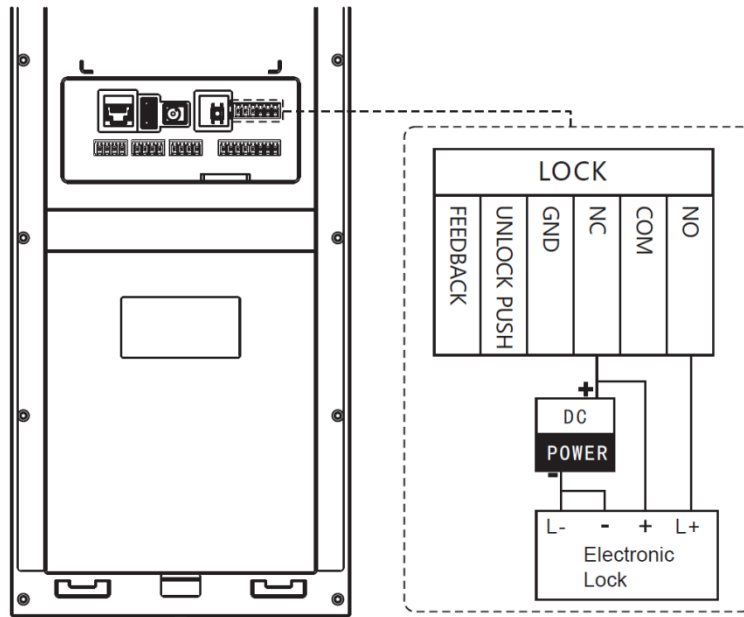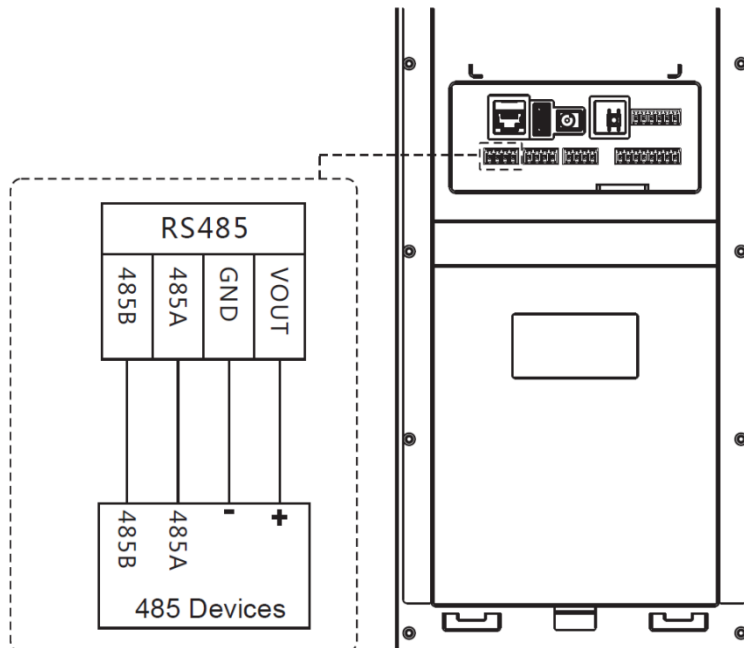Figure 2-5 Magnetic lock connection

Figure 2-6 Electronic lock connection

2.3.2 RS485 Port

This port can be used to connect to 485 devices. For the detailed connection method, see Figure 2-7.

Figure 2-7 485 devices connection

2.3.3 Wiegand Port

This port is reserved, which includes one set of input port and one set of output port. The Wiegand input port can connect to the Wiegand card reader, and the Wiegand output port can connect to the access controller. For the detailed connection method, see Figure 2-8.
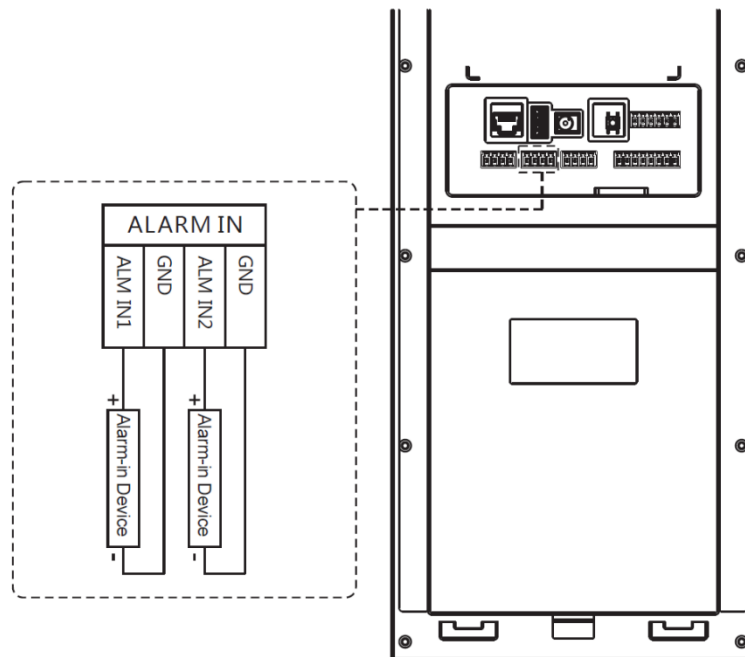
Figure 2-8 Wiegand input/output connection
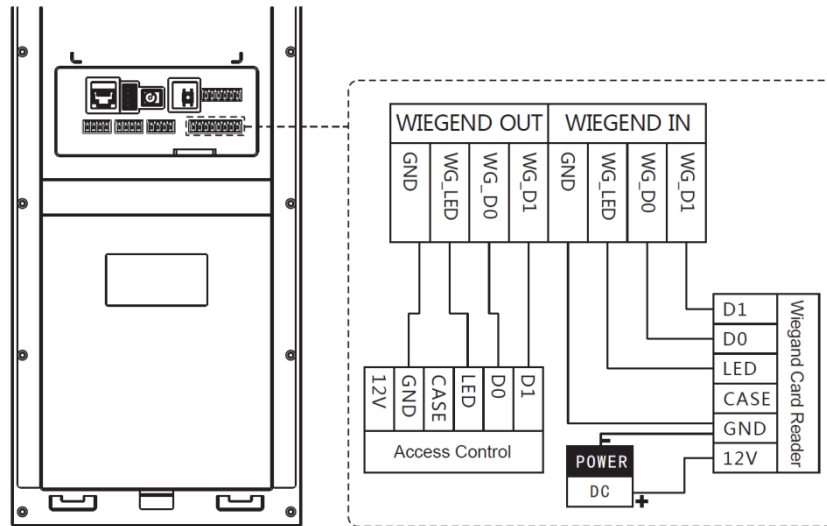
2.3.4 Alarm-in Port

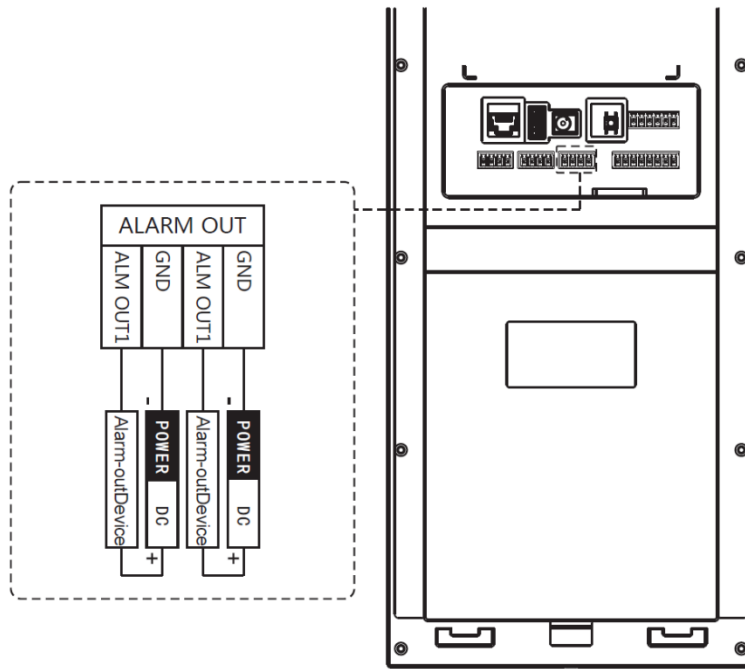There are two alarm-in ports, which can connect to two alarm input devices. See Figure 2-9.

