Face Recognition Apartment Outdoor Station

User's Manual

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.

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.

Foreword

General

This Manual introduces the function, structure, networking, mounting process, configuration process, WEB interface operation, and technical parameters of the device.

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

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 Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.

- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

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.

Table of Contents

1 Introduction

1.1 General

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.

1.2 Features

Video Intercom

Make video call with the management center or VTH users.

Group Call

When calling a master VTH, the extension VTH devices receive the call as well.

Area Surveillance

Monitor areas around the VTO from VTH or management center, and the VTO can send up to six video streams at a time.

Emergency Call

Single press to call the management center under emergency.

Auto Snapshot

The system takes snapshots automatically when unlocking or during video communication, and then save them to the FTP server.

Face Data Adding

Add data of up to 10,000 faces to the VTO or add them in batch from the server to realize face unlock.

Fingerprint Adding

Add data of up to 3,000 fingerprints to the VTO or add them in batch from the server to realize fingerprint unlock.

Alarm

Supports various alarms, including tamper alarm, door contact alarm, and duress password alarm. The alarm will also be sent to the management center.

Information Publishing

The VTO can send information to multiple VTH devices.

History Viewing

View call history, alarm history, and unlocking history.

Motion Detection

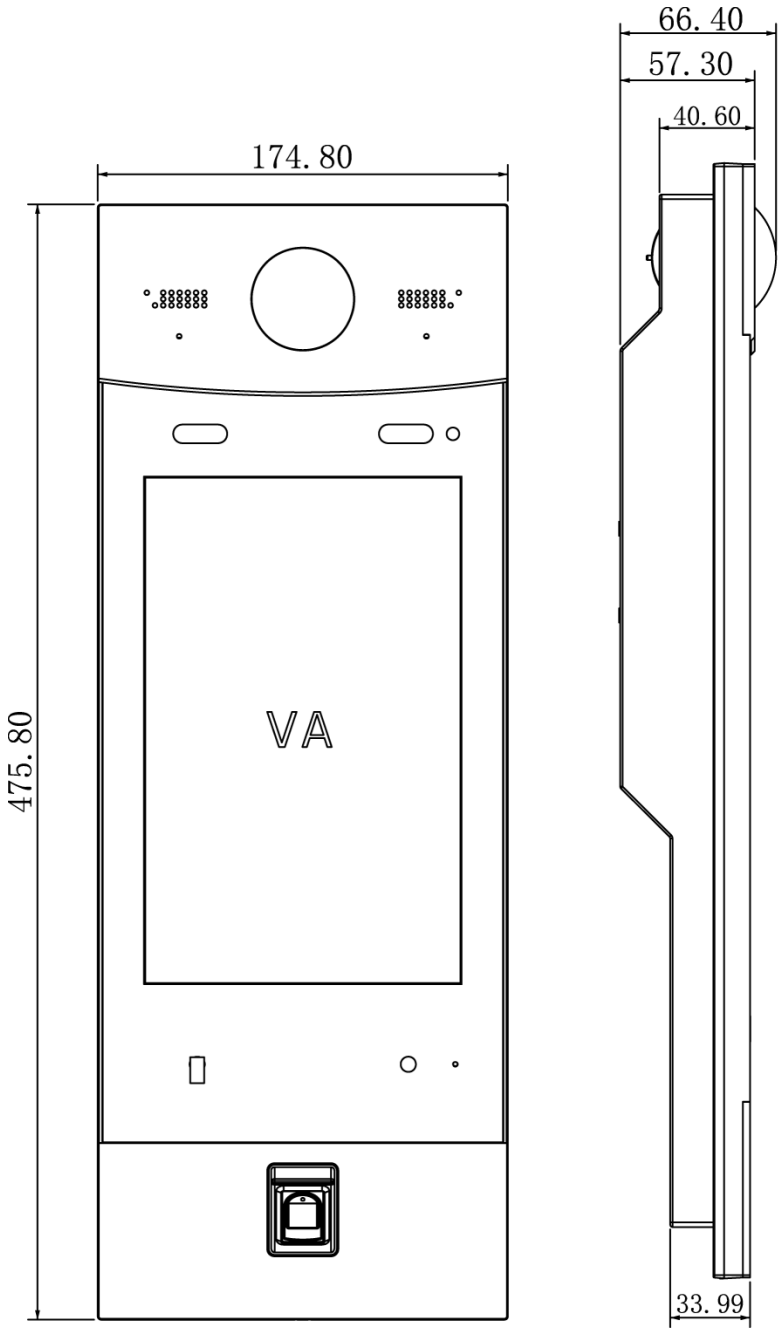
The VTO screen lights up when moving object approaching.

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

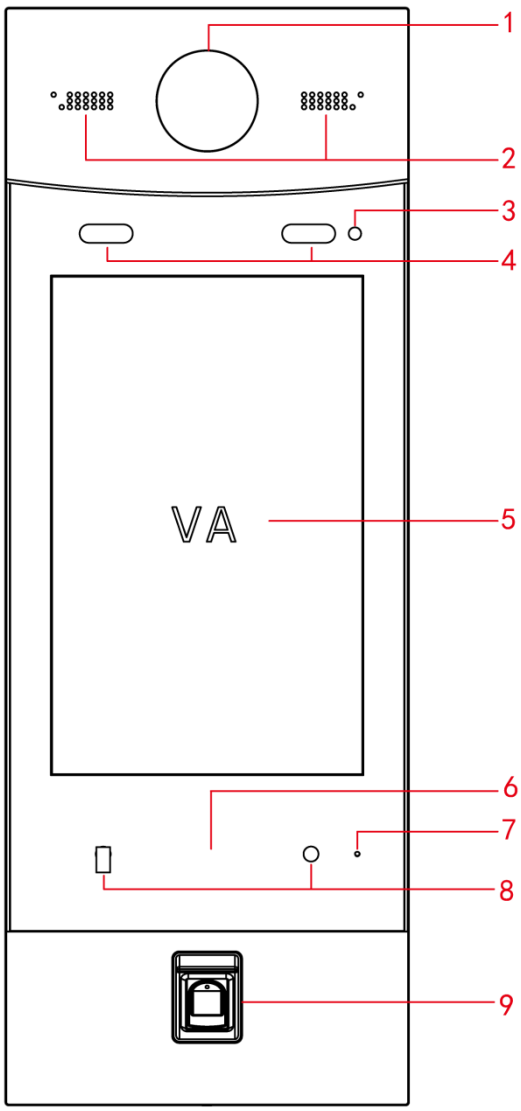


Table 2-1 Front panel description

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

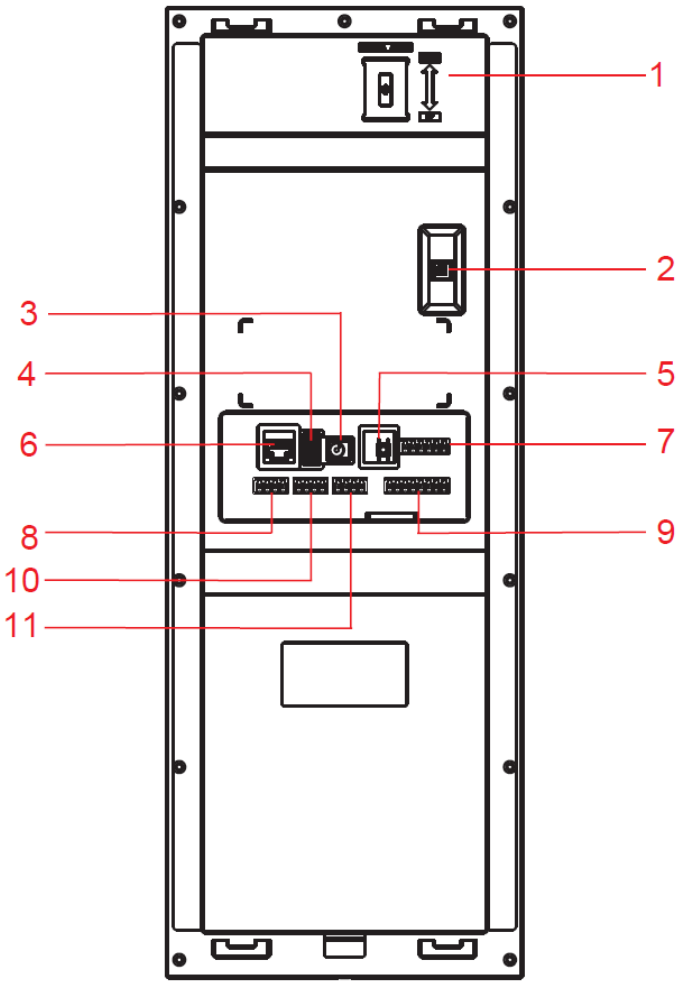


Table 2-2 Rear panel description

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

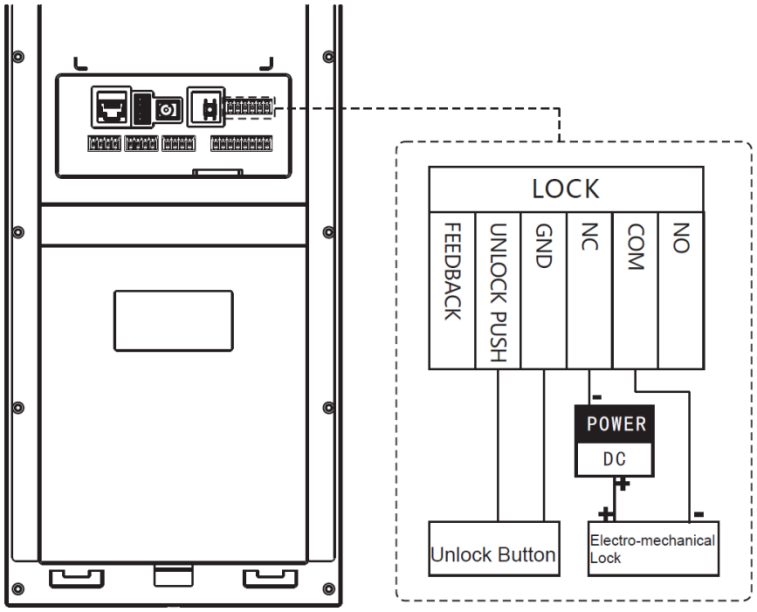


Figure 2-5 Magnetic lock connection

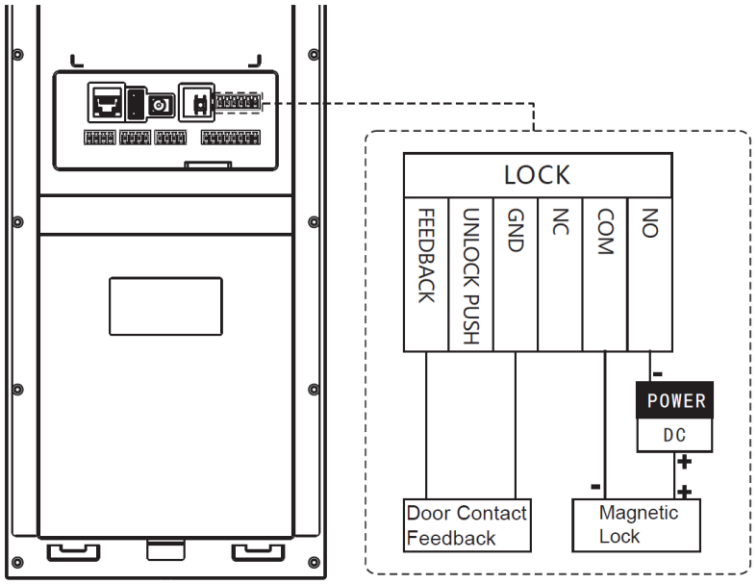
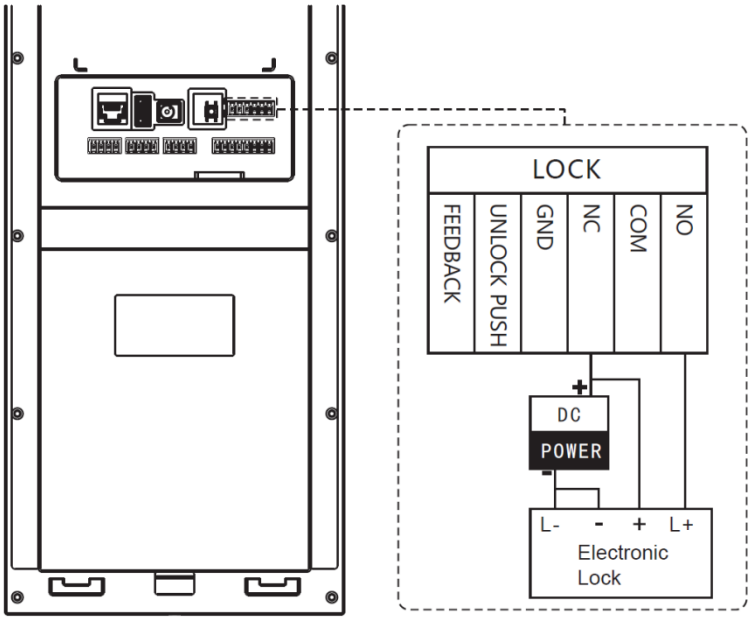


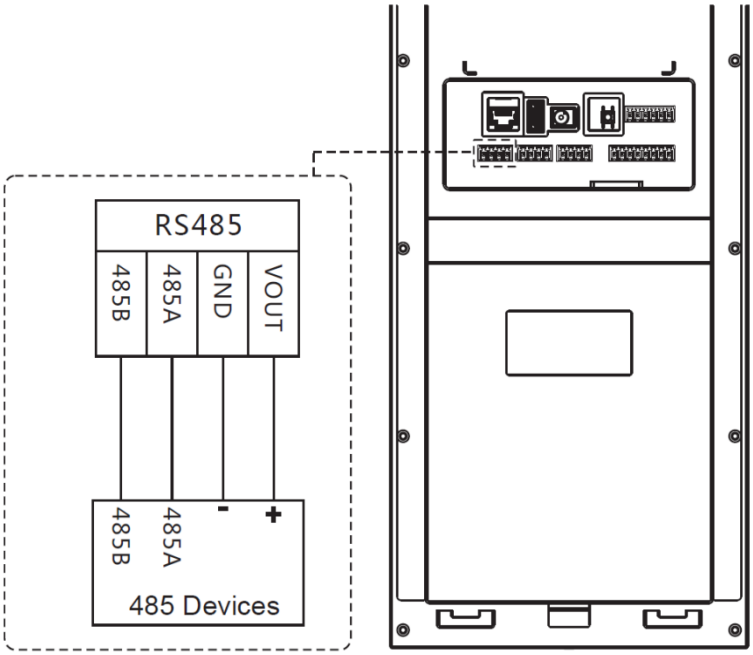
Figure 2-6 Electronic lock connection



2.3.2 RS485 Port

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

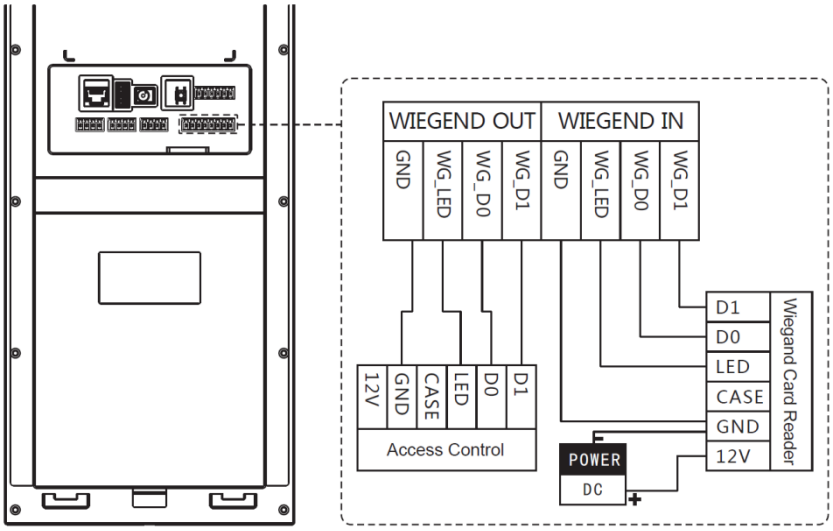
Figure 2-7 485 devices connection



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.

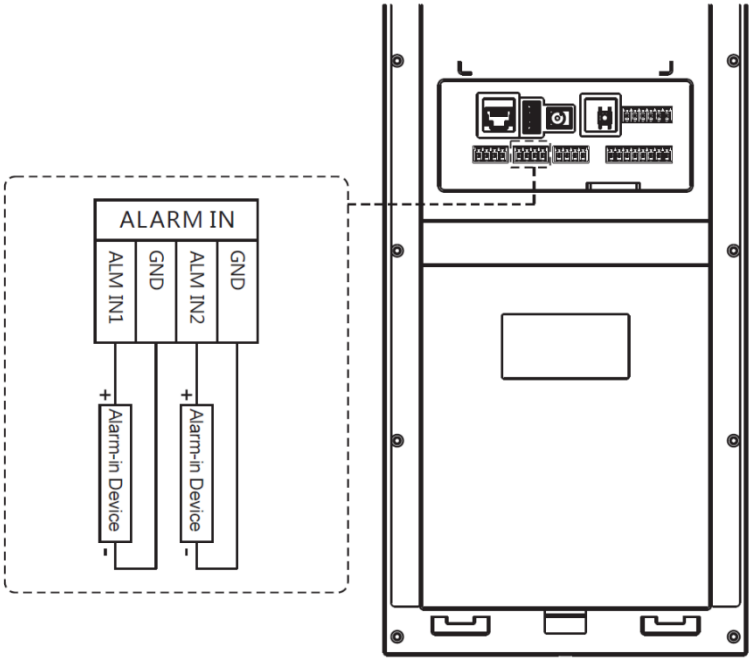
Figure 2-8 Wiegand input/output connection



2.3.4 Alarm-in Port

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

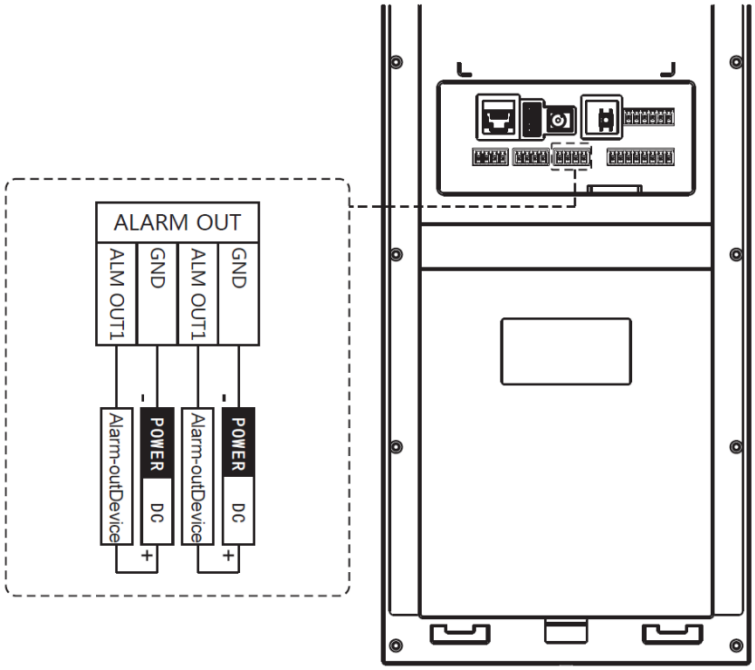
Figure 2-9 Alarm input device connection



2.3.5 Alarm-out Port

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

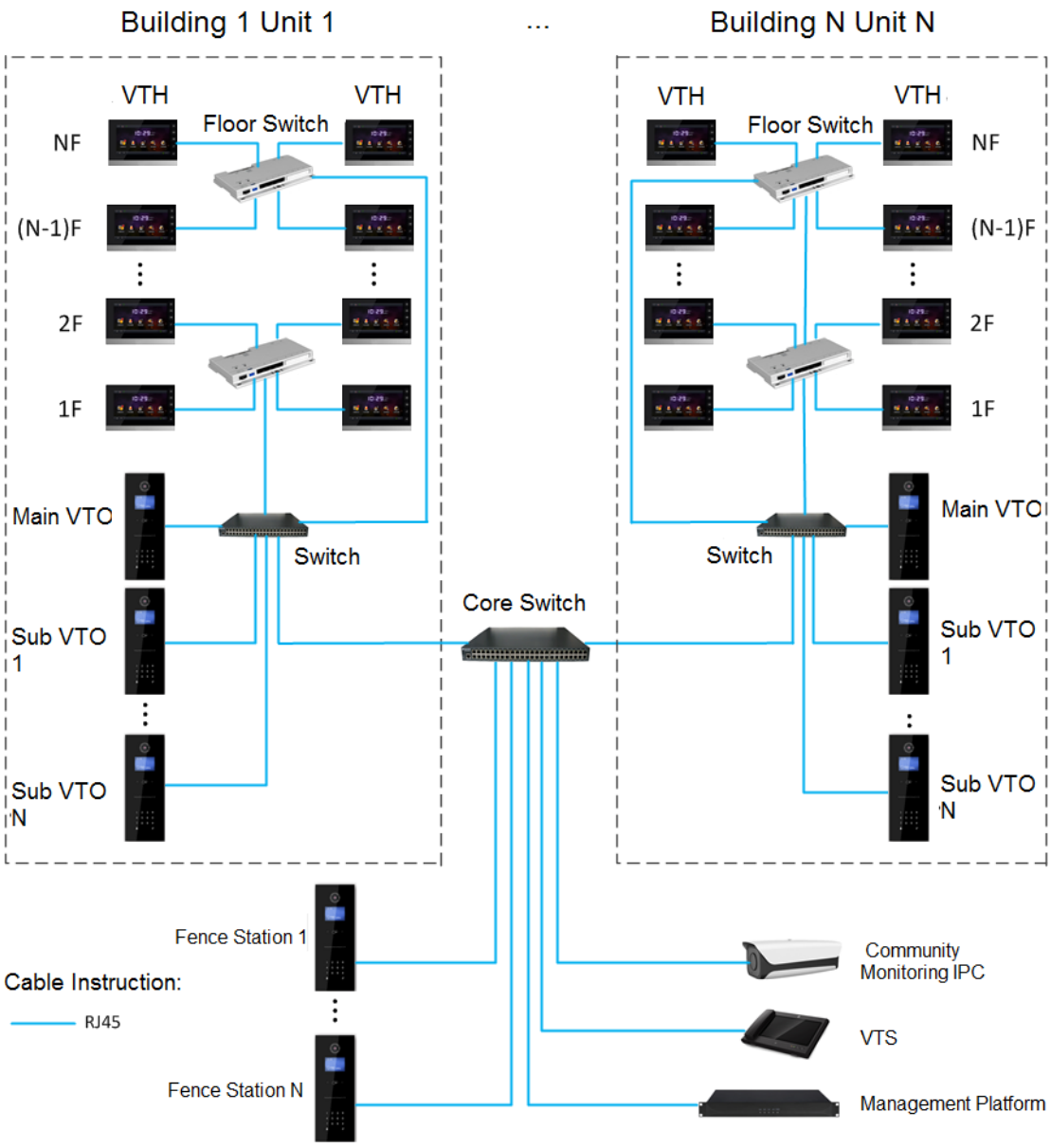
Figure 2-10 Alarm output device connection



3 Network Diagram

See Figure 3-1 for the network diagram of the VTO.

Figure 3-1 Network diagram



4 Installing the VTO

4.1 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.

4.2 Connecting Cable

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

4.3 Attaching the VTO

For the installation diagram, see Figure 4-1, and for the installation item list, see Table 4-1.

Figure 4-1 VTO installation

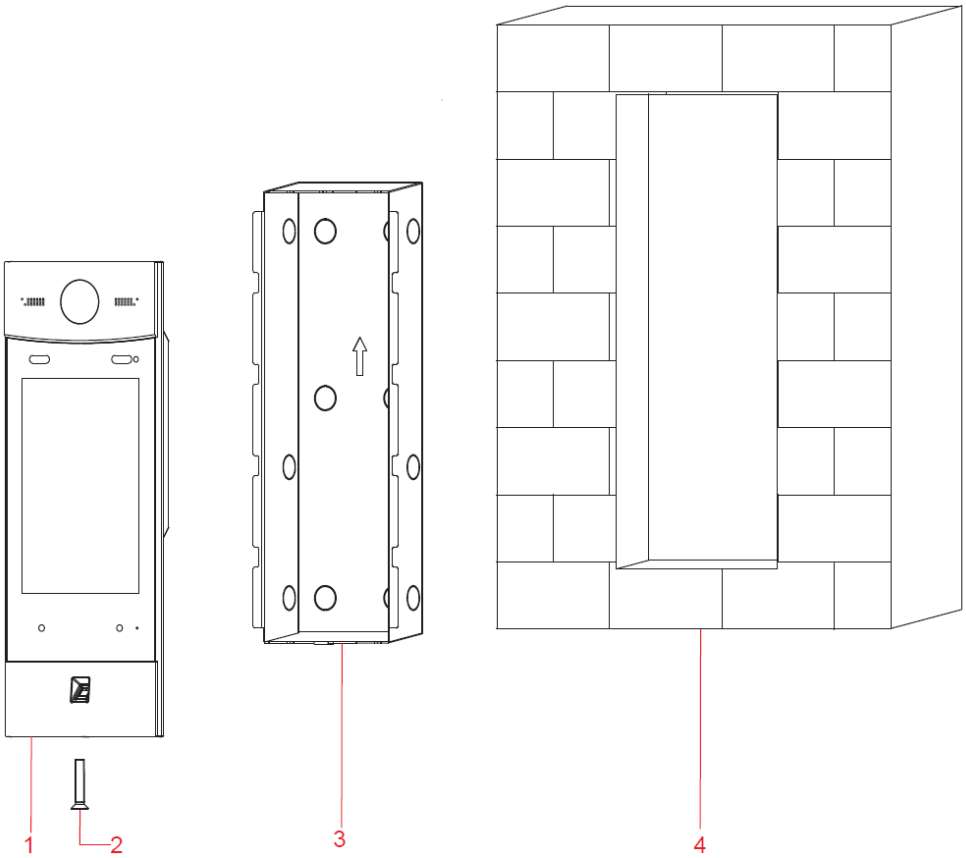


Table 4-1 Item list

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.

5 Configuring Devices

This chapter introduces how to make basic configurations and realize network connection, calling, and monitoring. 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.
- Properly plan the IP address, building number, and room number for every device.
- Confirm the location of the SIP server.

5.1 Configuration

- The VTO requires VTH devices with SIP system to function, and this manual takes configuring the 10-inch model VTH for example.
- You need to configure every VTO and VTH in the network.

5.1.1 Configuring VTO

5.1.1.1 Initializing VTO

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

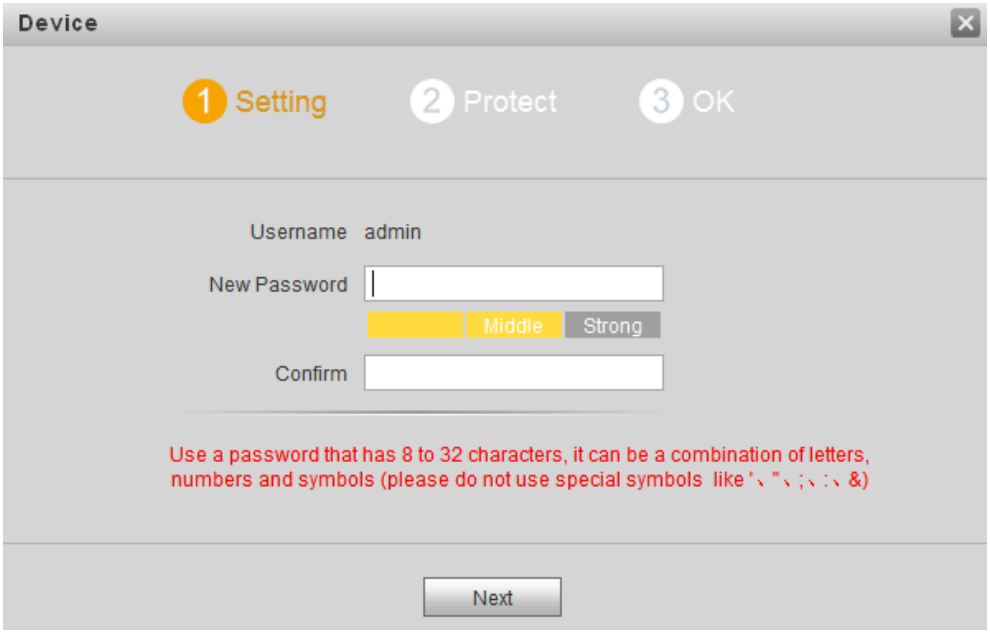
The default IP address of the VTO is 192.168.1.110, and make sure the PC is in the same network segment with the VTO.

