Villa VTO
(Version 3.1)
User’s Manual

V1.0.1

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. 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.

2. 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

1. Change Passwords Regularly

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

2. 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.

3. Enable HTTPS/SSL:

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

4. Enable IP Filter:

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

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

Foreword

General

This document mainly introduces function, structure, networking, mounting process, debugging process, WEB interface operation and technical parameters of villa VTO products.

Models

VTO6000A, VTO6110B, VTO6110BW, VTO6210B, VTO6000C, VTO6000CM, VTO6100C, VTO2000A and VTO2000A-2

Device Upgrade

Please don't cut off power supply during device upgrade. Power supply can be cut off only after the device has completed upgrade and has rebooted.

General Description about Keys

- OK: it is used to save the settings.
- Default: it is used to restore all parameters at the present interface to default system configurations.
- Refresh: restore parameters at the present interface to present system configurations.

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 No.	Revision Content	Release Date
1	V1.0.0	First release	2017.11.10
2	V1.0.1	Add privacy protection notice	2018.05.23

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 User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's 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 Guide (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.

Operating Requirement

- Please don't place and install the device in an area exposed to direct sunlight or near heat generating device.
- Please don't install the device in a humid, dusty or fuliginous area.
- Please keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Please don't drip or splash liquids onto the device; don't put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Please install the device at well-ventilated places; don't block its ventilation opening.
- Use the device only within rated input and output range.
- Please don't dismantle the device arbitrarily.
- Please transport, use and store the device within allowed humidity and temperature range.

Power Requirement

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

Table of Contents

1 Product Overview

1.1 Product Profile

Villa VTO (hereinafter referred to as VTO) combines with VTH, VTS and platform to establish a video intercom system. Support video call between a visitor and a resident, group call, emergency call, unlock, video preview and record search. It is mainly applied in villa system, and matched with management platform to realize all-round anti-theft, disaster prevention and monitoring function.

1.2 Product Function

Video Intercom

Call VTH users and realize video talk.

Group Call

Call multiple VTH users at one VTO simultaneously.

Be Monitored

VTH or Management Center can monitor VTO image, and support max. 6-channel video stream monitoring.

Emergency Call

Press the key to call the Center in case of an emergency.

Auto Snapshot

Snapshot pictures automatically during unlock or talk, and store them in FTP.

Unlock

Realize unlock with card, unlock with password and remote unlock.

Alarm

Support tamper alarm, door sensor alarm and alarm of unlock with duress password. Meanwhile, report the alarm info to Management Center.

Record Search

Search call records, alarm records and unlock records.

2 Product Structure

2.1 VTO6210B/VTO6210BW

2.1.1 Front Panel

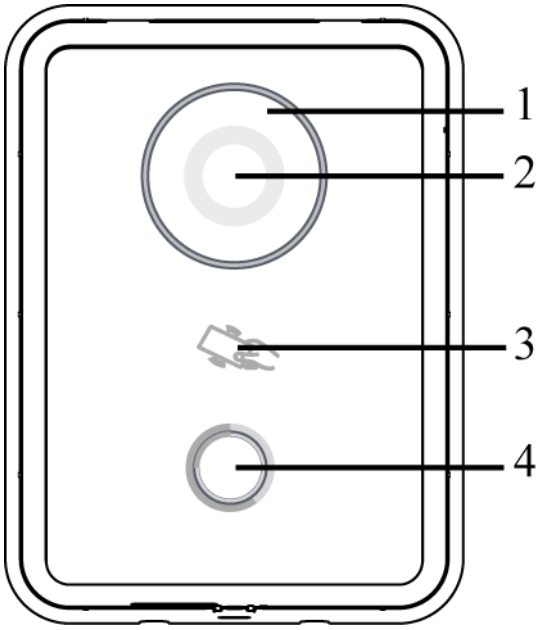

Figure 2-1

No.	Name	Description
1	Fill-in light	Provide fill-in light for camera in case of insufficient light.
2	Camera	Monitor the door area.
3	Card swiping area	Open the door with authorized IC card and swiping card. Note Ensure that access extension module has been connected.
4	Call key	Call management center or VTH.

Table 2-1

2.1.2 Rear Panel

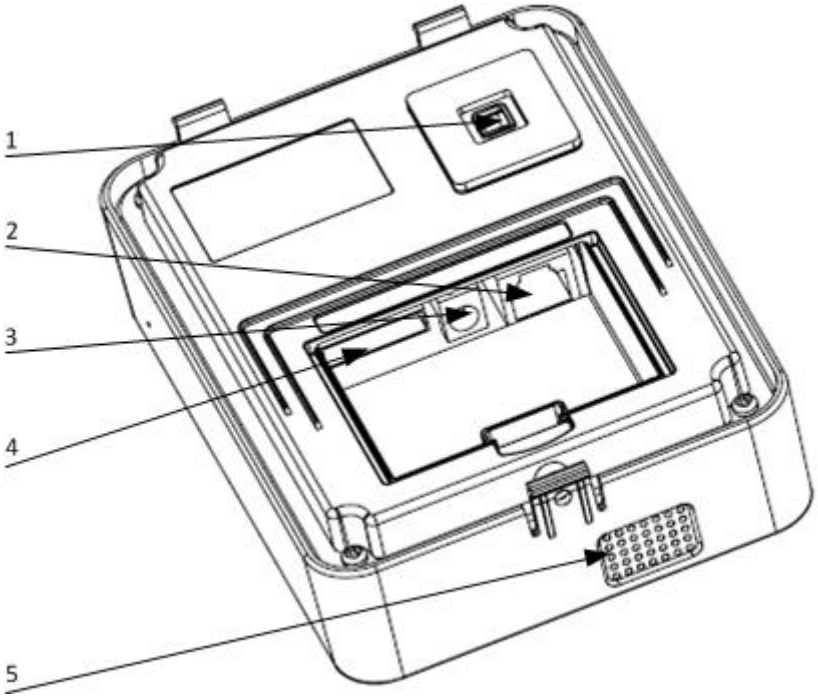

Figure 2-2

No.	Name	Description
1	Tamper switch	When VTO is detached from the wall forcibly, give out alarm sound and report alarm info to management center.
2	Network port	Insert network cable (RJ45 plug).
3	Power port	Connect 12V DC power supply.
4	10-core port	● Provide lock port, door sensor feedback port and exit button port to connect electric control lock, solenoid lock and exit button. Wiring method is shown in Figure 2-6 and Figure 2-7. ● Provide a reserved port to connect access extension module.
5	Speaker	Audio output.

Table 2-2

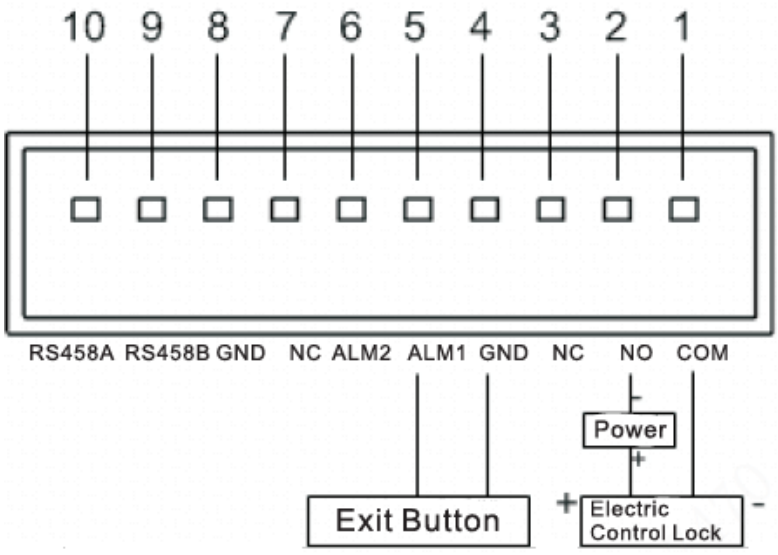

Figure 2-3

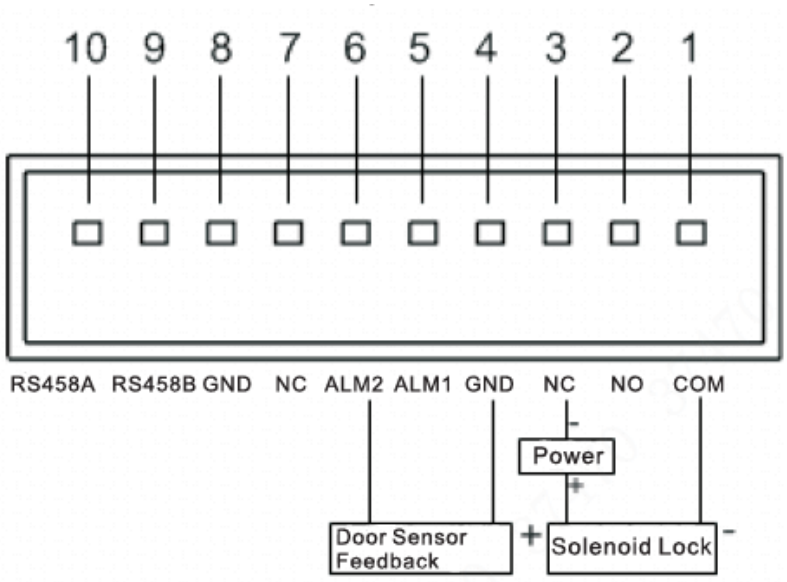

Figure 2-4

2.2 VTO6000CM/VTO6100C

2.2.1 Front Panel

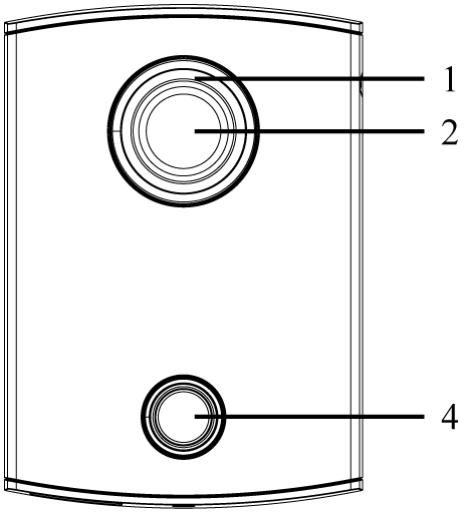

Figure 2-5

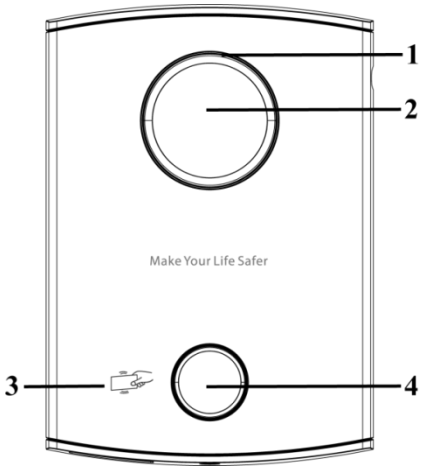

Figure 2-6

No.	Name	Description
1	Fill-in light	Provide fill-in light for camera in case of insufficient light.
2	Camera	Monitor the door area.
3	Card swiping area	Open the door with authorized IC card (card issuing function) and swiping card. Note Only VTO6100C supports to exit with IC card. Silkscreen icon of card swiping area may have different positions; the actual product shall prevail. This schematic diagram is only for your reference.
4	Call key	Call management center or VTH. Blue solid light: VTO is in standby status. Blue flashing light: VTO is calling or talking. Yellow: it is unlocked with IC card or there is a problem in calling.

Table 2-3

2.2.2 Rear Panel

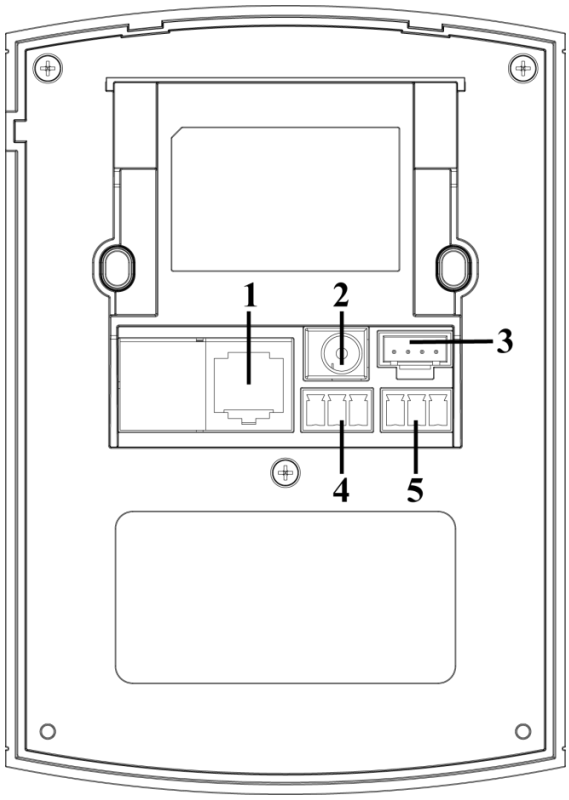

Figure 2-7

No.	Name	Description
1	Network port	Insert network cable (RJ45 plug).
2	Power port	Connect 12V DC power supply.
3	Debugging port	It is used by engineering personnel during debugging.
4	Green plug port 1	Provide lock port, door sensor feedback port and exit button port to connect electric control lock, solenoid lock and exit button. Wiring method is shown in Figure 2-8 and Figure 2-9.
5	Green plug port 2	