Figure 2-9 Alarm input device connection

2.3.5 Alarm-out Port

There are two alarm-out ports, which can connect to two alarm output devices. See Figure 2-10.

Figure 2-10 Alarm output device connection

3 Installing the VTO

3.1 Installation Requirement

● Do not install the VTO to places with condensation, high temperature, grease or dust, chemical corrosion, direct sunlight, or zero shelter.
● The installation and adjustment must be finished by professional crew, and do not disassemble the VTO by yourself.

3.2 Connecting Cable

For the connection method, see "2.3 Rear Panel."

3.3 Attaching the VTO

For the installation diagram, see Figure 3-1, and for the installation item list, see Table 3-1.
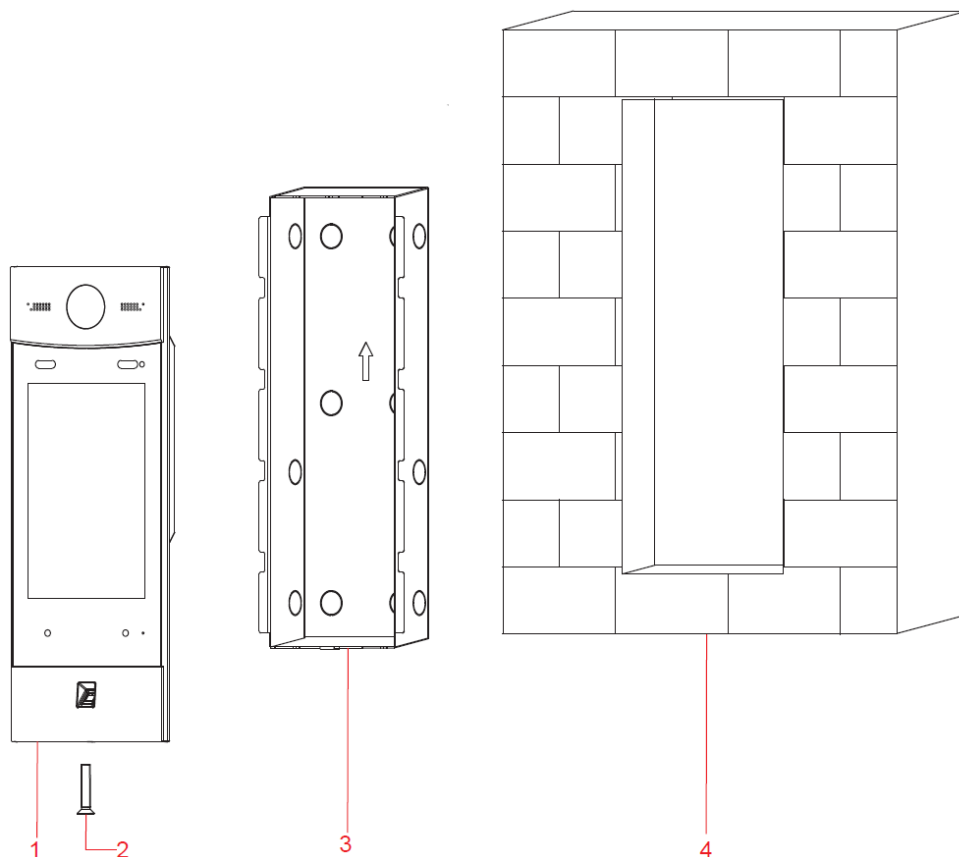
Figure 3-1 VTO installation

Table 3-1 Item list

No.	Item	No.	Item
1	VTO	2	Screw
3	Mounting box	4	Wall

📖

Keep the center of the VTO at 1.4 m to 1.6 m above the ground.

Step 1 Attach the VTO to the mounting box with the screw.

Step 2 Cut an opening with the size of the mounting box on the wall, and then put the mounting box and the VTO in the opening.

Step 3 Put sealant between the VTO, mounting box, and the wall.

4 Configuring Devices

This chapter introduces how to make basic configurations and realize network connection, calling, and monitoring. For the detailed configuration, see the user's Manual.

Before configuration, make sure the following works are finished.

- Make sure there is no short circuit or open circuit in the circuits, and then power up the devices.
- Plan IP address for every device, and also plan the unit number and room number you need.

4.1 Configuring VTO

4.1.1 Initializing VTO

For first time login, you need to create a new password for the Web interface.

📖

The default IP address of the VTO is 192.168.1.110, and make sure the PC is in the same network segment with the VTO.

Step 1　Connect the VTO to power source, and then boot it up.

Step 2　Open the internet browser on the PC, then enter the default IP address of the VTO in the address bar, and then press Enter.

　　　　The password setting interface is displayed. See Figure 4-1.

Figure 4-1 Password setting

📖

The default username is admin.

Step 3　Enter and confirm the password, and then click **Next**.

　　　　The Email setting interface is displayed.

Step 4 Select the **Email** check box, and then enter your Email address.

This Email address can be used to reset the password, and it is recommended to finish this setting.

Step 5 Click **Next**. The initialization succeeded.

Step 6 Click OK.

The login interface is displayed. See Figure 4-2.
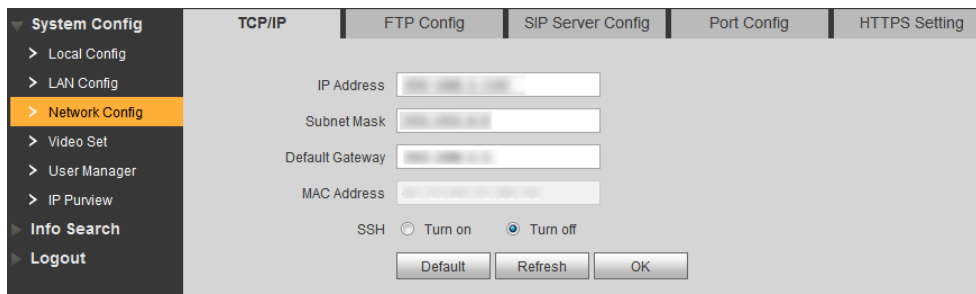
Figure 4-2 Login

4.1.2 Modifying VTO IP Address

Step 1 Log in the Web interface of the VTO, and then select **System Config > Network Config > TCP/IP**.

The **TCP/IP** interface is displayed. See Figure 4-3.

Figure 4-3 TCP/IP

Step 2 Enter the IP address, subnet mask, and default gateway you planned, and then click **OK**.

The VTO will reboot, and you need to modify the IP address of your PC to the same network segment with the VTO to log in again.

4.1.3 LAN Config

You can configure the VTO number and the type of the SIP serve. The VTO number can be used to differentiate each VTO, and it is normally configured according to unit or building number. SIP server is required in the network to transmit intercom protocol, and all the VTO and VTH devices connected to the same SIP server can make video call between each other.

Step 1 Select **System Config > LAN Config**, and then the **LAN Config** interface is displayed. See Figure 4-4.

Figure 4-4 LAN config

Step 2　Configure VTO number.

In the **No.** input box, enter the VTO number you planned for this VTO

Step 3　Configure SIP server

- If VTO works as SIP server, select **VTO** in **Server Type**.
- If third party server (Express by default) works as SIP server, select the server type you need at **Server Type**, and then see the corresponding manual for the detailed configuration.

Step 4　Click **OK** to save.

4.1.4 Configuring SIP Server

Select **System Config > Network Config > SIP Server Config**, and then the **SIP Server Config** interface is displayed. See Figure 4-5.