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 5-1.

Figure 5-1 Password setting

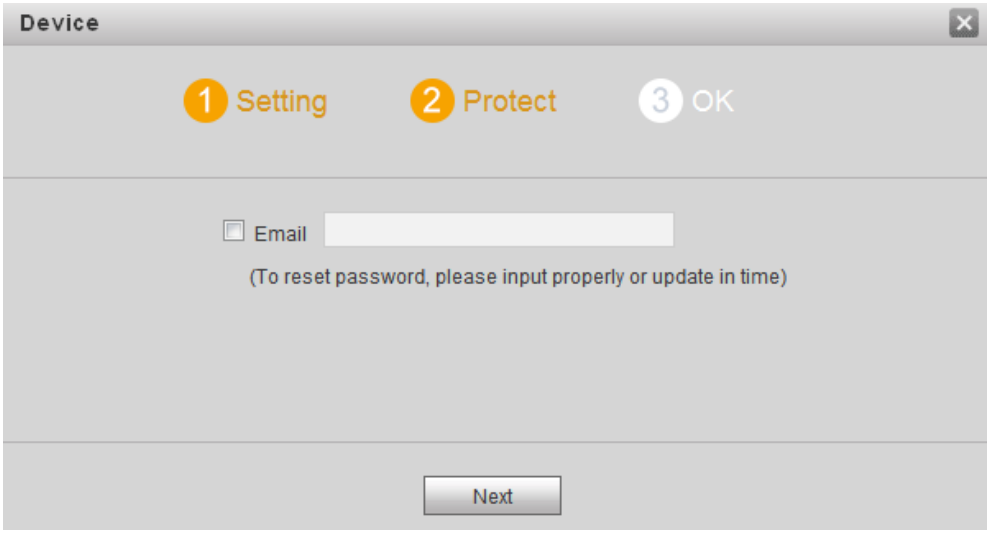


Step 3 Enter and confirm the password, and then click **Next**.

The Email setting interface is displayed. See Figure 5-2.

This password is to login the Web interface, and it should contain at least 8 digits and at least two types from number, letter, and symbol.

Figure 5-2 Email setting



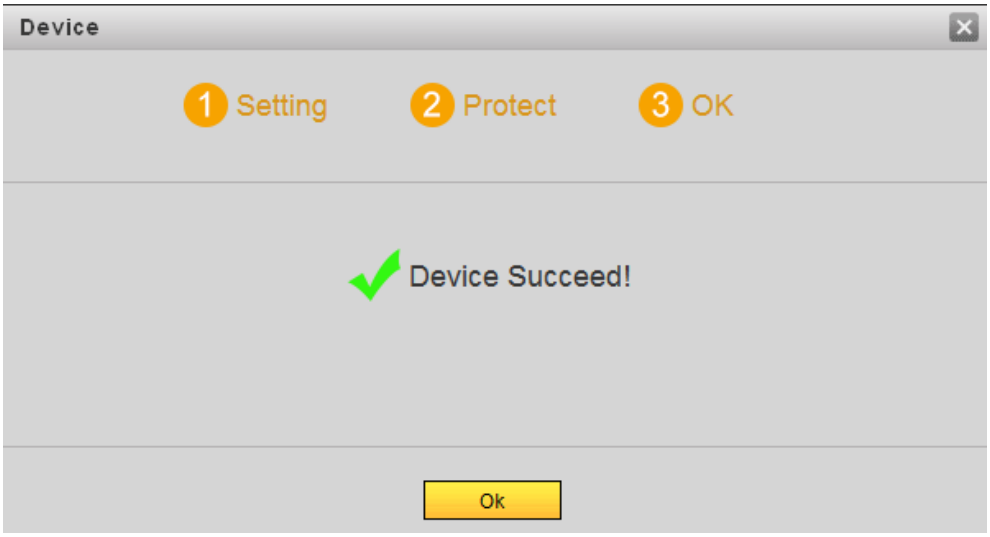
Step 4 Select the **Email** check box, and then enter your Email address.

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

Step 5 Click **Next**.

The **Device Succeed** interface is displayed. See Figure 5-3. The initialization is finished.

Figure 5-3 Device succeed



Step 6 Click **OK**.

The login interface is displayed. See Figure 5-4

Figure 5-4 Login

Step 7 Enter the username and the password, and then click **Login**.

- The default username is admin.
- The password is what you configured during initialization.

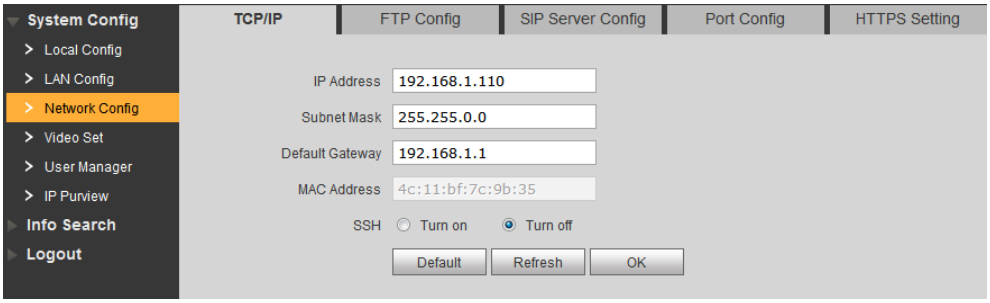
5.1.1.2 Modifying VTO IP Address

You can modify the default IP address of the VTO to the one you planned.

Step 1 Select **System Config > Network Config > TCP/IP**.

The **TCP/IP** interface is displayed. See Figure 5-5.

Figure 5-5 TCP/IP



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

The VTO will reboot after modification, and then there might be two conditions.

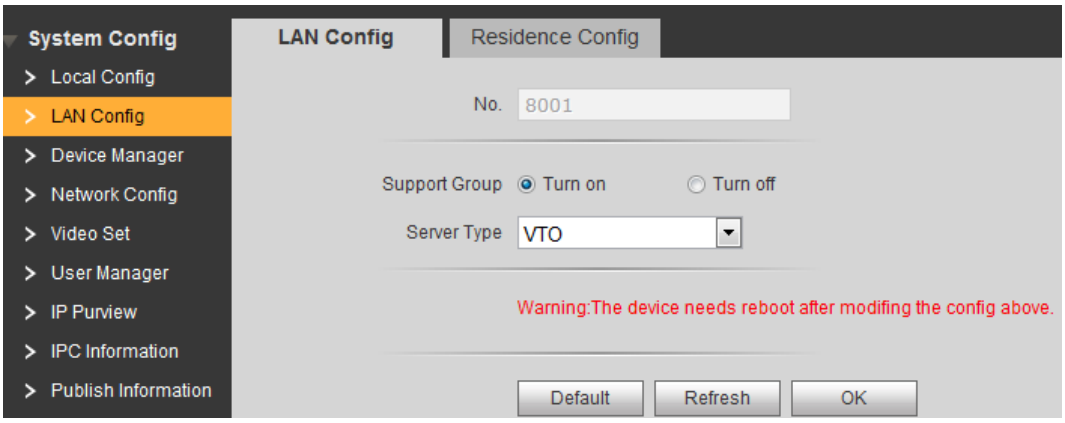
- If the PC IP address is within the planned network segment, the login interface with newly modified IP address is displayed, and you can login.
- If the PC IP address is not within the planned network segment, you need to modify its IP address and add it in the planned network segment, and then you can login.

5.1.1.3 LAN Config

You can configure the type of the SIP serve and the number of the VTO. 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.

Select **System Config > LAN Config**, and then the **LAN Config** interface is displayed. See Figure 5-6.

Figure 5-6 LAN config



- If VTO works as SIP server

  Select **VTO** in **Server Type**, and then click **OK**.
- If third party server (Express by default) works as SIP server

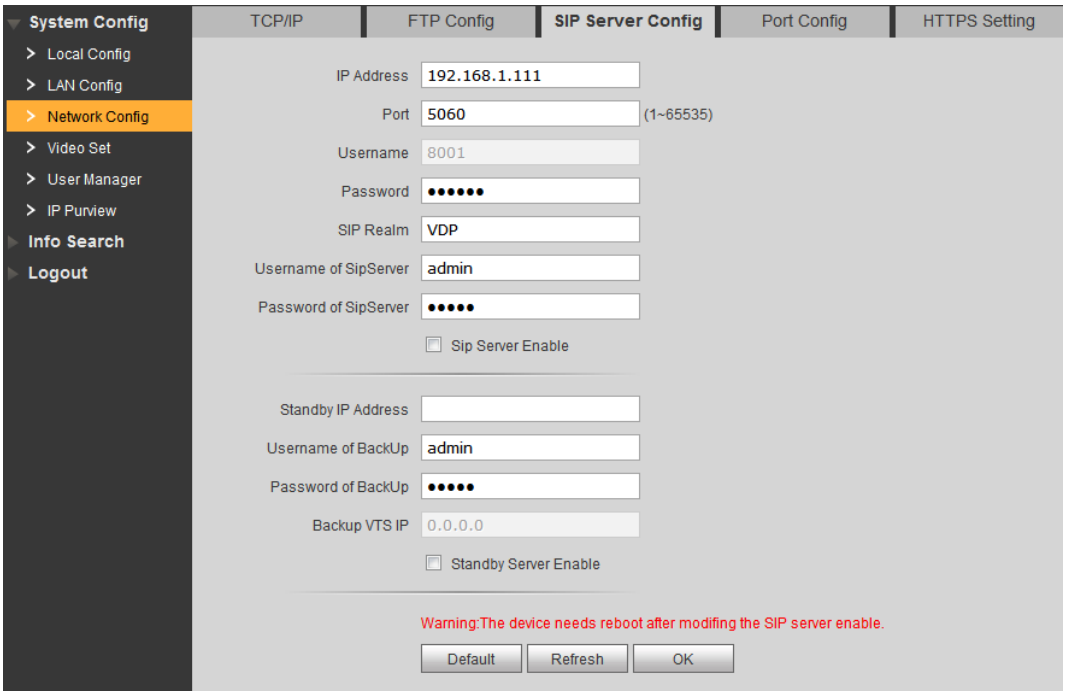
  Select the server type you need in **Server Type**, and then click **OK**.

When third party server works as SIP server, you can select **Turn on** at **Support Building** and **Support Unit** to configure building and unit number. For the detailed configuration, see the corresponding manual.

5.1.1.4 Configuring SIP Server

Select **System Config > Network Config > SIP Server Config**, and then the **SIP Server Config** interface is displayed. See Figure 5-7.

Figure 5-7 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 third party server or other VTO work as SIP server, do not select the **SIP Server Enable** check box, otherwise the connection will fail.

- If other VTO works as SIP server

  See Table 5-1 for the configuration, and then click **OK**. The VTO reboots, and then the login interface is displayed.

Table 5-1 SIP server config (1)

Parameter	Description
IP Address	The IP address of the VTO that works as SIP server.
Port	It is **5060** by default.
Username	Leave to the default.
Password	
SIP Domain	The **SIP Domain** is **VDP**.
Login UserName	The username and password of the SIP server.
Login PWD	

- If third party server works as SIP server

  See Table 5-2 for the configuration, and then click **OK**. The VTO reboots, and then the login interface is displayed.

Table 5-2 SIP server config (2)

Parameter	Description
IP Address	The IP address of the server that works as SIP server.
Port	It is **5080** by default.

Parameter	Description
Username	Leave to the default.
Password	
SIP Domain	Leave it blank or keep the default.
Login UserName	The username and password of the SIP server.
Login PWD	

If third party server is configured as SIP server, see the manual of the server for the detailed configuration.

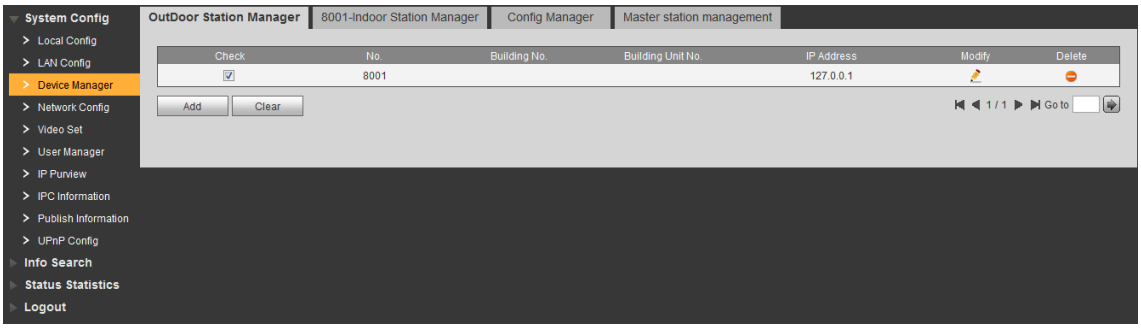
5.1.1.5 Adding VTO

Step 1 Login the Web interface of the VTO that is configured as SIP server.

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

The **Outdoor Station Manager** interface is displayed, see Figure 5-8.

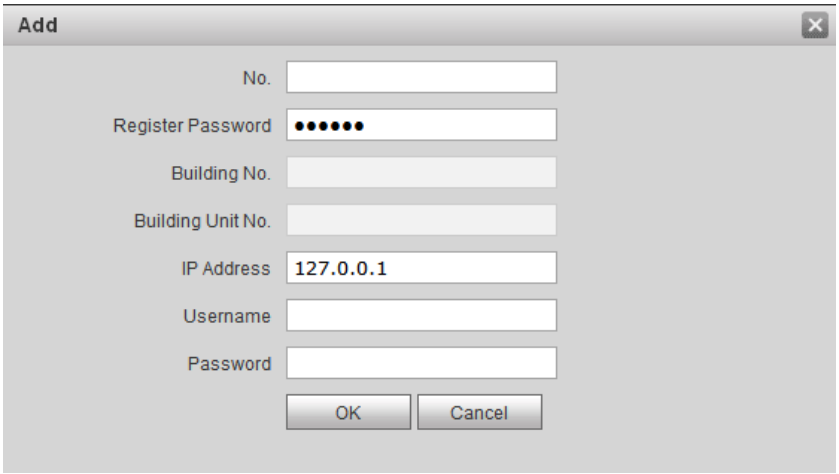
Figure 5-8 Outdoor station manager



Step 3 Click **Add**.

The **Add** interface is displayed. See Figure 5-9.

Figure 5-9 Add



Step 4 Configure VTO parameters. See Table 5-3 for the details.

Table 5-3 VTO parameters

Parameter	Description
No.	The number you planned for the VTO.
Register Password	Leave to the default.

Parameter	Description
IP Address	The IP address of the VTO.
Username	The username and password for the Web interface of the VTO.
Password	

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

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

5.1.1.6 Adding VTH

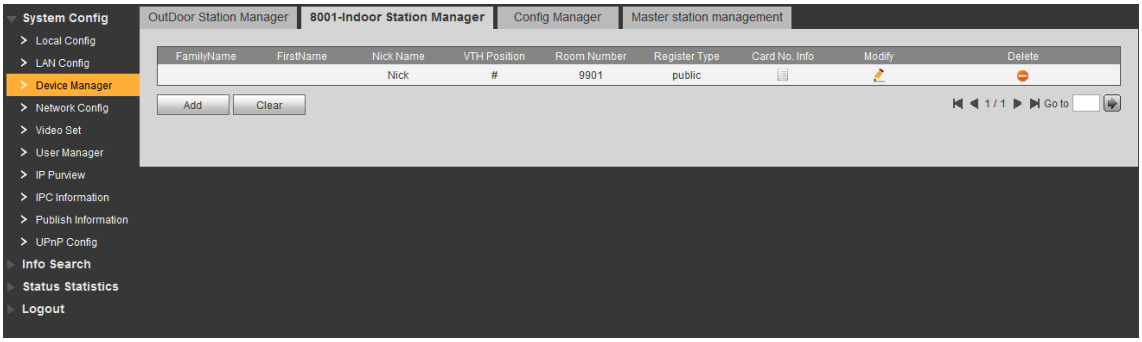
If there are master VTH and extension VTH being used, you need to add them all.

Step 1 Login the Web interface of the VTO that is configured as SIP server.

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

The **8001-Indoor Station Manager** interface is displayed, see Figure 5-10.

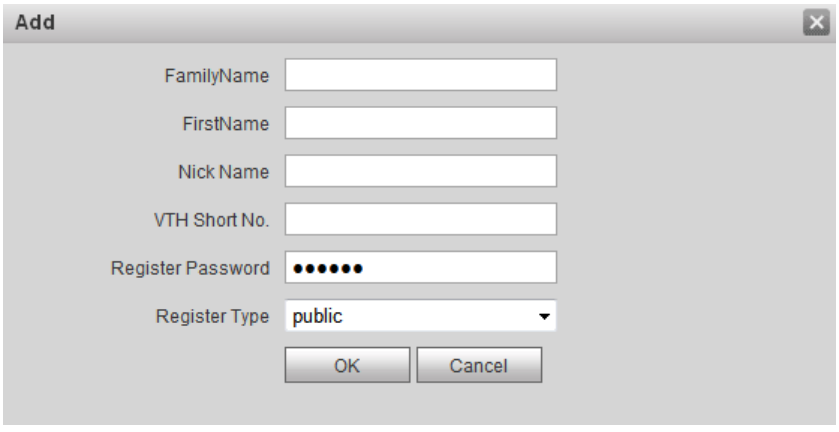
Figure 5-10 8001-indoor station manager



Step 3 Click **Add**.

The **Add** interface is displayed. See Figure 5-11.

Figure 5-11 Add VTH



Step 4 Configure VTH parameters. See Table 5-4 for the details.

Table 5-4 VTH parameters

Parameter	Description
FamilyName	Configure the name and nickname of the VTH users to differentiate them.
FirstName	
Nick Name	
VTH Short No.	The VTH short number should be the same as the room

Parameter	Description
	number you planned for the VTH. 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	Leave to the default.
Register Type	

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

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

5.1.2 Configuring VTH

5.1.2.1 Initializing VTH

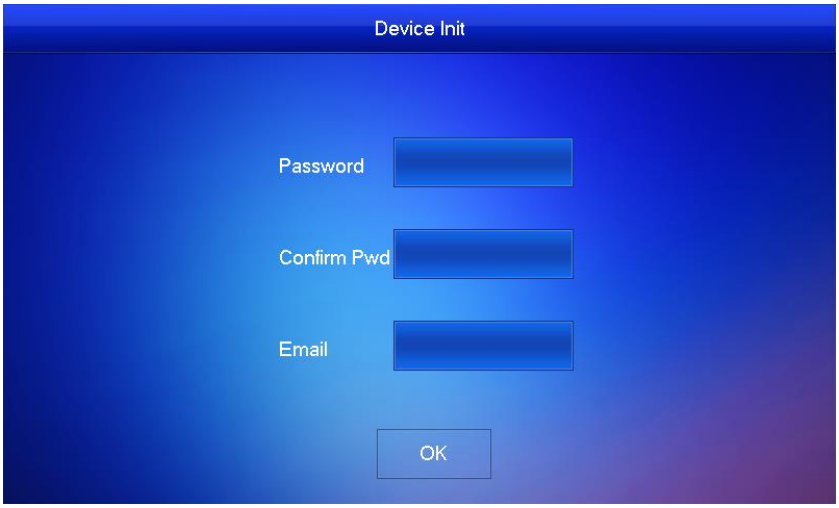
Configure VTH password and link to your Email.

- Password: it can be used to go to the engineering interface, mostly for admin people or engineers.
- Email: it can be used to reset the password.

Step 1 Power up the VTH.

The **WELCOME** sign is displayed, and then the **Device Init** interface. See Figure 5-12.

Figure 5-12 Device initialization

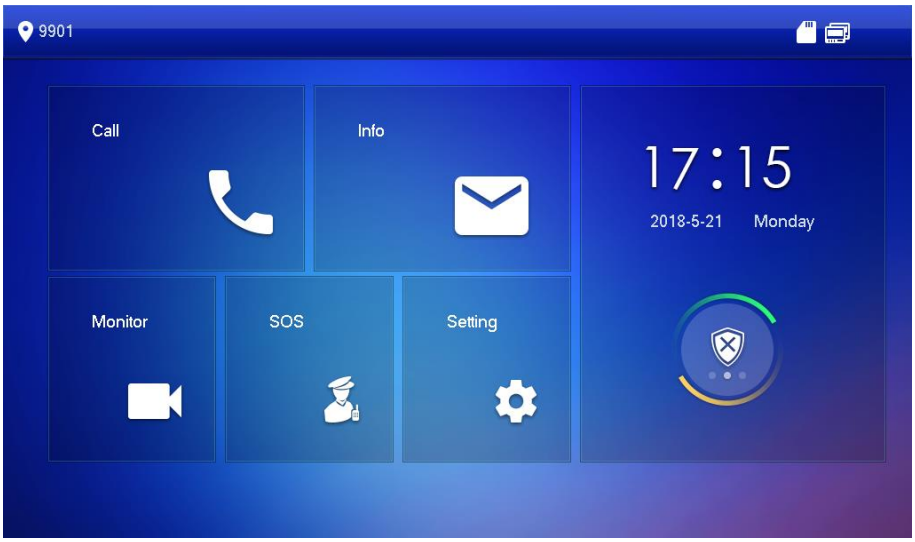


Step 2 Enter and confirm the password, and then enter the Email.

Step 3 Tap **OK**.

The main interface is displayed. See Figure 5-13.

Figure 5-13 Main interface



5.1.2.2 Configuring VTH Network

Make sure the VTH is in the same network segment with the VTO, otherwise the VTH cannot get information from the VTO.

Step 1 In the main interface, press and hold **Setting** until the **Password Verification** dialog box displays.

Step 2 Enter the password you configured during initialization, and then tap **OK**.

Step 3 Tap **Network**.

The **Network** interface is displayed. See Figure 5-14 or Figure 5-15.

Wireless function is available on select models.

Figure 5-14 Network(1)

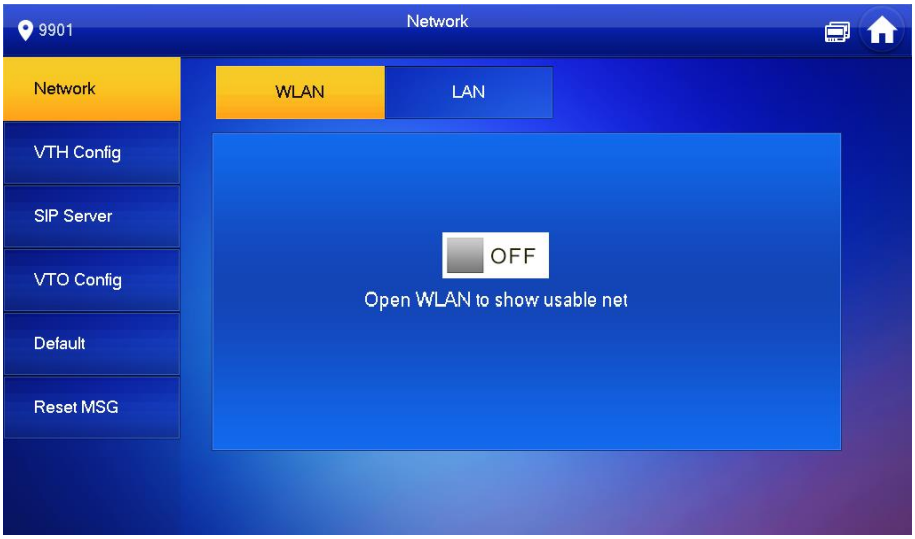
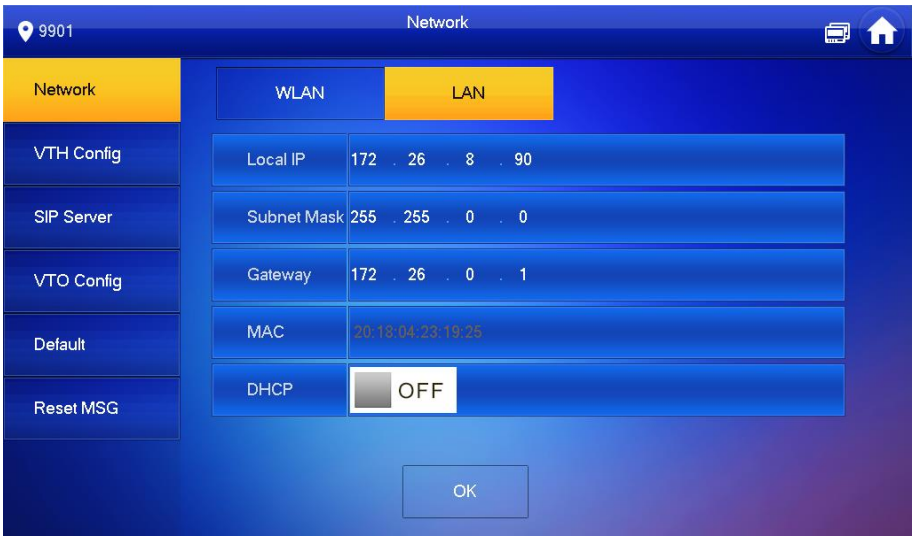


Figure 5-15 Network (2)



Step 4 Configure network with different access modes.

- LAN

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

If the VTH has wireless function, tap WLAN to configure network.

- WLAN

1) Tap OFF to enable Wi-Fi function.

The Wi-Fi networks that have been found are listed. See Figure 5-16.

Figure 5-16 Wi-Fi list

2) Connect Wi-Fi.

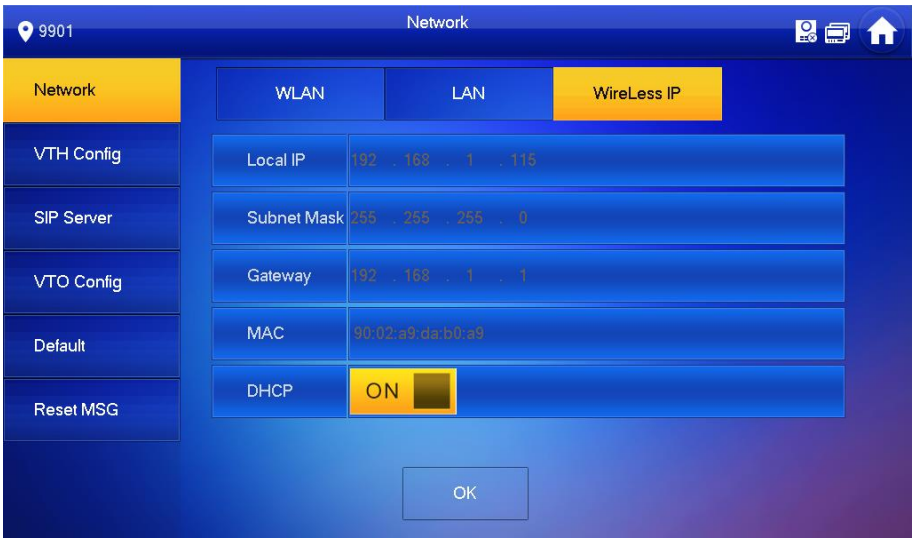
There are two ways to connect Wi-Fi:

◇ 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. See Figure 5-17.

To acquire IP address with DHCP, you need to connect the devices to a router with DHCP function.

Figure 5-17 Wireless IP



5.1.2.3 VTH Config

You can configure room number, VTH type, and Master IP.

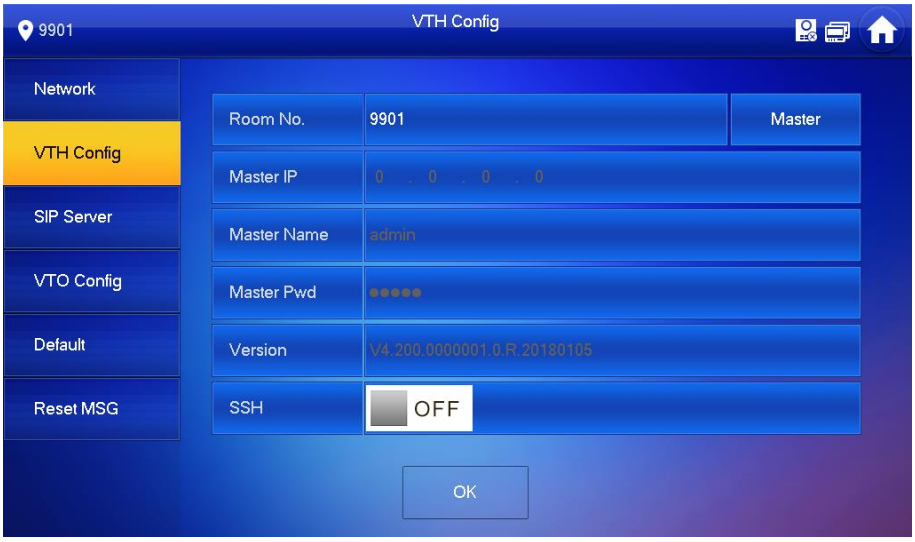
Step 1 In the main interface, press and hold **Setting** until the **Password Verification** dialog box displays.