Table 2-4

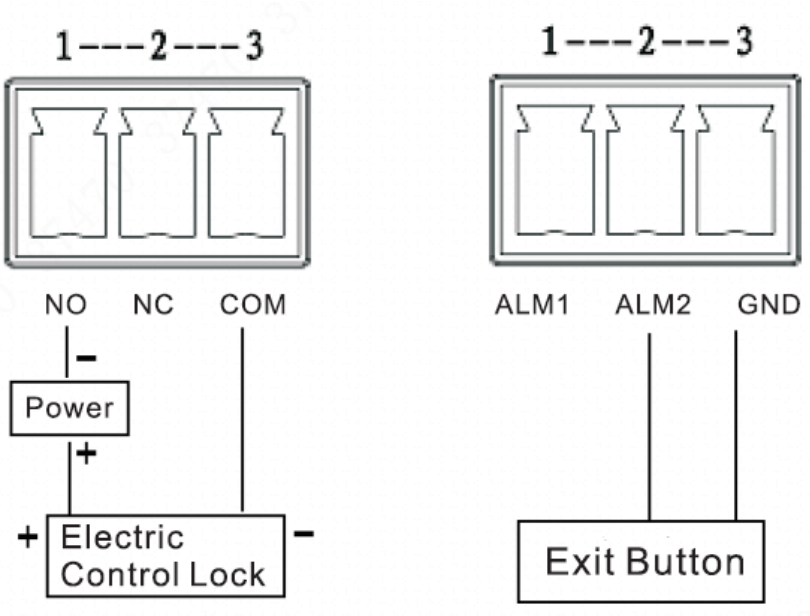

Figure 2-8

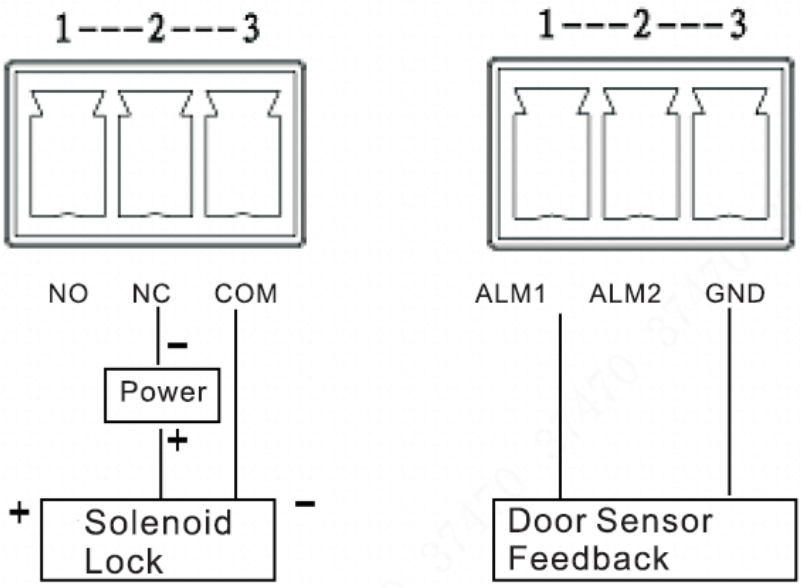

Figure 2-9

2.3 VTO2000A/VTO2000A-2

2.3.1 Front Panel

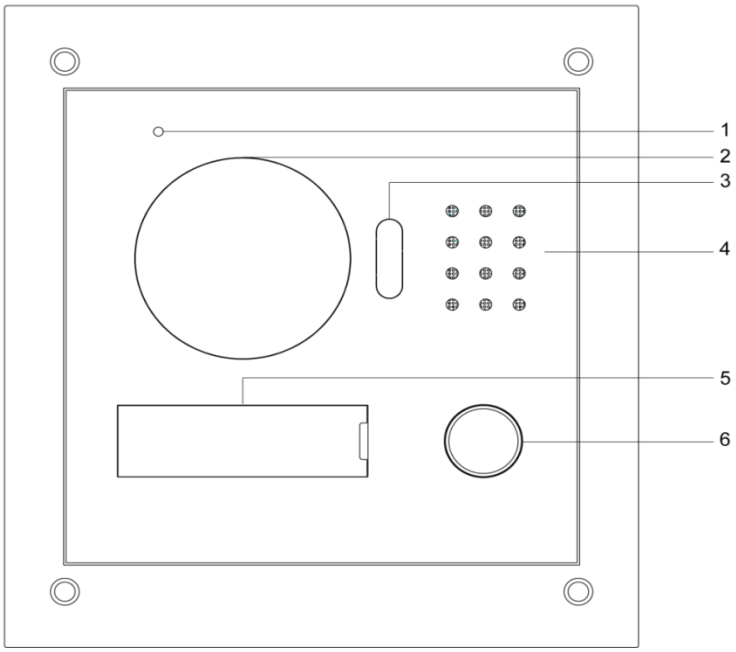

Figure 2-10

No.	Name	Description
1	Microphone	Audio input.
2	Camera	Monitor the door area.
3	Fill-in light	Provide fill-in light for camera in case of insufficient light.
4	Speaker	Audio output.

No.	Name	Description
5	User directory	Set user info.
6	Call key	Call management center or VTH.

Table 2-5

2.3.2 Rear Panel

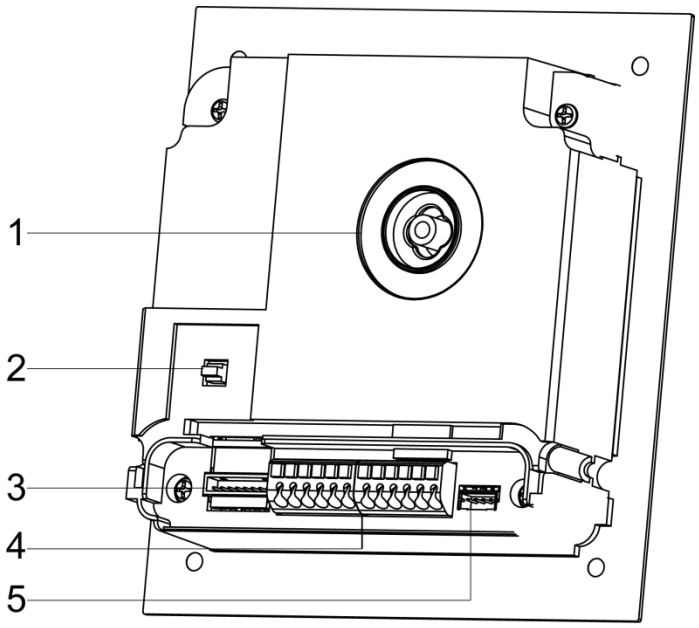

Figure 2-11

No.	Name	Description
1	Camera angle adjusting column	Adjust camera angle.
2	Tamper switch	When VTO is detached from the wall forcibly, give out alarm sound and report alarm info to management center.
3	Network port	Connect network cable (RJ45 plug) with adapter cable.
4	User port	Provide power port, lock port, door sensor feedback port and exit button port to connect power supply, electric control lock, solenoid lock and exit button. Wiring method is shown in Figure 2-15 and Figure 2-13.
5	Debugging port	It is used by engineering personnel during debugging.

Table 2-6

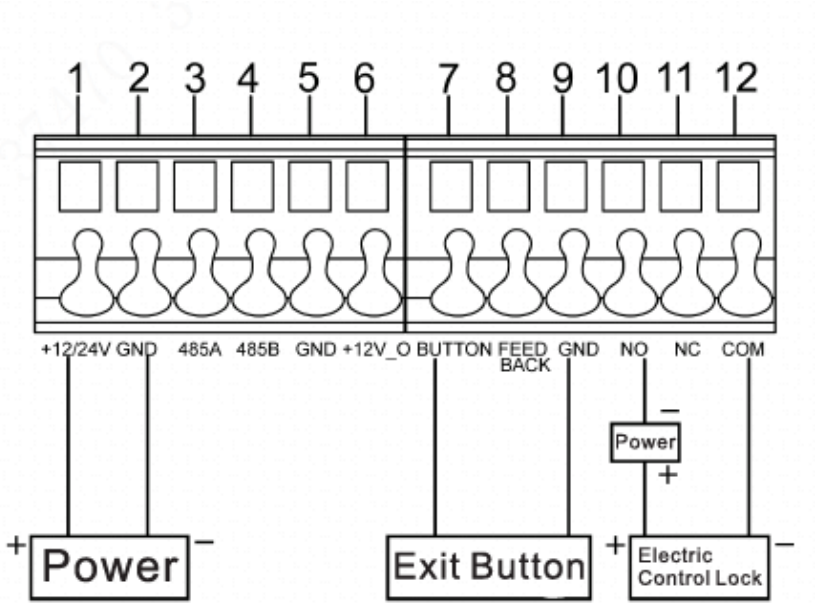

Figure 2-12

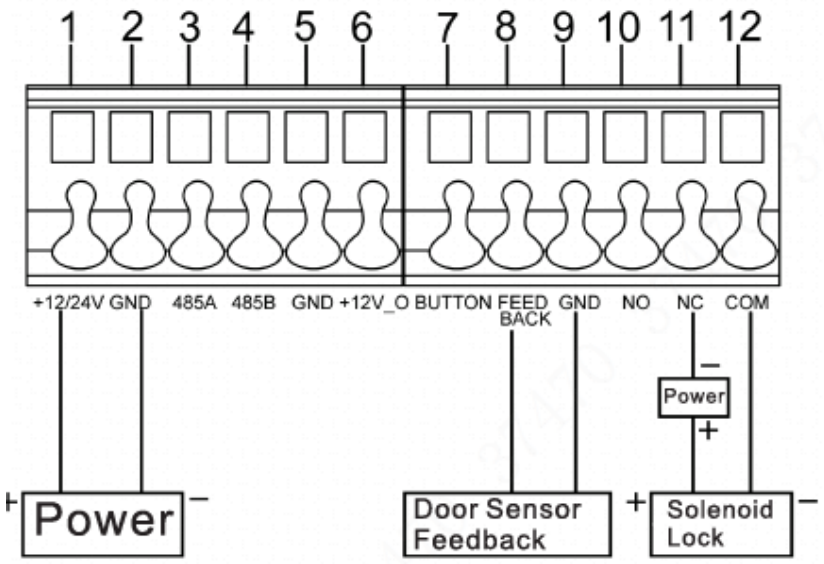

Figure 2-13

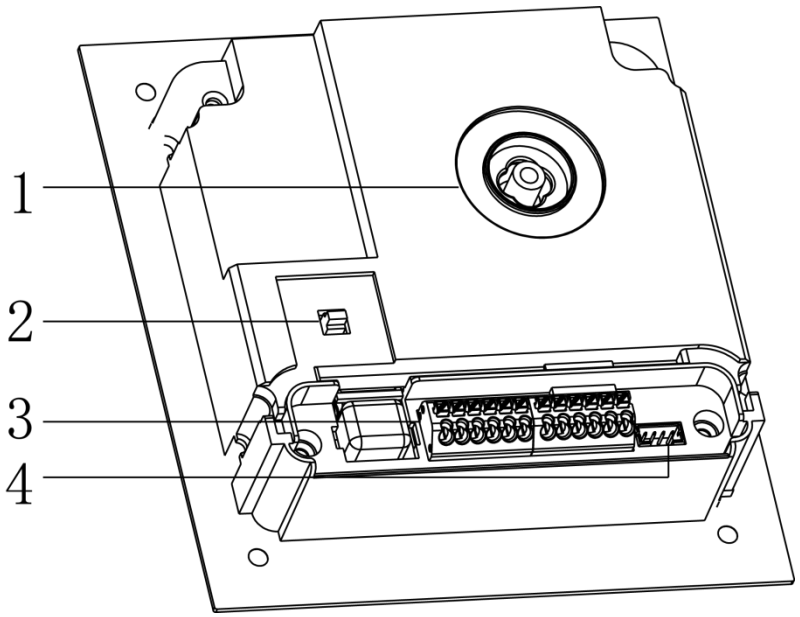

Figure 2-14

No.	Name	Description
1	Camera angle adjusting column	Adjust camera angle.
2	Tamper switch	When VTO is detached from the wall forcibly, give out alarm sound and report alarm info to management center.
3	User port	Provide power port, 2-wire port, lock port, door sensor feedback port and exit button port to connect power supply, 2-wire VTH, electric control lock, solenoid lock and exit button. Wiring method is shown in Figure 2-15 and Figure 2-16.
4	Debugging port	It is used by engineering personnel during debugging.

Table 2-7

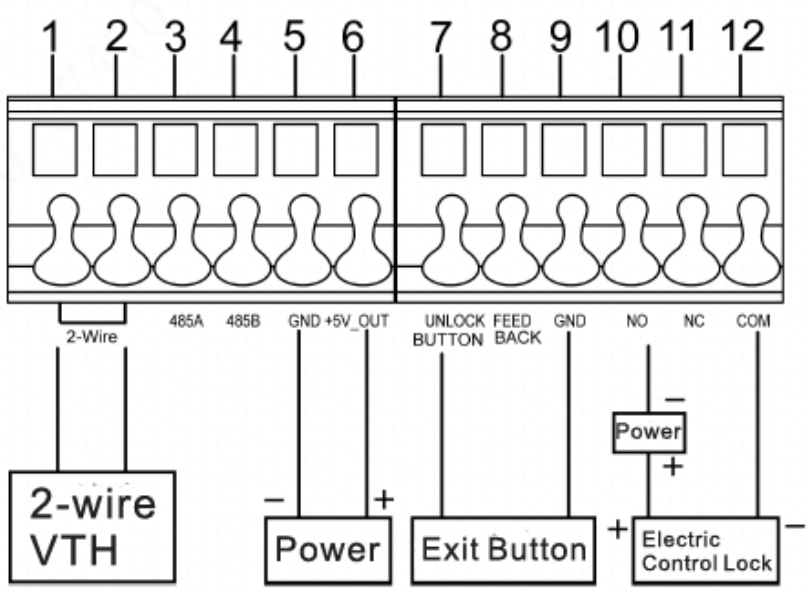

Figure 2-15

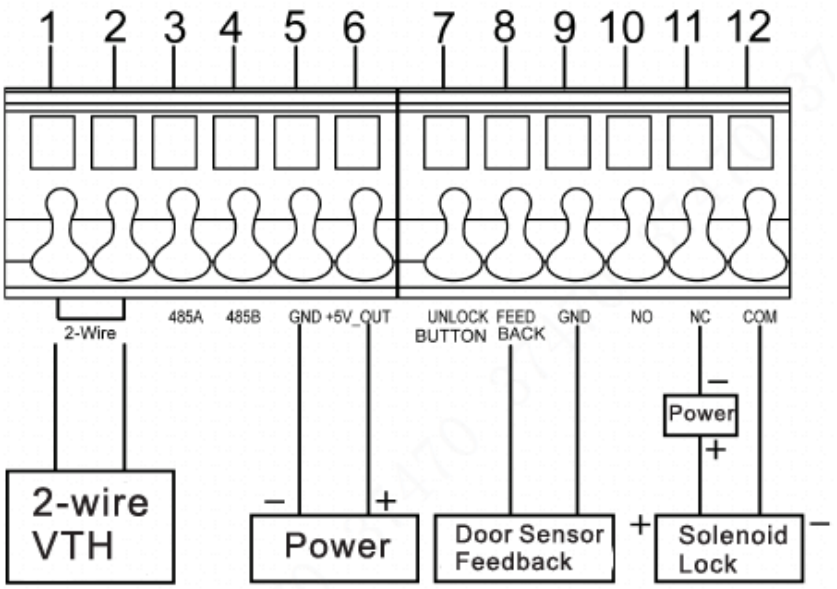
1 2 3 4 5 6 7 8 9 10 11 12
2-Wire
485A
485B
GND
+5V_OUT
UNLOCK BUTTON
FEED BACK
GND
NO
NC
COM
Power
2-wire VTH
Power
Door Sensor Feedback
Solenoid Lock

Figure 2-16

3 Networking Diagram

3.1 VTO6210B/VTO6210BW/VTO6000CM/VTO6100C/VTO 2000A

3.1.1 One-to-one Scene

Villa VTO connects with VTH directly. A visitor presses call key on villa VTO to call the resident (VTH) or Management Center. Take digital villa VTO VTO6110BW for example; its networking diagram is shown in Figure 3-1.