Figure 4-5 SIP server config

- If the VTO you are visiting works as SIP server

Select **SIP Server Enable**, and then click **OK**. The VTO reboots, and then the login interface is displayed. After logging in, the **Device Manager** will display in the menu. You need to add VTO and VTH then. See "5.1.1.5 Adding VTO" and "5.1.1.6 Adding VTH."

📖

If the VTO you are visiting does not work as SIP server, do not select the **Enable** check box at **SIP Server**, otherwise the connection will fail.

- If other VTO works as SIP server

Configuring Devices 　13

See Table 4-1 for the configuration, and then click **OK**.

Table 4-1 SIP server config

Parameter	Description
IP Address	The IP address of the VTO that works as SIP server.
Port	5060
Username	Leave to the default.
Password	
SIP Domain	VDP
Login UserName	The user name and password for the Web interface of the SIP server.
Login PWD	

● If third party server works as SIP server, see the corresponding manual for the detailed configuration.

# 4.1.5 Adding VTO

Step 1   Login the Web interface of the SIP server.

Step 2   Select System Config > Device Manager > Outdoor Station Manager.

The **Outdoor Station Manager** interface is displayed, see Figure 4-6.

Figure 4-6 Outdoor station manager
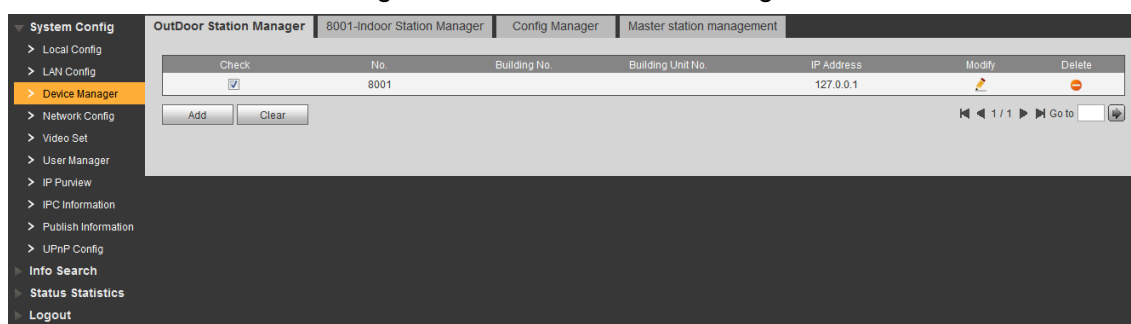
Step 3   Click **Add**.

The **Add** interface is displayed. See Figure 4-7.

Figure 4-7 Add VTO

Step 4   Configure VTO parameters, and be sure to add the SIP server itself too. See Table 4-2 for the details.

Table 4-2 VTO parameters

Parameter	Description
No.	The number you planned for the VTO.
Register Password	Leave to the default.
IP Address	The IP address of the VTO.
Username	The username and password for the Web interface of the
Password	VTO.

Step 5 Click **OK** to finish configuration.

Do the operation above repeatedly to add more VTO devices in the network.

4.1.6 Adding VTH

⚠

If there are master VTH and extension VTH being used, you need to add them all.

Step 1 Login the Web interface of the SIP server.

Step 2 Select System Config > Device Manager > 8001-Indoor Station Manager.

The **8001-Indoor Station Manager** interface is displayed, see Figure 4-8.

📖

8001 is a default VTO number, and it changes to the number of the VTO you select.

Figure 4-8 8001-indoor station manager
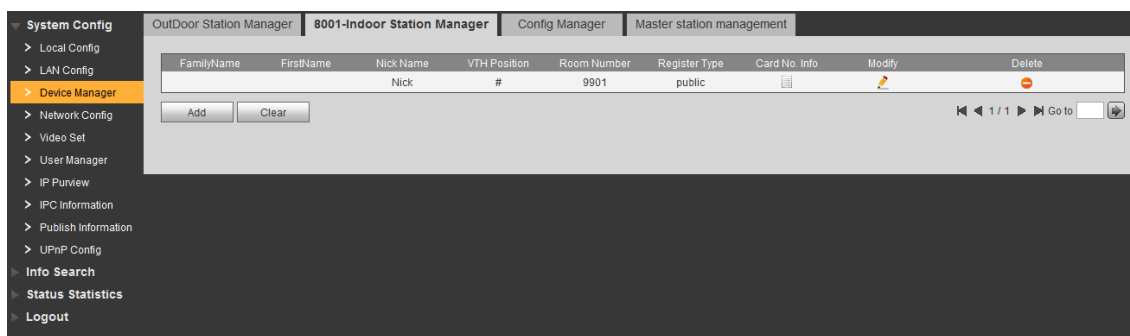
Step 3 Click **Add**.

The **Add** interface is displayed. See Figure 4-9.

Figure 4-9 Add VTH

Step 4 Configure VTH parameters. See Table 4-3 for the details.

Table 4-3 VTH parameters

Parameter	Description
FamilyName	Configure the name and nickname of the VTH users to differentiate them.
FirstName	
Nick Name	
VTH Short No.	The room number you planned. 📖 If there are master VTH and extension VTH being used, the short number of the master VTH should be "room number#0", and the extension VTH to be #1, #2, and #3 and so on.
Register Password	Keep the default value.
Register Type	

Step 5 Click **OK** to finish configuration.

Do the operation above repeatedly to add more VTH devices in the network.

4.2 Configuring VTH

Connect the VTH devices to the VTO devices with network cable, and then properly configure every VTH device.
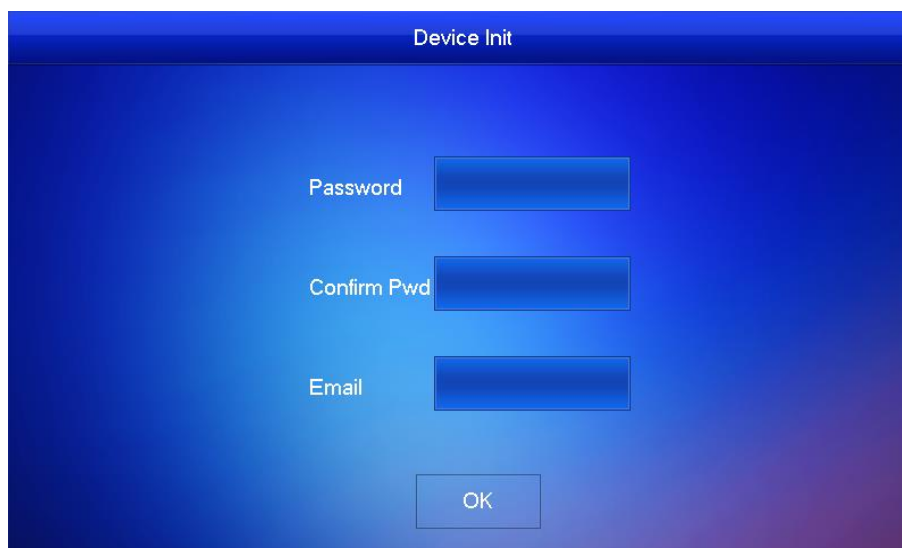
4.2.1 Initializing VTH

For first time use, you need to create a new password for the VTH.

Step 1 Power up the VTH.