Step 2 Enter the password you configured during initialization, and then tap **OK**.

Step 3 Tap **VTH Config**.

The **VTH Config** interface is displayed. See Figure 5-18.

Figure 5-18 VTH Config



Step 1 Configure the VTH information.

- Configure master VTH

  Enter the room number (such as 9901).

  - If you only use single VTH, the room number should be the same as the VTH short number you configured.
  - 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.

- Configure extension VTH

1. Tap **Master**, and then the VTH type changes to **Extension**.
2. Enter the room number (such as 9901#1), the IP address of the master VTH, master name, and the master password.

   The master name and the master password are the username and password of the master VTH. The username is admin by default, and the password is what you configured during initialization.

Step 2 (Optional) Tap 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 3 Tap **OK** to save.

5.1.2.4 Configuring SIP Server

You can enter the SIP server information and connect the VTH to the SIP server.

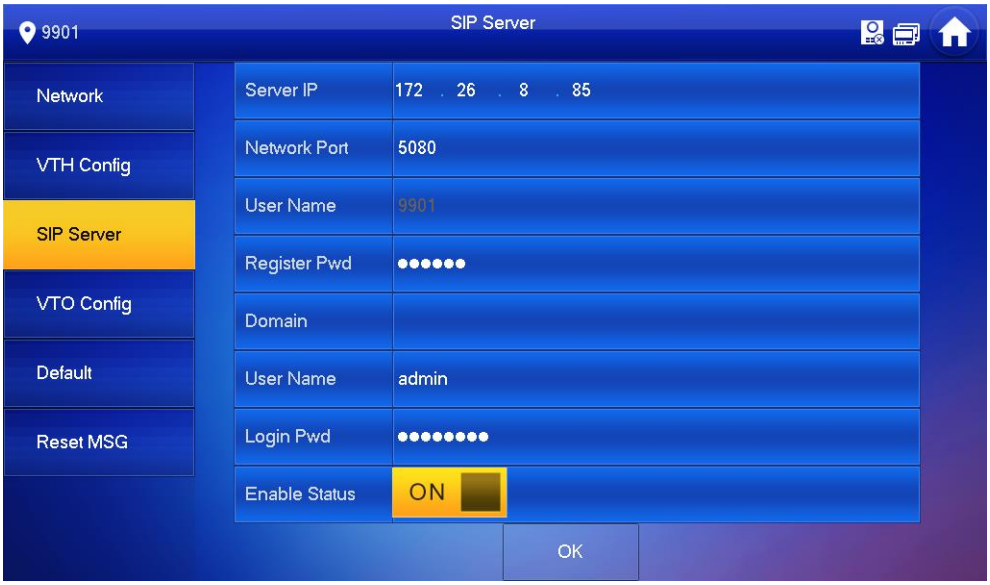
Step 1 In the main interface, press and hold **Setting** until the **Password Verification** dialog box displays.

Step 2 Enter the password you configured during initialization, and then tap **OK**.

Step 3 Tap **SIP Server**.

The **SIP Server** interface is displayed. See Figure 5-19.

Figure 5-19 SIP server



Step 4 Configure SIP server parameters. For the detailed description, see Table 5-5.

Table 5-5 SIP server parameter

Parameter	Description
Server IP	● If third party server works as SIP server, enter the server's IP address. ● If VTO works as SIP server, enter the VTO's IP address.
Network Port	● If third party server works as SIP server, enter 5080. ● If VTO works as SIP server, enter 5060.
User Name	Leave to the default.
Register Pwd	
Domain	Leave it blank or keep the default.

Parameter	Description
	If VTO works as SIP server, the **Domain** should be VDP.
User Name	The username and password of the SIP server.
Login Pwd	

Step 5 Set the **Enable Status** to ON.

The SIP server function is enabled.

Step 6 Tap **OK** to save.

5.1.2.5 VTO Config

You can enter the VTO information and connect the VTH to the VTO.

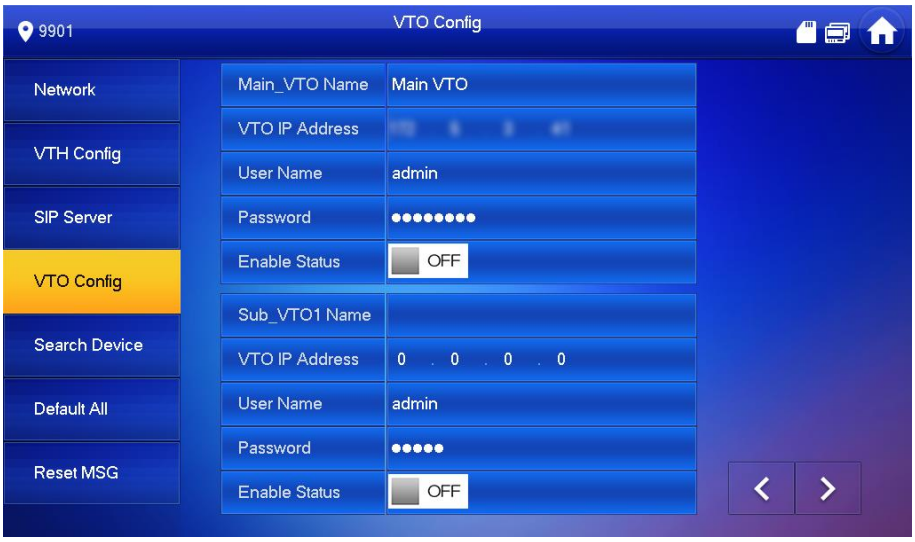
Step 1 In the main interface, press and hold **Setting** until the **Password Verification** dialog box displays.

Step 2 Enter the password you configured during initialization, and then tap **OK**.

Step 3 Tap VTO Config.

The **VTO Config** interface is displayed. See Figure 5-20.

Figure 5-20 VTO Config



Step 4 Add VTO or fence station.

If you use single VTO, then only enter the VTO information at **Main_VTO Name**; if you use multiple VTO devices, you can select any one as the main VTO, and then the other VTO devices will be sub VTO, and they sync information from the main VTO.

- Add main VTO

1) Enter the name and IP address of the main VTO, and then its username and password. See Figure 5-20.

1) Set the **Enable Status** to ON.

Be sure to enter the username and password for the Web interface of the main VTO, otherwise the connection will fail.

- Add sub VTO or fence station

2) Enter the name and IP address of the sub VTO or fence station, and then their username and password.

3) Set the **Enable Status** to ON.

5.2 Verifying Configuration

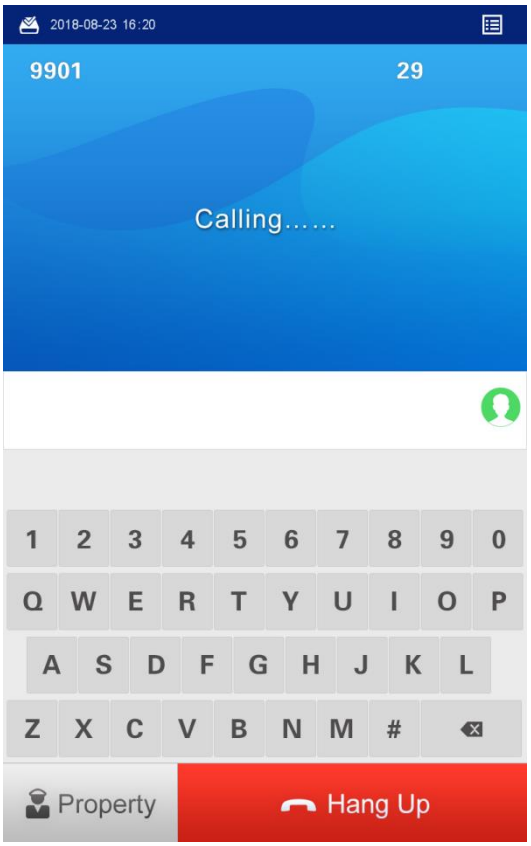
5.2.1 Calling VTH from VTO

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 then the calling request lasts for 30 s. See Figure 5-21.

Figure 5-21 Calling the VTH



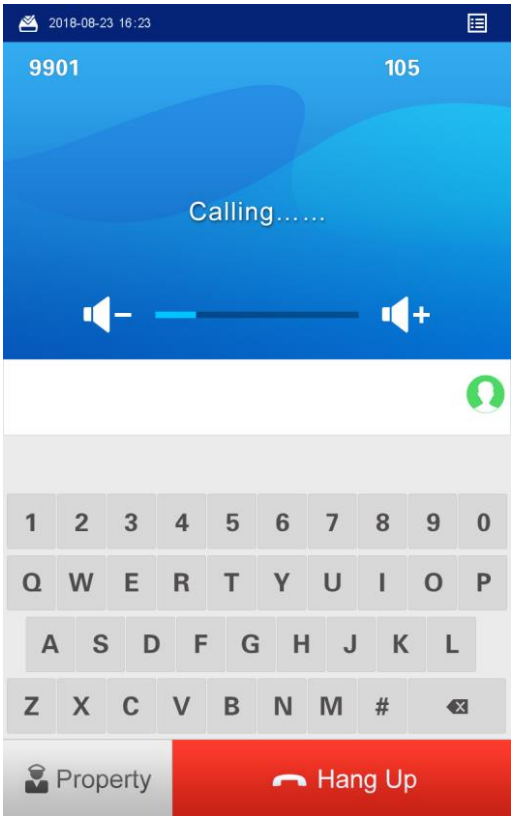
Step 3 The call screen is displayed on the VTH. See Figure 5-22.

Figure 5-22 Call screen

Step 4 Tap on the VTH to answer the call.

The VTO is in the phone call state. See Figure 5-23, and the configuration succeeded.

Figure 5-23 Phone call state

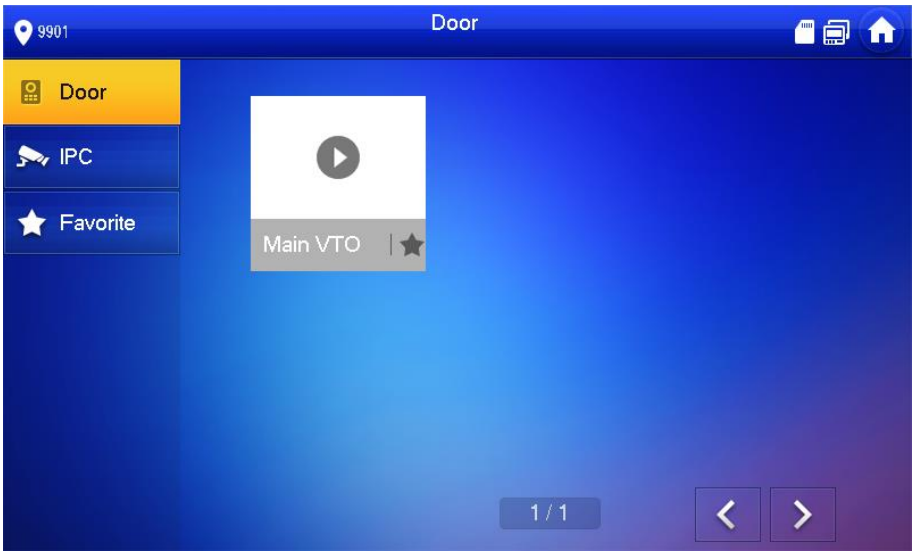


5.2.2 Doing monitor from VTH

You can monitor the area that VTO covers from VTH.

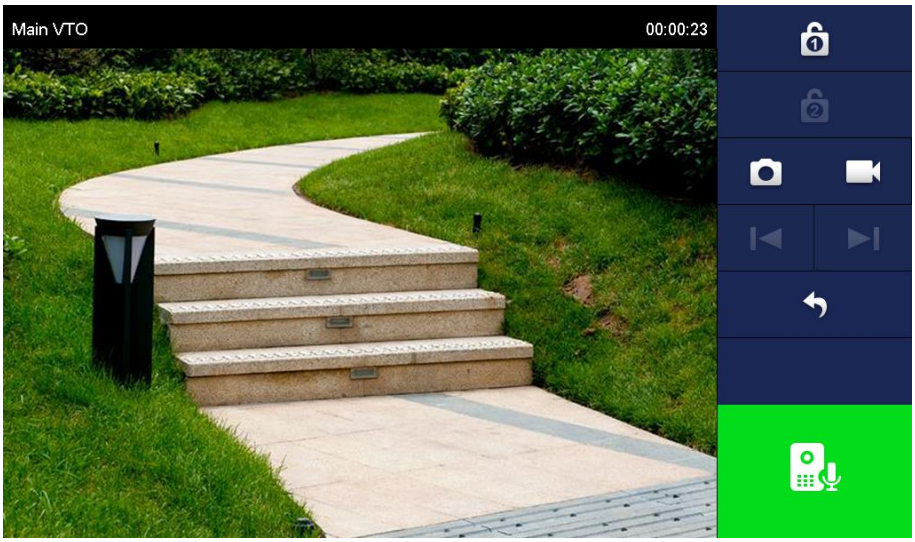
Step 1 In the main interface of the VTH, select **Monitor > Door**, and then the **Door** interface is displayed. See Figure 5-24.

Figure 5-24 Door



Step 2 Select the VTO you need to do monitor, see Figure 5-25.

Figure 5-25 Monitor screen



6 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.

6.1 Main interface

The main interface is displayed after booting. See Figure 6-1. For the detailed description, see Table 6-1.

Figure 6-1 Main interface

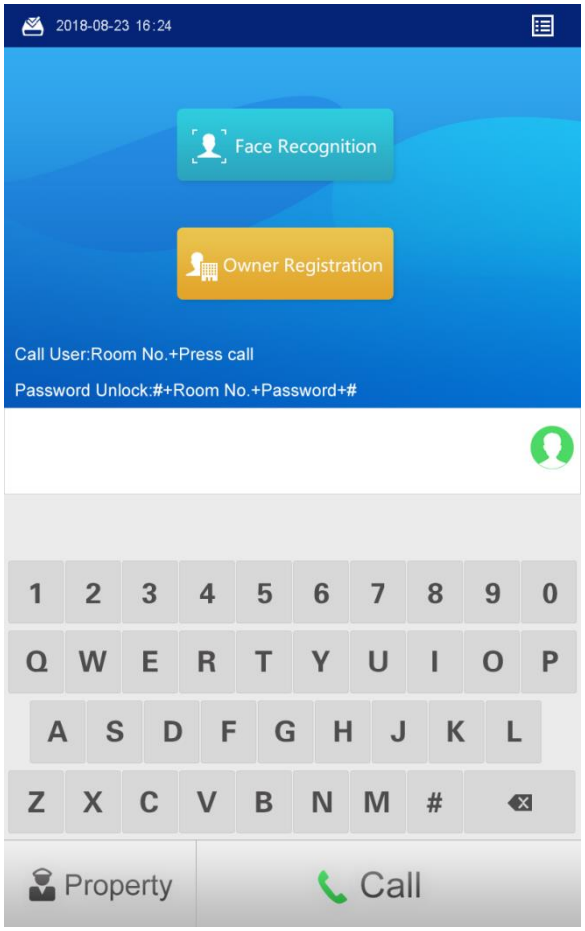


Table 6-1 Main interface description

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 "6.6.1 Engineering Interface."
Backspace	Delete the entered content.
Call	Tap to call residents.
Property	Tap to call the management center.

6.2 Call Function

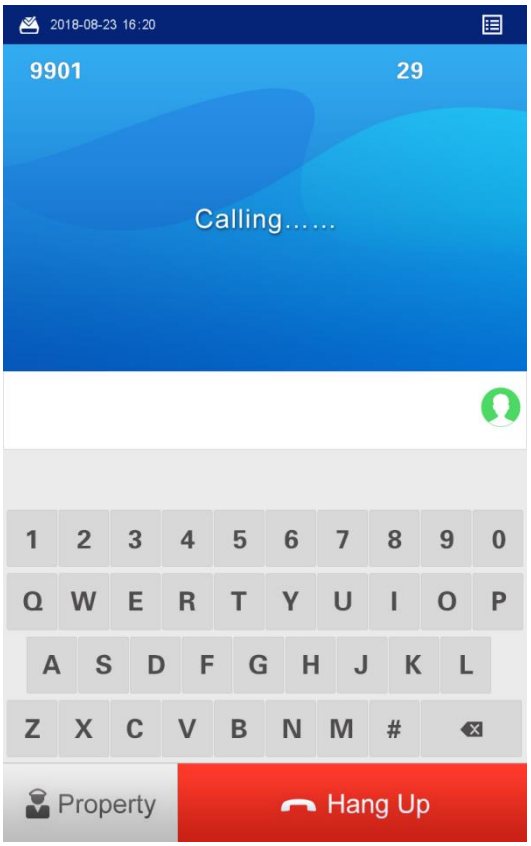
6.2.1 Calling VTH

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 then the calling request lasts for 30 s. See Figure 6-2.

Figure 6-2 Calling VTH



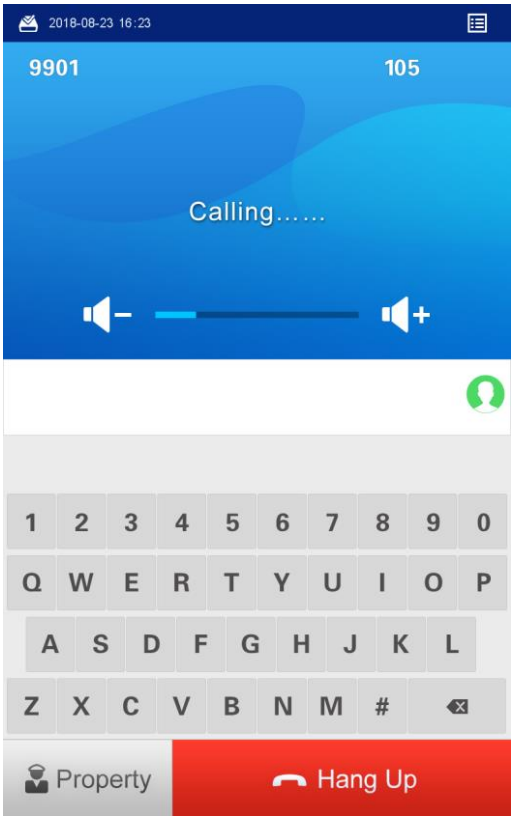
Step 3 The call screen is displayed on the VTH. See Figure 6-3.

Figure 6-3 Call screen

Step 4 Tap  on the VTH to answer the call.

The VTO is in the phone call state. See Figure 6-4.

Figure 6-4 Phone call state



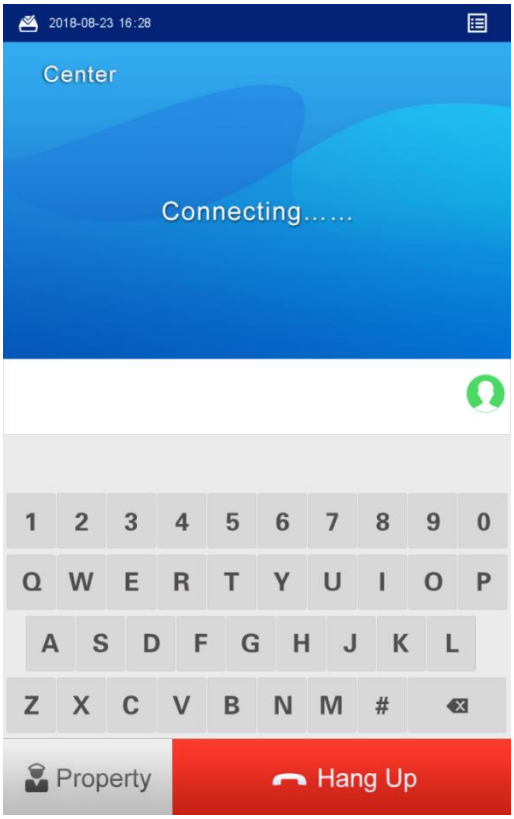
6.2.2 Calling Property (management center)

Step 1 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 then the calling request lasts for 30 s. See Figure 6-5.

The number of the management center is 888888 by default, and you can select **System Config > Local Config > Local Config** in the Web interface to change it. See the details in "7.3.1 Local Config."

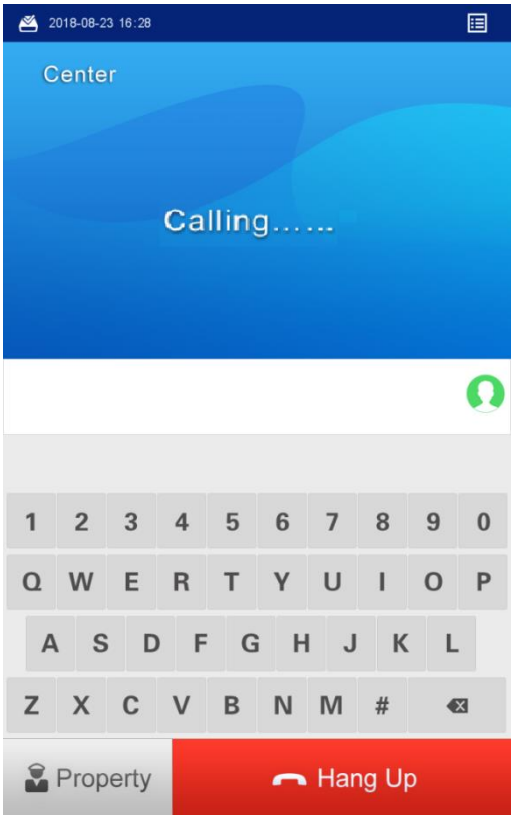
Figure 6-5 Calling management center



Step 2 The management center answers the call.

The VTO is in the phone call state. See Figure 6-6.

Figure 6-6 Phone call state



6.3 Unlocking Method

6.3.1 Face Unlock

On Sleeping Screen

When people approaching, the screen lights up, and then starts face recognition.

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.

In Main Interface

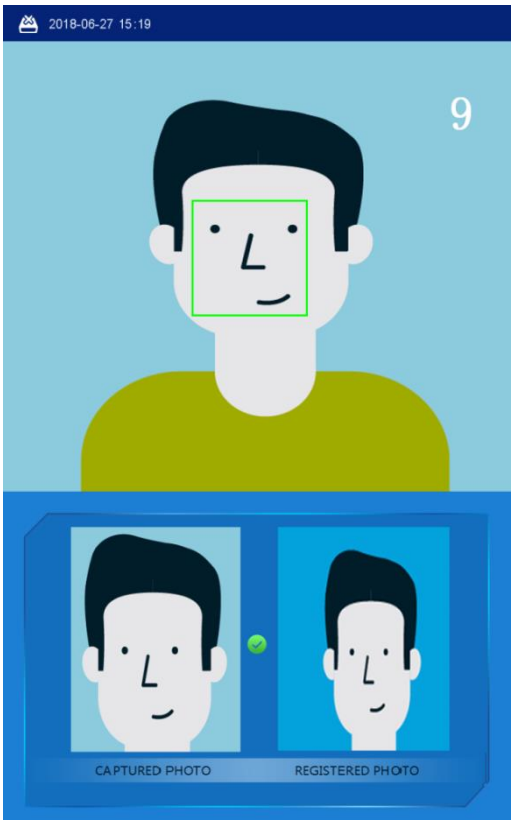
Step 1 Tap **Face Recognition**.

Step 2 Come close and face to the camera.

The VTO starts face recognition. See Figure 6-7.

- 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.

Figure 6-7 Face recognition



6.3.2 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 "6.4.2 Fingerprint Registration."

6.3.3 Password Unlock

Enter "#+your 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. For the details, see "7.3.2 A&C Manager."

6.3.4 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 "6.4.3 Issuing Card."

6.3.5 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.

Tap the Unlock button on the VTH. The "**Door opened**" notice displays on the VTO, and the "The door is unlocked" voice notice comes up.

6.3.6 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.

Click the Unlock button on the management center interface. The "**Door opened**" notice displays on the VTO, and the "The door is unlocked" voice notice comes up.

6.4 Registration

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

6.4.1 Face Registration

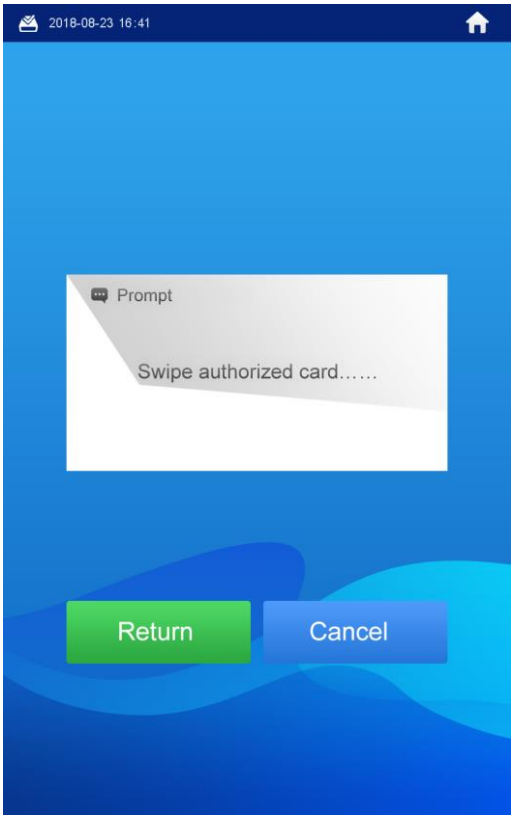
6.4.1.1 Face Registration by VTO Users

The VTO users can add new face data to the VTO with the authorized access card.

Step 1 In the main interface, tap **Owner Registration**.

The **Swipe authorized card** notice is displayed. See Figure 6-8.

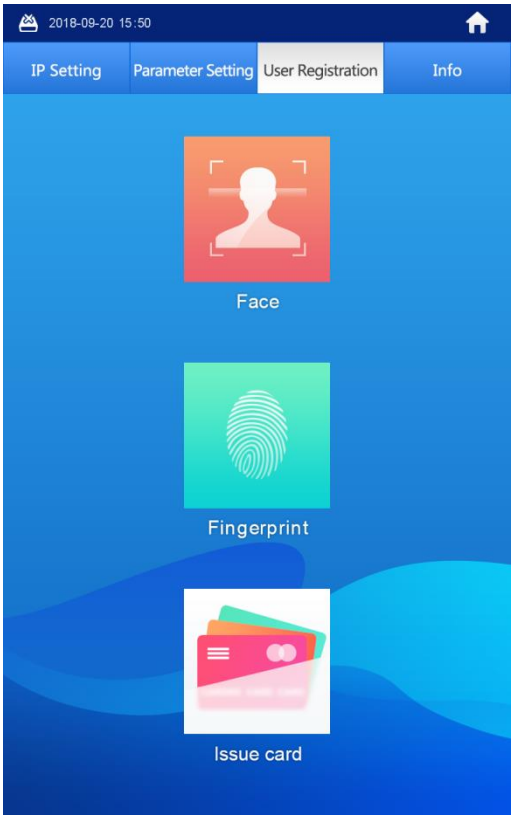
Figure 6-8 Swipe authorized card



Step 2 Swipe the authorized card**.**

The registration interface is displayed. See Figure 6-9.

Figure 6-9 Registration



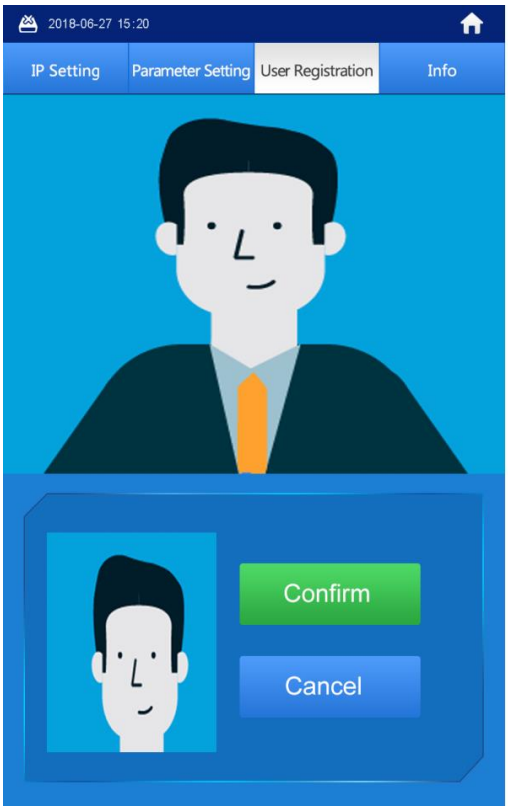
Step 3 Select **Face > Add face**.