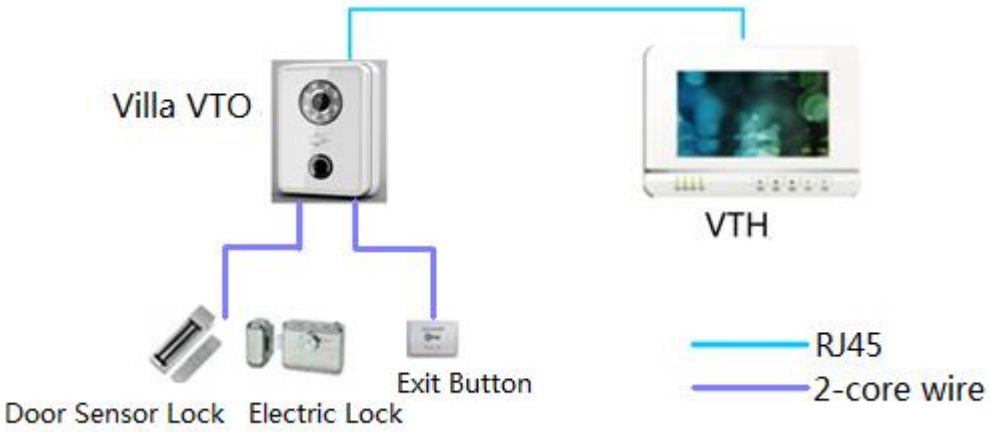

Figure 3-1

3.1.2 One-to-many Scene

Generally, unit VTO is installed at the gate of apartment building, whereas villa VTO is installed at the resident's gate. The operation process is as follows.

Step 1 The visitor calls any resident with unit VTO.

The resident's VTH rings. After unlocking, the visitor goes into the apartment building.

Step 2 Call the resident with villa VTO, and ask the resident to unlock the house.

Take digital villa VTO6110BW for example; its networking diagram is shown in Figure 3-2.

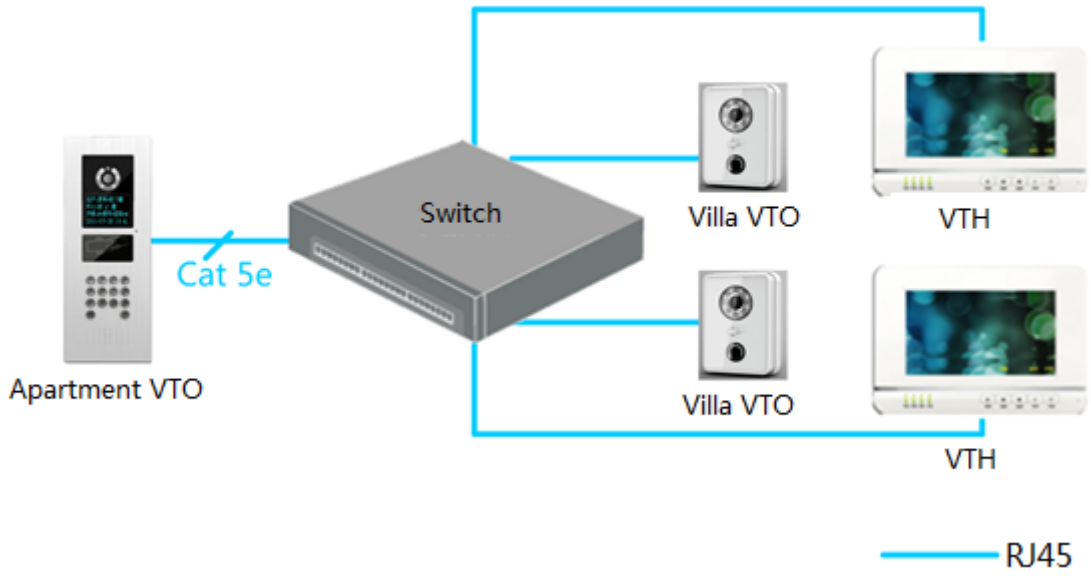

Figure 3-2

3.1.3 Group Call Scene

When the visitor presses call key on villa VTO, multiple VTHs ring at the same time; the resident can pick up, hang up or unlock on any VTH.

Take digital villa VTO6110BW for example; its networking diagram is shown in Figure 3-1.

Note

VTH consists of master VTH and extension VTH. There is 1 master VTH at most and 5 extension VTHs at most.

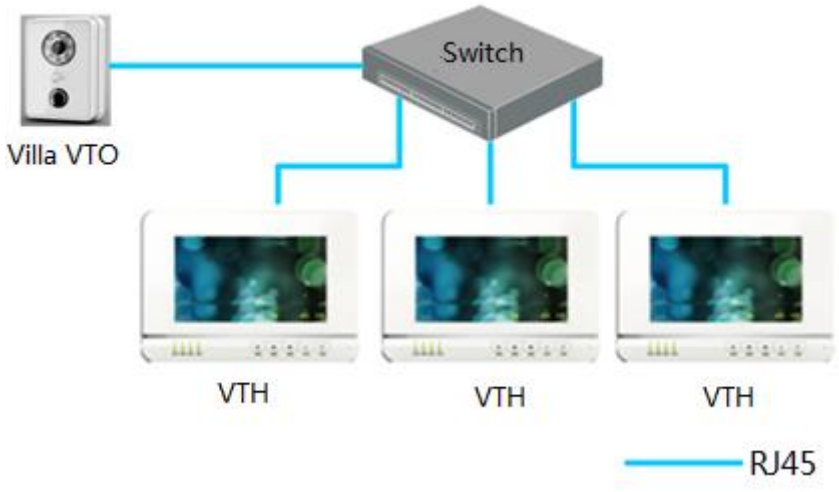

Figure 3-3

3.2 VTO2000A-2

3.2.1 One-to-one Scene

The visitor presses call key to call the resident (VTH) or Management Center, as shown in Figure 3-4.

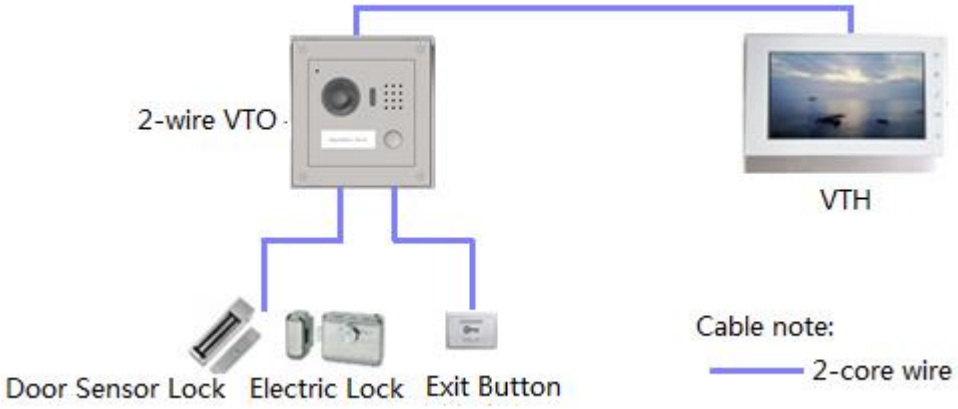

Figure 3-4

3.2.2 Group Call Scene

When the visitor presses call key on villa VTO, multiple VTHs ring at the same time; the resident can pick up, hang up or unlock on any VTH, as shown in Figure 3-5.

Note

VTH consists of master VTH and extension VTH. There is 1 master VTH at most and 4 extension VTHs at most.

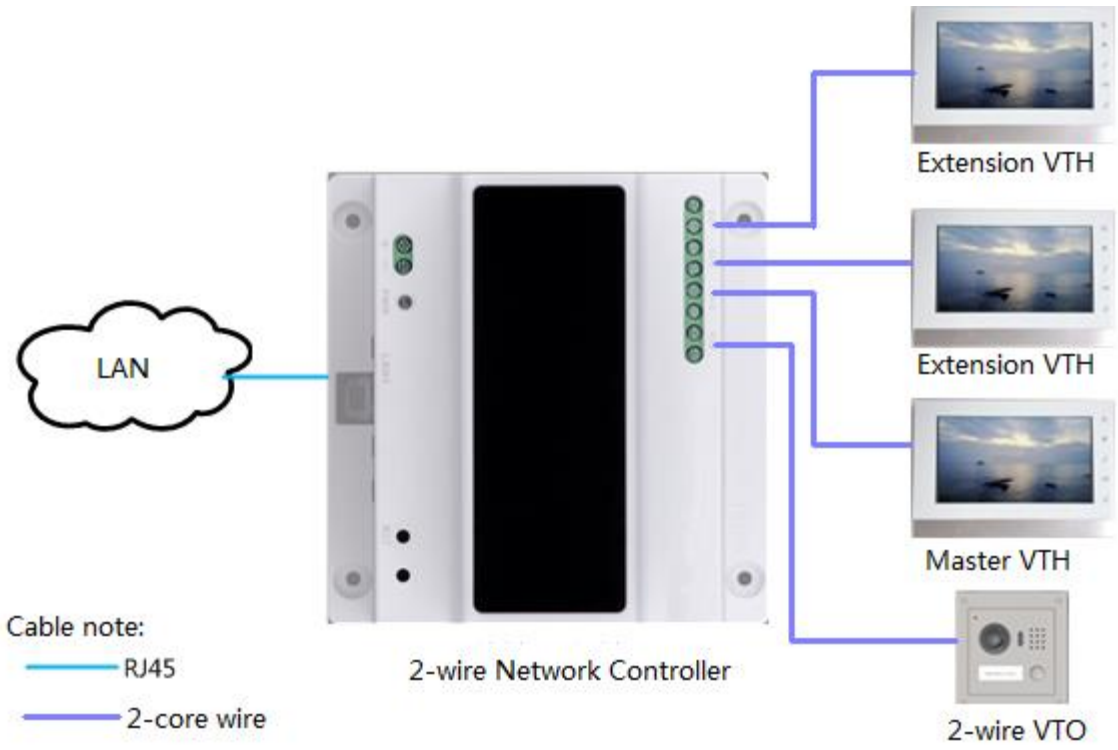
Extension VTH
Extension VTH
LAN
Master VTH
Cable note:
RJ45
2-core wire
2-wire Network Controller
2-wire VTO

Figure 3-5

4 Device Mounting

4.1 Mounting Flow Chart

VTO mounting flow chart is shown in Figure 4-1. Please install VTO in the following steps.

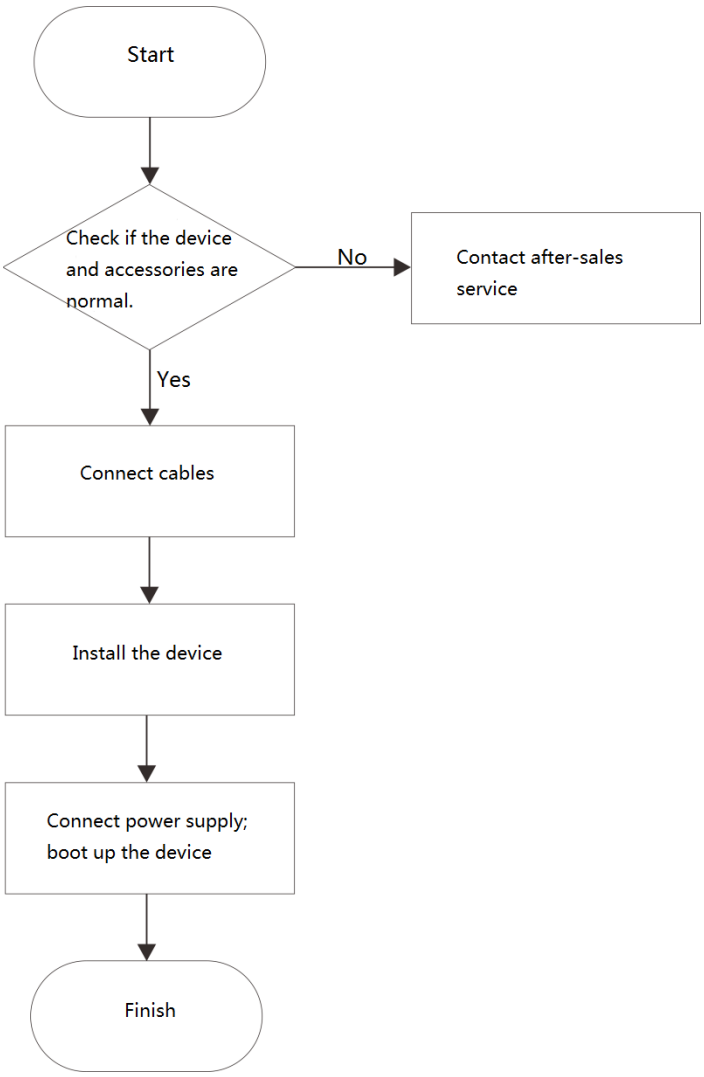

Figure 4-1

Note

- For cable connection, please refer to “2 Product Structure”.
- For device mounting, please refer to “4.4 Device ”.

4.2 Open-case Inspection

Please carry out open-case inspection when receiving the device. Please timely contact our

after-sales service personnel in case of any problems.

Sequence	Item		Content
1	Overall package	Appearance	Inspect whether there are obvious damages.
		Package	Inspect whether there are accidental impacts.
		Fittings	Inspect whether fittings are complete.
2	Model and label	Device model	Inspect whether it is consistent with order contract.
		Label on the device	Inspect whether it is torn or damaged. Note Don't tear or discard the label, otherwise warranty service won't be provided. When dialing our after-sales hotline, please provide serial number of the product.
3	Device	Appearance	Inspect whether there are obvious damages.

Table 4-1

4.3 Mounting Requirement

- Don't install VTO in bad environment, such as condensation, high temperature, stained, dusty, chemically corrosive, direct sunshine or unshielded environment.
- Engineering mounting and debugging shall be done by professional teams. Please don't dismantle or repair arbitrarily in case of device failure.

4.4 Device Mounting

4.4.1 VTO6210B and VTO6210BW

Caution

Before installing the bracket or flush mount box, cables in the wall shall be led through the bracket or flush mount box.

Mounting method of VTO6210B and VTO6210BW is the same. Take "VTO6210B" for example.

Step 1 Fix the mounting bracket onto the wall.

1. Fix the bracket onto 86 box with M4 screws. Screw holes are located in Points 3 as shown in the figure.
2. To strengthen product firmness, tighten it with ST3.0 screws in Points 4 as shown in the figure.

Step 2 Connect cables. Please refer to "2.1.2 Rear Panel" for details.

Step 3 Put the bare device onto the mounting bracket; fit the upper edge first and then push the lower edge gently.

Step 4 Fix the whole device onto the bracket with M3 screws.

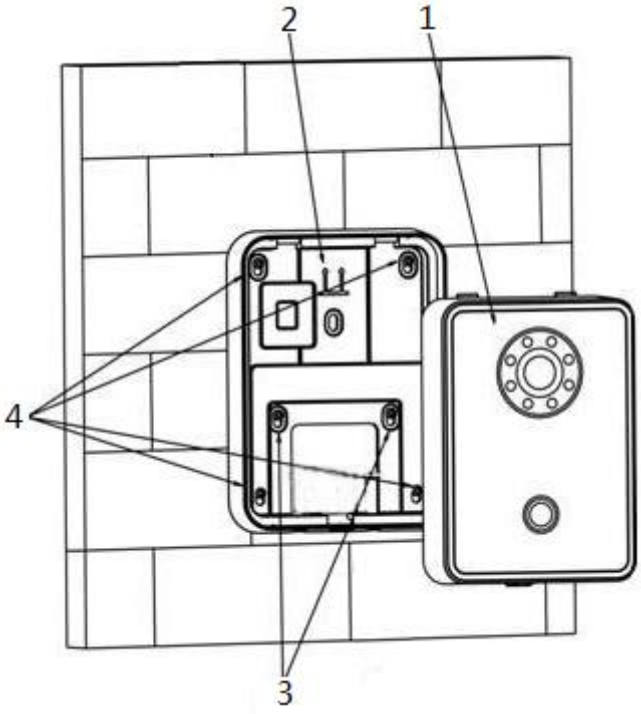

Figure 4-2

4.4.2 VTO6000CM and VTO6100C

Caution

- Before installing the bracket or flush mount box, cables in the wall shall be led through the bracket or flush mount box.
- Try not to install VTO6100C onto an iron door directly. Otherwise, signals may be shielded and card induction may be poor.