The **Device Init** interface is displayed. See Figure 4-10.
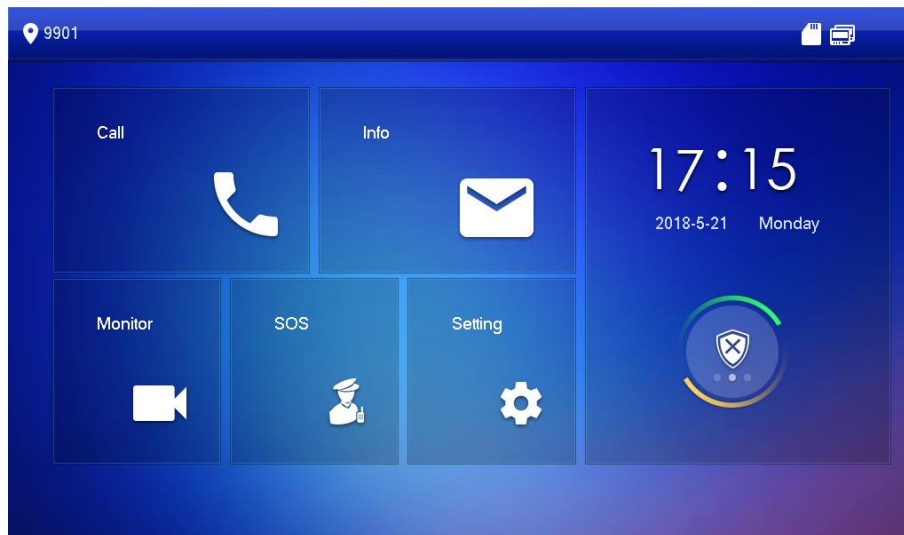
Figure 4-10 Device initialization

Step 2 Enter and confirm the password, and then enter the Email. The Email can be used to reset the password.

Step 3 Tap **OK**.

The main interface is displayed. See Figure 4-11.

Figure 4-11 Main interface

Step 4 In the main interface, you can get into two types of settings.
● Tap **Setting** once, then enter the password, and then the basic settings are displayed. See Figure 4-12.

Figure 4-12 Basic settings

● Press and hold **Setting** until the **Password Verification** dialog box displays. Enter the password, and then the advanced settings are displayed. See Figure 4-13.

Figure 4-13 Advanced settings
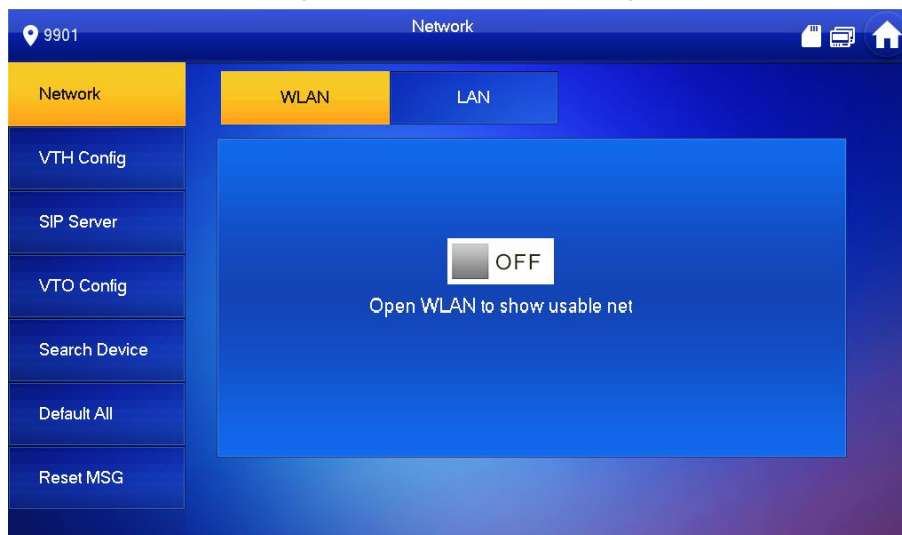
4.2.2 Configuring Network Parameters

Make sure VTH devices are in the same network segment with VTO devices, otherwise VTH devices cannot connect to VTO devices. To acquire IP address with DHCP, you need to connect VTO and VTH devices to a router with DHCP function.

Step 1 In the Advanced settings interface (see Figure 4-13), tap **Network**.

The **Network** interface is displayed. See Figure 4-14.

📖

WLAN is available on select models.

Figure 4-14 Network

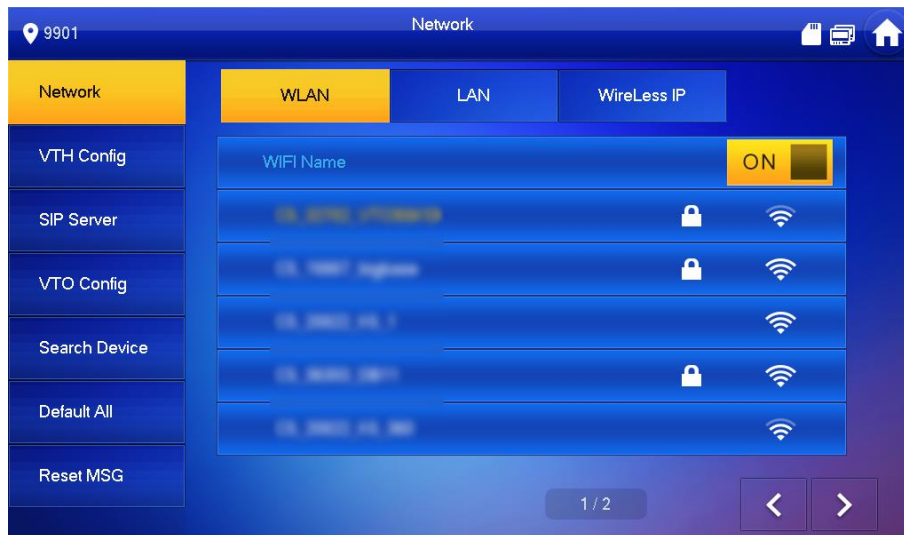Step 2 Configure network with different access modes.

● LAN

Enter the IP address, subnet mask, and gateway you planned, and then click **OK**; Tap ▣OFF to enable DHCP and acquire IP address automatically.

● WLAN

1) Tap **WLAN**, and then tap ▣OFF to enable Wi-Fi function.

The Wi-Fi networks that have been found are listed. See Figure 4-15.

Figure 4-15 Wi-Fi list

2) Connect Wi-Fi.

There are two ways to connect Wi-Fi:

◇ Select the Wi-Fi you need in the list, and then tap **Wireless IP**. Enter the IP address, subnet mask, and gateway, and then click **OK**.

◇ Select the Wi-Fi you need in the list, and then tap **Wireless IP**. Tap ▬ OFF to enable DHCP and acquire IP address automatically.

4.2.3 Configuring Room Number

Step 1 In the advanced settings interface (see Figure 4-13), select **VTH Config**.

The **VTH Config** interface is displayed. See Figure 4-16.

Figure 4-16 VTH Config
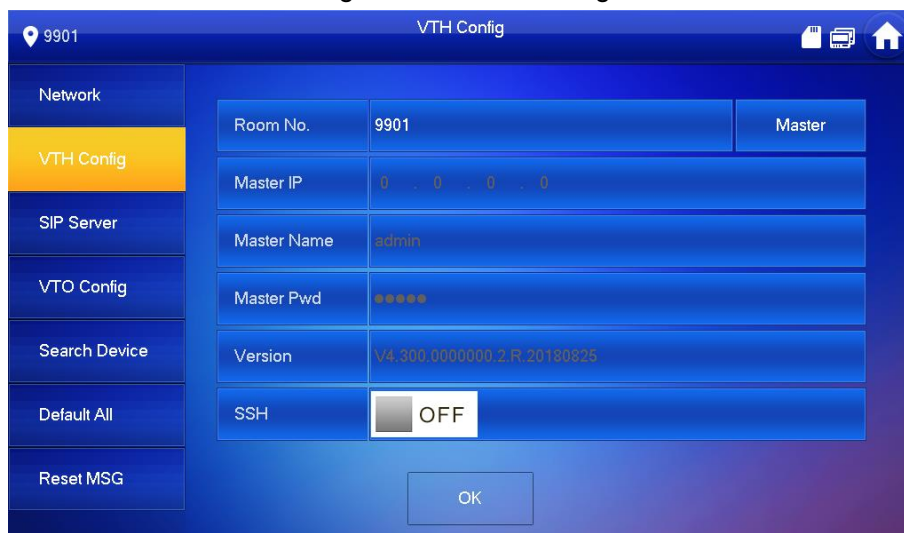
Step 2 Configure room number.