The face recognition interface is displayed.

Step 4 The VTO starts face recognition. See Figure 6-10.

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

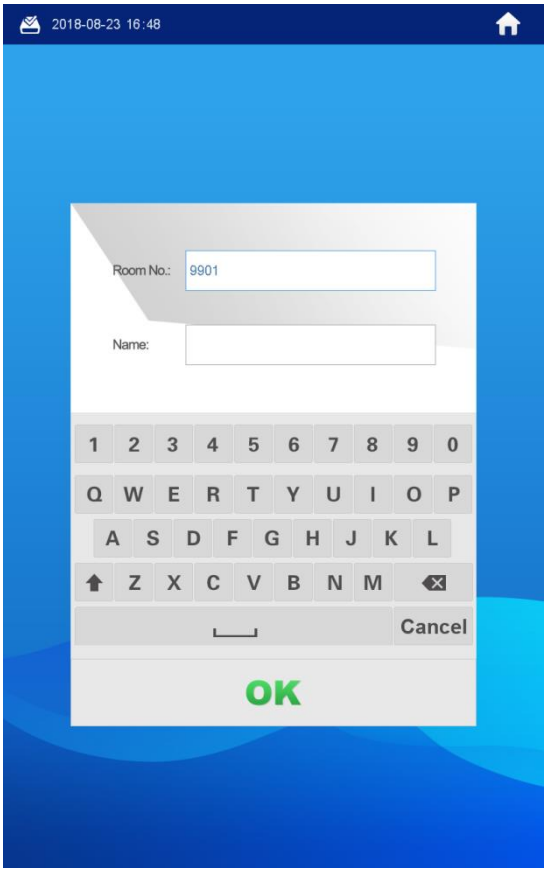
Figure 6-10 Face recognition



Step 5 After the registration finished, tap **Confirm**.

The information registration interface is displayed. See Figure 6-11.

Figure 6-11 Information registration



Step 6 Enter the room number and name for the newly added face.

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

Step 7 Tap **OK** to save.

The face data list of this room number is displayed.

Tap to exit.

6.4.1.2 Face Registration by Admin People

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

The **IP Setting** interface is displayed.

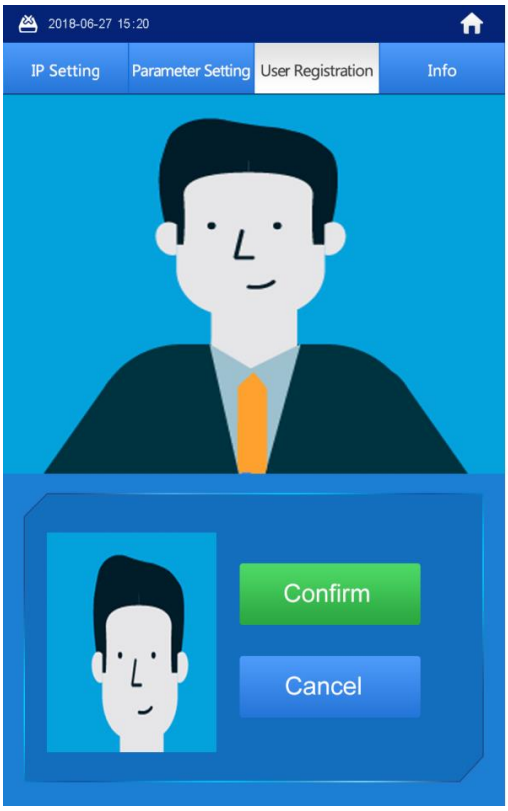
Step 2 Select **User Registration > Face > Add face**.

The face recognition interface is displayed.

Step 3 The VTO starts face recognition. See Figure 6-12.

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

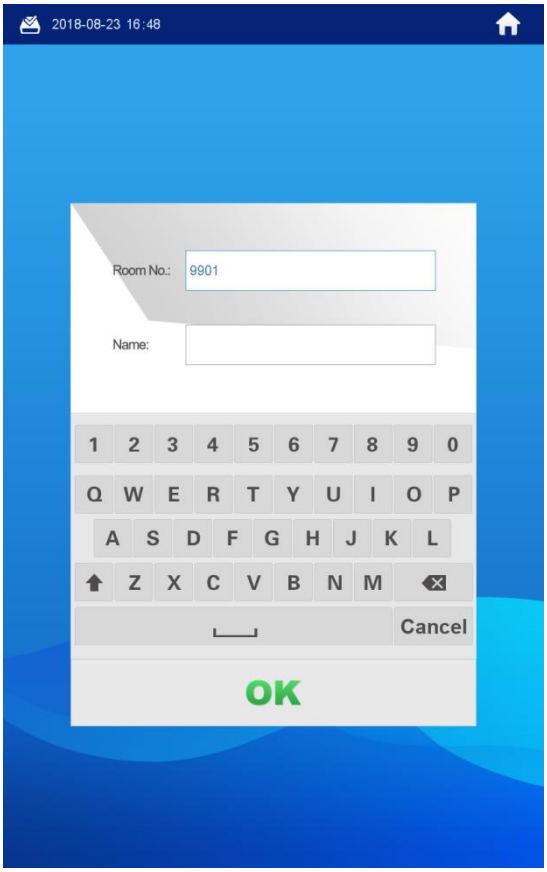
Figure 6-12 Face recognition



Step 4 After the registration finished, tap **Confirm**.

The information registration interface is displayed. See Figure 6-13.

Figure 6-13 Information registration



Step 5 Enter the room number and name for the newly added face.

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

Step 6 Tap **OK** to save.

Tap to exit.

6.4.2 Fingerprint Registration

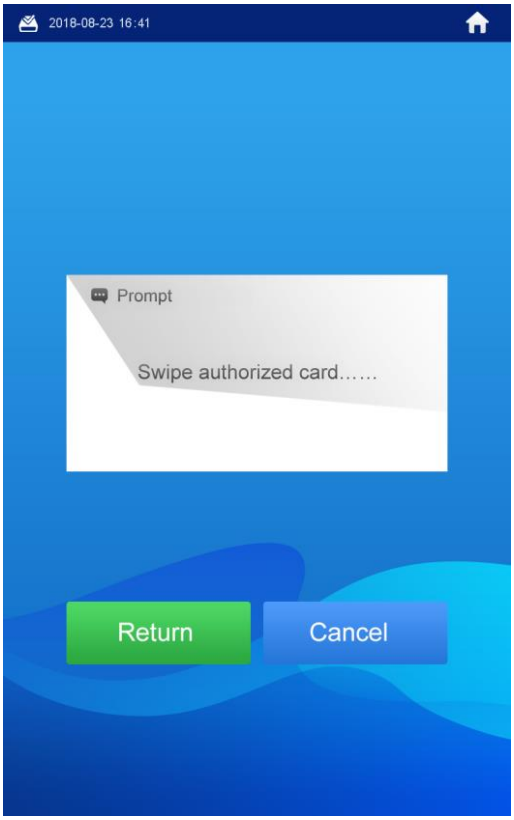
6.4.2.1 Fingerprint Registration by VTO Users

The VTO users can add new fingerprint data to the VTO with the authorized access card.

Step 1 In the main interface, tap **Owner Registration**.

The **Swipe authorized card** notice is displayed. See Figure 6-14.

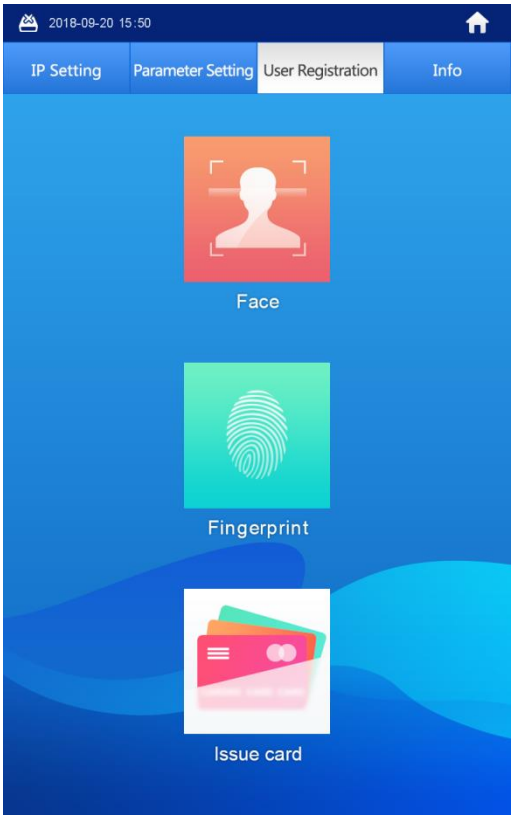
Figure 6-14 Swipe authorized card



Step 2 Swipe the authorized card**.**

The registration interface is displayed. See Figure 6-15.

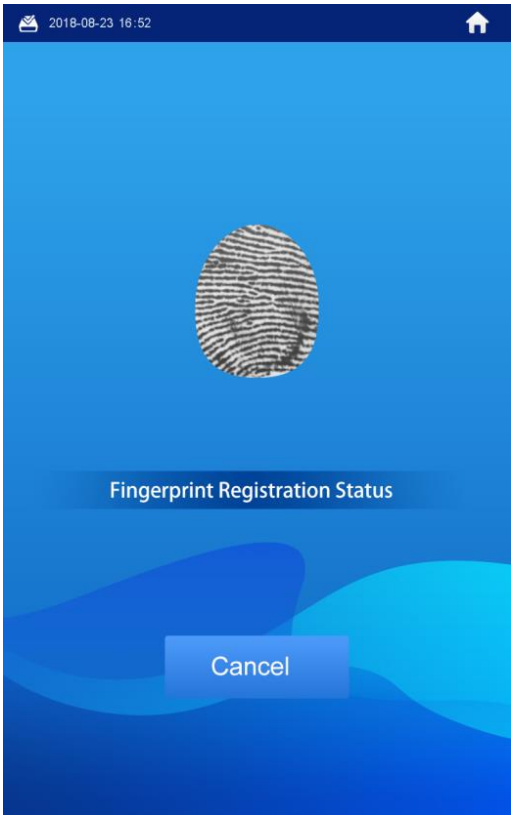
Figure 6-15 Registration



Step 3 Select **Fingerprint > Add Fingerprint**.

The fingerprint recognition interface is displayed. See Figure 6-16.

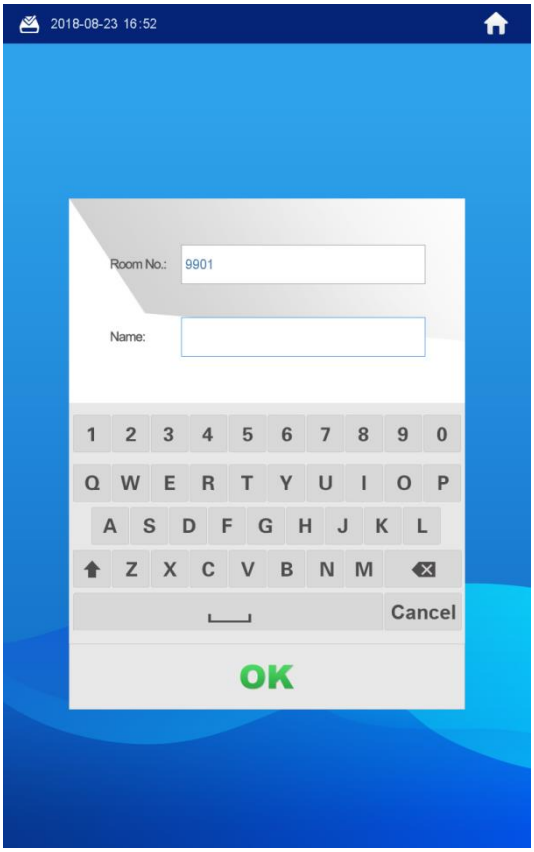
Figure 6-16 Fingerprint recognition



Step 4 Tap the fingerprint sensor as instructed.

After the registration finished, the information registration interface is displayed. See Figure 6-17.

Figure 6-17 Information registration



Step 5 Enter the room number and name for the newly added fingerprint.

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

Step 6 Tap **OK** to save.

Tap to exit.

6.4.2.2 Fingerprint Registration by Admin People

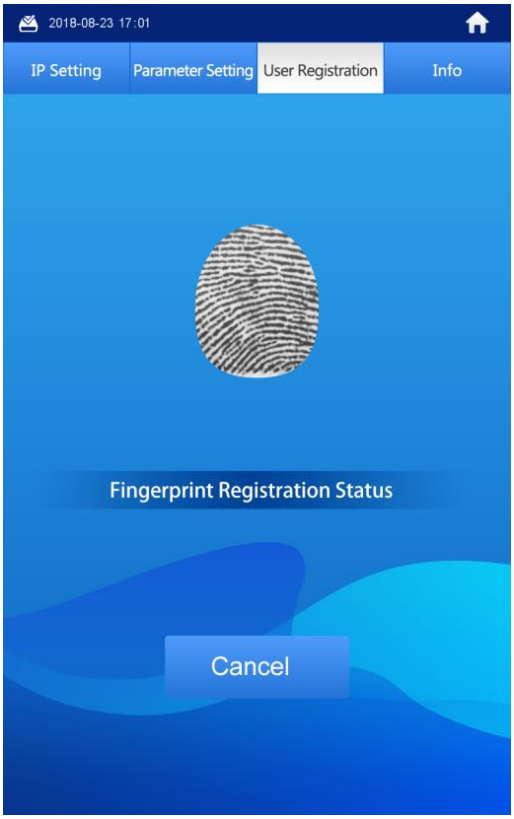
Step 1 In the main interface, enter #VTO password#.

The **IP Setting** interface is displayed.

Step 2 Select **User Registration > Fingerprint > Add Fingerprint**.

The fingerprint recognition interface is displayed. See Figure 6-18.

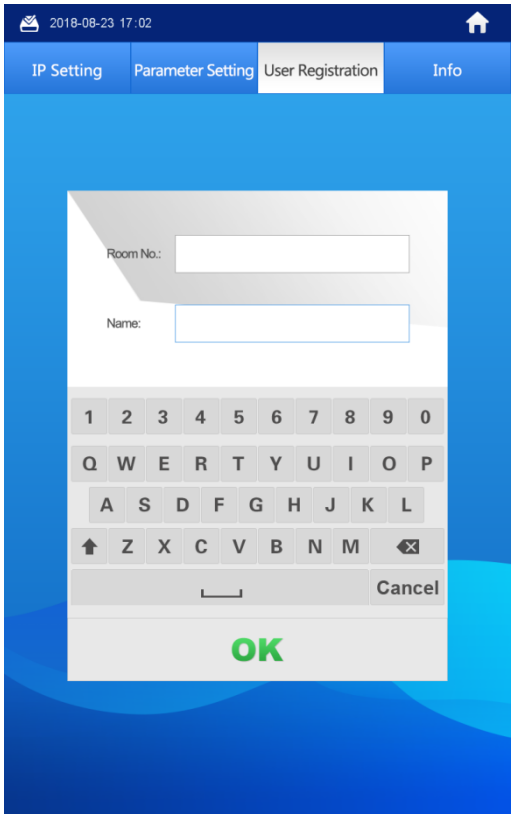
Figure 6-18 Fingerprint recognition



Step 3 Press the fingerprint sensor as instructed.

After the registration finished, the information registration interface is displayed. See Figure 6-19.

Figure 6-19 Information registration



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.

6.4.3 Issuing Card

This function is only for admin people or engineer.

6.4.3.1 Issuing Card by Password

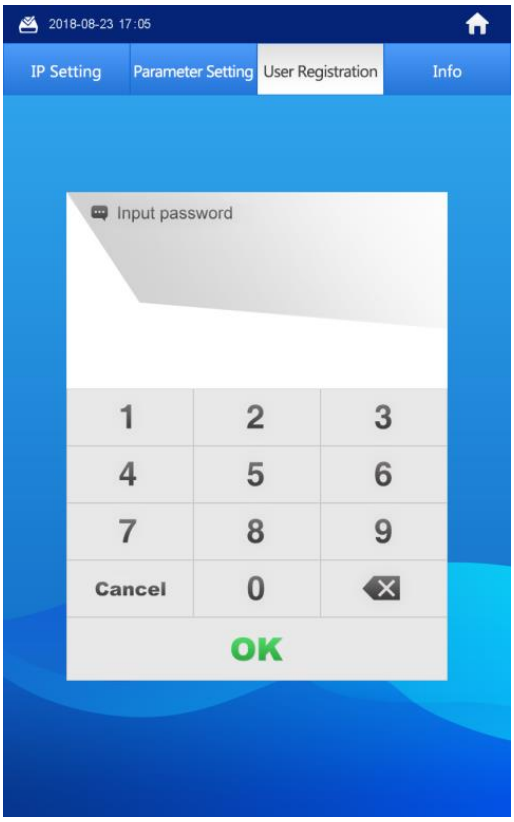
Step 1 In the main interface, enter #VTO password#.

The **IP Setting** interface is displayed.

Step 2 Select **User Registration > Card > Password**.

The **Input password** interface is displayed. See Figure 6-20.

Figure 6-20 Input password

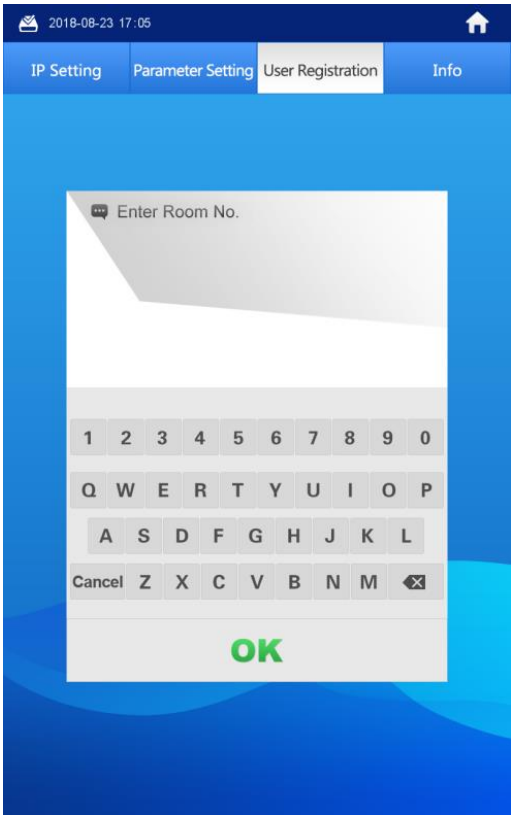


Step 3 Enter the card issuing password, and then tap **OK**.

The **Enter Room No.** interface is displayed. See Figure 6-21.

The card issuing password is 002236 by default, and you can change it in **System Config > Local Config > Local Config** in the Web interface. See the details in "7.3.2 A&C Manager."

Figure 6-21 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.

6.4.3.2 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 "7.5.3.1 Setting Master Card."

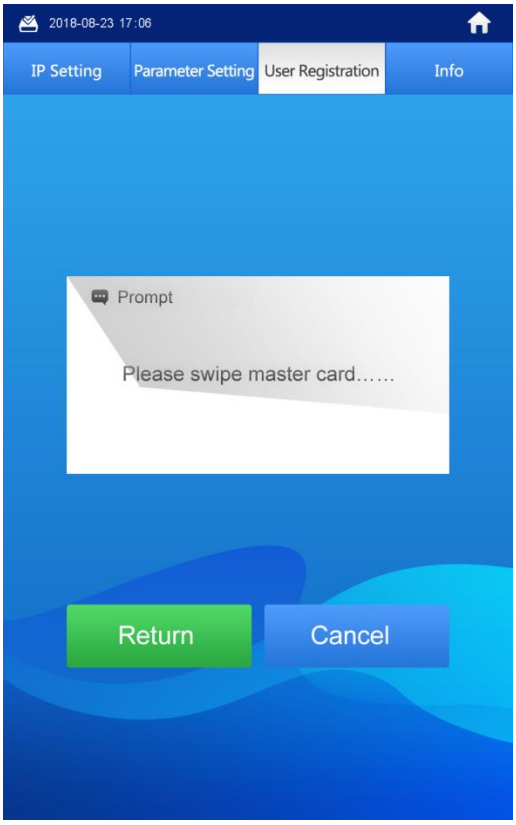
Step 1 In the main interface, enter #VTO password#.

The **IP Setting** interface is displayed.

Step 2 Select **User Registration > Card >Master card**.

The **Swipe master card** notice is displayed. See Figure 6-22.

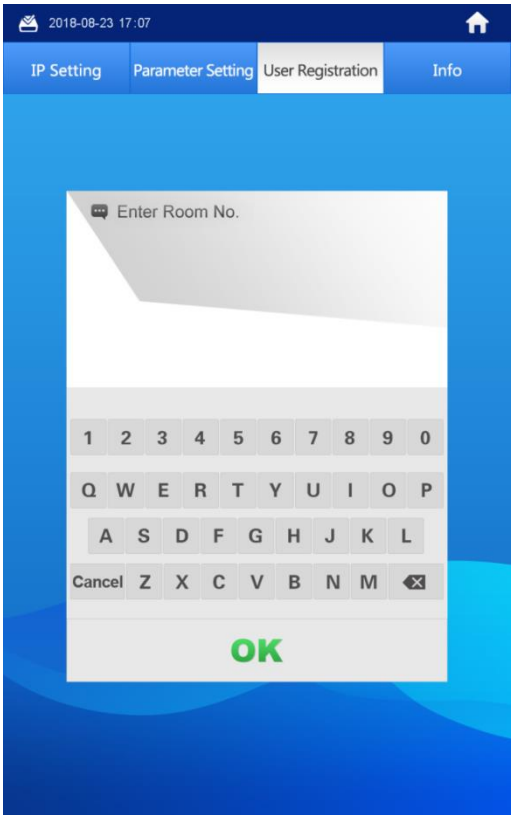
Figure 6-22 Swipe master card.



Step 3 Swipe the master card**.**

The **Enter Room No.** interface is displayed. See Figure 6-23.

Figure 6-23 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 planned for 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.

6.5 Viewing Function

6.5.1 Viewing Face Data

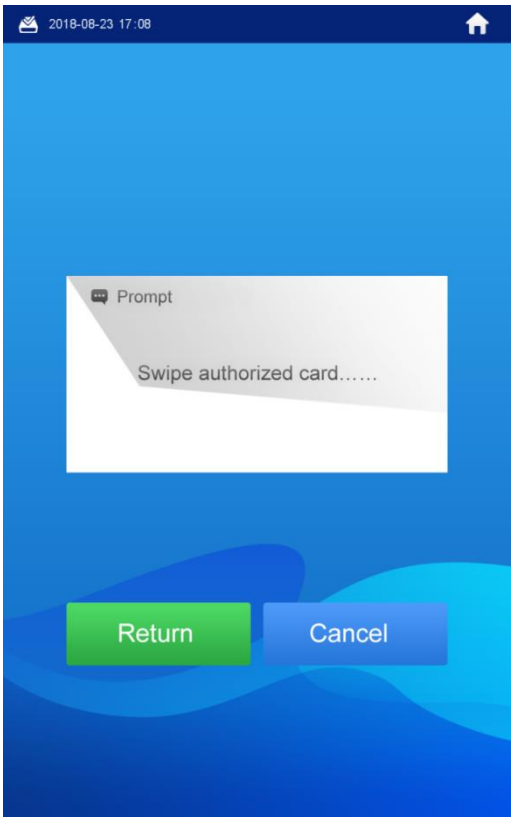
6.5.1.1 Viewing by VTO Users

The VTO users can view and maintain the face data under their room number with the authorized card.

Step 1 In the main interface, tap **Owner Registration**.

The **Swipe authorized card** notice is displayed. See Figure 6-24.

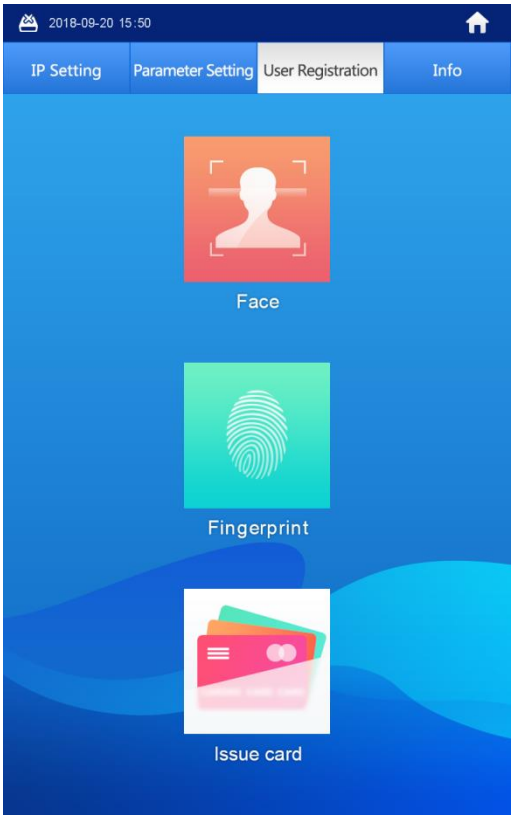
Figure 6-24 Swipe authorized card



Step 2 Swipe the authorized card.

The registration interface is displayed. See Figure 6-25.

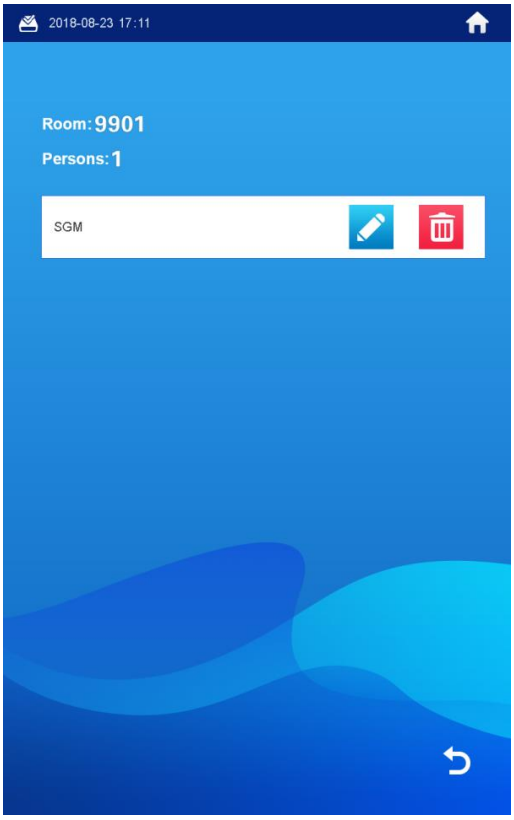
Figure 6-25 Registration



Step 3 Select **Face > Face Query**.

The face data are listed. See Figure 6-26.

Figure 6-26 Face data



- Editing face data

1) Tap  .

The **Do you want to register face again?** notice is displayed. If you need to register face again, tap **Yes**, then face to the scan box, and then add face data as instructed; if you do not need it, tap **No**.

2) Edit room number and name.

If you did not register face again, you can only modify the name.

3) Tap **OK** to finish.

- Deleting face data

1) Tap  .

The Do you want to delete face info? notice is displayed.

2) Tap **Yes**.

- Exiting query interface

Tap  repeatedly to exit.

6.5.1.2 Viewing by Admin People

The admin people or engineer can view and maintain the face data under a certain room number.

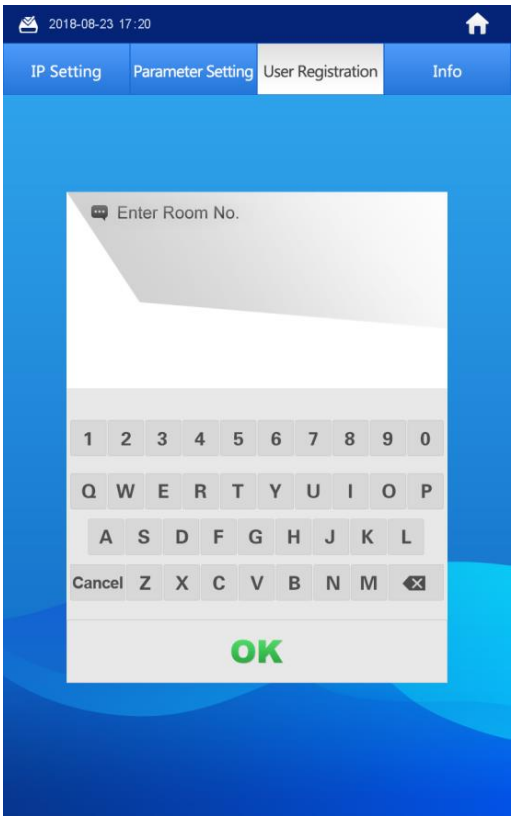
Step 1 In the main interface, enter #VTO password#.