Step 1 Dismantle M3 screws at the bottom of VTO and take off the decorative cap.

Step 2 Connect cables. Please refer to “2.2.2 Rear Panel” for details.

Step 3 Fix the bare device onto 86 box with M4 screws. Screw holes are located in Points 3 as shown in the figure.

Step 4 To strengthen product firmness, after 86 box is in place, tighten it with ST3.0 screws in Points 6 as shown in the figure.

Step 5 Install the decorative cap onto the bare device, and fix it with M3 screws.

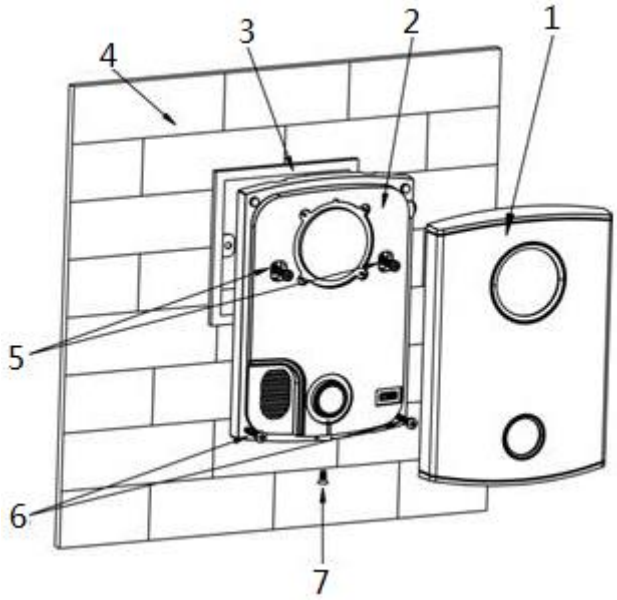

Figure 4-3

4.4.3 VTO2000A/VTO2000A-2

VTO2000A and VTO2000A-2 devices support the same mounting method and process. Take “VTO2000A” for example.

4.4.3.1 Surface Mounting

Step 1 Drill holes according to hole positions of sheet metal bracket, and put expansion pipe in place.

Step 2 Connect cables. Please refer to “2.3.2 Rear Panel” for details.

Step 3 Fix sheet metal bracket onto the wall with ST3×18 screws.

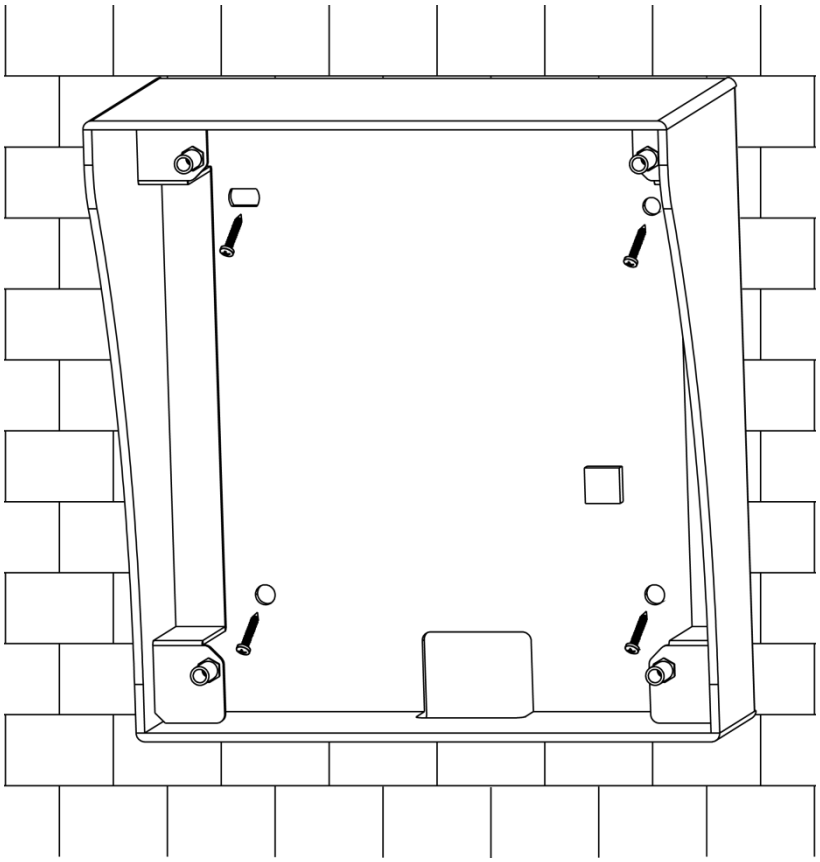

Figure 4-4

Step 4 Fix the bare device onto sheet metal bracket with M3×6 screws.

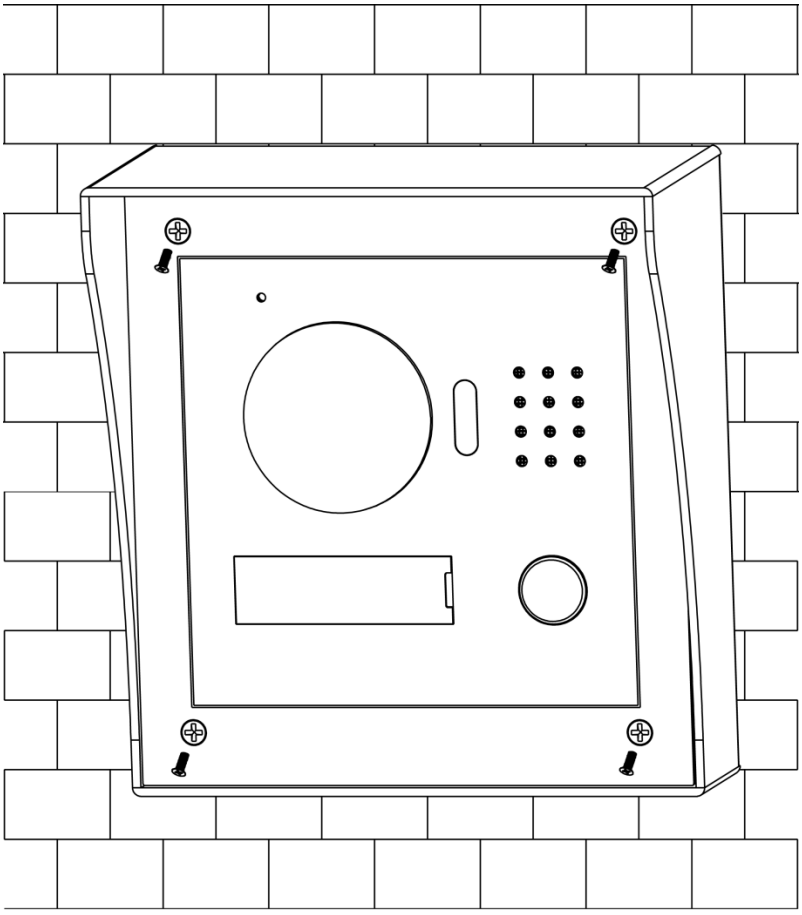

Figure 4-5

4.4.3.2 Flush Mounting

Step 1 Dig a hole in the wall, embed flush mounting box into the wall, and ensure that box edge clings to the wall.

Note

- Hole dimension is 117mm×128mm×80mm.
- During flush mounting, lead cables out from the wall.

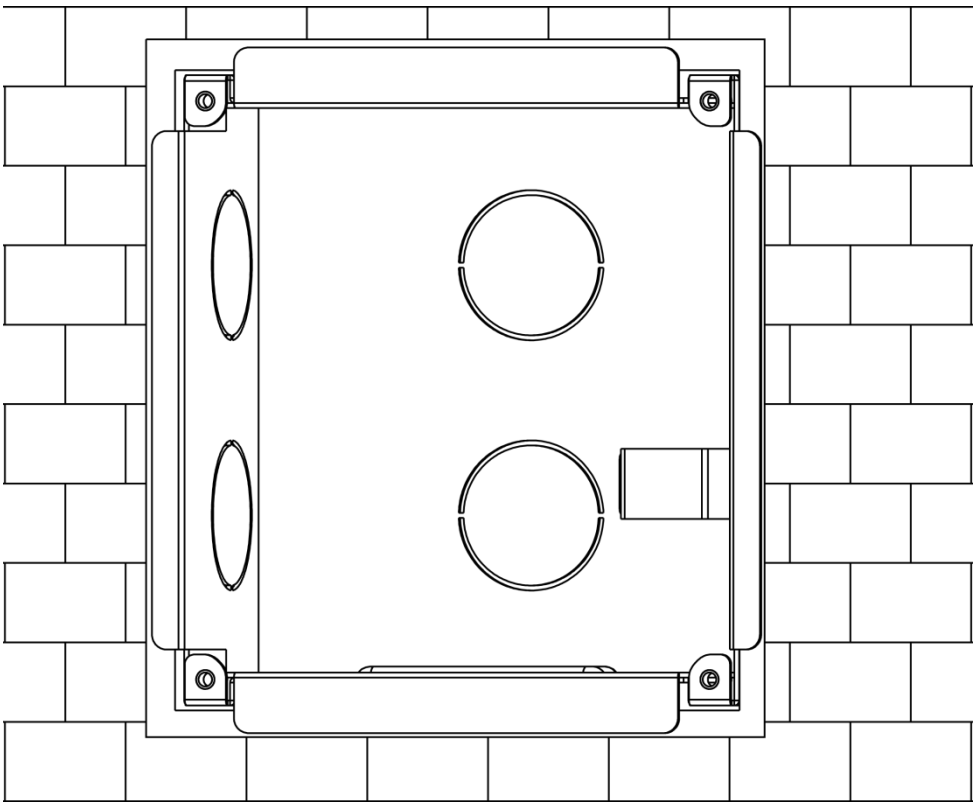

Figure 4-6

Step 2 Connect cables. Please refer to “2.3.2 Rear Panel” for details.

Step 3 Fix the bare device onto the box with M3×8 screws.

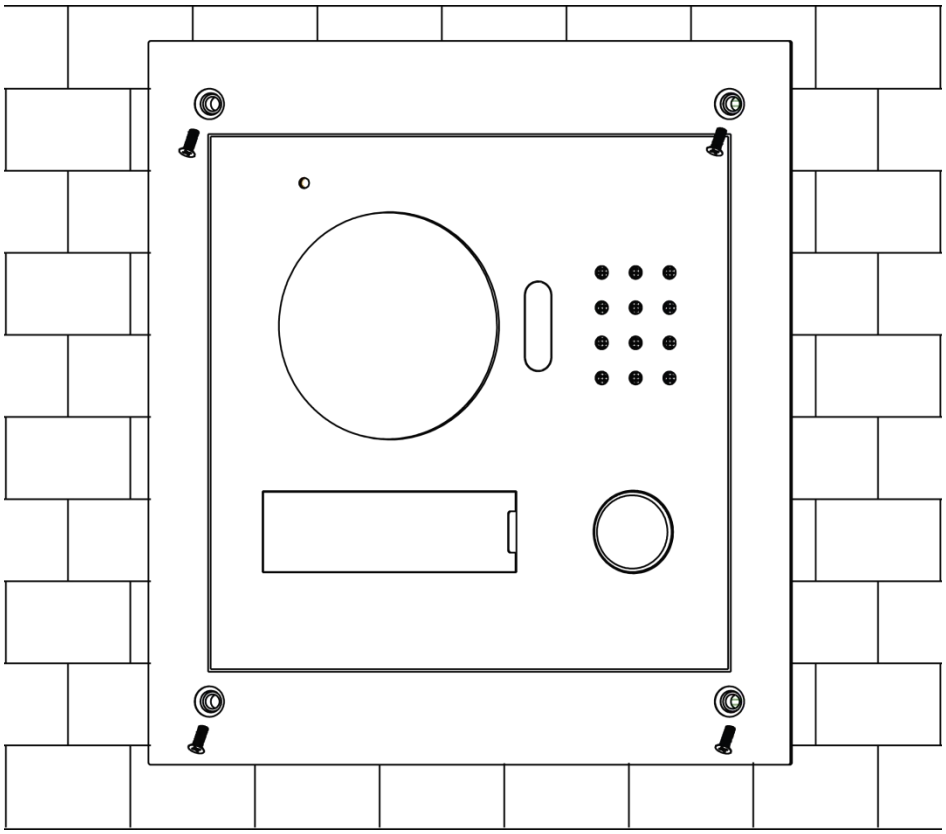

Figure 4-7

5 Device Debugging

Carry out debugging to ensure that the device can realize basic network access, call and monitoring functions after installation. Before debugging, please check whether the following work has been completed.

- Debugging personnel shall get familiar with relevant documents in advance, and get to know device mounting, wiring and use.
- Check whether there is short circuit or open circuit. Power on the device only after the circuit is confirmed to be normal.
- IP and no. (or room no.) of every VTO and VTH have been planned.

5.1 Debugging Settings

5.1.1 VTO Settings

5.1.1.1 Initialization

For the first time, please initialize login password.

Note

Please ensure that default IP addresses of PC and VTO are in the same network segment. Default IP address of VTO is 192.168.1.110.

Step 1 Connect VTO power and boot up.

Step 2 Enter default IP address of VTO at the address bar of PC browser.

The system displays “Setting” interface, as shown in Figure 5-1.