● If you use single VTH, make sure there is **Master** displayed behind the room number.

Enter the room number you planned in the **Room No.** input box.

● If you use multiple VTH devices, the room number of the master VTH should be "room number#0", and you also need to configure extension VTH.

1) On the extension VTH device, go to the **VTH Config** interface, then tap the **Master** behind the room number, and then it switches to **Extension**.

Configuring Devices   19

2) Configure extension VTH information. See Table 4-4.

Table 4-4 Extension VTH configuration

Parameter	Description
Room No.	The room number of the extension VTH should be "room number#1", "room number#2", and so on.
Master IP	The IP address of the master VTH.
Master Name	admin
Master Pwd	The password of the master VTH.

Step 3 (Optional) Press ![OFF] to enable SSH.

If the SSH is enabled, you can login the VTH through SSH protocol with debugging terminal, and do operations and debugging.

Step 4 Tap **OK** to save.

4.2.4 Adding SIP Server

Enter the SIP server information to connect the VTH to the network, and then all the VTO and VTH devices connected to the same SIP server can make video call between each other.

Step 1 In the advanced settings interface (see Figure 4-13), select **SIP Server**.

The **SIP Server** interface is displayed. See Figure 4-17.

Figure 4-17 SIP server
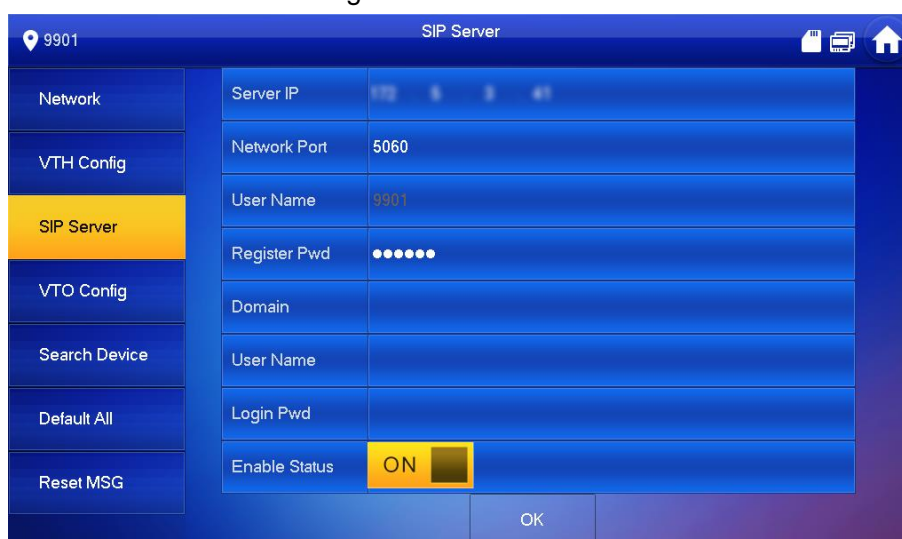
Step 2 Configure SIP server information. See Table 4-5.

Table 4-5 SIP server configuration

Parameter	Description
Server IP	The IP address of the SIP server.
Network Port	● If third party server works as SIP server, enter 5080. ● If VTO works as SIP server, enter 5060.
User Name	Keep the default value.
Register Pwd	
Domain	VDP
User Name	The user name and password for the Web interface of the SIP server.
Login Pwd	

Parameter	Description
Enable Status	Tap to turn it on, and then the SIP server function is enabled.

Step 3   Tap **OK** to save.

4.2.5 Adding VTO Devices

Step 1   In the advanced settings interface (see Figure 4-13), select **VTO Config**.
The **VTO Config** interface is displayed. See Figure 4-18.

Figure 4-18 VTO config

Step 2   Enter VTO information.
- ● If there is only one VTO
  Edit the name you want for the VTO in the **Main_VTO Name** input box, and then its IP address, user name and password.
- ● If there are multiple VTO devices, select any one as the main VTO and input its information, and then the other VTO devices will be sub VTO.
  Edit the name you want for the sub VTO in the **Sub_VTO1 Name** input box, and then its IP address, user name and password. Tap the arrow to go to the new page to add more sub VTO devices.

Step 3   Set the **Enable Status** to ON .
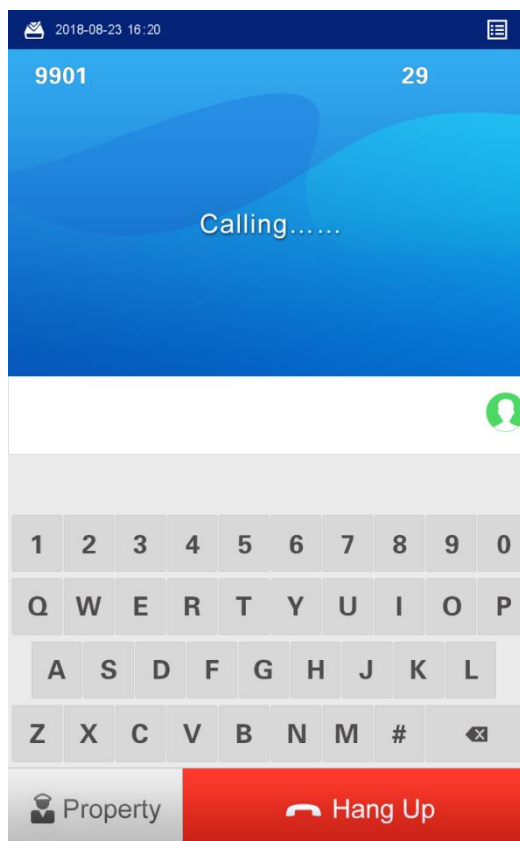
4.3 Verifying Configuration

4.3.1 Calling VTH from VTO

Step 1   Enter the room number of the VTH on the VTO.
Step 2   Tap **Call**.
The "Calling now, please wait a moment" voice notice comes up, and the calling interface is displayed. See Figure 4-19.

Figure 4-19 Calling

Step 3   The call screen is displayed on the VTH. See Figure 4-20.
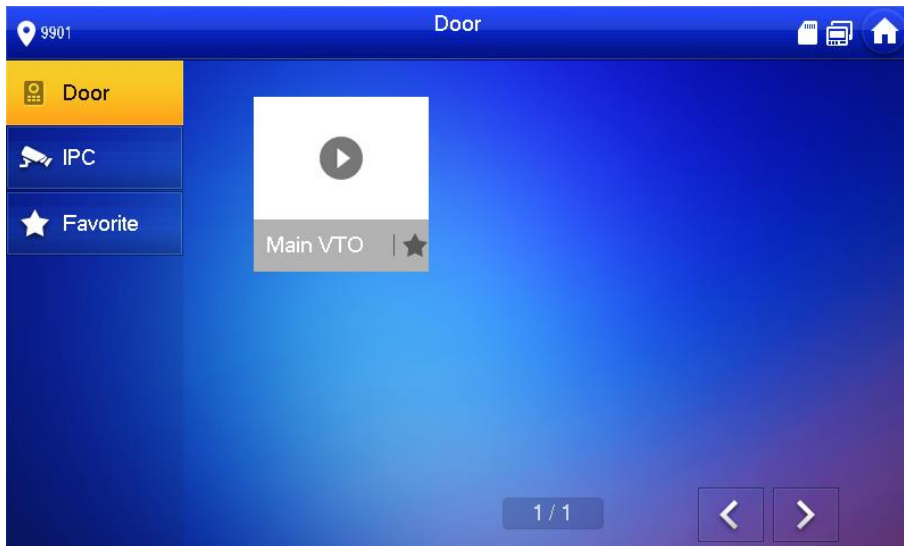
Figure 4-20 Call screen

Step 4   Tap   on the VTH to answer the call.