The **IP Setting** interface is displayed.

Step 2 Select **User Registration > Face > Face Query**.

The **Enter Room No.** interface is displayed. See Figure 6-27.

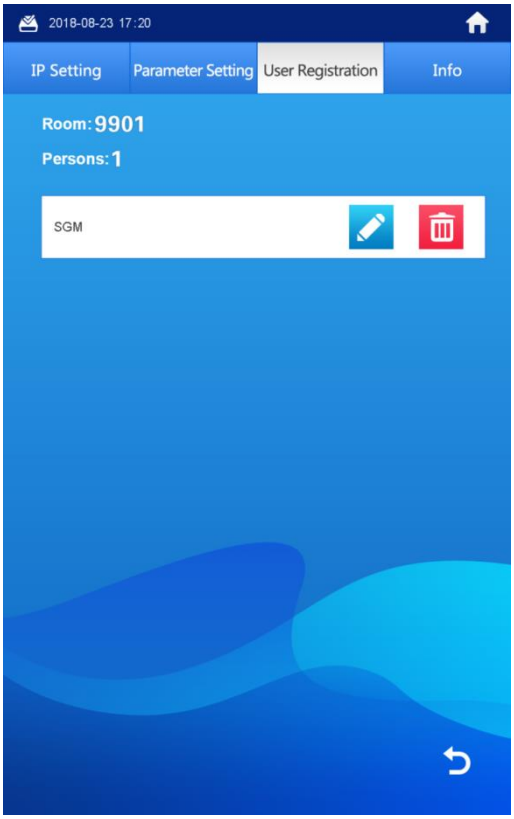
Figure 6-27 Enter room number



Step 3 Enter the room number, and then tap **OK**.

The face data of this room are listed. See Figure 6-28.

Figure 6-28 Face data



- Editing face data

1) Tap  .
   The Do you want to register face again? notice is displayed.
2) Tap **Yes**.
   The face recognition interface is displayed.
3) Face to the scan box, and then add face data as instructed.
   After the registration is finished, the information editing interface is displayed.
4) Edit room number and name.
5) Tap **OK** to finish.

- Deleting face data

6) Tap  .
   The Do you want to delete face info? notice is displayed.
7) Tap **Yes**.

- Exiting query interface

  Tap  repeatedly to exit.

6.5.2 Viewing Fingerprint

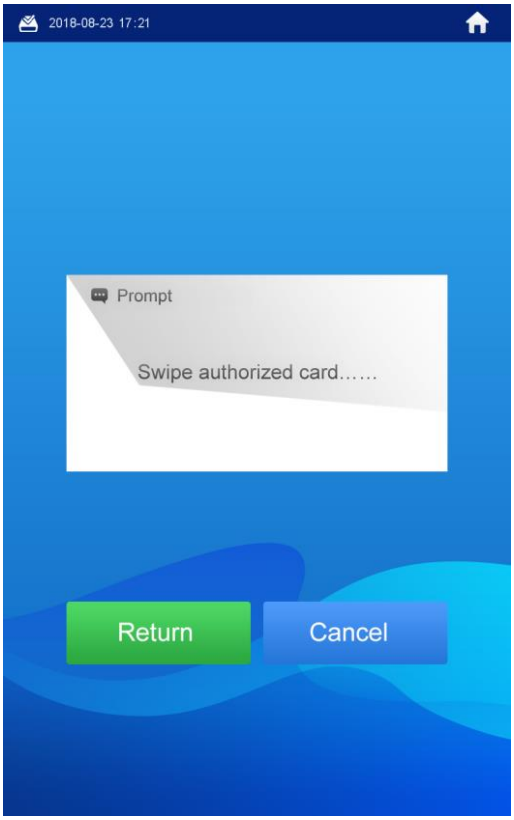
6.5.2.1 Viewing by VTO Users

The VTO users can view and maintain the fingerprint data under their room number with the authorized card.

Step 1 In the main interface, tap **Owner Registration**.

The **Swipe authorized card** notice is displayed. See Figure 6-29.

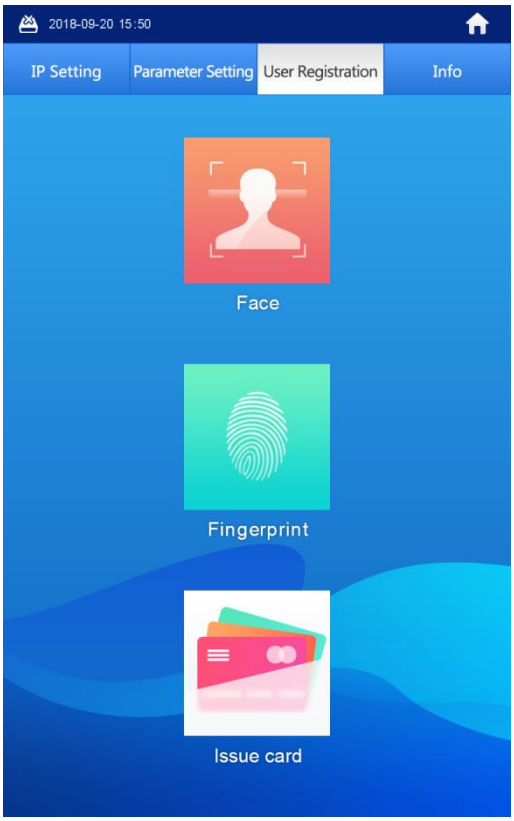
Figure 6-29 Swipe authorized card



Step 2 Swipe the authorized card.

The registration interface is displayed. See Figure 6-30.

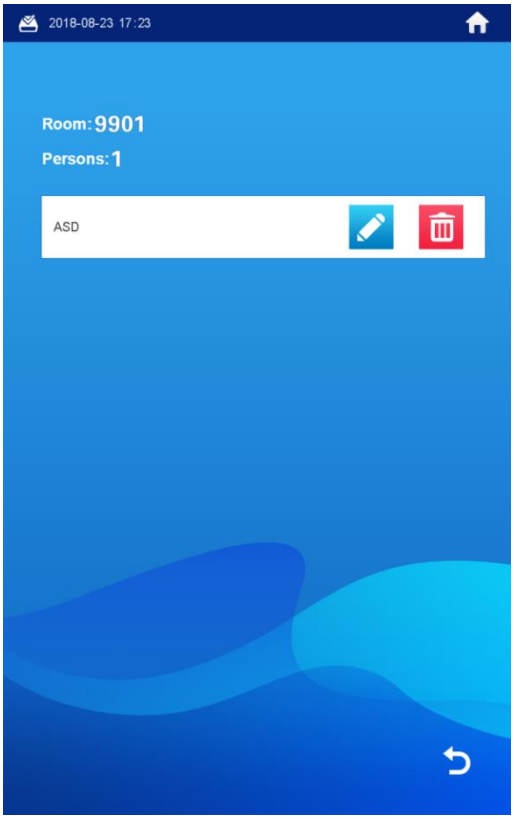
Figure 6-30 Registration



Step 3 Select **Fingerprint > Fingerprint Query**.

The fingerprint data are listed. See Figure 6-31.

Figure 6-31 Fingerprint data



- Editing fingerprint

1) Tap  .
   The information editing interface is displayed.
2) Edit name.
3) Tap **OK** to finish.

- Deleting fingerprint

1) Tap  .
   The Do you want to delete fingerprint info? notice is displayed.
2) Tap **Yes**.

- Exiting query interface

  Tap  repeatedly to exit.

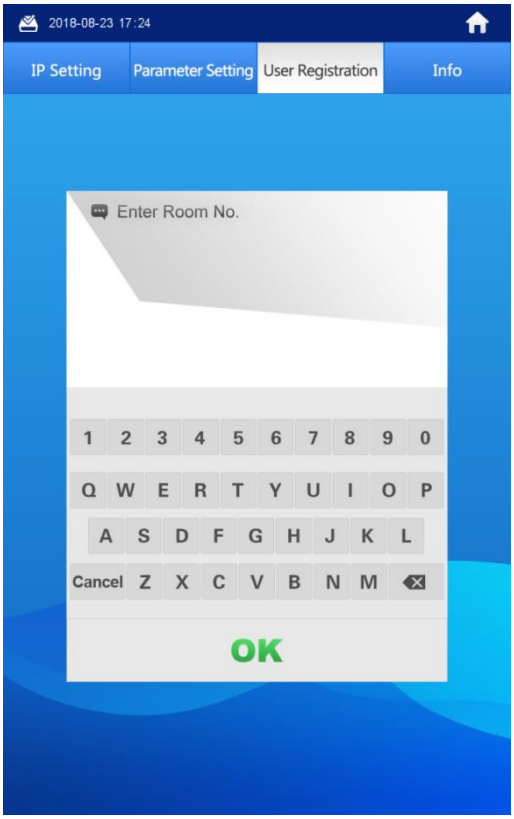
6.5.2.2 Viewing by Admin People

The admin people can view and maintain the fingerprint data under a certain room number.

Step 1 In the main interface, enter #VTO password#.
The **IP Setting** interface is displayed.

Step 2 Select **User Registration > Fingerprint > Fingerprint Query**.
The **Enter Room No.** interface is displayed. See Figure 6-32.

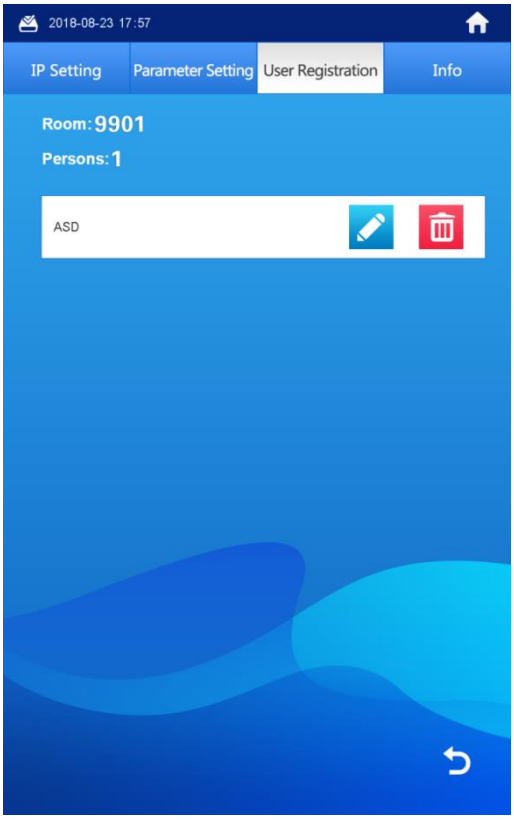
Figure 6-32 Enter room number



Step 3 Enter the room number, and then tap **OK**.

The fingerprint data of this room are listed. See Figure 6-33.

Figure 6-33 Fingerprint data



Step 4 Maintaining fingerprint

- Editing fingerprint

1) Tap  .

The information editing interface is displayed.

2) Edit name.
3) Tap **OK** to finish.

- Deleting fingerprint

1) Tap  .

The Do you want to delete fingerprint info? notice is displayed.

2) Tap **Yes**.

- Exiting query interface

Tap  repeatedly to exit.

6.5.3 Viewing Card Information

You can view the card information on the VTO Web interface or on the server. For the viewing operation on the Web interface, see "7.5.3 Card Info"; for the operation on the server, see the user's manual of the server.

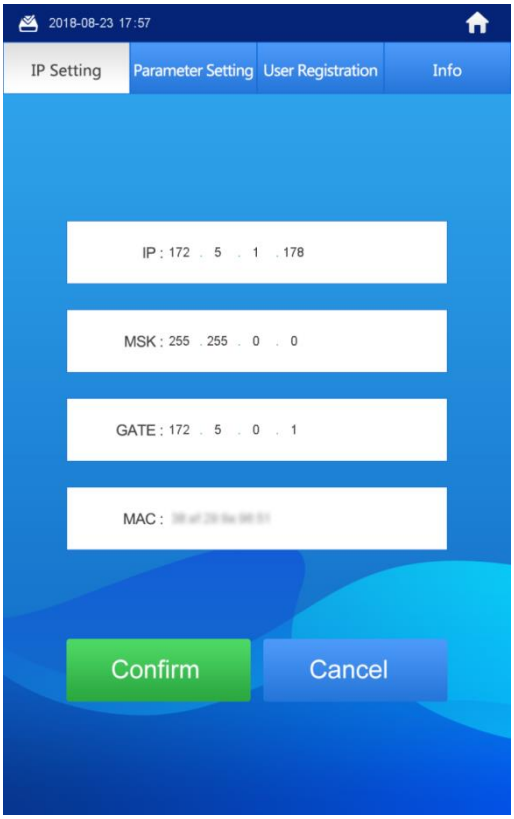
6.6 Configuring VTO Parameter

6.6.1 Engineering Interface

This function is only for admin people or engineer.

In the main interface, enter "#VTO password#", and then the engineering interface is displayed. See Figure 6-34.

Figure 6-34 Engineering interface



The VTO password is 888888 by default, and be sure to change the password in the Web interface after the first use. See the details in "7.3.2 A&C Manager."

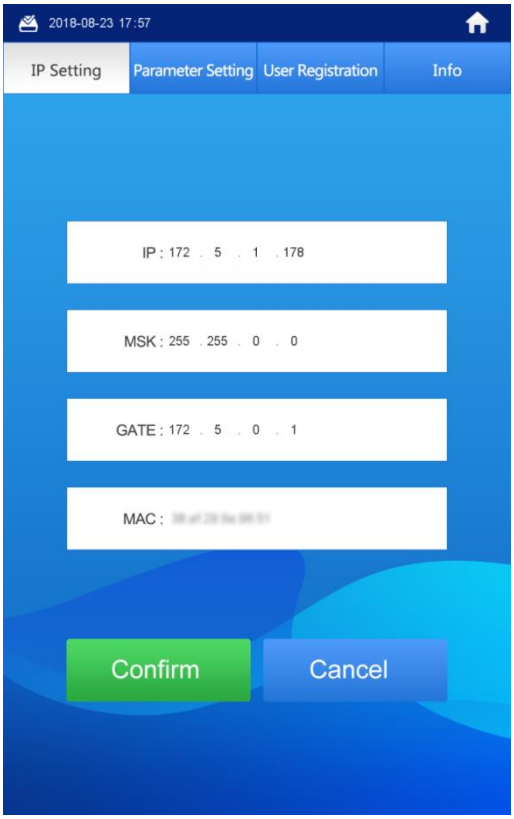
6.6.2 Configuring the IP Address

You can configure the IP address, subnet mask, and default gateway of the VTO.

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

The **IP Setting** interface is displayed. See Figure 6-35.

Figure 6-35 IP setting



Step 2 Tap the input box of **IP**, **MSK**, and **Gate**.
The keyboard is displayed.

Step 3 Tap ← to backspace, and then tap the numbers to input.

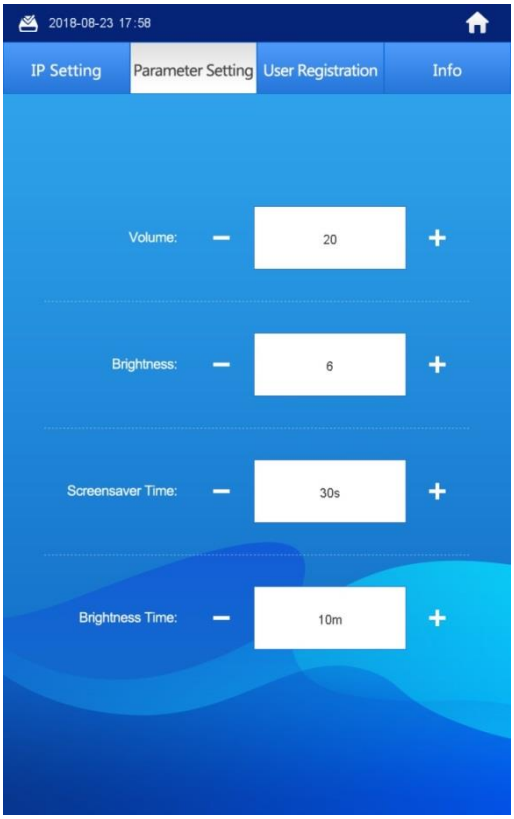
Step 4 Tap **Confirm** to save.
The VTO reboots.

6.6.3 Configuring Volume/Screensaver Time/Brightness

Step 1 In the main interface, enter #VTO password#.
The **IP Setting** interface is displayed.

Step 2 Tap **Parameter Setting**.
The **Parameter Setting** interface is displayed. See Figure 6-36.

Figure 6-36 Parameter setting



Step 3 Tap **+** or **-** to add or reduce the value.

- The volume range is 0–100.
- The brightness range is 1–9.
- The **Screensaver Time** is the time that the VTO idles until the screensaver comes up, and the range is 30 s–300 s.
- The **Brightness Time** includes the **Screensaver Time** and the duration of the screensaver, and when the **Brightness Time** ends, the VTO screen is off. The **Brightness Time** range is 10 m–300 m.

6.7 Info

6.7.1 Viewing Device Information

This can be used by the technical support to do troubleshooting.

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

The **IP Setting** interface is displayed.

Step 2 Tap **Info**.

The **Web Port**, **Main Version**, and **MCU Version** are displayed. See Figure 6-37.

Figure 6-37 Info

6.7.2 Viewing Notices

In the main interface, tap  to view the text notice from the SIP server.

7 Web Interface

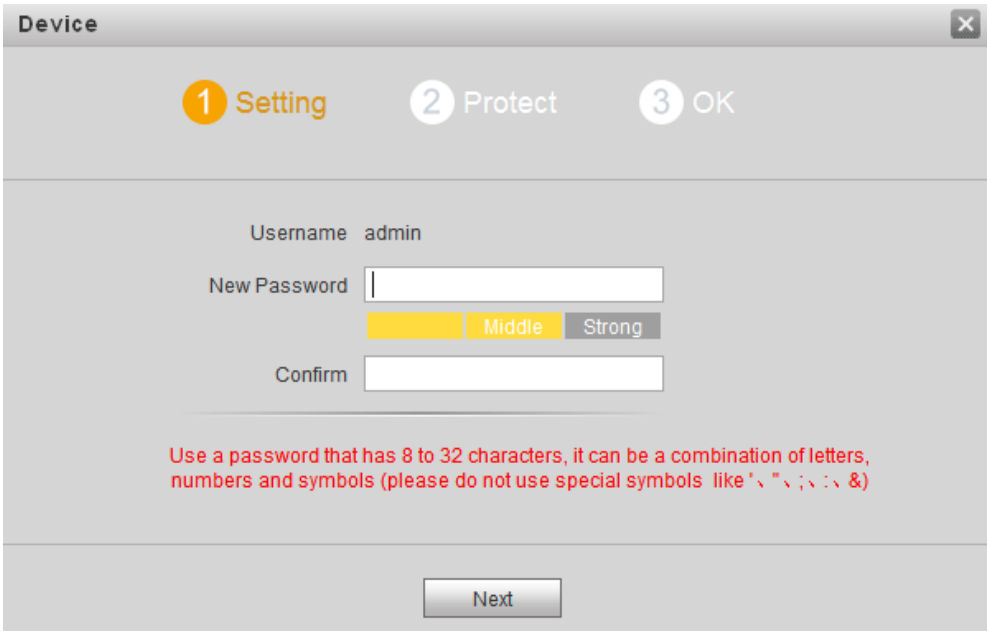
7.1 Initializing VTO

- For first time login or after the VTO being reset, you need to initialize the Web interface.
- Make sure the PC is in the same network segment with the VTO.

Step 1 Enter the default IP address of the VTO in the address bar, and then press Enter.

The password setting interface is displayed. See Figure 7-1.

Figure 7-1 Password setting

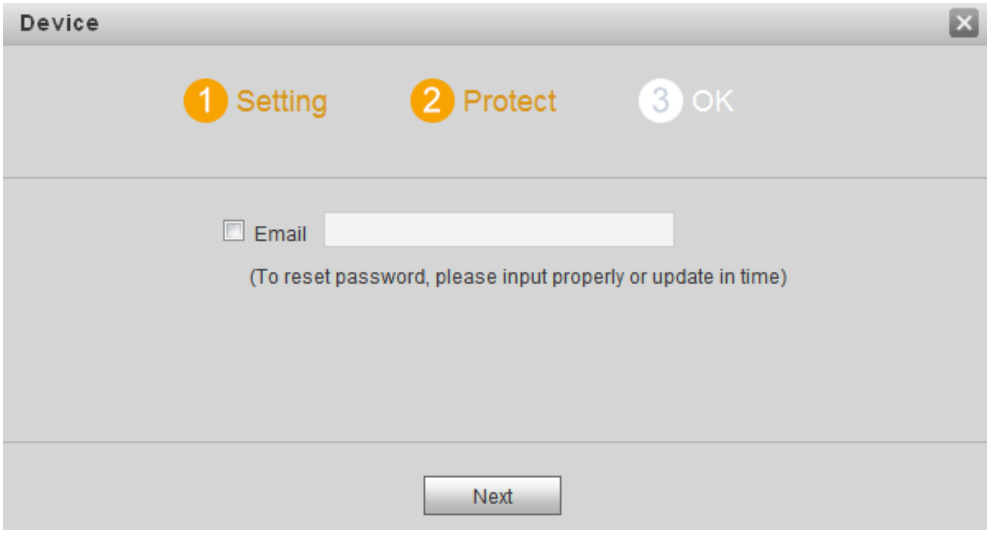


Step 2 Enter and confirm the password, and then click **Next**.

The Email setting interface is displayed. See Figure 7-2.

This password is to login the Web interface, and it should contain at least 8 digits and at least two types from number, letter, and symbol.

Figure 7-2 Email setting



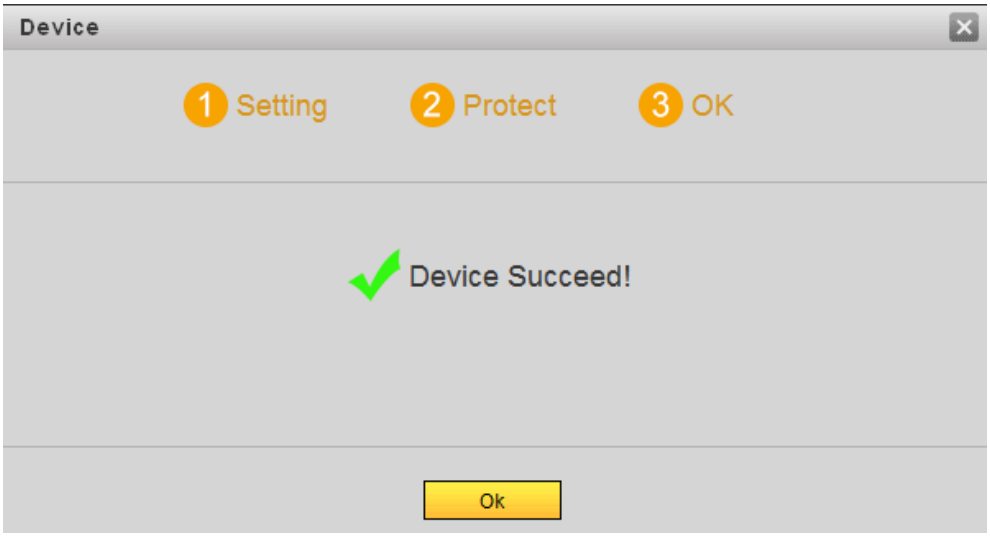
Step 3 Select the **Email** check box, and then enter your Email address.

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

Step 4 Click **Next**.

The **Device Succeed** interface is displayed, and the initialization is finished. See Figure 7-3.

Figure 7-3 Device succeed



Step 5 Click **OK**.

The login interface is displayed.

7.2 Login

Make sure the PC is in the same network segment with the VTO.

Step 1 Enter the default IP address of the VTO in the address bar, and then press enter.

The login interface is displayed. See Figure 7-4.

Figure 7-4 Login

Step 2 Enter the user name and the password, and then click **Login**.

- The default user name is admin.
- The password is what you configured during initialization.

7.3 System Config

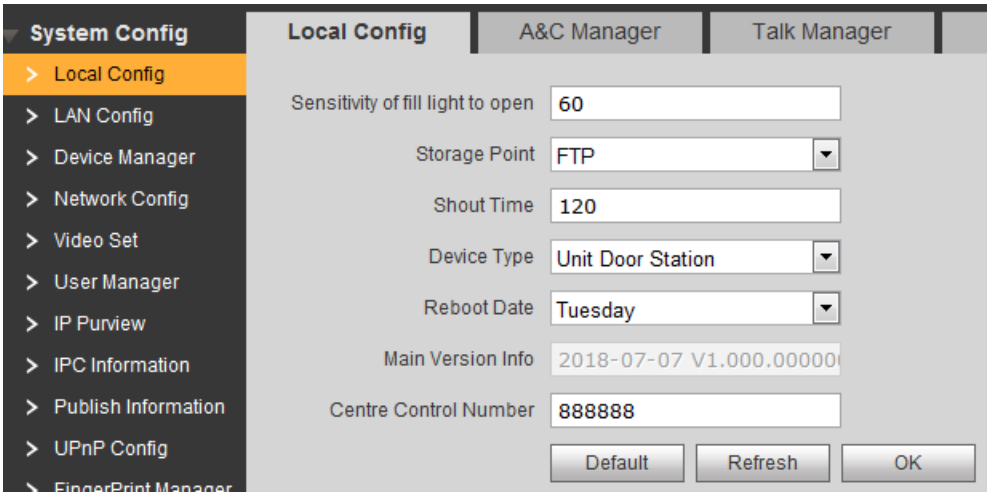
7.3.1 Local Config

This section introduces how to configure fill light sensitivity, storage path, shout time, device type, reboot date, and center control number.

Step 1 Select **System Config > Local Config > Local Config**.

The **Local Config** interface is displayed. See Figure 7-5.

Figure 7-5 Local config



Step 2 Configure parameters, and for the detailed description, see Table 7-1.

Table 7-1 Local config parameter

Parameter	Description
Sensitivity of fill light to open	The bigger the value is, the more sensitive the fill light will be.

Parameter	Description
Storage Point	The storage path for the recorded videos and snapshots. You can select **FTP** or **SD card**. ● For the FTP configuration, see "7.6.2 FTP Config." ● If you select **SD card**, make sure the SD card is inserted or the VTO supports SD card.
Shout Time	The max time for which the management center or the VTH can shout to the VTO.
Device Type	**Unit Door Station** by default.
Reboot Date	Configure the time at which the VTO auto reboots. The time is 2:00, Tuesday by default.
Main Version Info	The version of the VTO system.
Centre Control Number	The number of the management center, and it is 888888 by default.

Step 3 Click **OK** to save.

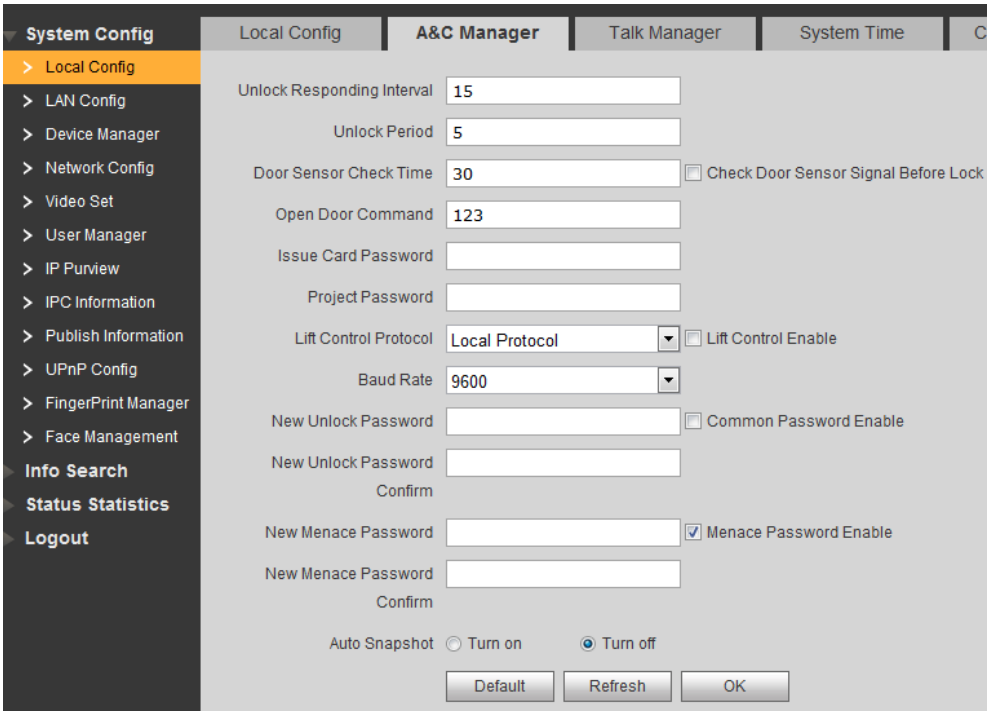
7.3.2 A&C Manager

This section introduces how to configure the lock, including unlock responding interval, open door command, issue card password, and lift control protocol.