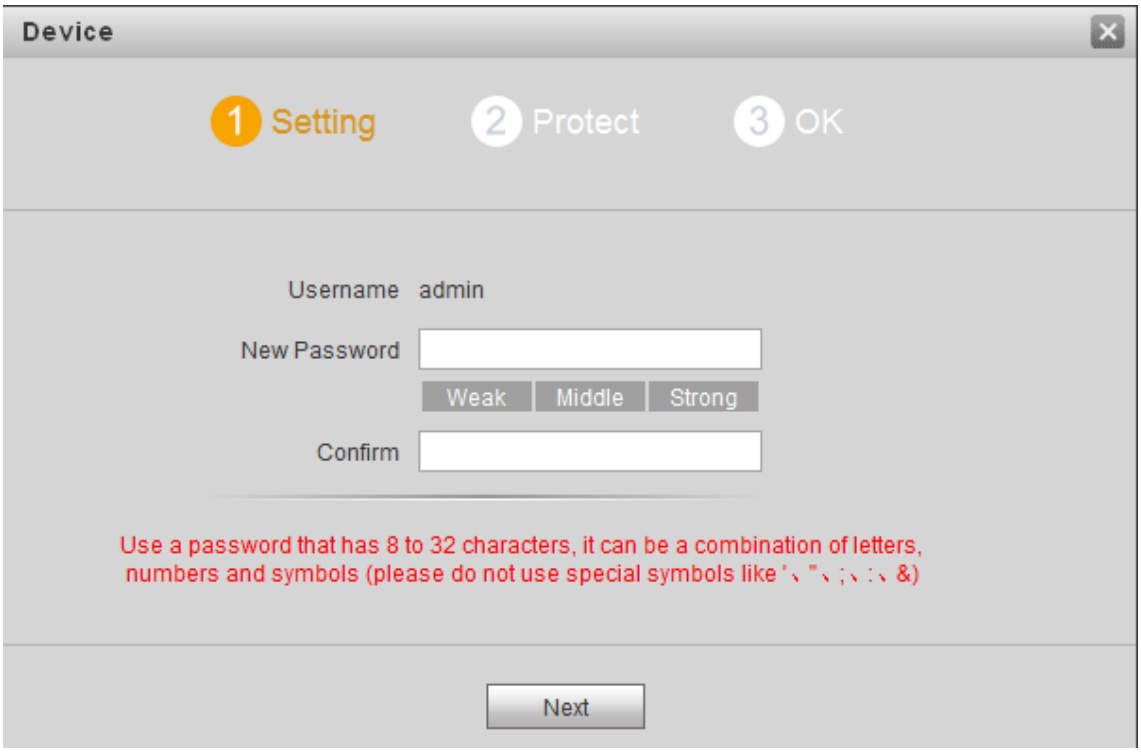

Figure 5-1

Step 3 Enter “New Password” and “Confirm”, and click “Next”.

The system displays “Protect” interface, as shown in Figure 5-2.

Note

This password is used to login WEB interface. It shall be at least 8 characters, and shall include at least two types of number, letter and symbol.

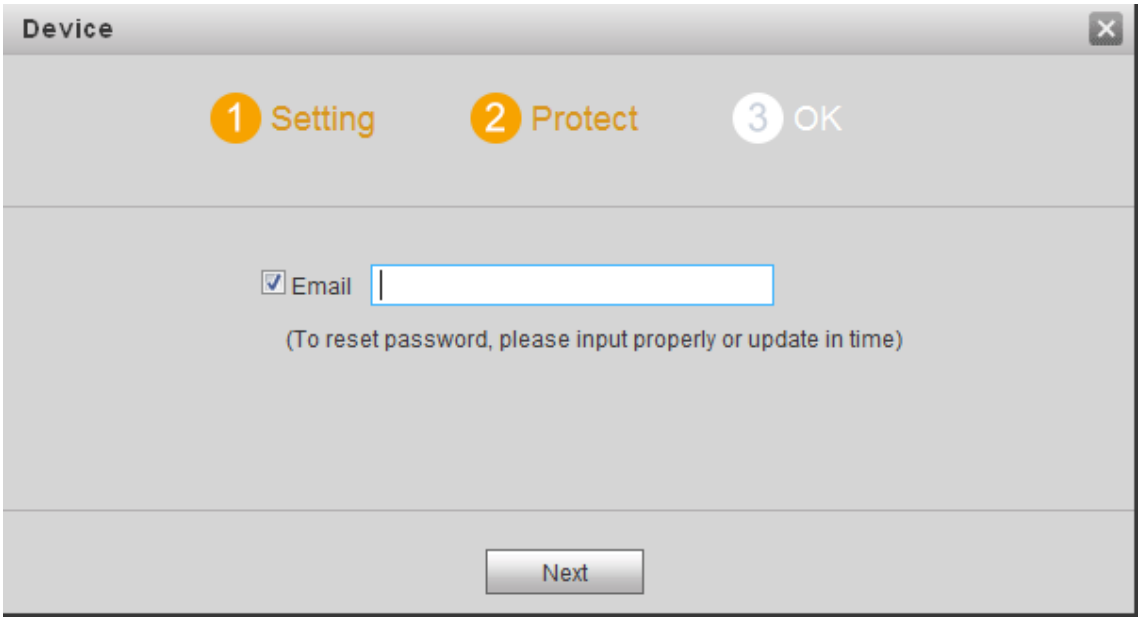

Figure 5-2

Step 4 Select “Email” and enter your Email address.

This Email address is used to reset the password, so it is recommended that it should be set.

Step 5 Click “Next”.

The system displays “OK” interface, as shown in Figure 5-3, and shows “Device succeeded!”

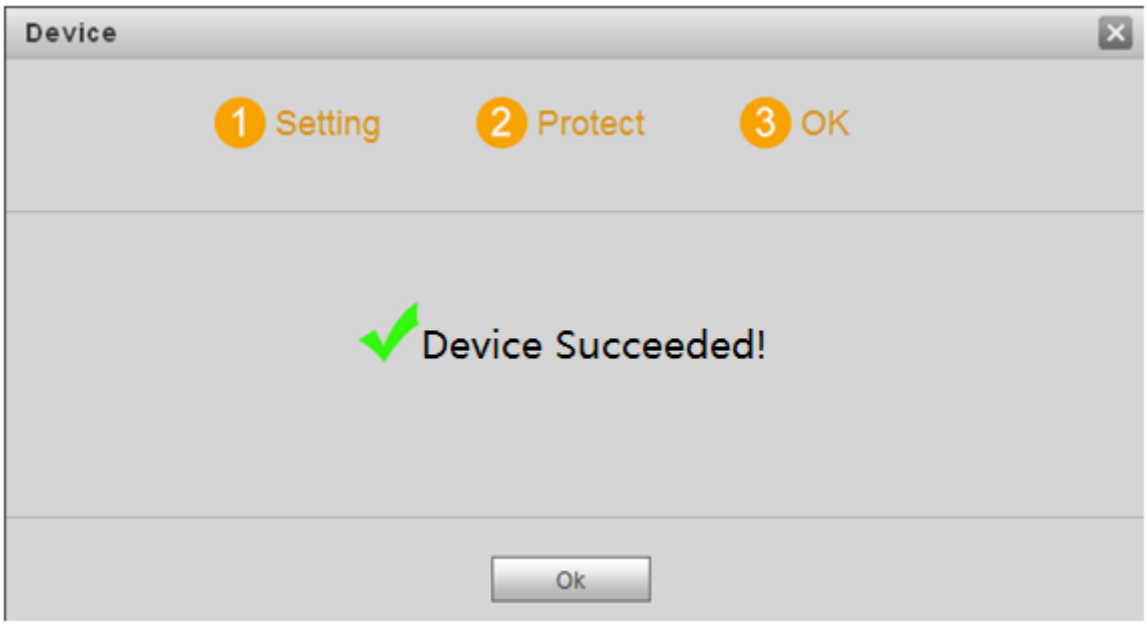

Figure 5-3

Step 6 Click “OK”.

The system displays WEB login interface, as shown in Figure 5-4.

Figure 5-4

Step 7 Enter username and password, and click “Login”.

Log in the WEB interface of the device.

Note

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

5.1.1.2 Network Config

Modify IP address of VTO to be planned IP address.

Step 1 Select “System Config > Network Config > TCP/IP”.

The system displays “TCP/IP” interface, as shown in Figure 5-5.

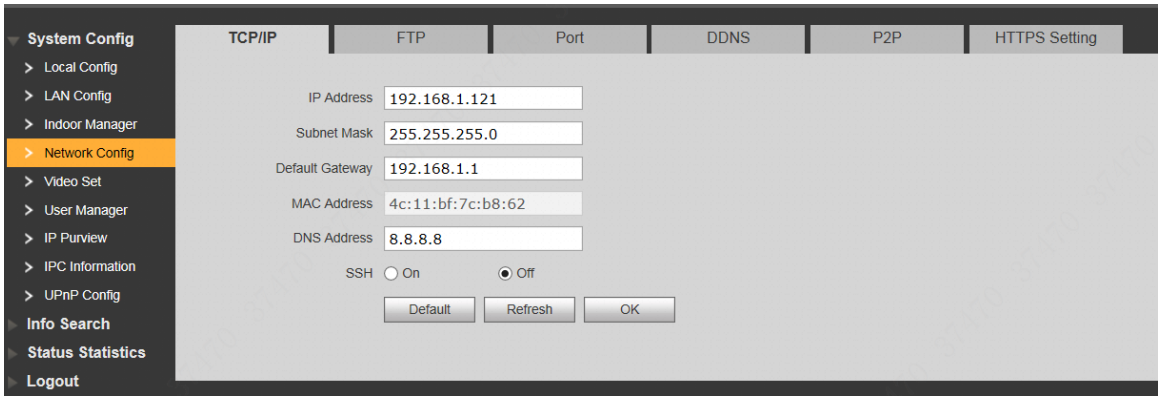

Figure 5-5

Step 2 Enter the planned “IP Address”, “Subnet Mask” and “Default Gateway”, and click “OK”. After modification is completed, VTO reboots automatically, while the following two cases occur at WEB interface.

- If PC is in the planned network segment, WEB interface jumps to new IP login interface automatically.
- If PC is not in the planned network segment, the webpage cannot be displayed. Please add PC into the planned network segment and login WEB interface again.

5.1.1.3 LAN Config

Set building no., unit no. and VTO no..

Step 1 Select “System Config > LAN Config”.

The system displays “LAN Config” interface, as shown in Figure 5-6.

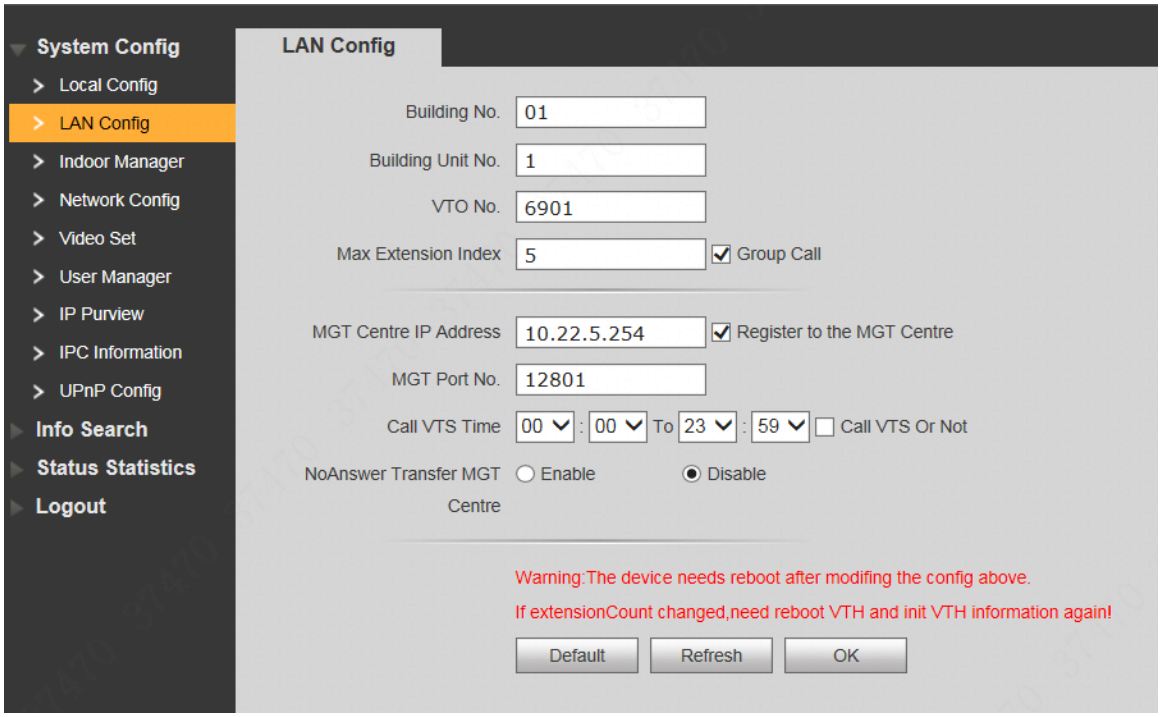

Figure 5-6

Step 2 Enter VTO “Building No.”, “Building Unit No.” and “VTO No.”.

Note

- To call management centre, please select “Register to the MGT Centre”; set “MGT Centre IP Address” and “MGT Port No.”. Set “Call VTS Time” and tick “Call

VTS or Not”.

- To provide group call, please select “Group Call” and set “Max Extension Index” which can be 5 at most.

Step 3 Click “OK”.

5.1.1.4 Add VTH

Add VTH info. After VTH and VTO debugging is completed, VTH will be registered to VTO automatically, in order to realize binding.

Note

- Add master VTH only.
- After “Network Terminal” interface of extension VTH adds main VTO and enables it, VTO interface will obtain extension VTH info automatically.

Step 1 Select “System Config > Digital Indoor Station Manager”.

The system displays “Digital Indoor Station Manager” interface, as shown in Figure 5-7.

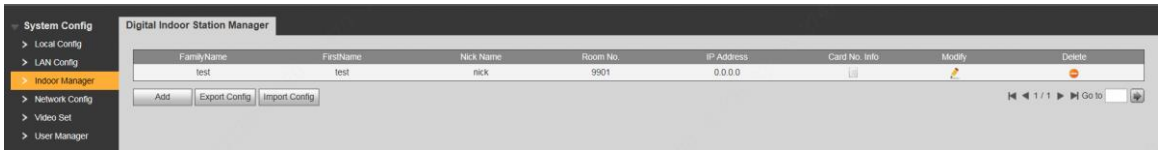

Figure 5-7

Step 2 Click “Add”.

The system displays “Add” interface, as shown in Figure 5-8.

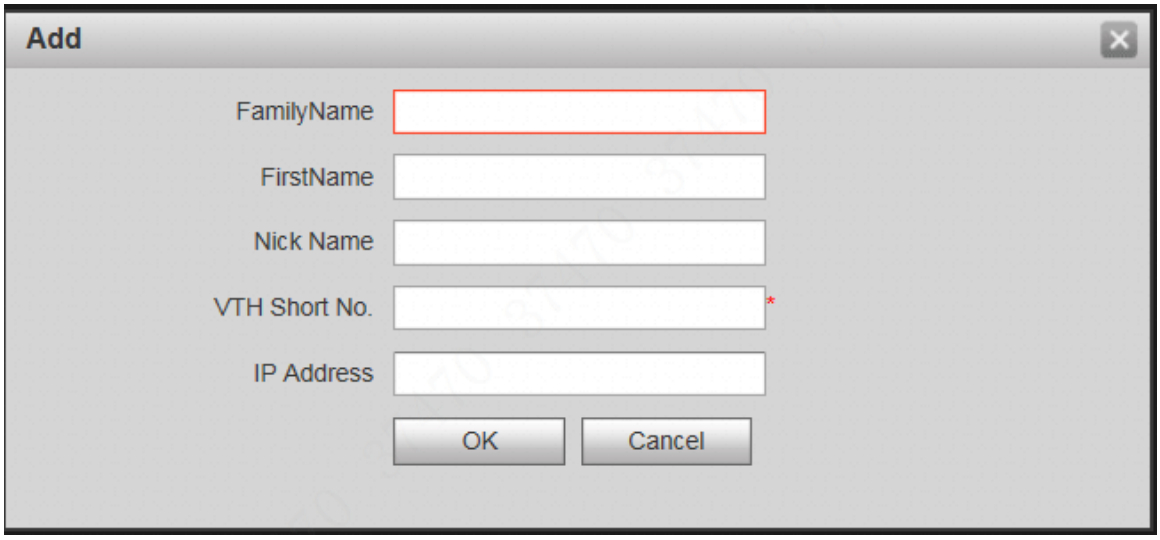

Figure 5-8

Step 3 Enter VTH “Family Name”, “First Name”, “Nick Name”, “VTH Short No.” (VTH room no.) and “IP Address”.