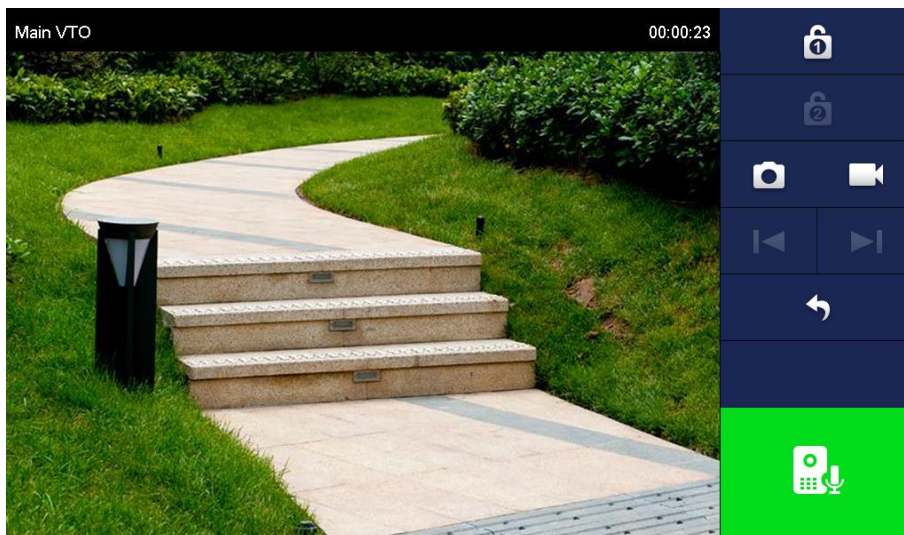## 4.3.2 Doing monitor from VTH

Step 1   In the main interface of the VTH, select **Monitor > Door**, and then the **Door** interface is
displayed. See Figure 4-21.

Figure 4-21 Door

Step 2   Select the VTO you need to do monitor, see Figure 4-22.

Figure 4-22 Monitor screen

5 Operating VTO

This chapter introduces the functions of the VTO, including calling residents, unlock, adding and searching face/fingerprint/access card, system configuration, and information searching.

5.1 Main interface

The main interface is displayed after booting. See Figure 5-1. For the detailed description, see Table 5-1.
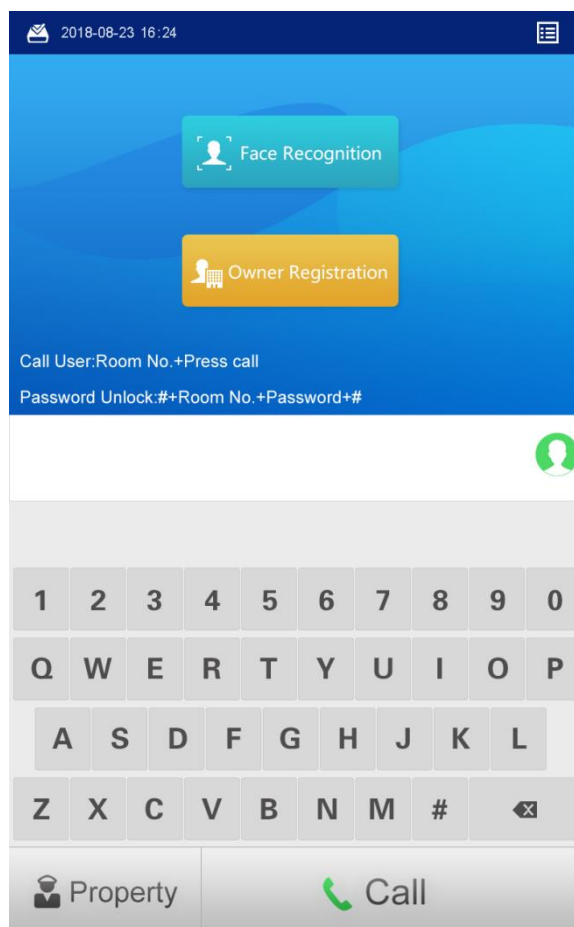
Figure 5-1 Main interface

Table 5-1 Main interface description

Name	Description
Function list	The functions that the residents can use, and tap to open.
Keyboard	● Dial numbers to make phone call. ● The "#" can be used to go to the engineering interface, see the details in the User's Manual.
Backspace	Delete the entered content.
Call	Tap to call residents.
Property	Tap to call the management center.

5.2 Call Function

5.2.1 Calling VTH

See 4.3.1 Calling VTH from VTO.

5.2.2 Calling Property (management center)

Tap **Property** on the VTO; or enter the number of the management center, and then tap **Call**.

The "Calling now, please wait a moment" voice notice comes up, and the calling interface is displayed. See Figure 4-19.

5.3 Unlocking Method

5.3.1 Face Unlock

Step 1 Face unlock happens under the following two situations.
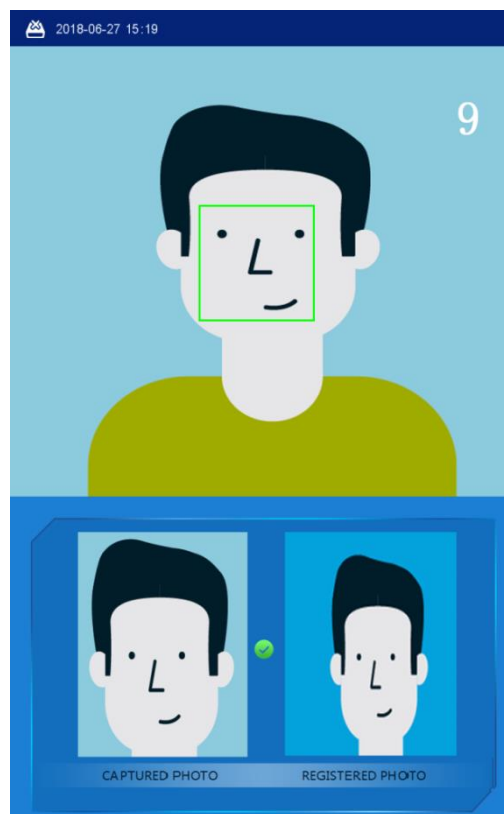● On Sleeping Screen

When people approaching, the screen lights up, and then starts face recognition. See Figure 5-2.
● In Main Interface
1) Tap Face Recognition.
2) Come close and face to the camera. The VTO starts face recognition. See Figure 5-2.

Figure 5-2 Face recognition

<u>Step 2</u> If the recognition passes, the ✅ displays and the "The door is unlocked" voice notice comes up; If the "**failed to scan**" notice displays after 10 s, the unlocking failed, and you need to check if the face data was added to the VTO.

5.3.2 Fingerprint Unlock

Press the fingerprint sensor on the VTO with your finger, and if the recognition passes, the **Door opened** notice displays, and the "The door is unlocked" voice notice comes up; if the "Unregistered fingerprint" voice notice comes up, you need to add the fingerprint. For the details, see "5.4.2 Fingerprint Registration."

5.3.3 Password Unlock

Enter "#+unlock password+#" on the VTO, and if the recognition passes, the "**Door opened**" notice displays, and the "The door is unlocked" voice notice comes up; If the "**Wrong password**" notice is displayed, you need to check the password.

5.3.4 Access Card Unlock

Swipe the authorized access card on the VTO, and if the recognition passes, the "**Door opened**" notice displays, and the "The door is unlocked" voice notice comes up; if the "**Card Error**" notice is displayed, and the beep sound comes up, you need to check the whether the access card is authorized. For the details, see "5.4.3 Issuing Card."

5.3.5 VTH Unlock

VTH unlock is available in the following conditions:
- VTO is calling VTH.
- VTO and VTH are making phone call.
- VTH is monitoring the area that VTO covers.

5.3.6 Management Center Unlock

Management center unlock is available in the following conditions:
- When VTO is calling management center,
- VTO and management center are making phone call,
- Management center is monitoring the area that VTO covers.