Step 1 Select **System Config > Local Config > A&C Manager**.

The **A&C Manager** interface is displayed. See Figure 7-6.

Figure 7-6 A&C manager



Step 2 Configure A&C manager parameters. See Table 7-2 for the details.

Table 7-2 A&C manager parameter

Parameter	Description
Unlock Responding Interval	The time interval to unlock again after the previous unlock, and the unit is second.

Parameter	Description
Unlock Period	The time amount for which the lock stays open after unlock, and the unit is second.
Check Door Sensor Signal Before Lock	Select the **Check Door Sensor Signal Before Lock** check box to enable alarm function, and If the unlock time exceeds the **Door Sensor Check Time**, the door sensor alarm is triggered, and the alarm will be sent to the management center.
Door Sensor Check Time	
Open Door Command	You can connect a third-party phone such as SIP phone to your VTO, and use the command to open the door remotely.
Issue Card Password	This password can be used to issue new card. ● This password is only for admin people or engineer. ● It is 002236 by default.
Project Password	It can be used to go to the engineering interface, and it is 888888 by default. Project password is only for admin people or engineers.
Lift Control Protocol	Select **Lift Control Protocol** and **Lift Control Enable** to enable the lift control function, and then you can configure the floors that lift users can go to.
Lift Control Enable	
Baud Rate	Enter the baud rate of the third party 485 device that you need.
New Unlock Password	Select **Common Password Enable**, then configure unlock password, and then all the residents in this unit can open the door with this password.
New Unlock Password Confirm	
Common Password Enable	
New Menace Password	Select **Menace Password Enable** to configure duress password function. Once the duress password is used, the alarm is triggered, and it will be sent to the management center.
New Menace Password Confirm	
Menace Password Enable	
Auto Snapshot	Select **Turn on**, and then the system takes 2 snapshots when unlocking, and then upload to the FTP.

Step 3 Click **OK** to save.

7.3.3 Talk Manager

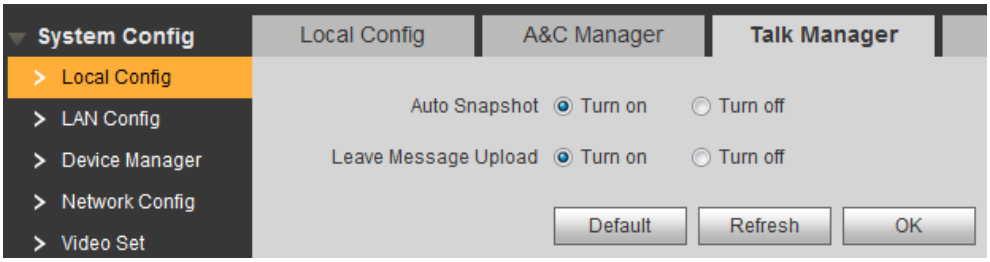
Upload the snapshots and the video and audio messages to the FTP. Make sure the FTP is properly configured.

This section introduces how to configure auto snapshot and how to leave messages during phone call.

Step 1 Select **System Config > Local Config > Talk Manager**.

The **Talk Manager** interface is displayed. See Figure 7-7.

Figure 7-7 Talk manager



Step 2 Configure Talk manager parameters. See Table 7-3 for the details.

Table 7-3 Talk manager parameter

Parameter	Description
Auto Snapshot	Select **Turn on**, and then the system takes 2 snapshots when calling, and 1 snapshot after the call is answered. The snapshots will be upload to the FTP.
Leave Message Upload	⚠ • If the SD card is not available or supported, you can enable this function and configure FTP to make it work. • If the SD card is available, the messages will be saved in the SD card by default, and this option is invalid. Select **Enable,** and then the meaasges from visitors will be uploaded to the FTP server. If the call from the VTO to the VTH is not answered, the "No one answers" voice notice comes up. Tap 1 to leave a video or audio message. The message will be upload to the FTP, and the VTO users can view the messages on the **VTH**.

Step 3 Click **OK** to save.

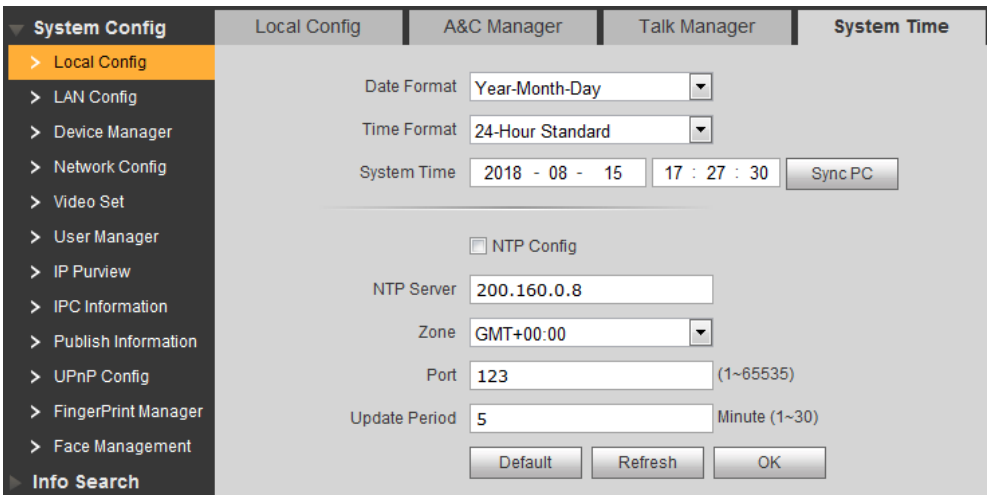
7.3.4 System Time

This section introduces how to configure the date format, time format, and the NTP server.

Step 1 Select **System Config > Local Config > System Time**.

The **System Time** interface is displayed. See Figure 7-8.

Figure 7-8 System time



Step 2 Configure System time parameters. See Table 7-4 for the details.

Table 7-4 System time parameter

Parameter	Description
Date format	You can select from **Year-Month-Day**, **Month-Day-Year**, and **Day-Month-Year**.
Time format	Configure the time format, and you can select from **12-Hour** or **24-Hour**.
System Time	Configure the VTO system date, time and time zone, and then click **OK**. Do not change the system time arbitrarily; it might cause problems on video searching and publishing snapshot or notice. Before changing the system time, turn off video recording or auto snapshot.
Sync PC	Click to sync the VTO system time and the PC system time.
NTP Config	Select the check box to enable NTP timing.
NTP Server	Enter the domain name and the IP address of the NTP server.
Zone	The time zone of the current area.
Port	The port number of the NTP server.
Update Period	The time interval that the VTO syncs time with the NTP server, and it is 30 min at most.

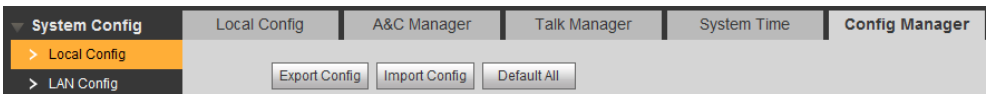
Step 3 Click **OK** to save.

7.3.5 Config Manager

This section introduces how to import or export the system config, network config, and video config, and how to reset the VTO.

Select **System Config > Local Config > Config Manager**, and then the **Config Manager** interface is displayed. See Figure 7-9.

Figure 7-9 Config manager



- Export Config
  Click **Export Config** to export the system config, network config, and video config to local storage, and the exported config can be used to restore config or import into other VTO.
- Import Config
  Click **Import Config** to import the local config files into the VTO; you can restore or sync data with this function.
- Default All
  Click **Default All**, and then confirm. The VTO will reboot, and all the parameters except IP address will be reset to the factory settings.

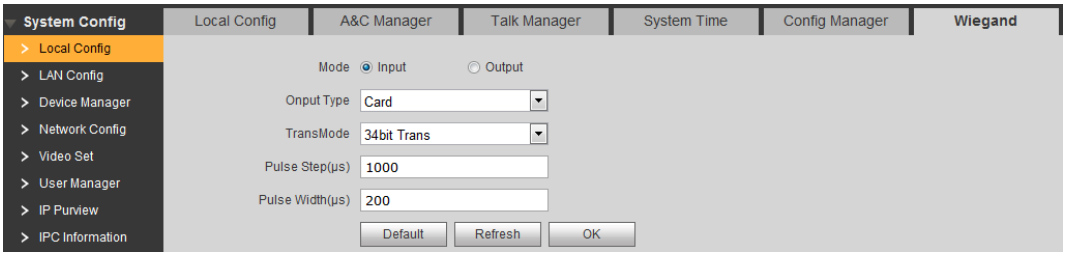
7.3.6 Wiegand

You can configure the parameters of Wiegand sensors.

Step 1 Select **System Config > Local Config > Wiegand**

The **Wiegand** interface is displayed. See Figure 7-10.

Figure 7-10 Wiegand



Step 2 Configure Wiegand parameters. See Table 7-5 for the details.

Table 7-5 Wiegand parameter

Parameter	Description
Mode	Supports single Wiegand input or output.
Output Type	ID or Card
TransMode	Select transmitting speed from **26 bit**, **34 bit**, and **64 bit**. The bigger the value is, the faster the transmission will be.
Pulse Step (μs)	It is 1000 by default.
Pulse Width (μs)	It is 200 by default.

Step 3 Click **OK** to save.

7.4 LAN Config

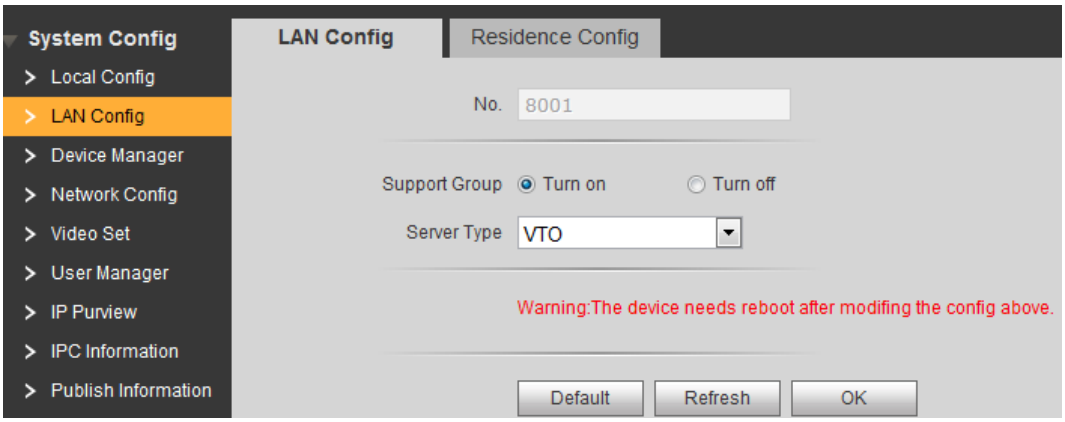
7.4.1 LAN Config

This section introduces how to configure server type and group call.

Step 1 Select **System Config > LAN Config > LAN Config**.

The **LAN Config** interface is displayed. See Figure 7-11.

Figure 7-11 LAN config



Step 2 Configure parameters. See Table 7-6 for the details.

Table 7-6 LAN config parameter

Parameter	Description
No.	The number of the VTO. If the VTO you are visiting works as SIP server, the **No.** is not editable. For the configuration of SIP server, see "7.6.3 SIP Server Config."
Support Group	Select **Turn on** to enable group call, and when the VTO is calling a VTH, all the extension VTH would receive the call. After turning on or off the group call, the configuration takes effect after the VTO reboots.
Server Type	Select the SIP server type. ● If VTO works as SIP server, select **VTO**. ● If third party server works as SIP server, select the type you need.

Step 3 Click **OK** to save.

7.4.2 Residence Config

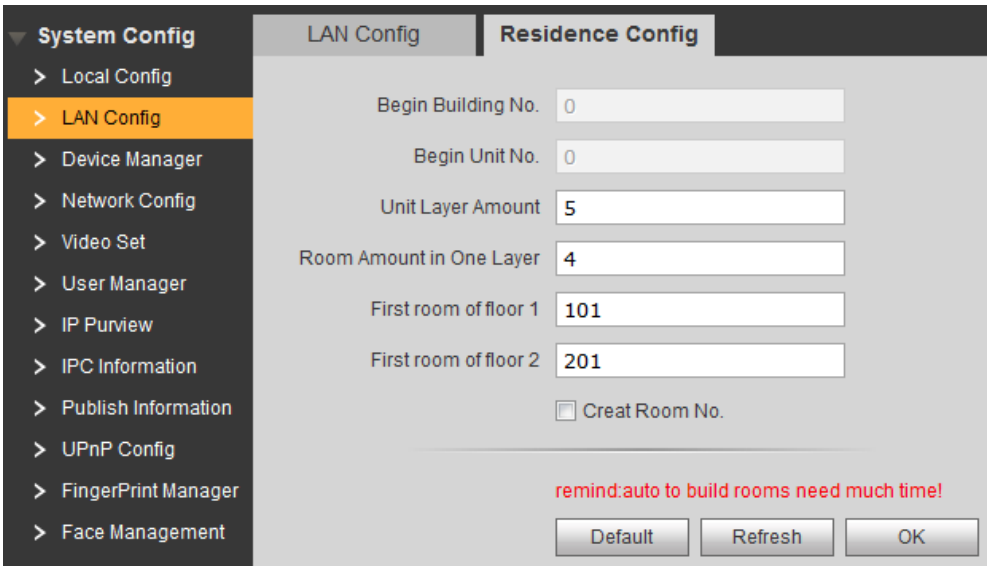
This section introduces how to configure the beginning building and unit number, unit layer amount, and room amount in one layer.

This function is valid only when VTO works as SIP server.

Step 1 Select **System Config > LAN Config > Residence Config**.

The **Residence Config** interface is displayed. See Figure 7-12.

Figure 7-12 Residence config



Step 2 Configure parameters. See Table 7-7 for the details.

Table 7-7 Residence config parameter

Parameter	Description
Begin Building No.	Configure the first building number.
Begin Unit No.	Configure the first unit number.
Unit Layer Amount	Configure the layer amount in one unit.
Room Amount in One Layer	Configure the room amount in one layer.
First room of floor 1	Configure the first room number in floor 1 for starter.
First room of floor 2	Configure the first room number in floor 2 for starter.
Creat Room No.	Select **Creat Room No.**, and then the VTO can create numbers in batch with the input information.

Step 3 Click **OK** to save.

7.5 Device Manager

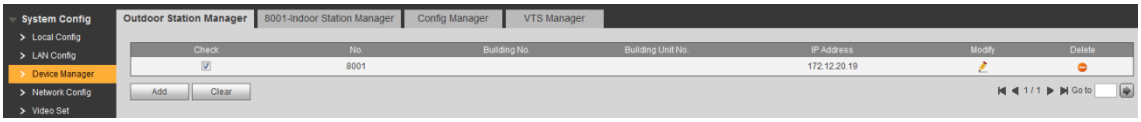
This function is displayed only when the VTO you are visiting works as SIP server.

7.5.1 Outdoor Station Manager

This section introduces how to manage other VTO devices in the network.

Select **System Config > Device Manager > Outdoor Station Manager**, and then the **Outdoor Station Manager** interface is displayed. See Figure 7-13.

Figure 7-13 Outdoor station manager

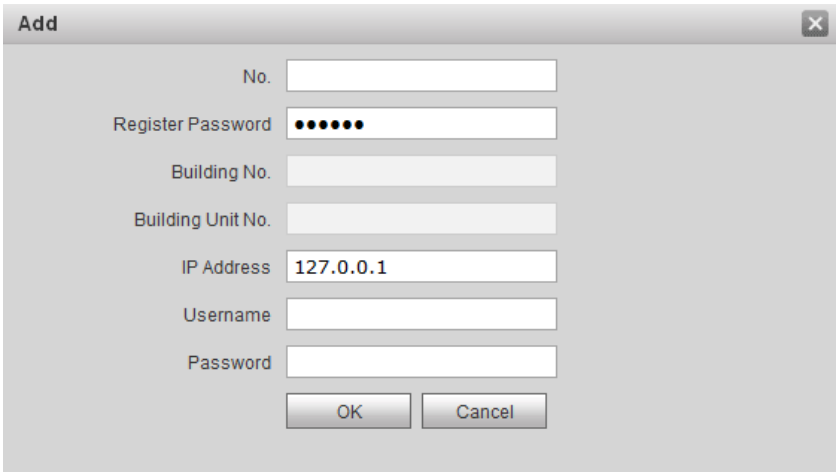


7.5.1.1 Adding VTO

Step 1 Click **Add**.

The **Add** interface is displayed. See Figure 7-14.

Figure 7-14 Add VTO



Step 2 Configure VTO parameters. See Table 7-8 for the details.

Table 7-8 VTO parameters

Parameter	Description
No.	The number of the VTO.
Register Password	Leave to the default.
Building No.	Configure the number of the building that the VTO is being installed. This option is editable only when third party server works as SIP server and the **Support Building** is enabled.
Building Unit No.	Configure the number of the building unit that the VTO is being installed. This option is editable only when third party server works as SIP server and the **Support Unit** is enabled.
IP Address	The IP address of the VTO
Username	The username and password for the Web interface of the VTO.
Password	

Step 3 Click **OK** to finish configuration.

The VTO information is listed.

7.5.1.2 Modifying VTO

The VTO that is currently at use cannot be modified or deleted.

Step 1 Click  .

The **Modify** interface is displayed.

Step 2 Modify the register password, username, and password of the VTO. See Table 7-8.

Step 3 Click **OK** to finish.

7.5.1.3 Deleting VTO

The VTO that is currently at use cannot be modified or deleted.

Click to delete VTO one by one; click **Clear** to delete all the VTO.

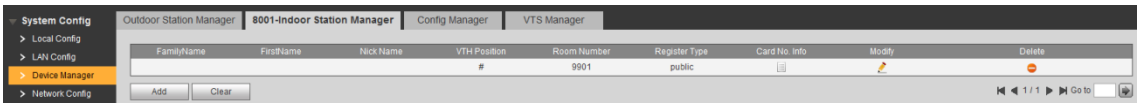
7.5.2 8001-Indoor Station Manager

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

This section introduces how to manage other VTO devices and the access cards in the network.

Select **System Config > Device Manager > 8001-Indoor Station Manager**, and then the **8001-Indoor Station Manager** interface is displayed. See Figure 7-15.

Figure 7-15 8001-indoor station manager

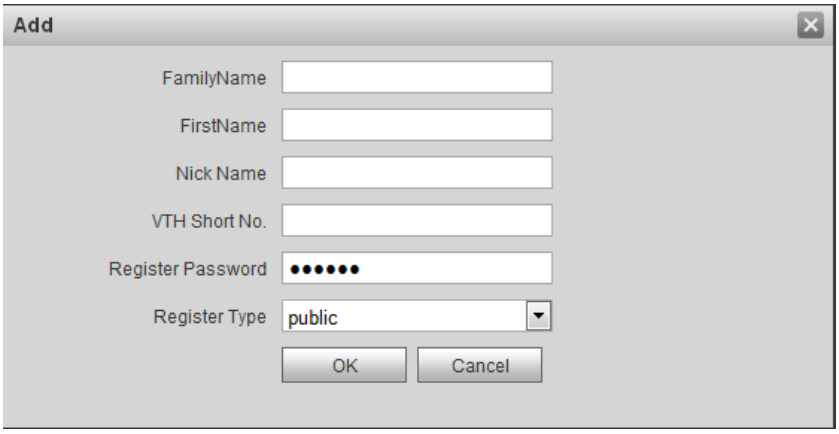


7.5.2.1 Adding VTH

Step 1 Click **Add**.

The **Add** interface is displayed. See Figure 7-16.

Figure 7-16 Add VTH



Step 2 Configure VTH parameters. See Table 7-9 for the details.

Table 7-9 VTH parameters

Parameter	Description
FamilyName	Configure the name and nickname of the VTH user, in order to differentiate.
FirstName	
Nick Name	
VTH Short No.	Configure the room number of the VTH. ● The VTH short number should be the same as the room

Parameter	Description
	number you configured on the VTH. ● 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, #3 and so on.
Register Password	Leave to the default.
Register Type	

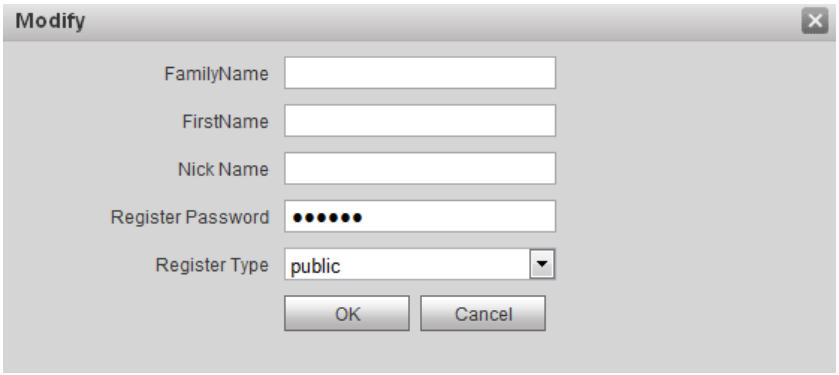
Step 3 Click **OK** to finish configuration.

7.5.2.2 Modifying VTH

Step 1 Click  .

The **Modify** interface is displayed. See Figure 7-17.

Figure 7-17 Modifying VTH



Step 2 Modify all the parameters of the VTH. See Table 7-9.

Step 3 Click **OK** to finish.

7.5.2.3 Deleting VTH

Click  to delete VTH one by one; click **Clear** to delete all the VTH.

7.5.3 Card Info

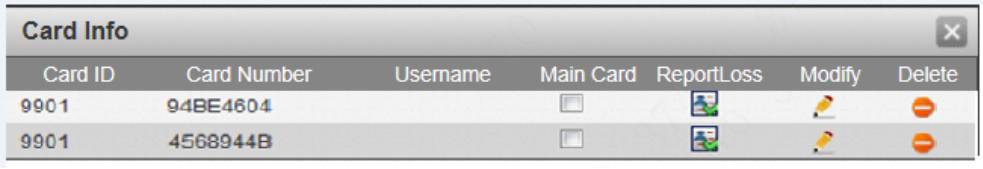
This section introduces how to define master card, report loss, cancel report, and modify card user.

Before using this function, make sure the VTO already has authorized card, otherwise, there will be no card. For the card registration, see "6.4.3 Issuing Card."

Select **System Config > Device Manager > 8001-Indoor Station Manager**, and then click  ,

The **Card Info** interface is displayed. See Figure 7-18.

Figure 7-18 Card info



7.5.3.1 Setting Master Card

Select the **Main Card** check box of a certain card, and then the card is configured as the master card. The master card can be used to authorize other cards.

7.5.3.2 Report Loss

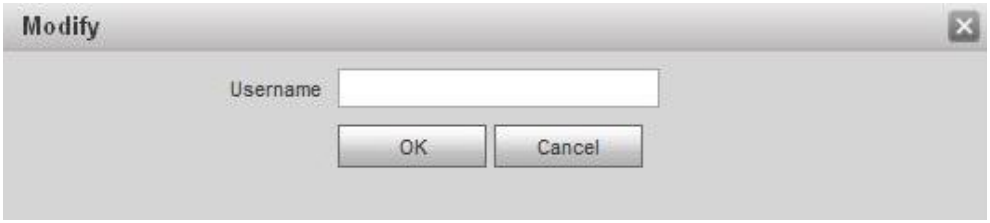
Click  to report loss for a certain card. The icon changes to  , and the card is not valid any more. Click  to cancel the report, and the card is valid again.

7.5.3.3 Modifying Card

Step 1 Click  .

The **Modify** interface is displayed. See Figure 7-19.

Figure 7-19 Modifying card username



Step 2 Modify the card username

Step 3 Click **OK**.

7.5.3.4 Deleting Card

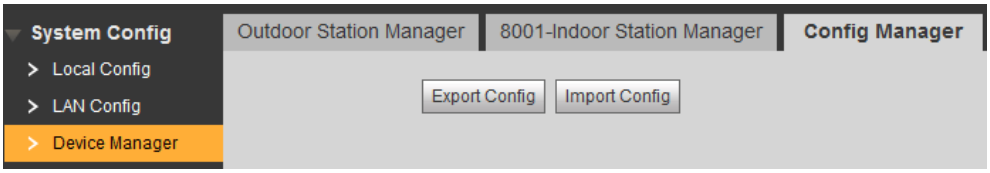
Click  to delete a certain card, and the card is not valid any more.

7.5.4 Config Manager

This section introduces how to import or export the device information, password, access cards, and login information in **Device Manager**.

Select **System Config > Device Manager > Config Manager**, and then the **Config Manager** interface is displayed. See Figure 7-20.

Figure 7-20 Config manager



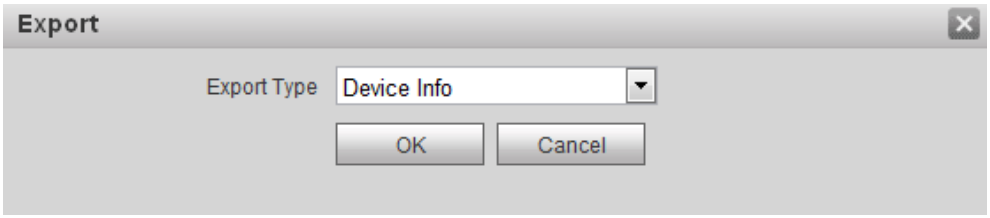
Export Config

Click **Export Config** to export the config files to local storage, and the exported config can be used to restore config or import into other VTO.

Step 1 Click Export Config.

The **Export** interface is displayed. See Figure 7-21.

Figure 7-21 Export config



Step 2 Select the **Type** you need, and then click **OK**.

Step 3 Enter the password, and then click **OK**.

Step 4 The PC downloads the file automatically.

Import Config

Import the local config files into a VTO to apply the config.

Step 1 Click **Import Config**.

The **File Upload** interface is displayed.

Step 2 Click **File**, then select the .log file you need, and then click **Upload**.

7.6 Network Config

This section introduces how to configure IP address, FTP, SIP server, DDNS, and UPnP.

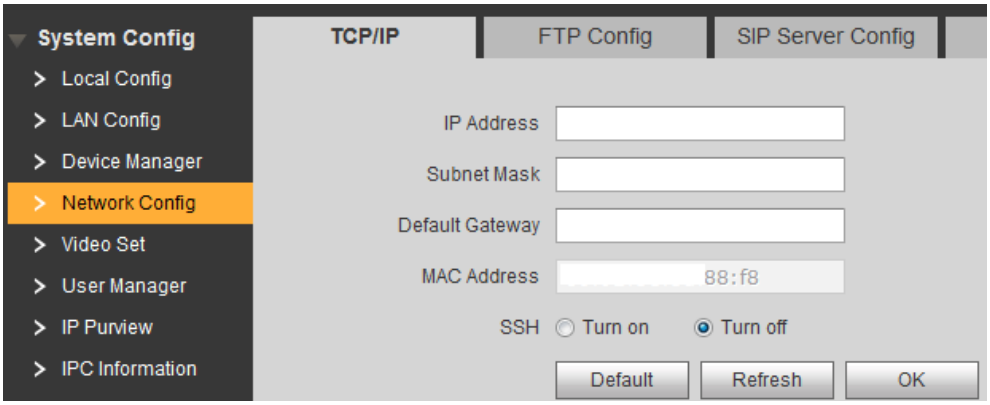
7.6.1 TCP/IP

This section introduces how to configure the IP address of the VTO.

Step 1 Select **System Config > Network Config > TCP/IP**.

The **TCP/IP** interface is displayed. See Figure 7-22.

Figure 7-22 TCP/IP



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

Step 3 You can enable SSH as needed.

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

Step 4 Click **OK** to save.

7.6.2 FTP Config

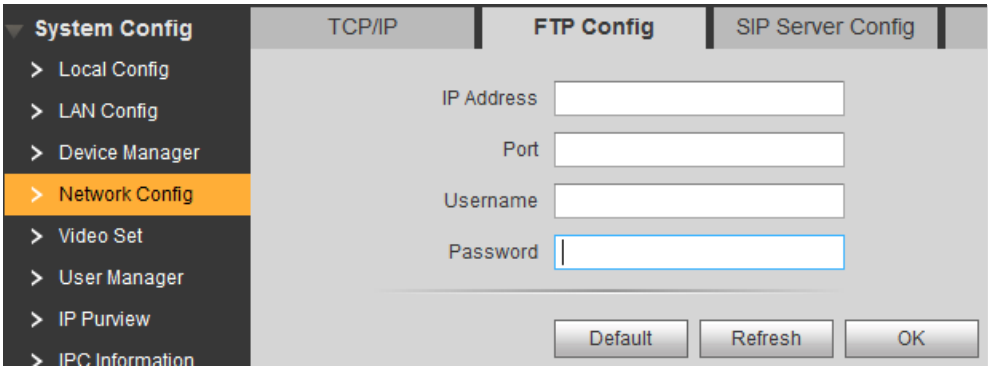
Configure FTP server, and then you can save the recorded videos and snapshots to the FTP server.