Note

It is OK if IP address is not filled in. After VTH is registered to VTO successfully, VTO will obtain IP address of VTH.

Step 4 Click “OK”.

5.1.2 VTH Config (Version 3.1)

5.1.2.1 Initialization

Set the password and bind your Email.

- Password: it is used to enter project setting interface.
- Email: it is used to retrieve your password when you forget it.

Step 1 Power on the device.

The system displays “Welcome” and enters “Device Initialization” interface, as shown in Figure 5-9.

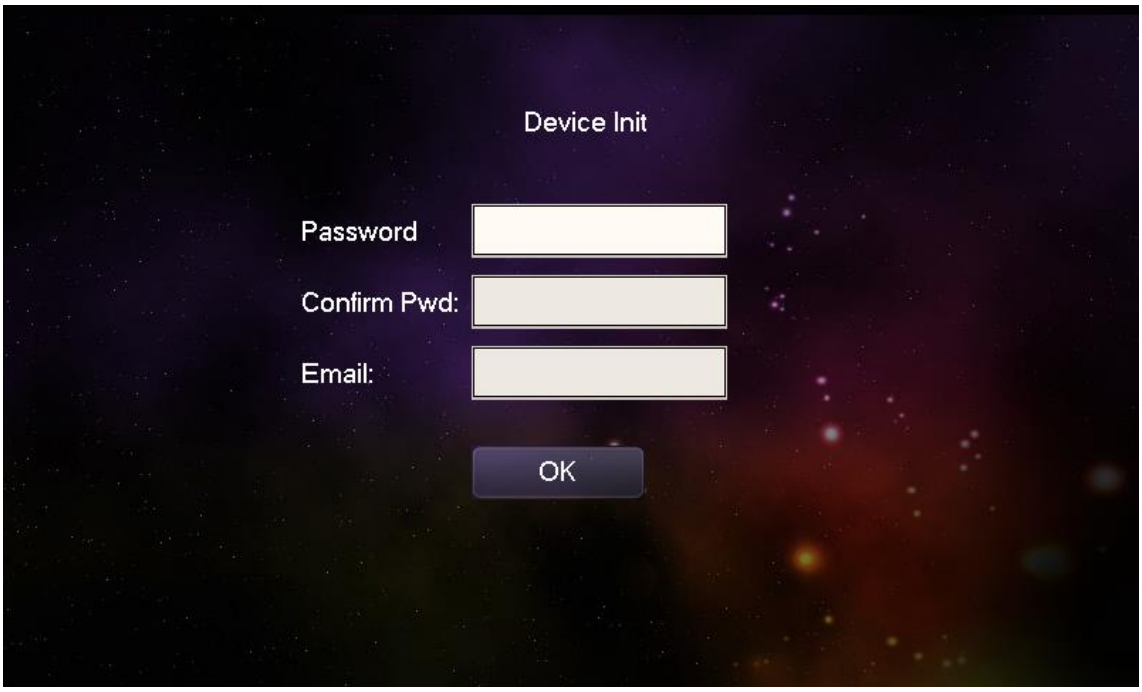

Figure 5-9

Step 2 Enter “Password”, “Confirm Pwd” and “Email”. Click [OK].

Step 3 Click “OK”.

The system displays “Info Init” interface. Press  to turn it off.

5.1.2.2 Network Setting

Set VTH network information; Support static IP and DHCP.

Note

- IP addresses of VTH and VTO shall be in the same network segment. Otherwise, VTH will fail to obtain VTO info after configuration.
- To obtain IP with DHCP, please ensure the connected router has DHCP function and DHCP function has been enabled.

Step 1 Select “System Config >Project Settings”.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and click [OK].

Step 3 Click [Net Set].

The system displays “Net Set” interface, as shown in Figure 5-10.

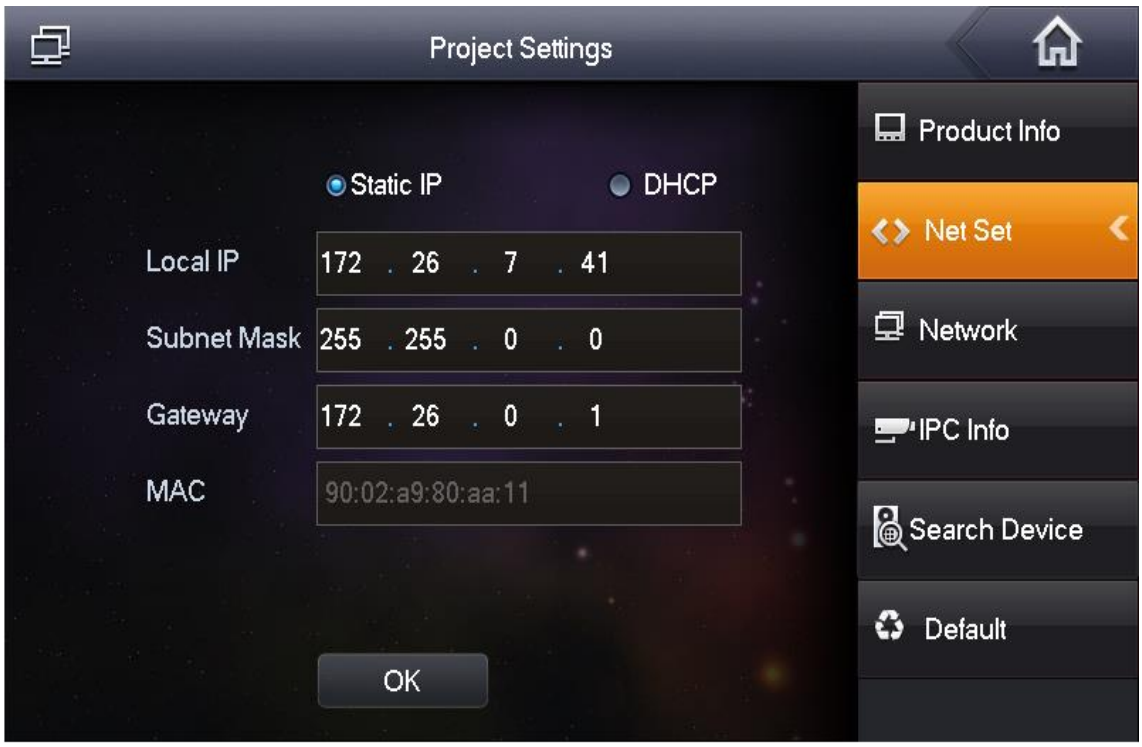

Figure 5-10

Step 4 Set according to actual network access mode.

- Static IP

1. Select “Static IP”.
2. Enter “Local IP”, “Subnet Mask” and “Gateway”.

- DHCP

Select “DHCP” to obtain IP address automatically.

Step 5 Click [OK] to save the settings.

5.1.2.3 Product Info

Set VTH “Room No.”, type and “Master IP”.

Step 1 Select “System Config >Project Settings”.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and click [OK].

Step 3 Press [Product Info].

The system displays “Product Info” interface, as shown in Figure 5-11.

Figure 5-11

Step 4 Set VTH info.

- Be used as a master VTH.

Enter “Room No.” (such as 9901).

Note

“Room no.” shall be the same with “VTH Short No.”, which is set when adding VTH at WEB interface. Otherwise, it will fail to connect VTO.

- Be used as an extension VTH.

1. Press [Master] and switch to “Extension”.
2. Enter “Room No.” (such as 9901-1) and “Master IP” (IP address of master VTH).

   Note

   “Username” and “Password” are the username and password of master VTH. Default username is admin, and the password is the one set during device initialization.

Step 5 Click [OK] to save the settings.

5.1.2.4 Set Network

Add VTO and fence station info; at VTH interface, bind VTH with VTO and fence station.

Step 1 Select “System Config >Project Settings”.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and click [OK].

Step 3 Press [Network].

The system displays “Network” interface, as shown in Figure 5-12.

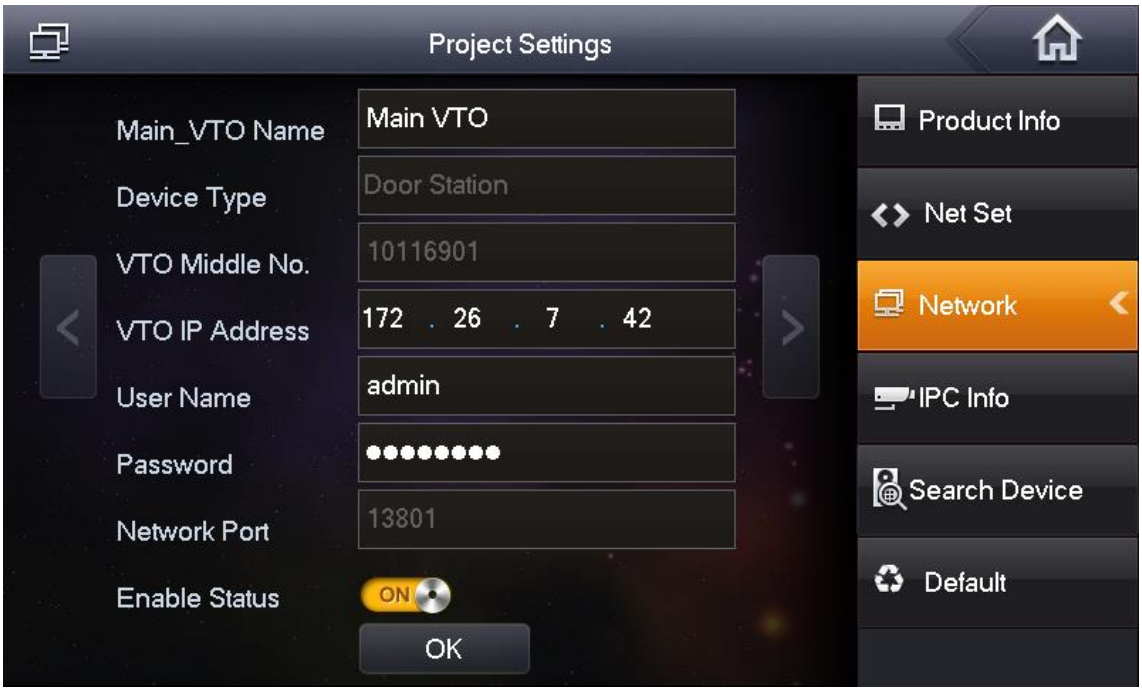

Figure 5-12

Step 4 Add VTO or fence station.

- Add main VTO.

1. In Figure 5-12, enter main VTO name, IP address, “Username” and “Password”.
2. Switch “Enable Status” to ON.

Note

- “Username” and “Password” shall be consistent with WEB login username and password of VTO. Otherwise, it will fail to connect.
- “Enable status” of main VTO is “ON” by default. After setting VTO info, please turn it off and then reboot, in order to put it into effect.

- Add fence station.

1. Press > to switch to sub VTO setting interface.
2. Select device type to be “fence station”; enter sub VTO name (fence station name), VTO middle no. (fence station middle no.), “Username” and “Password”.
3. Switch “Enable Status” to ON.

Step 5 Click [OK] to save the settings.

5.1.3 VTH Settings (Version 4.0)

5.1.3.1 Initialization

Set the password and bind your Email.

- Password: it is used to enter project setting interface.

- Email: it is used to retrieve your password when you forget it.

Step 1 Power on the device.

The system displays “Welcome” and enters “Device Initialization” interface, as shown in Figure 5-13.

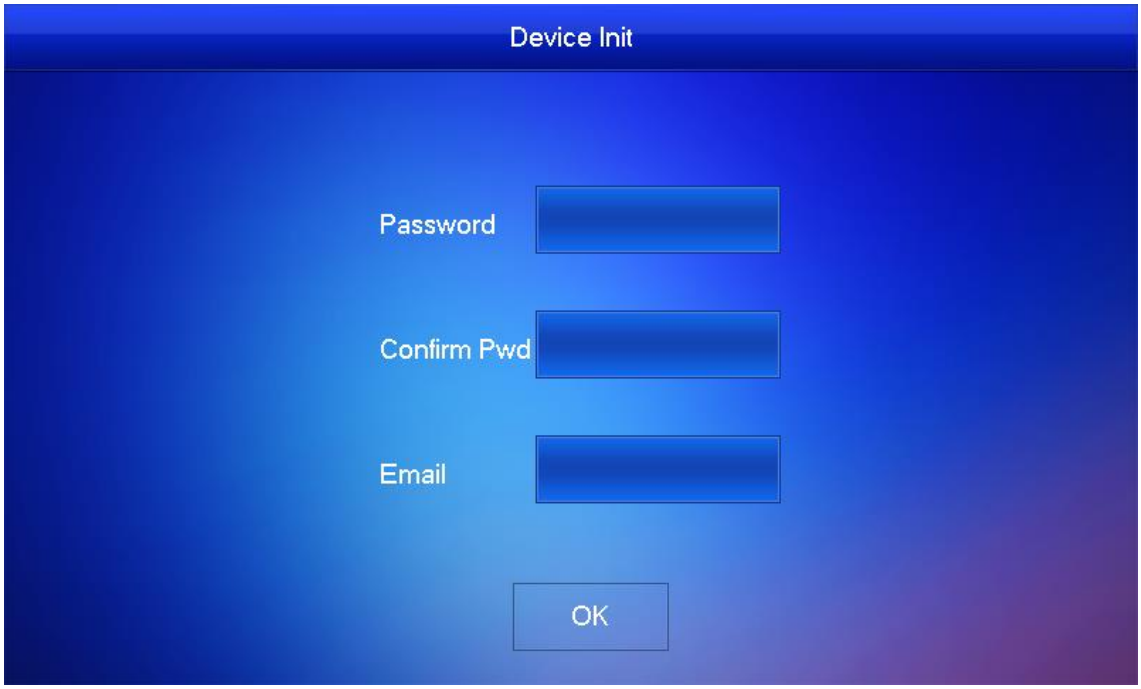

Figure 5-13

Step 2 Enter “Password”, “Confirm Pwd” and “Email”. Click [OK].

The system displays main interface.

5.1.3.2 Set Network

According to available network connection modes, configure VTH network information.

Note

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

Step 1 Press [Setting] for more than 6 seconds.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and click [OK].

Step 3 Click [Network].

The system displays “Network” interface, as shown in Figure 5-14 or Figure 5-15.

Note

Only devices with the wireless function can access to wireless network.