5.4 Registration

⚠️

Only when VTO device is configured as SIP server, then the VTO users can register face and fingerprint on the VTO.
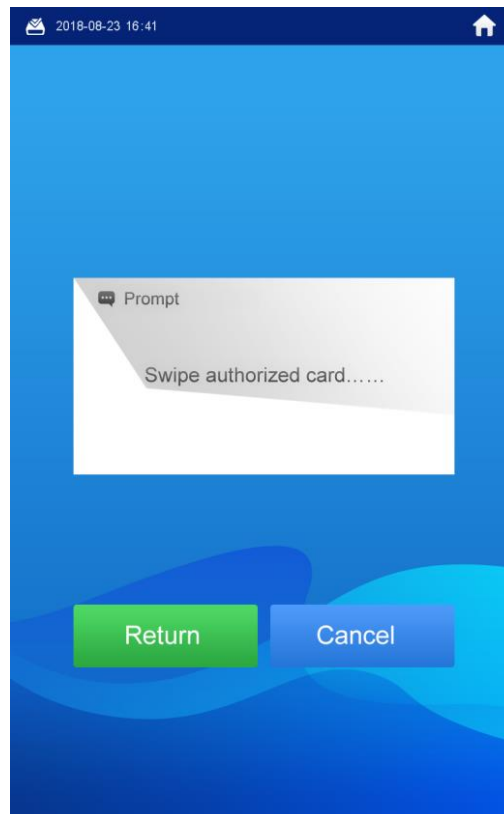
5.4.1 Face Registration

Step 1 Face registration can be done by VTO users or admin people.

● Face Registration by VTO Users
1) In the main interface, tap **Owner Registration**.
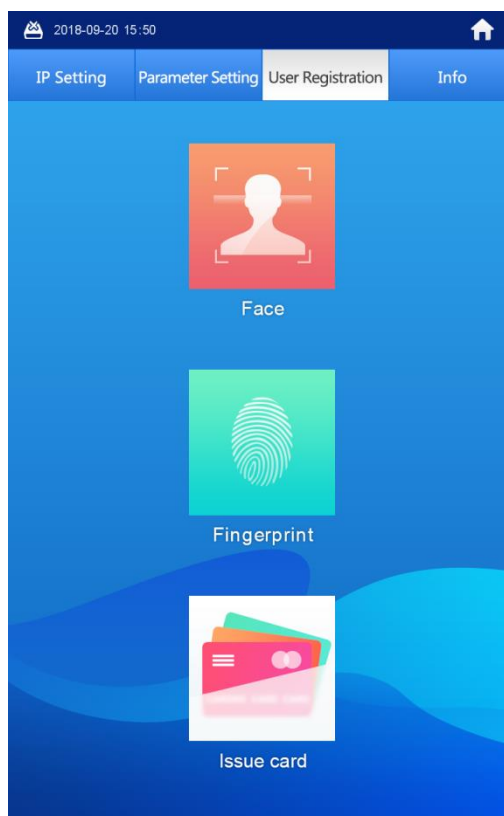   The **Swipe authorized card** notice is displayed. See Figure 5-3.

Figure 5-3 Swipe authorized card

2) Swipe the authorized card**.**
   The registration interface is displayed. See Figure 5-4.

Figure 5-4 Registration

3) Select **Face > Add face**.
● Face Registration by Admin People
1) In the main interface, enter #VTO password#.

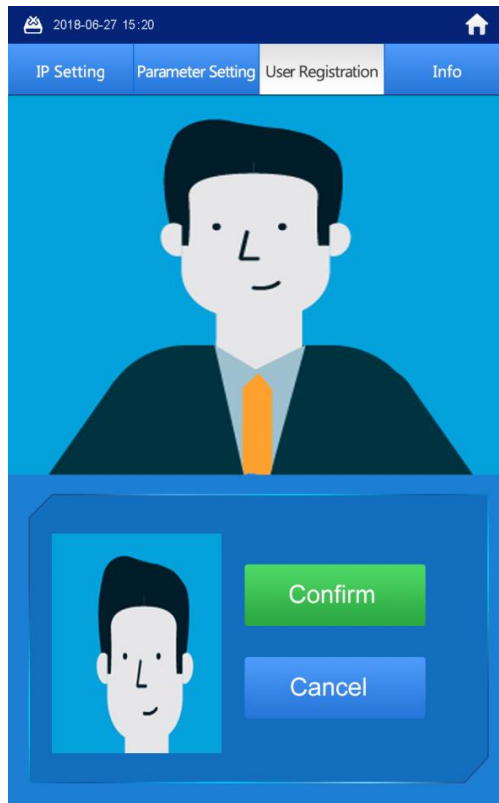The default VTO password is 888888, for more information, see the users' Manual.

The **IP Setting** interface is displayed.

2) Select User **Registration > Face > Add face**.

Step 2 The VTO starts face recognition. See Figure 5-5.

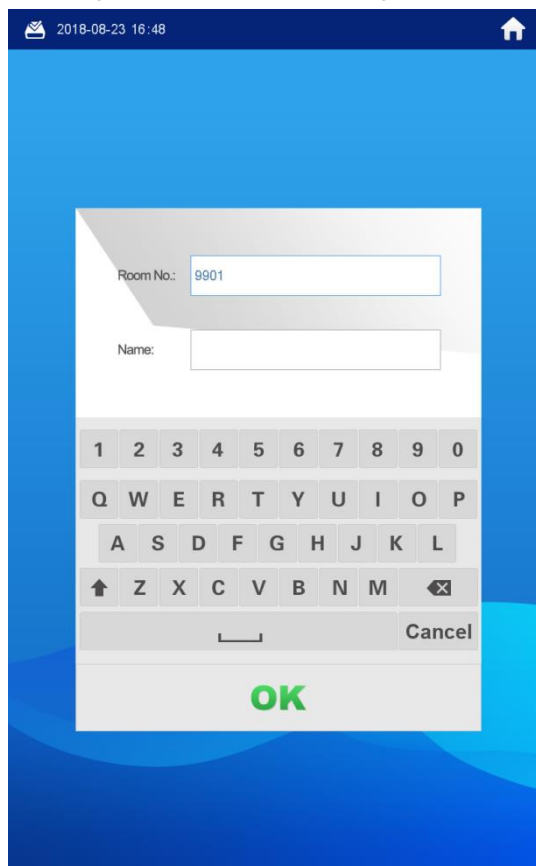To restart the registration, tap **Cancel**.

Figure 5-5 Face recognition

Step 3 After the registration finished, tap **Confirm**.

The information registration interface is displayed. See Figure 5-6.

Figure 5-6 Information registration

Step 4 Enter the room number and name for the newly added face.

You can add 50 faces at most under one room number.

Step 5 Tap **OK** to save.

The face data list of this room number is displayed.

Tap 🔙 to exit.

5.4.2 Fingerprint Registration

Step 1 Fingerprint registration can be done by VTO users or admin people.
- Fingerprint registration by VTO Users
1) In the main interface, tap **Owner Registration**.
   The **Swipe authorized card** notice is displayed. See Figure 5-3.
2) Swipe the authorized card**.**
   The registration interface is displayed. See Figure 5-4.
3) Select **Fingerprint > Add Fingerprint**.
- Fingerprint registration by Admin People
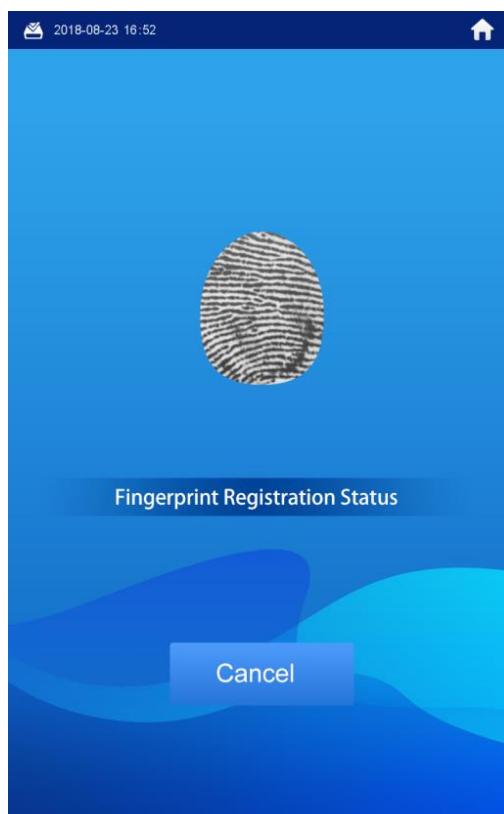1) In the main interface, enter #VTO password#.