You need to plan the FTP server in advance.

Step 1 Select **System Config > Network Config > FTP Config**.

The **FTP Config** interface is displayed. See Figure 7-23.

Figure 7-23 FTP Config



Step 2 Configure parameters. See Table 7-10 for the details.

Table 7-10 FTP config parameter description

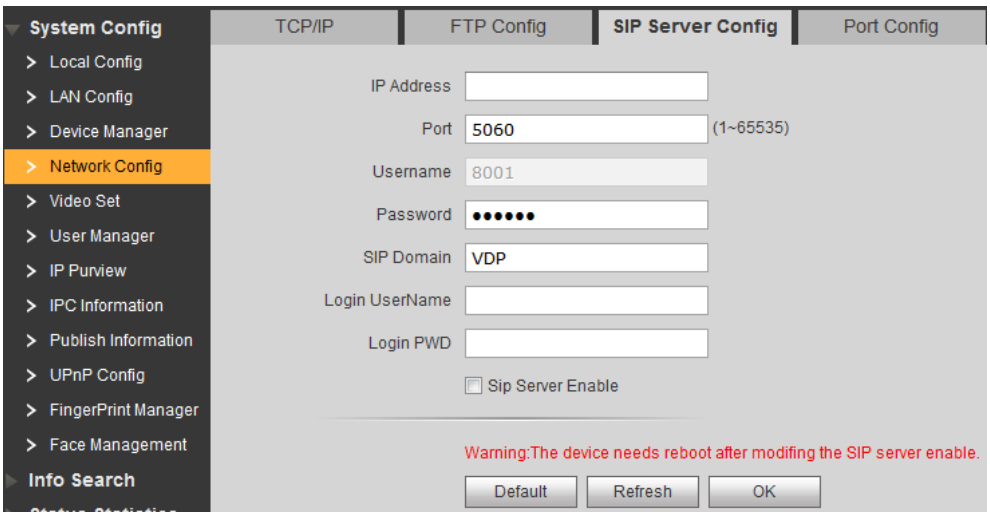
Parameter	Description
IP Address	The IP address of the FTP server.
Port	It is 21 by default.
Username	The username and password of the FTP server.
Password	

Step 3 Click **OK** to save.

7.6.3 SIP Server Config

Select **System Config > Network Config > SIP Server Config**, and then the **SIP Server Config** interface is displayed. See Figure 7-24.

Figure 7-24 SIP server configuration



- 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.
- If other VTO works as SIP server

Step 1 Configure parameters. See Table 7-11 for the details.

Table 7-11 SIP server config (1)

Parameter	Description
IP Address	The IP address of the VTO that works as SIP server.
Port	It is 5060 by default.
Username	Leave to the default.
Password	
SIP Domain	The **SIP Domain** is **VDP**.
Username	The username and password of the SIP server.
Password	

Step 2 Click **OK** to save.

The VTO reboots, and then the login interface is displayed.

- If third party server works as SIP server

Step 1 Configure parameters. See Table 7-12 for the details.

Table 7-12 SIP server config (2)

Parameter	Description
IP Address	The IP address of the server that works as SIP server.
Port	5080
Username	Leave to the default.
Password	
SIP Domain	Leave it blank or keep the default..
Username	The username and password of the SIP server.

Parameter	Description
Password	

Step 2 Click **OK** to save.

The VTO reboots, and then the login interface is displayed.

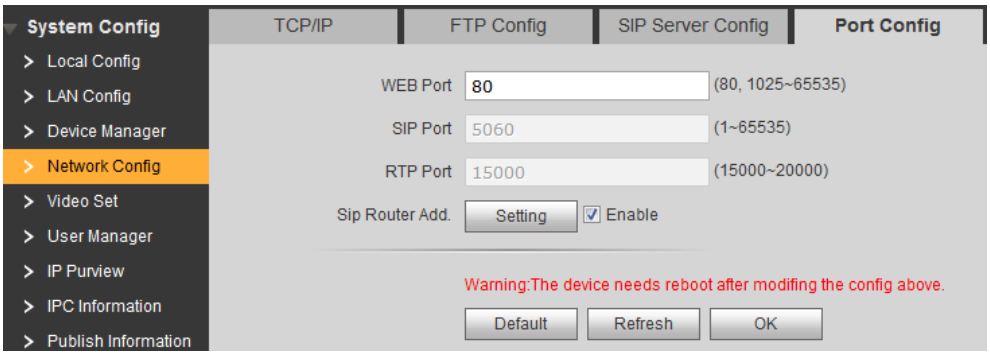
7.6.4 Port Config

Configure the port that is used to login the VTO Web interface.

Step 1 Select **System Config > Network Config > Port Config**.

The **Port Config** interface is displayed. See Figure 7-25.

Figure 7-25 Port Config



Step 2 Web Port

It is 80 by default, if it is occupied, you can use numbers from 1025 to 65535.

Step 3 Click **OK** to save.

If the port is changed, enter "http://VTO IP address: web port" in the address bar of the Internet browser to login the Web interface of the corresponding VTO.

7.6.5 DDNS Config

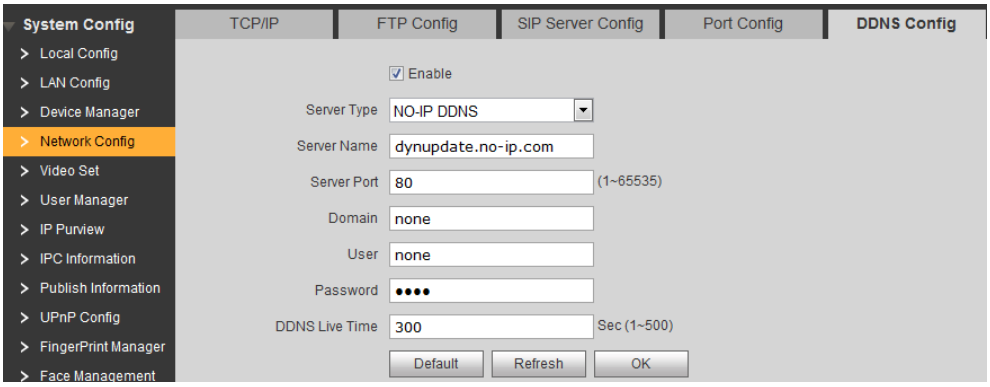
Properly configure DDNS, and then you can always visit your VTO with a constant domain name no matter how much your VTO IP address changes.

- Before start, check whether your VTO supports the servers in **Server Type**, and then go to the DDNS website and register the username, password, and domain name.
- Finish register, then log in the DDNS website, and then you can view all the connected devices in your account.

Step 1 Select **System Config > Network Config > DDNS Config**.

The **DDNS Config** interface is displayed. See Figure 7-26.

Figure 7-26 DDNS Config



Step 2 Select **Enable** to enable DDNS.

Step 3 Configure parameters. See Table 7-13 for the details.

Table 7-13 DDNS parameter description

Parameter	Description
Server Type	The name and web address of the DDNS service provider, see the matching relationship below: ● The web address of **Dyndns DDNS**: members.dyndns.org. ● The web address of **NO-IP DDNS**: dynupdate.no-ip.com.
Server Name	
Server Port	The port number of the DDNS server.
Domain	The domain name you registered on the DDNS website.
User	Enter the user name and password you got from the DDNS service provide. You need to register an account (with user name and password) on the DDNS service provides' website.
Password	
DDNS Live Time	The time interval that the VTO syncs IP address with the DDNS server. To avoid too much burden on the network, it is recommended that this value be configured around 300.

Step 4 Click **OK** to save.

Open the browser, then enter the domain name you registered on the DDNS website at the address bar, and then press Enter, if the login interface is displayed, configure succeeded; if not, check it again.

7.7 Video Set

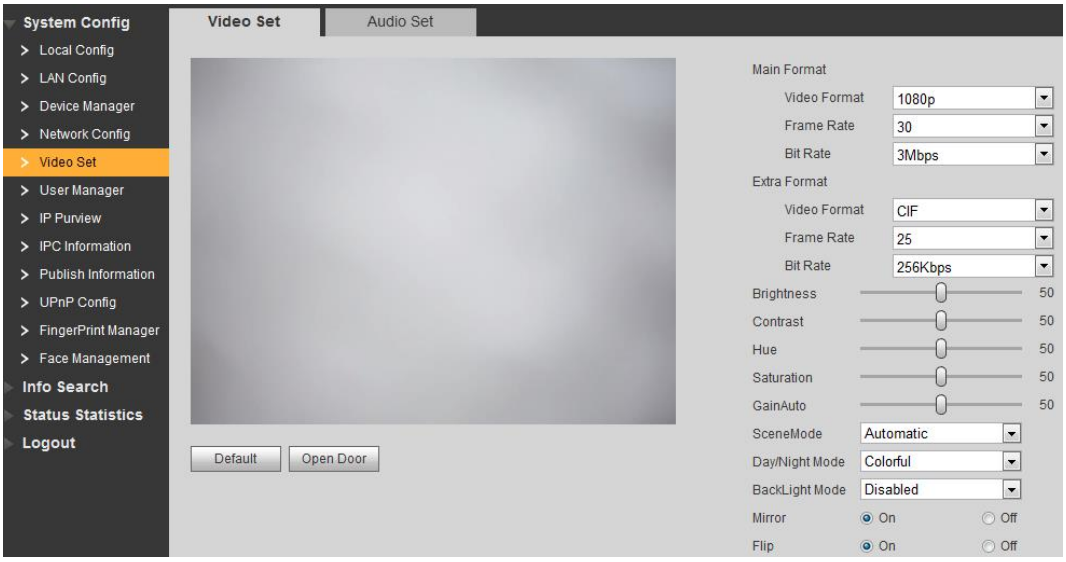
This section introduces how to configure the size of the video and audio that the VTO recorded.

7.7.1 Video Set

Step 1 Select **System Config > Video Set > Video Set**.

The **Video Set** interface is displayed. See Figure 7-27. Click **Open Door**, and then the door opens.

Figure 7-27 Video set



Step 2 Configure video parameters. See Table 7-14 for the details.

Table 7-14 Video parameter description

Parameter		Description
Main Format	Video Format	Select the video resolution from **1080P**, **720P**, **WVGA**, and **D1**.
	Frame Rate	Configure the number of frames in 1 second. You can select from **3**, **23**, and **30**. The larger the value is, the smoother the video will be.
	Bit Rate	Configure the data amount that transmitted in 1 second. You can select from **256Kbps**, **1Mbps**, **2Mbps**, and **3Mbps**. The larger the value is, the better the video quality will be.
Extra Format	Video Format	Select the video resolution from **CIF**, **WVGA**, **QVGA**, and **D1**.
	Frame Rate	Configure the number of frames in 1 second. You can select from **3**, **23**, and **30**. The larger the value is, the smoother the video will be.
	Bit Rate	Configure the data amount that transmitted in 1 second. You can select from **256Kbps**, **1Mbps**, **2Mbps**, and **3Mbps**. The larger the value is, the better the video quality will be.
Brightness		Changes the value to adjust the picture brightness. The bigger the value is, the brighter the picture will be, and the smaller the darker. The picture might be hazy if the value is configured too big.
Contrast		Changes the contrast of the picture. The bigger the value is, the more the contrast will be between bright and dark areas, and the smaller the less. If the value is set too big, the dark area would be too dark and bright area easier to get overexposed. The picture might be hazy if the value is set too small.
Hue		Makes the color deeper or lighter. The default value is made by the light sensor, and it is recommended.
Saturation		Makes the color deeper or lighter. The bigger the value is, the deeper the color will be, and the lower the lighter. Saturation value doesn't change image brightness.

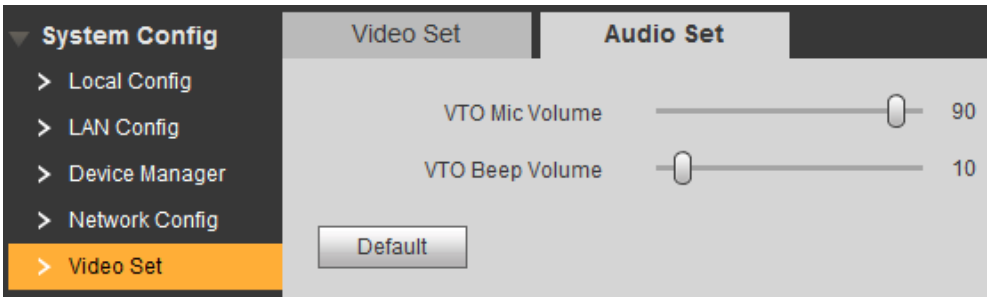
GainAuto	Amplify the video signal to increase image brightness. If the value is too big, there will be more noise in the image.
SceneMode	Adjust the video to adapt to different scenarios. You can select from **Automatic**, **Sunny**, **Night** and **Disabled**. It is **Automatic** by default.
Day/Night Mode	You can select from **Automatic**, **Colorful** or **Black White** mode.
BackLight Mode	You can select from the following modes: ● **Disabled**: no back light. ● **BackLight**: the camera gets clearer image of the dark areas on the target when shooting against light. ● **Wide dynamic**: the system dims bright areas and compensates dark areas to ensure the clarity of all the area. ● **Inhibition**: the system constrains bright areas and reduces halo size to dim the overall brightness.
Mirror	Select **On**, and then the image would display with left and right side reversed.
Flip	Select **On**, and then the image would be displayed upside down.

7.7.2 Audio Set

Select **System Config > Video Set > Audio Set**, and then the **Audio Set** interface is displayed. See Figure 7-28. You can adjust the volume of the MIC and the speaker on the VTO.

Click **Default**, and then the volume of the MIC and the speaker are restored to default configuration.

Figure 7-28 Audio Set

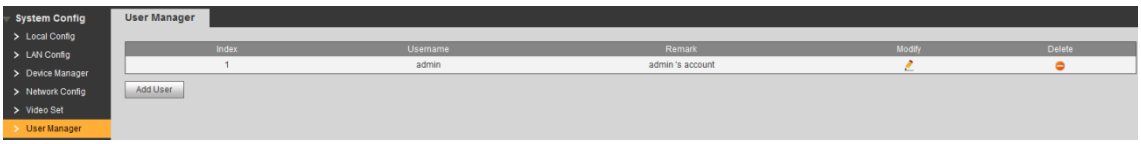


7.8 User Manager

You can add, delete, or modify Web user information.

Select **System Config > User Manager > User Manager**, and then the **User Manager** interface is displayed. See Figure 7-29.

Figure 7-29 User Manager



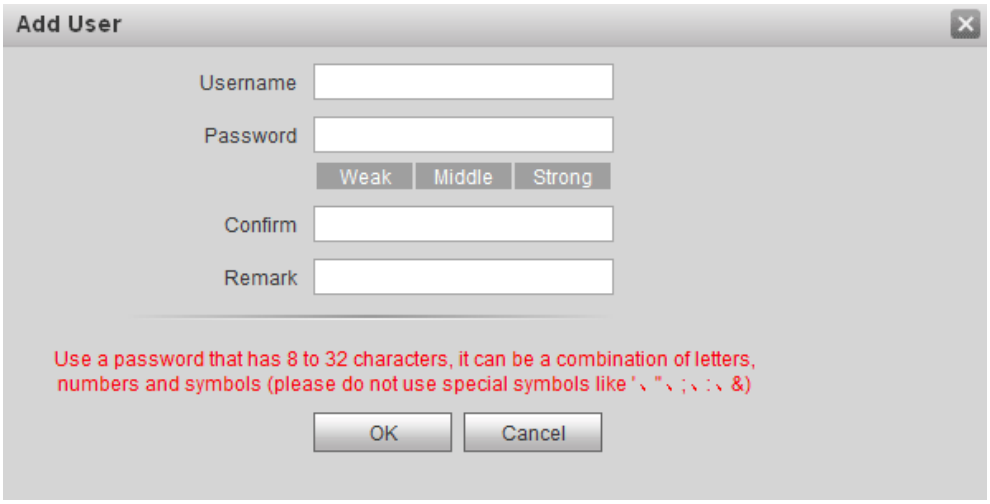
7.8.1 Add User

You can add users with all the authorities except adding user and admin user management.

Step 1 Click Add User.

The **Add User** interface is displayed. See Figure 7-30.

Figure 7-30 Add user



Step 2 Enter username, password, then confirm password, and then enter user description in the **Remark** input box.

This password is should contain at least 8 digits, and at least two types from number, letter, and symbol.

Step 3 Click **OK** to finish configuration.

7.8.2 Modifying User

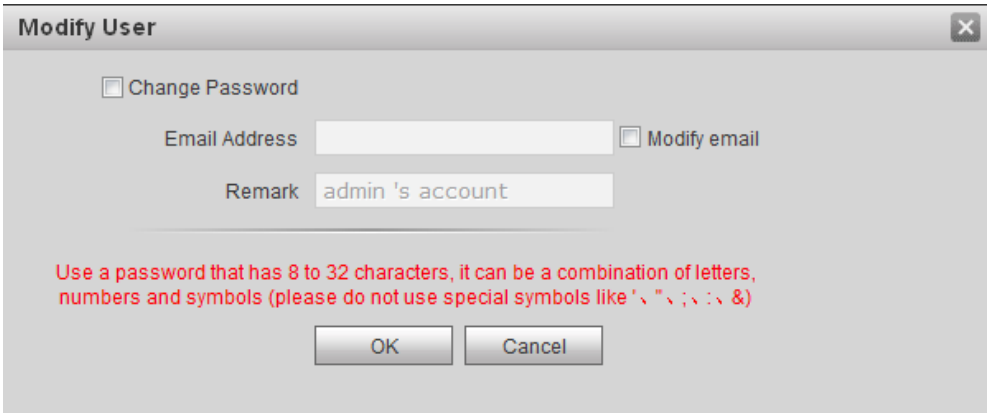
7.8.2.1 Modify Admin User

The admin user can modify his own password and email address. The email address is for password reset purpose.

Step 1 Click  in the admin user information bar.

The **Modify User** interface is displayed. See Figure 7-31.

Figure 7-31 Modify user (1)

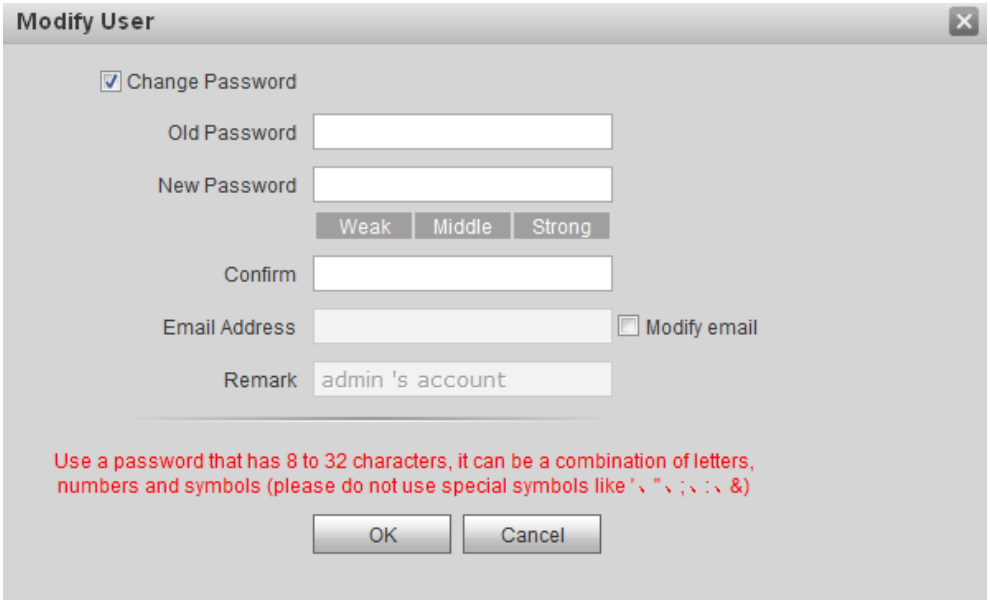


Step 2 Modifying user information

3) Select Change Password.

The password changing options are displayed. See Figure 7-32.

Figure 7-32 Modify user (2)



4) Enter old password, new password, and then confirm password.
5) Select the **Modify email** check box to change your Email address.
6) Click **OK**.

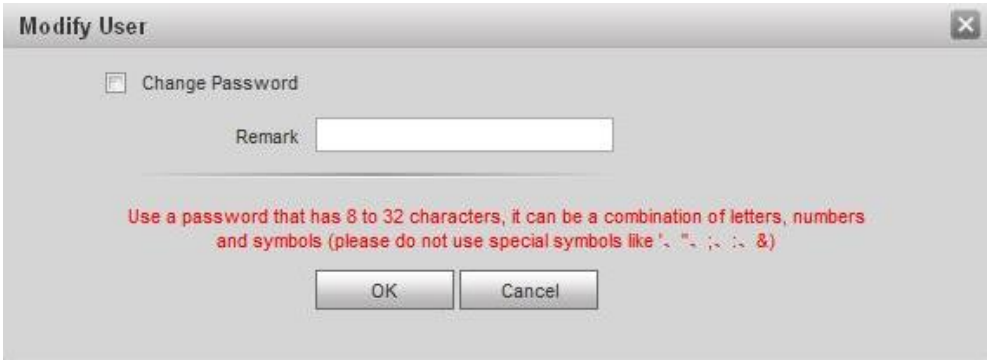
7.8.2.2 Modifying Normal User

Normal user includes all the users except the admin user. Admin user can modify all the uses' information and password, while normal users can only modify their own. This Manual takes admin user as example.

Step 1 Click  in the normal user information bar.

The **Modify User** interface is displayed. See Figure 7-33.

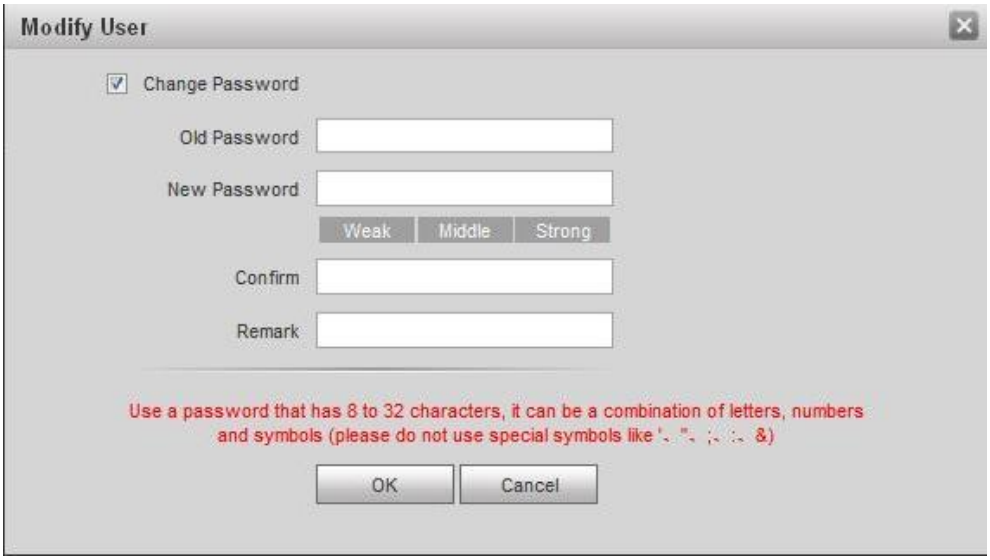
Figure 7-33 Modify user (1)



Step 2 Modifying user information. See Figure 7-34.

1) Select Change Password.
   The password changing options are displayed. See Figure 7-34.

Figure 7-34 Modify user (2)



2) Enter old password, new password, and then confirm password.
3) Modify the description.
4) Click **OK**.

7.8.3 Deleting User

Click in the user information bar to delete a certain user.

7.9 IP Purview

To enhance network and data security, you need to configure access authority.

- White list: only the IP addresses in the list can login the VTO.
- Black list: all the IP addresses in the list are prohibited from login the VTO.

If the **IP Purview** is enabled and there is IP address added to the white list, then only the added IP addresses can login the VTO.

Step 1 Select System Config > IP Purview.

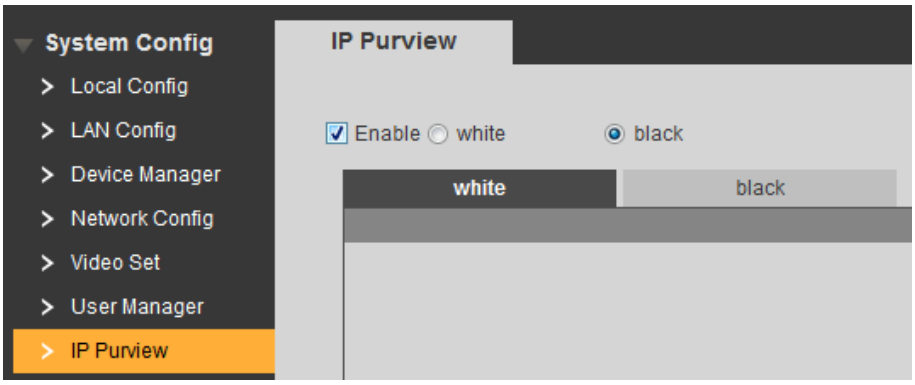
The **IP Purview** interface is displayed. See Figure 7-35.

Figure 7-35 IP Purview

Step 2 Select **Enable**.

The **white** option and **black** option are displayed. See Figure 7-36.

Figure 7-36 White option and black option

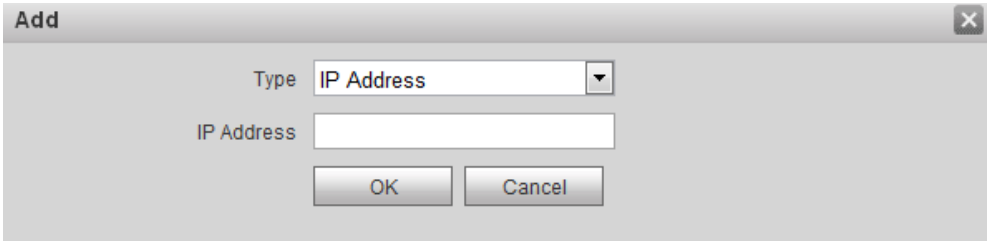


5) Select **white** or **black**.

6) Click **Add**.

The **Add** interface is displayed. See Figure 7-37.

Figure 7-37 Add IP address



7) Configure IP address. See Table 7-15 for the details.

The system supports 64 IP addresses at most.

Table 7-15 IP address parameter description

Type	Description
IP Address	Enter the IPv4 IP address, such as 192.168.1.120.
IP Range	Enter the start IP address and end IP address of the target IP segment.

8) Click **OK**.

The **IP Purview** interface is displayed.

Step 3 Click **OK** to finish configuration.

You can log in the VTO Web interface with the IP addresses in the white list. Logging in the VTO Web interface with the IP addresses in the black list will fail.

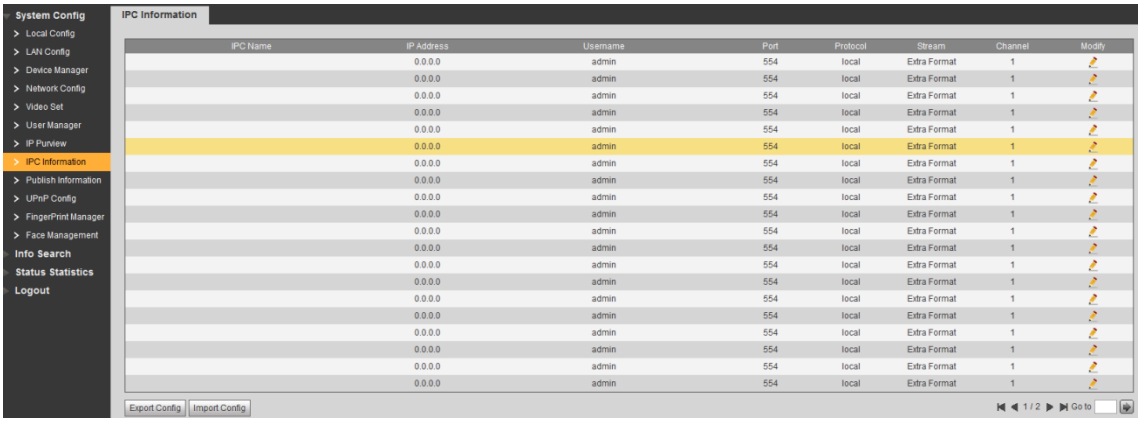
7.10 IPC Information

This function is displayed only when the VTO you are visiting works as SIP server.