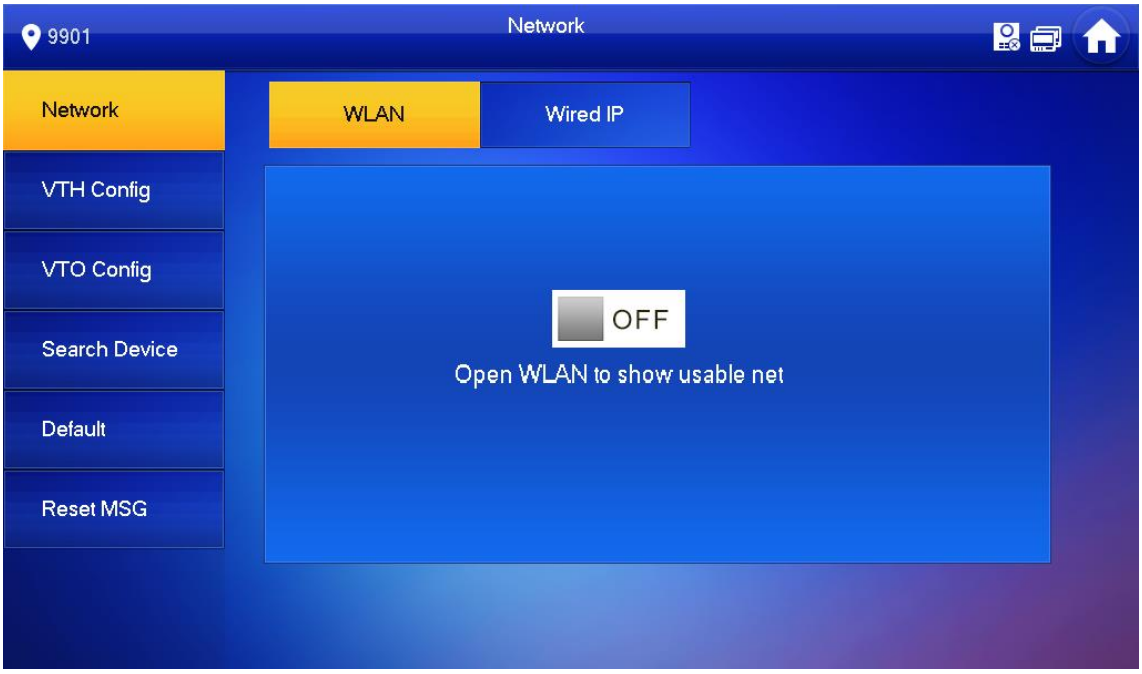

Figure 5-14

Figure 5-15

Step 4 Set according to actual network access mode.

- Wired IP

Enter “Local IP”, “Subnet Mask” and “Gateway”, press [OK]. Or press OFF to enable DHCP function and obtain IP info automatically.

Note

If the device has wireless function, please click “Wired IP” tab to set it.

- WLAN

1. Press OFF to enable WIFI function.

   The system displays available WIFI list, as shown in Figure 5-16.

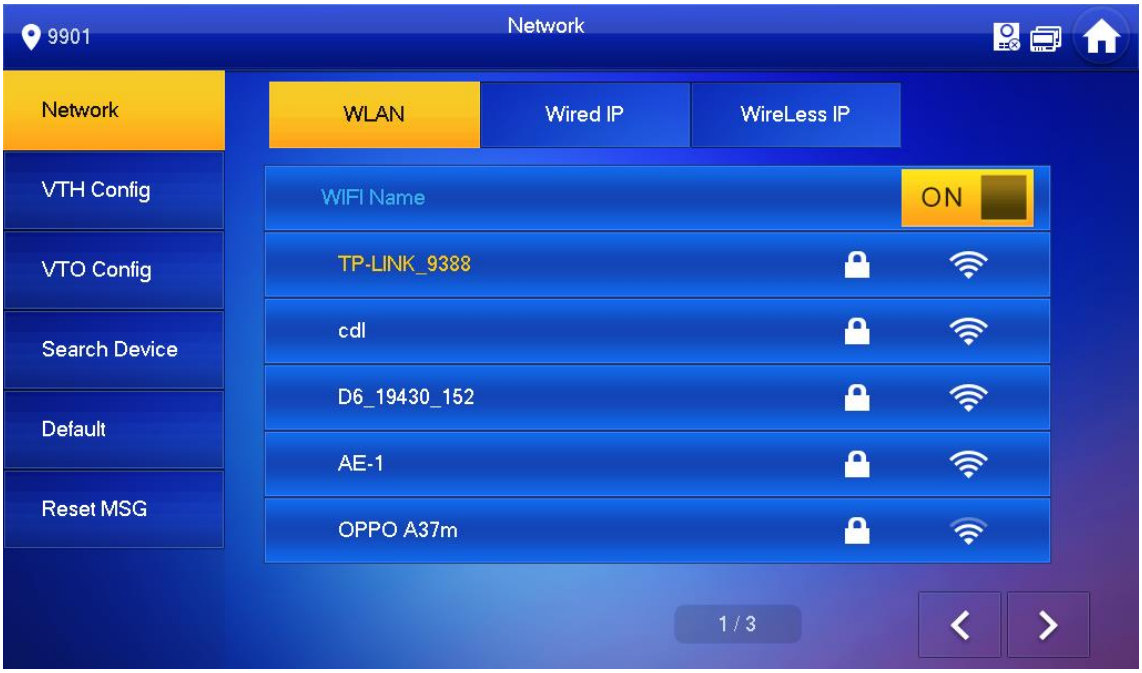

Figure 5-16

2. Connect WIFI.

   The system has 2 access ways as follows.

   ◇ At “WLAN” interface, select WIFI, click “Wireless IP” tab to enter “Local IP”, “Subnet Mask” and “Gateway”, and press [OK].

   ◇ At “WLAN” interface, select WIFI, click “Wireless IP” tab, press OFF to enable DHCP function and obtain IP info automatically, as shown in Figure 5-17.

   Note

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

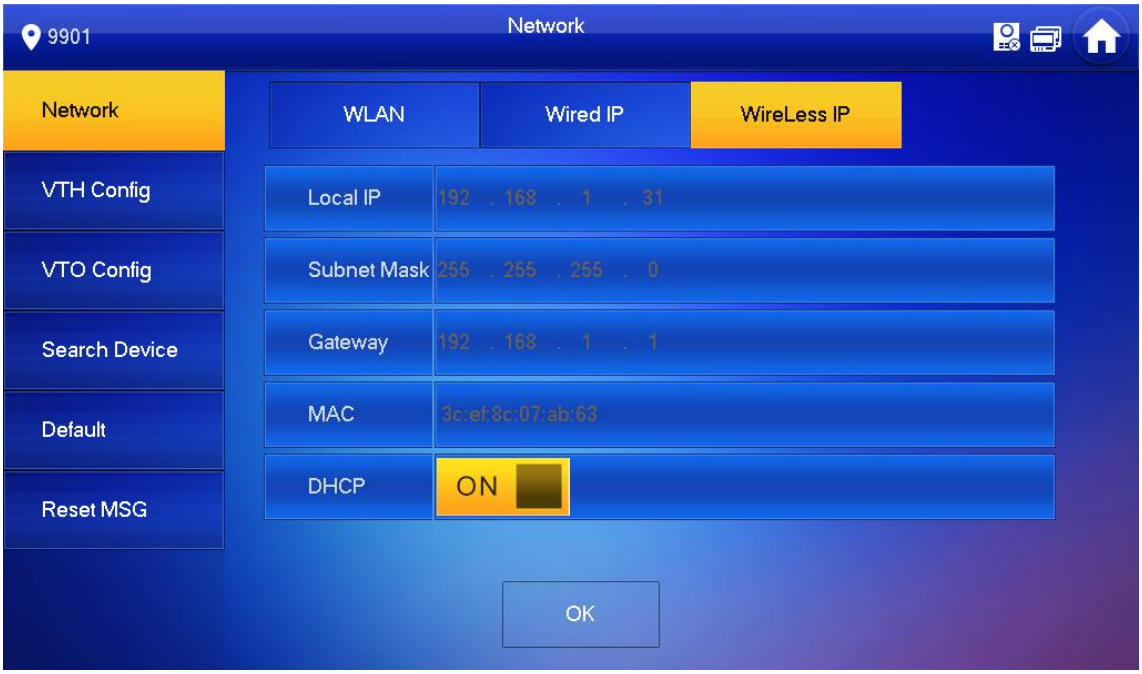

Figure 5-17

5.1.3.3 VTH Config

Set VTH “Room No.”, type and “Master IP”.

Step 1 Press [Setting] for more than 6 seconds.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and click [OK].

Step 3 Click [VTH Config].

The system displays “VTH Config” interface, as shown in Figure 5-18.

Figure 5-18

Step 4 Set VTH info.

- Be used as a master VTH.

Enter “Room No.” (such as 9901).

Note

“Room no.” shall be the same with “VTH Short No.”, which is set when adding VTH at WEB interface. Otherwise, it will fail to connect VTO.

- Be used as an extension VTH.

1. Press [Master] and switch to “Extension”.
2. Enter “Room No.” (such as 9901-1) and “Master IP” (IP address of master VTH).

   Note

   “Master Name” and “Master Pwd” are the username and password of master VTH. Default username is admin, and the password is the one set during device initialization.

Step 5 Press [OK] to save settings.

5.1.3.4 VTO Config

Add VTO and fence station info; at VTH interface, bind VTH with VTO and fence station.

Step 1 Press [Setting] for more than 6 seconds.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and click [OK].

Step 3 Click [VTO Config].

The system displays “VTO Config” interface, as shown in Figure 5-19.

Figure 5-19

Step 4 Add VTO or fence station.

- Add main VTO.

1. In Figure 5-19, enter main VTO name, VTO IP, “Username” and “Password”.
2. Switch the “Enable Status” to be ON.

Note

- “Username” and “Password” shall be consistent with WEB login username and password of VTO. Otherwise, it will fail to connect.
- “Enable Status” of main VTO is “ON” by default. After setting VTO info, it will take effect after turning it off and then turning it on again.

- Add fence station.

1. Press to switch to sub VTO setting interface.
2. Select device type to be “Fence Station”, enter Sub VTO name (fence station name), middle no. (fence station no.), “Username” and “Password”.
3. Switch the “Enable Status” to be ON.

5.2 Debugging Verification

5.2.1 Verification with Version 3.1 VTH

5.2.1.1 VTO Calls VTH

Press call key at VTO, to call VTH. VTH pops up monitoring image and operating keys, as shown in Figure 5-20. It represents successful debugging.

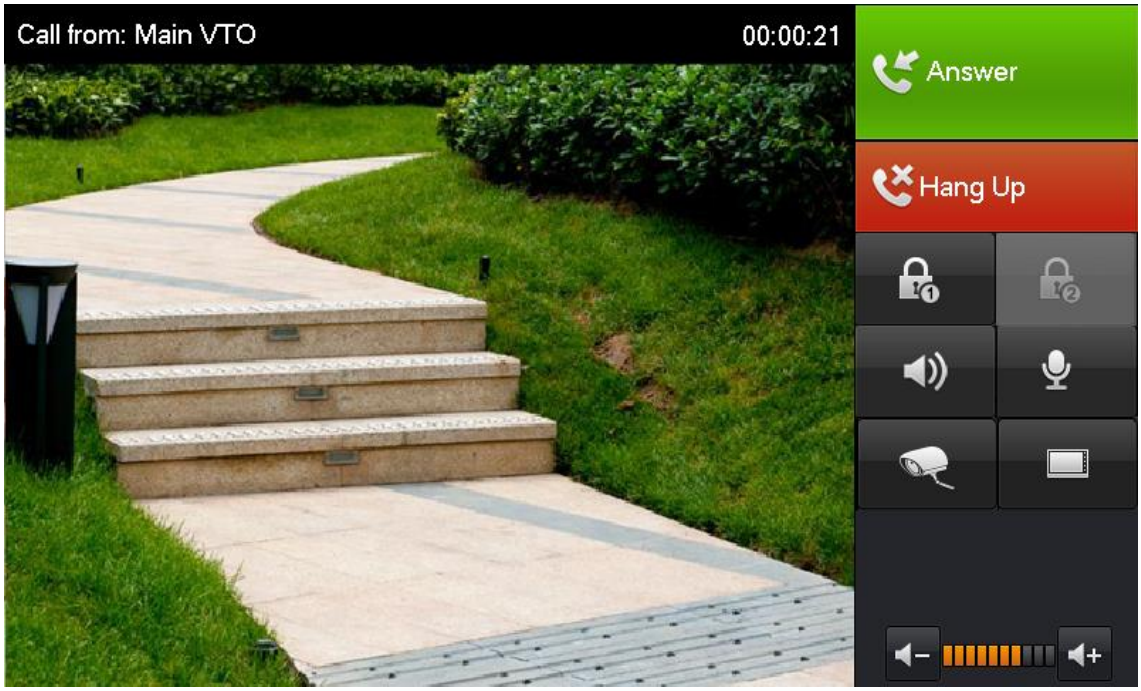

Figure 5-20

5.2.1.2 VTH Monitors VTO

VTH is able to monitor VTO, fence station or IPC. Take “VTO” for example.

Select “Video Talk > Monitor > Door Station”, as shown in Figure 5-21. Select the VTO to enter monitoring image, as shown in Figure 5-22.