   The default VTO password is 888888, for more information, see the users' Manual.
   The **IP Setting** interface is displayed.
2) Select **User Registration > Fingerprint > Add Fingerprint**.

Step 2 The fingerprint recognition interface is displayed. See Figure 5-7.

Figure 5-7 Fingerprint recognition

Step 3 Tap the fingerprint sensor as instructed.

After the registration finished, the information registration interface is displayed. See Figure 5-6.

Step 4 Enter the room number and name for the newly added fingerprint.

📖

You can add 7 fingerprints at most under one room number.

Step 5 Tap **OK** to save.

Tap ↩ to exit.

5.4.3 Issuing Card

This function is only for admin people or engineer.

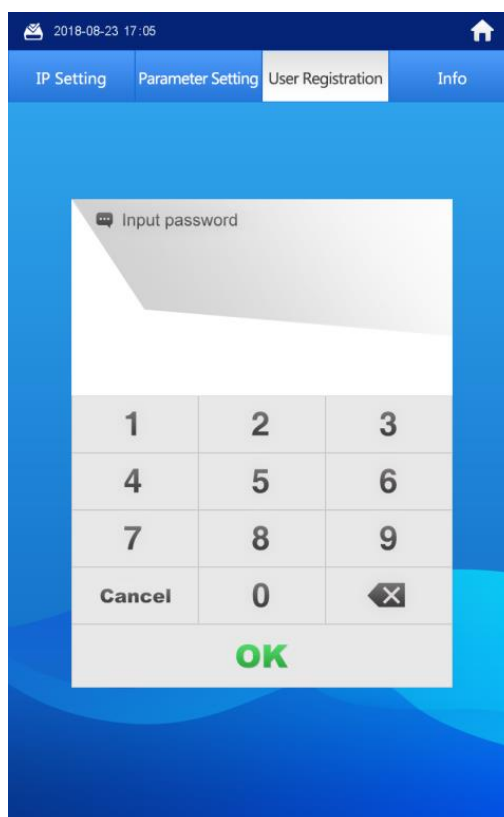## 5.4.3.1 Issuing Card by Password

Step 1 In the main interface, enter #VTO password#.

The **IP Setting** interface is displayed.

Step 2 Select User Registration > Card > Password.

The **Input password** interface is displayed. See Figure 5-8.
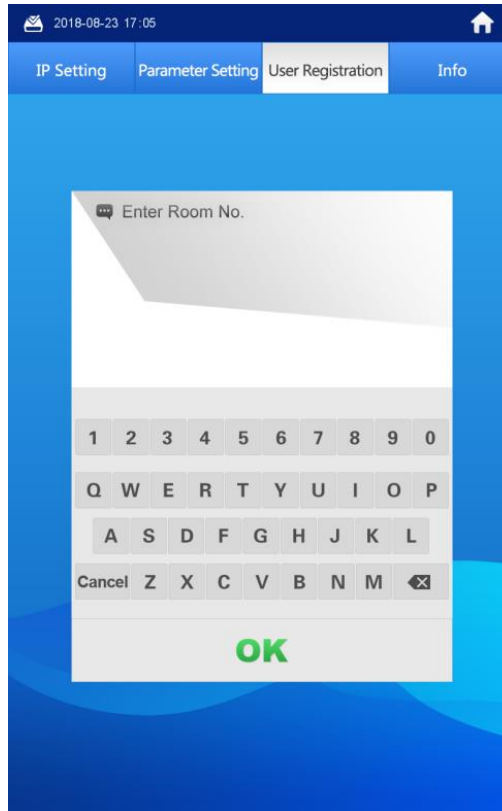
Figure 5-8 Input password

Step 3 Enter the card issuing password, and then tap **OK**.

The **Enter Room No.** interface is displayed. See Figure 5-9.

📖

The card issuing password is 002236 by default.

Figure 5-9 Enter room number

Step 4   Enter the room number, and then tap **OK**.

The **Swipe authorized card** notice is displayed.

The room number is what you configured on the VTH.

Step 5   Swipe the access card you need to authorize**.**

The succeeded notice is displayed, and the card issuing succeeded.

You can swipe new cards repeatedly to authorize more cards.

Step 6   Tap **Cancel** to finish.

Tap   repeatedly to exit.

5.4.3.2 Issuing Card by Master Card

● Issuing card by master card is only available on the VTO.
● Before issuing card by master card, make sure the master card is available. If not, register an access card by password on the VTO, and then set it to be the master card in **System Config > Device Manager > 8001-Indoor Station Manager**. See the details in the User's Manual.
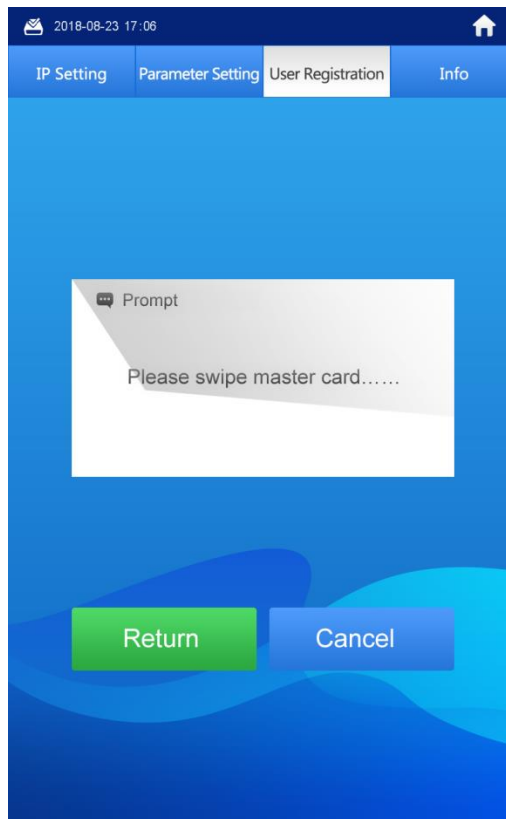
Step 1   In the main interface, enter #VTO password#.

The **IP Setting** interface is displayed.

Step 2   Select User Registration > Card >Master card.

The **Swipe master card** notice is displayed. See Figure 5-10.

Figure 5-10 Swipe master card.

Step 3 Swipe the master card**.**

The **Enter Room No.** interface is displayed. See Figure 5-9.

Step 4 See the rest of the operation from "Step 4" in "5.4.3.1 Issuing Card by Password."

Appendix 1 Specification

Model		VTO9341D
System	Processor	Embedded high performance processor
	Operation system	LINUX
Video	Video format	H.264
	Camera	2MP HD Camera
	Night vision	Support
	Back light	Support
	Auto Fill light	Support
Audio	MIC	Omni-directional microphone
	Speaker	Built-in speaker
	Intercom	Two-way intercom
Display	Screen	10-Inch IPS touch screen
	Resolution	1280×800
Card reader		Built-in card reader
Fingerprint		Support
Motion sensor	Human body approaching	Support
Alarm	Tamper alarm	Support
Access control	NO output	Support
	NC output	Support
	Unlock button	Support
	Door status detection	Support
Network	Ethernet	10Mbps/100Mbps
	Network protocol	TCP/IP
Standard	Power	DC 12V 5A
	Power consumption	Standby≤5W; Working≤24W
	Environmental	-20℃-+60℃
	Requirements	10%RH-95%RH
	Protection class	IP55; IK07
	dimension	475mm×174mm×58mm

Packing List

Open the package and check whether all the components are included.

Name	Quantity	Info
Face Recognition Apartment Outdoor Station	1	
Power adapter	1	
Quick Start Guide	1	
Screw package	1	