You can add 32 channels of IPC to the VTO, and you can view the IPC images from the VTH.

Select **System Config > IPC Information > IPC Information**, and then the **IPC Information** interface is displayed, see Figure 7-38.

Figure 7-38 IPC information

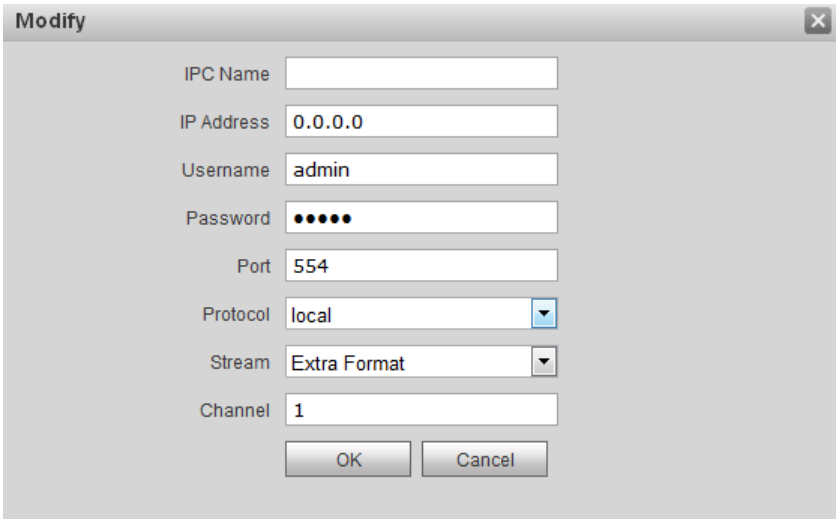


7.10.2 Adding single IPC

Step 1 Click  .

The **Modify** interface is displayed. See Figure 7-39.

Figure 7-39 Modify



Step 2 Configure IPC parameters. See Table 7-16 for the details.

Table 7-16 IPC parameter description

Parameter	Description
IPC Name	The name of the IPC/NVR/XVR/HCVR.
IP Address	The IP address of the IPC/NVR/XVR/HCVR.
Username	The username and password for the Web interface of the IPC/NVR/XVR/HCVR.
Password	
Port	It is 554 by default.
Protocol	Select from **Local** and **Onvif**, you can select according to the device you want to connect to the VTO..
Stream	Select **Main Format** or **Extra Format** as needed. ● **Main Format**: It has large bit rate value and image with high resolution, but also requires large bandwidth. ● **Extra Format**: It has small bit rate value and smooth image, and requires little bandwidth. This option is normally used to replace main stream when bandwidth is not enough.
Channel	● It you connect IPC to the VTO, the value is 1 by default. ● It you connect NVR/XVR/HCVR to the VTO, configure the value to the channel number of the IPC on the NVR/XVR/HCVR.

Step 3 Click **OK** to finish configuration.

7.10.3 Import Config

You can import IPC Information from local storage to the VTO.

Step 1 Click **Import Config**, and then the **File Upload** interface is displayed.

Step 2 Click **File**, then select the .csv file you need,.

Step 3 Click **Upload**.

Step 4 Enter the password for the Web interface, and then click **OK**.

7.10.4 Export Config

You can export the IPC information from the VTO to the local storage for future use.

Click **Import Config**.

Enter the password for the Web interface.

7.11 Publish Information

This function is displayed only when the VTO you are visiting works as SIP server.

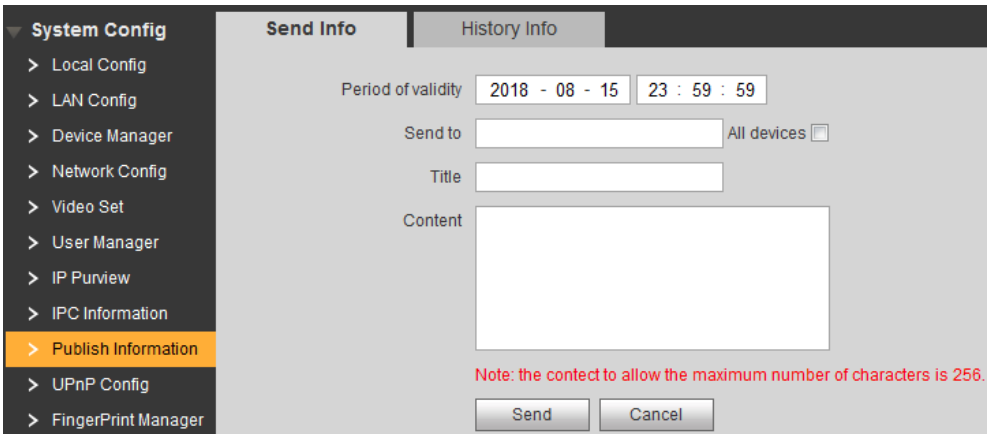
If the VTO you are visiting works as SIP server, you can publish information to the VTH users, and you can view the publish history in **System Config > Publish Information > History Info**.

7.11.1 Send Info

Step 1 Select **System Config > Publish Information > Send Info**.

The **Send Info** interface is displayed. See Figure 7-40.

Figure 7-40 Send Info



Step 2 Configure send info parameters. See Table 7-17 for the details.

Table 7-17 Send info parameter description

Parameter	Description
Period of validity	Send the information before the **Period of validity**, otherwise, the VTH users can not receive the information. All the sent information would display in the **History Info** whether the VTH users received them or not.
Send to	The information receiver. ● If you need to send to single user, input his room number. ● If you need to send to all the users, select the **All devices** check box.
All devices	
Title	The title of the information.
Content	256 character's at most.

Step 3 Click **Send**.

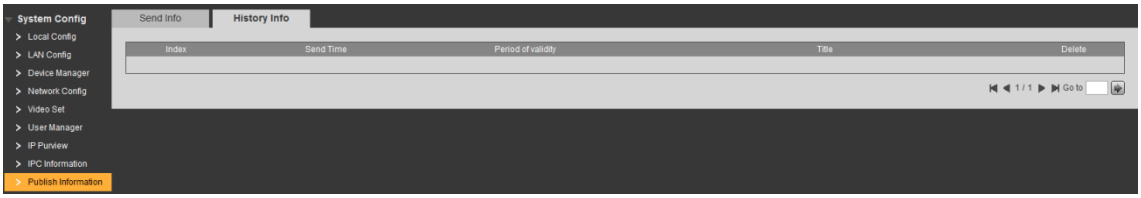
The information is sent to the VTH users.

7.11.2 History Info

Select **System Config > Publish Information > History Info**, and then the **History Info** interface is displayed, see Figure 7-41.

Click  to delete publish history.

Figure 7-41 History Info



7.12 UPnP Config

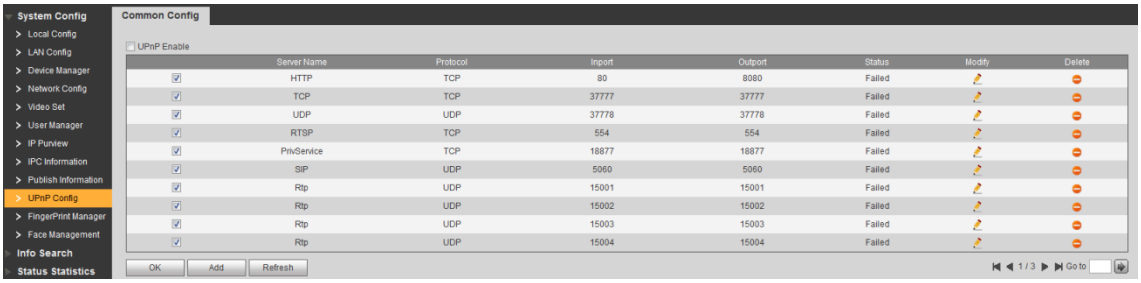
Universal Plug and Play, a protocol that establishes mapping relation between local area and wide area networks. This function enables you to visit local area device through wide area IP address.

This function is valid only when VTO works as SIP server.

- This function is needed only when the VTO is connected to a router.
- Enable the UPnP function of the router, and then configure the IP address of the WAN port to set up Internet connection.
- Connect your device to the LAN port of the router.

Select **System Config > UPnP Config**, and then the **Common Config** interface is displayed. See Figure 7-42.

Figure 7-42 Common Config



7.12.2 Enabling UPnP

There have been some mapping relations done in the factory; you can enable to use them.

Step 1 Select **UPnP Enable** to enable UPnP function.

Step 2 Select the service you need to map.

Step 3 Click **OK** to save.

Open the web browser on PC and enter "http:// wide area IP address: external port number", and then you can visit the local area device with corresponding port.

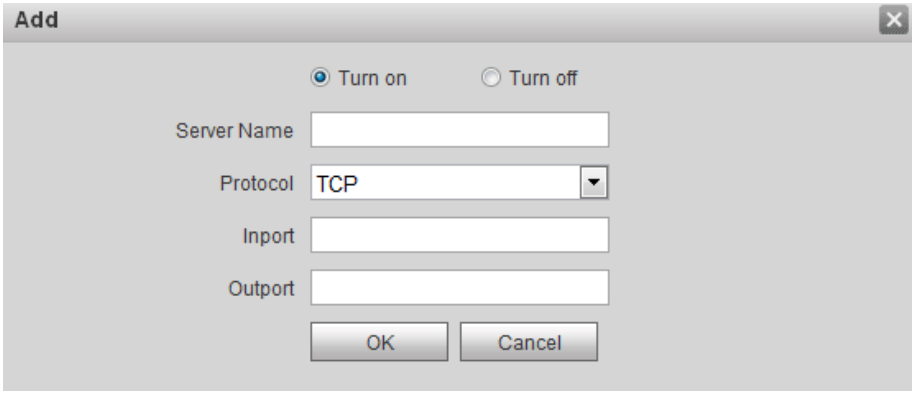
7.12.3 Adding Service

You can add new mapping relations.

Step 1 Click **Add**.

The **Add** interface is displayed. See Figure 7-43.

Figure 7-43 Add mapping relation



Step 2 Configure parameters. See Table 7-18 for the details.

Table 7-18 UPnP parameter description

Parameter	Description	
Turn on/Turn off	Select **Turn on**, and then the mapping relation is enabled. Select **Turn off**, then the mapping relation will not be enabled, and you can select it later in the list.	
Server Name	The name of the server.	
Protocol	You can select from **TCP** and **UDP**. For the transmission stability, **TCP** is recommended.	
Inport	The port on the VTO that need to be mapped.	 • Try to use port number between 1024 to 5000 and not between 1 to 255 and 256 to 1023 when mapping ports with router to avoid conflict. • When mapping multiple devices to the external ports, do the planning in advance to avoid mapping different devices to the same external port. • Make sure the ports you are using are not being used or constrained. • The external ports of TCP and UDP must be the same.
Outport	The port on the router that the VTO port is being mapped to.	

Step 3 Click **OK** to finish configuration.

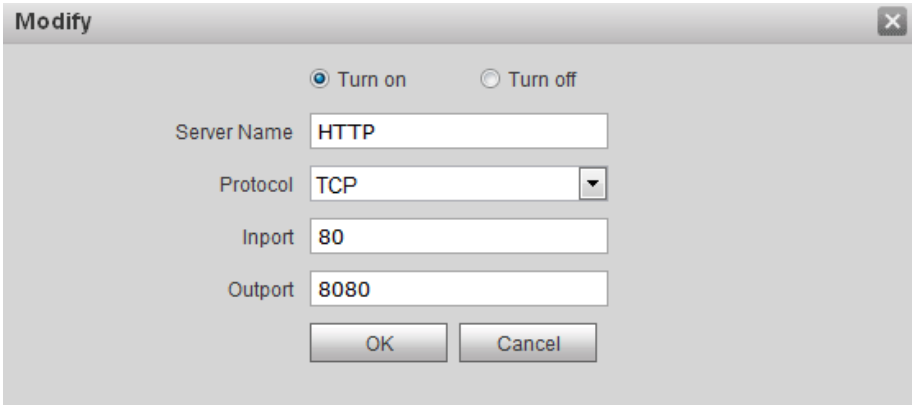
7.12.4 Modifying Service

You can modify the mapping relations in the list.

Step 1 Click  .

The **Modify** interface is displayed. See Figure 7-44.

Figure 7-44 Modify mapping relation



Step 2 Configure parameters. See Table 7-18 for the details.

Step 3 Click **OK** to finish.

7.12.5 Deleting Service

You can delete the mapping relations in the list.

Click  to delete mapping relation.

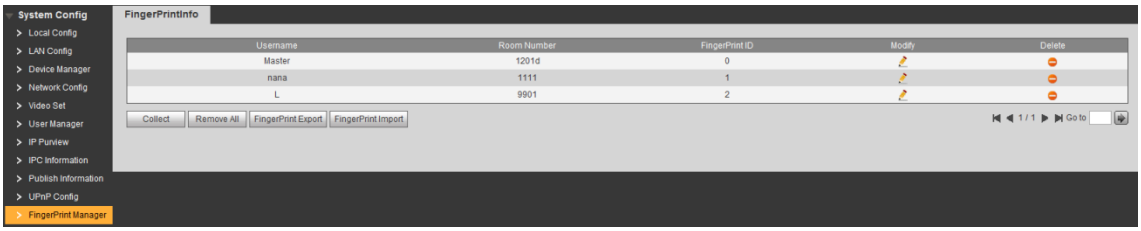
7.13 Fingerprint Manager

You can add, delete, import, and export fingerprint data.

The VTO supports 3000 fingerprints at most.

Select **System Config > Fingerprint Manager**, and then the **FingerPrintInfo** interface is displayed. See Figure 7-45.

Figure 7-45 Fingerprint manager



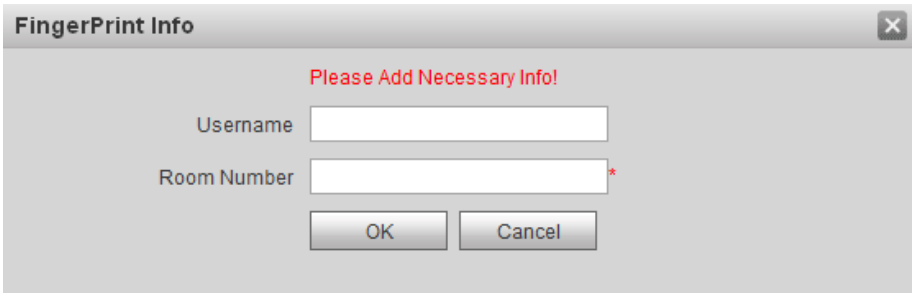
7.13.2 Adding Fingerprint

You can unlock with the added fingerprint.

Step 1 Click **Collect**.

The **FingerPrintInfo** interface is displayed. See Figure 7-46.

Figure 7-46 Add fingerprint (1)



Step 2 Enter username and room number, and then click **OK**.

The input fingerprint notice is displayed.

The room number is what you configured on the VTH.

Step 3 Press the fingerprint sensor on the VTO as instructed.

- The success notice is displayed in the Web interface, and the added fingerprint is displayed in the list.
- If the fail notice is displayed, add it again.

7.13.3 Modifying Fingerprint

Click  to modify the username and room number for a fingerprint.

7.13.4 Deleting Fingerprint

Click  to delete fingerprint.

Click **Remove All** to delete all the fingerprints.

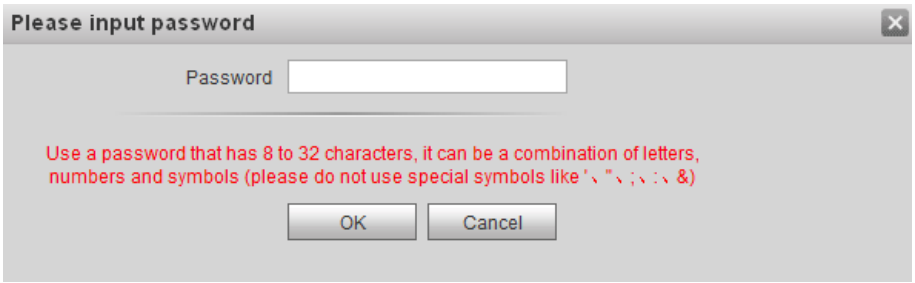
7.13.5 Export Fingerprint

Export the fingerprint information as .xls file to the local storage.

Step 1 Click **FingerPrint Export**.

The **Input password** interface is displayed. See Figure 7-47.

Figure 7-47 Input password



Step 2 Enter the password for the Web interface, and then click **OK** to export fingerprint.

7.13.6 Import Fingerprint

Step 1 Click **FingerPrint Import**.

Step 2 Select the .csv file.

Step 3 Click **File**, and then select the .csv file you need.

Step 4 Click **Upload**.

Step 5 Enter the password for the Web interface, and then click **OK**.

The success notice is displayed.

7.14 Face Management

This section introduces how to configure face recognition and how to manage face data.

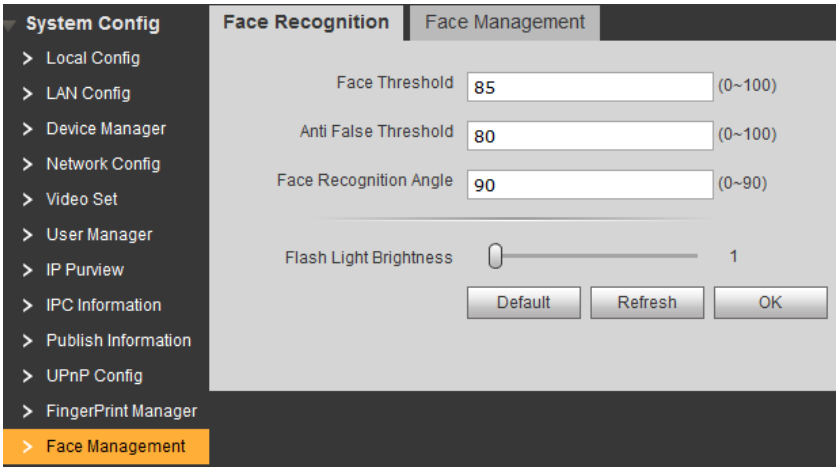
7.14.1 Configuring Face Recognition

This section introduces how to configure face recognition threshold, anti-false threshold, and face recognition angle.

Step 1 Select **System Config > Face Management > Face Recognition**.

The **Face Recognition** interface is displayed. See Figure 7-48.

Figure 7-48 Face recognition



Step 2 Configure face recognition parameters. For the detailed description. See Table 7-19.

Table 7-19 Face recognition parameter description

Parameter	Description
Face Threshold	The bigger the value is, the more similar the target and the saved face data is required to open the door.
Anti False Threshold	The bigger the value is, the less the chance that the system defines a target as human face, hence the more accurate it will be.
Face Recognition Angle	The bigger the value is, the bigger the angle that the target is allowed to turn his face during recognition.
Flash Light Brightness	The brightness of the fill light when providing light to face recognition.

Step 3 Click **OK** to finish configuration.

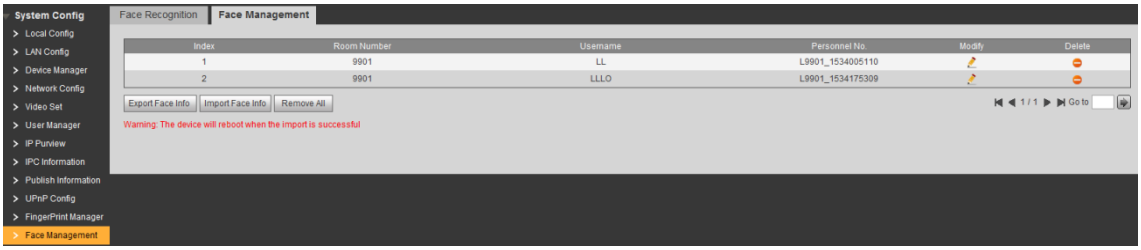
7.14.2 Face Management

You can add, delete, import, and export face data.

The VTO can save 10,000 faces at most.

Select **System Config > Face Management > Face Management**, and then the **Face Management** interface is displayed. See Figure 7-49.

Figure 7-49 Face management



7.14.2.1 Importing Face Data

Step 1 Click Import Face Info.

Step 2 Click **File**, and then select the file you need.

Step 3 Click **Upload**.

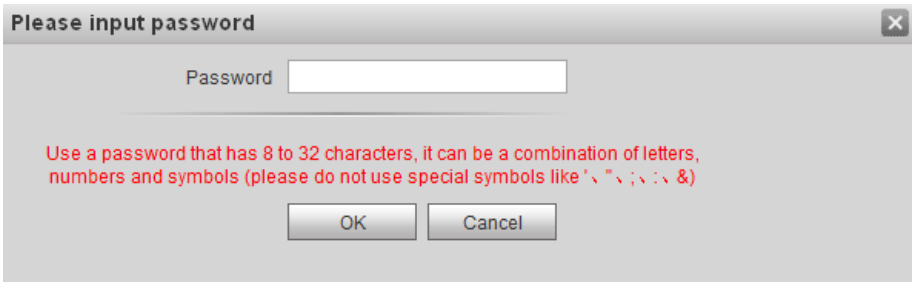
If third party server works as SIP server, this operation can only be done on the third party server.

7.14.2.2 Exporting Face Data

Step 1 Click Export Face Info.

The **Input password** interface is displayed. See Figure 7-50.

Figure 7-50 Input Password



Step 2 Enter the password for the Web interface, and then click **OK** to export face data.

7.14.2.3 Deleting Face Data

Click to delete face data.

Click **Remove All** to delete all the face data.

7.15 Info Search

You can view call history, alarm record, and unlock record.

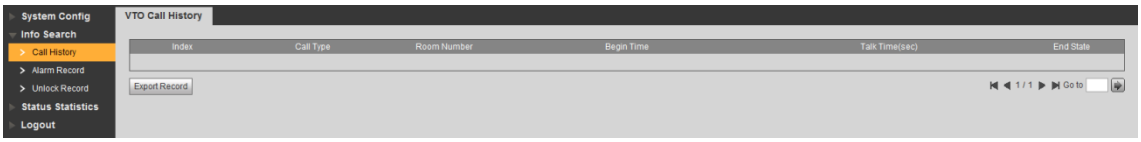
7.15.1 Call History

You can view the call history and phone call record of the VTO, it can save 1024 records at most.

Select **System Config > Info Search > Call History**, and then the **VTO Call History** interface is displayed. See Figure 7-51.You can view the call type, room number, begin time, talk time, and end time.

Click **Export Record** to export the records.

Figure 7-51 VTO call history



7.15.2 Alarm Record

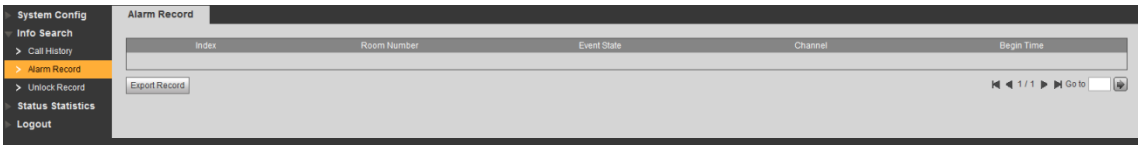
This function is displayed only when the VTO you are visiting works as SIP server.

You can view the VTH alarm record and duress password alarm record, the VTO can save 1024 records at most.

Select **System Config > Info Search > Alarm Record**, and then the **Alarm Record** interface is displayed. See Figure 7-52.

Click **Export Record** to export the alarm records.

Figure 7-52 Alarm record

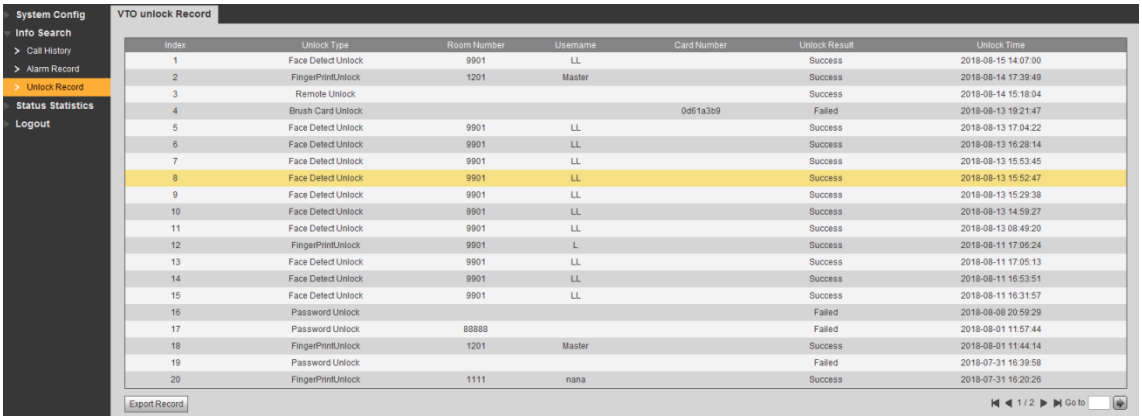


7.15.3 Unlock Record

You can view various unlock records, including face unlock, fingerprint unlock, access card unlock, password unlock, remote unlock, and press button unlock, and the VTO can save 1,000 unlock record at most.

Select **System Config > Info > Unlock Record**, and then the **VTO unlock Record** interface is displayed. See Figure 7-53. You can view information such as unlock type, unlock time, and unlock result.

Figure 7-53 VTO unlock Record



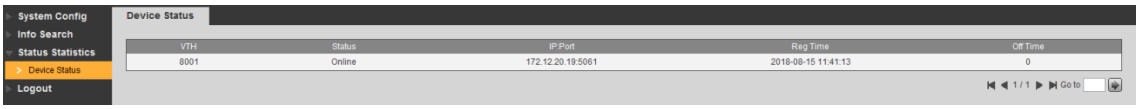
Click **Export Record** to export the unlock records.

7.16 Status Statistics

You can view the on line and off line status of the VTO and the VTH.

Select **System Config > Status Statistics > Device Status**, and then the **Device Status** interface is displayed. See Figure 7-54. You can view information such as device status, IP port, register time, and off time.

Figure 7-54 Device status



There are **Online** and **Offline** in the **Status** column.

- **Offline**: the VTO is not connected with VTH, and it cannot make phone call, do area monitor or talk to the VTH.
- **Online**: the VTO is connected with VTH, and it can make phone call, do area monitor or talk to the VTH.

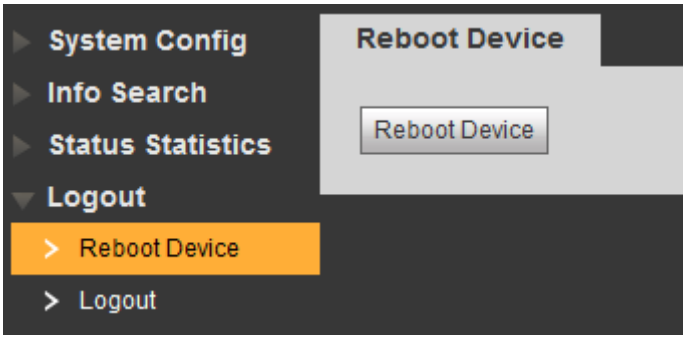
7.17 Rebooting Device

You can reboot the VTO from the Web interface.

Select **System Config > Logout > Reboot Device**, and then the **Reboot Device** interface is displayed. See Figure 7-55.

Click **Reboot Device**, and then the VTO reboots, and then the login interface is displayed.

Figure 7-55 Reboot device

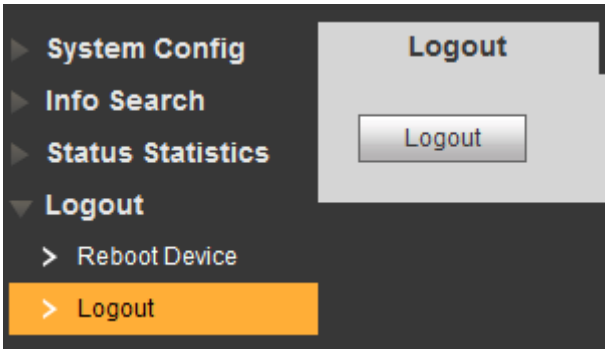


7.18 Logout

Select **System Config > Logout > Logout**, and then the **Logout** interface is displayed. See Figure 7-56.

Click **Logout**, and then the login interface is displayed.

Figure 7-56 Logout



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 Requirements	-20℃-+60℃
		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**	
User's Manual	**1**	
Screw package	**1**	