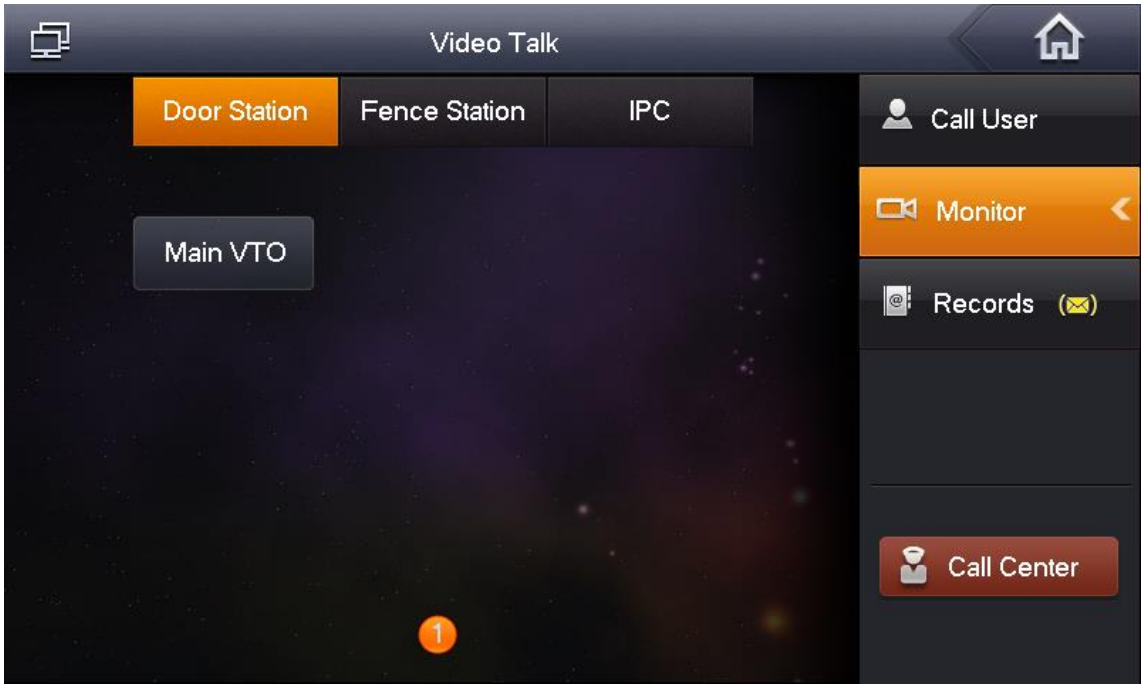

Figure 5-21

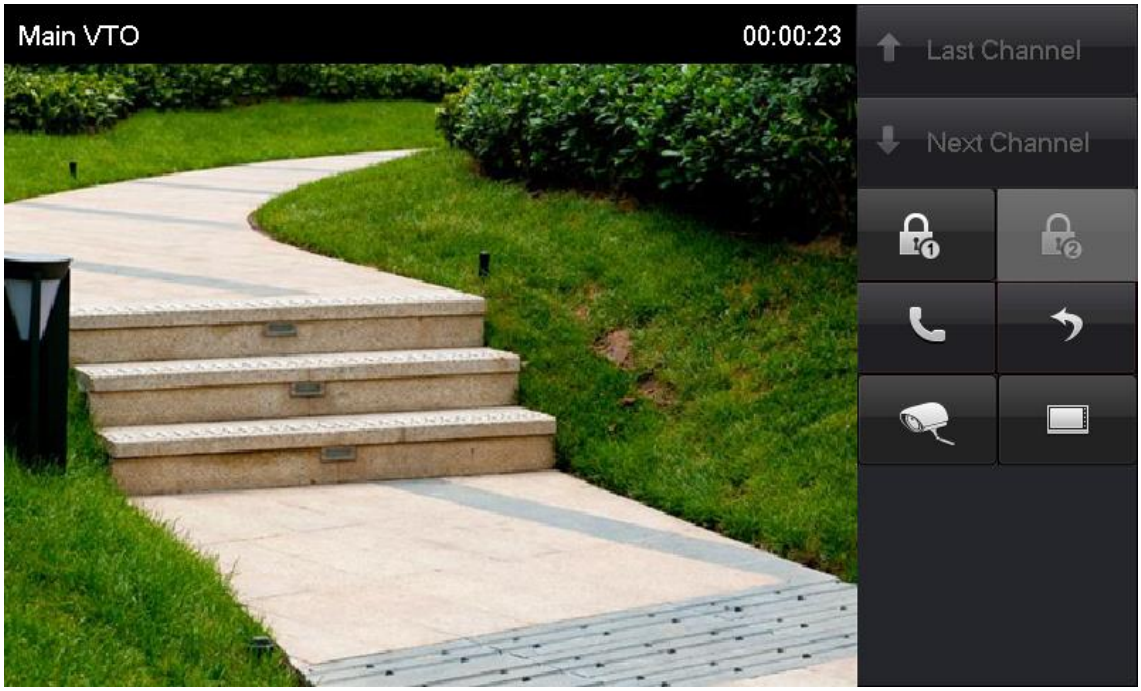

Figure 5-22

5.2.2 Verification with Version 4.0 VTH

5.2.2.1 VTO Calls VTH

Press call key at VTO, to call VTH. VTH pops up monitoring image and operating keys, as shown in Figure 5-23. It represents successful debugging.

Note

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

Figure 5-23

5.2.2.2 VTH Monitors VTO

VTH is able to monitor VTO, fence station or IPC. Take “VTO” for example.

Select “Monitor > Door”, as shown in Figure 5-24. Select the VTO to enter monitoring image, as shown in Figure 5-25.

Note

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

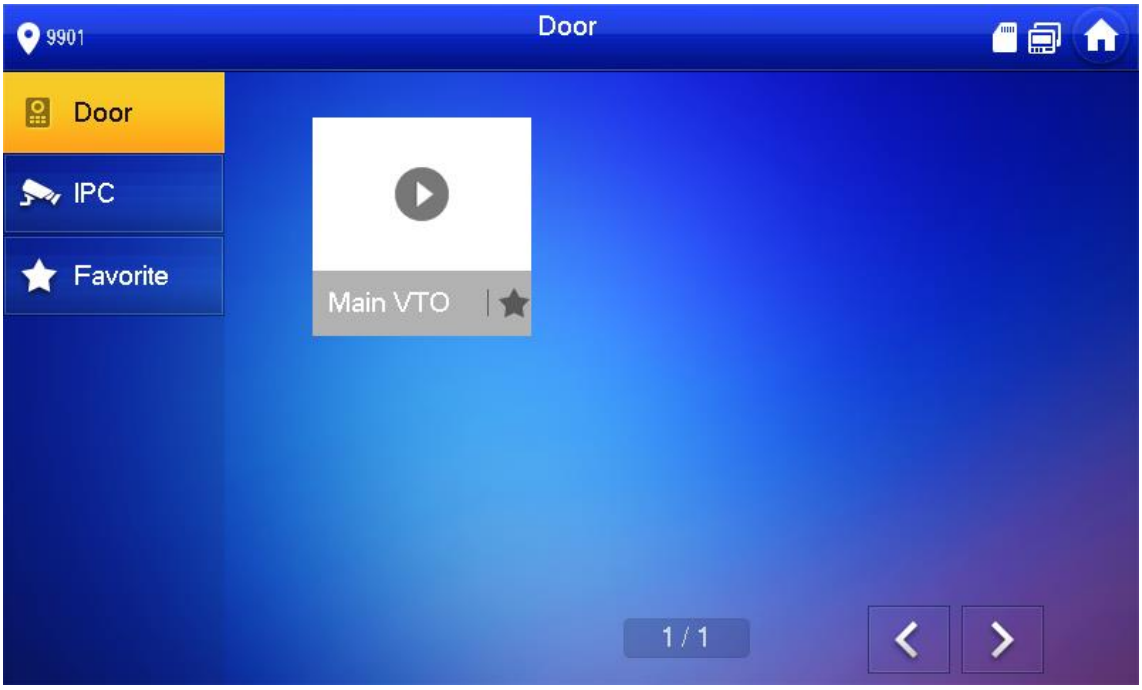

Figure 5-24

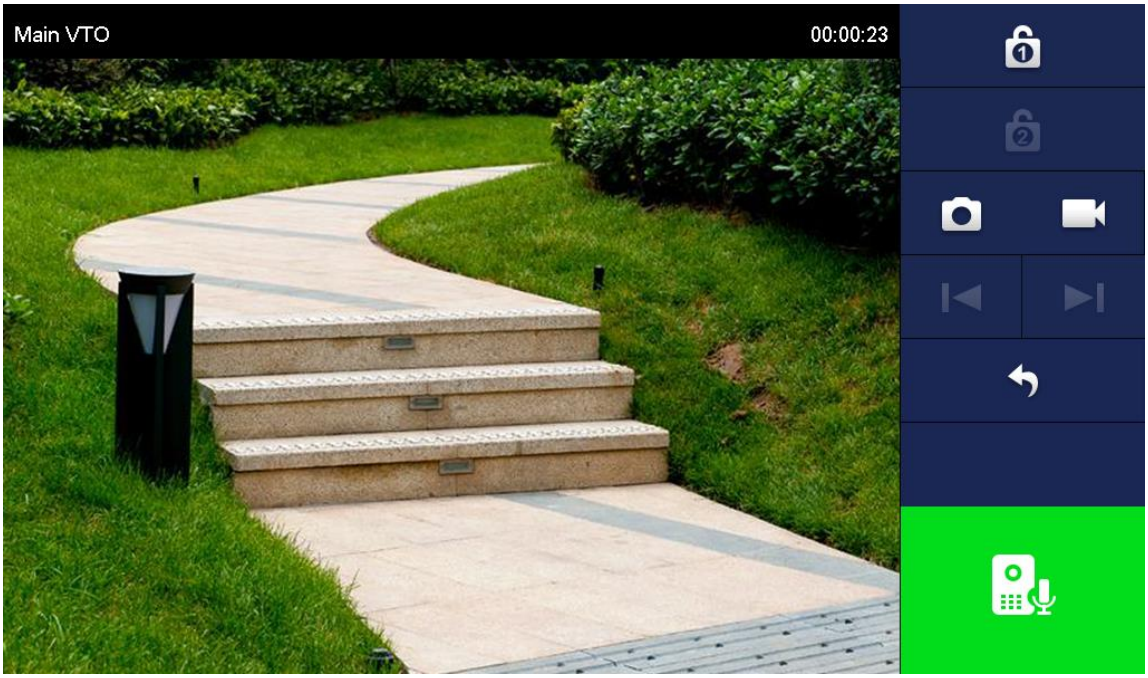

Figure 5-25

6 Basic Function

6.1 Call Function

6.1.1 Call Management Centre

Press the call key of VTO within the set time period, to call management centre only and realize video talk.

Configure the following parameters before calling.

Step 1 Select “System Config >LAN Config”.

The system displays “LAN Config” interface.

Step 2 Select “Register to the MGT Centre”; set “MGT Centre IP Address” and “MGT Port No.”.

Register the VTO at management center.

Step 3 Set “Call VTS Time” and select “Call VTS or Not”.

Enable to call the management centre within the set time period.

Step 4 Click “OK” to save the settings.

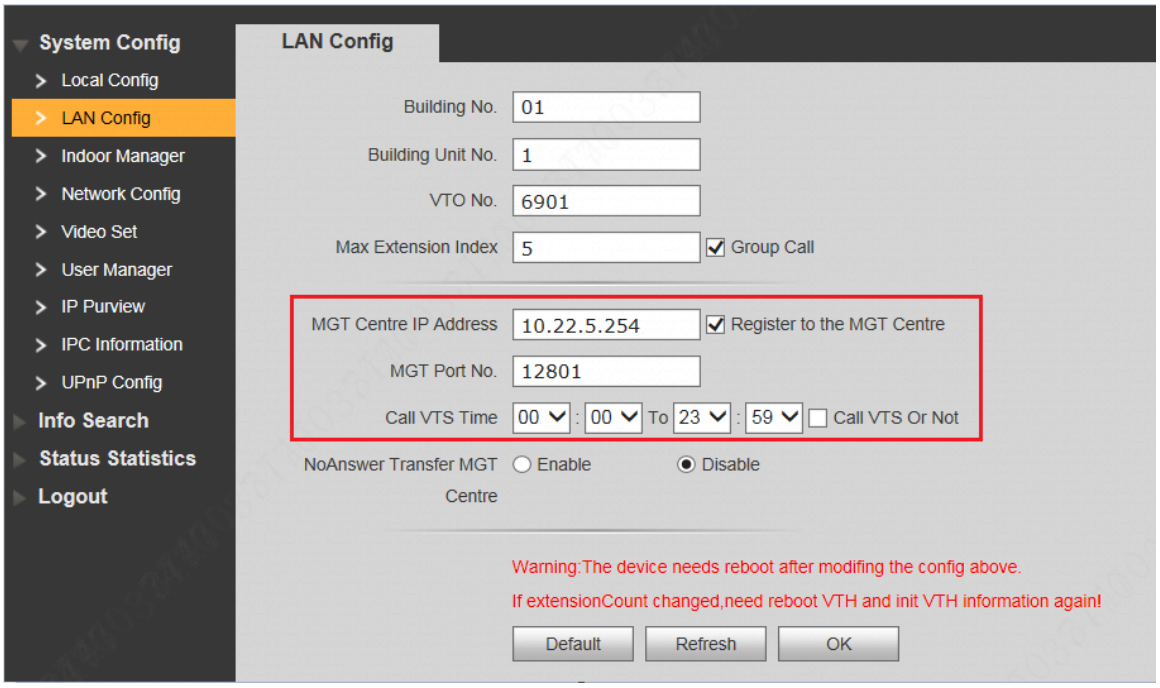

Figure 6-1

6.1.2 Single Call of VTH

Single call applies to the scene where one door corresponds to one VTH. Press the call key of VTO, to call the VTH directly.

To realize single call function, ensure that VTO doesn't enable call of management centre. Specific settings are as follows.

Step 1 Select "System Config > LAN Config".

The system displays "LAN Config" interface.

Step 2 Confirm if you select "Call TVS or Not".

If it is not selected, press the call key to call VTH; if it is selected, please cancel the selection.

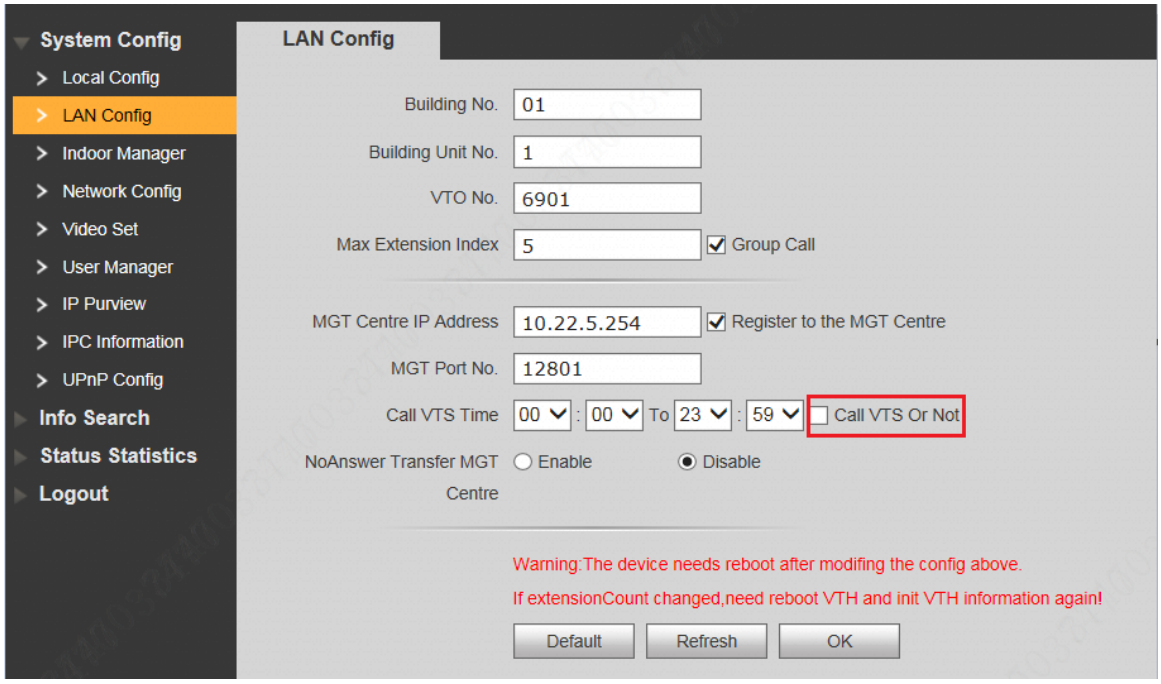

Figure 6-2

6.1.3 Group Call

Group call applies to the scene where one door corresponds to multiple VTHs. Press the call key of VTO, to call multiple VTHs directly.

Caution

- Please ensure that single call between VTO and VTH works normally. If single call fails, please check the configuration by reference to "5.1 Debugging Settings".
- Room no. of extension VTH ends up with "-1, -2…" based on room no. of master VTH. For example, if master VTH is 9901, the extension VTH will be 9901-1, 9901-2…
- At WEB interface of VTO, select "System Config > LAN Config", set "Max Extension Index" and tick "Group Call" to enable group call function. There is one master VTH at most and five extension VTHs at most, as shown in Figure 6-3.
- Please confirm that "Call VTS or Not" has been canceled, as shown in Figure 6-3.

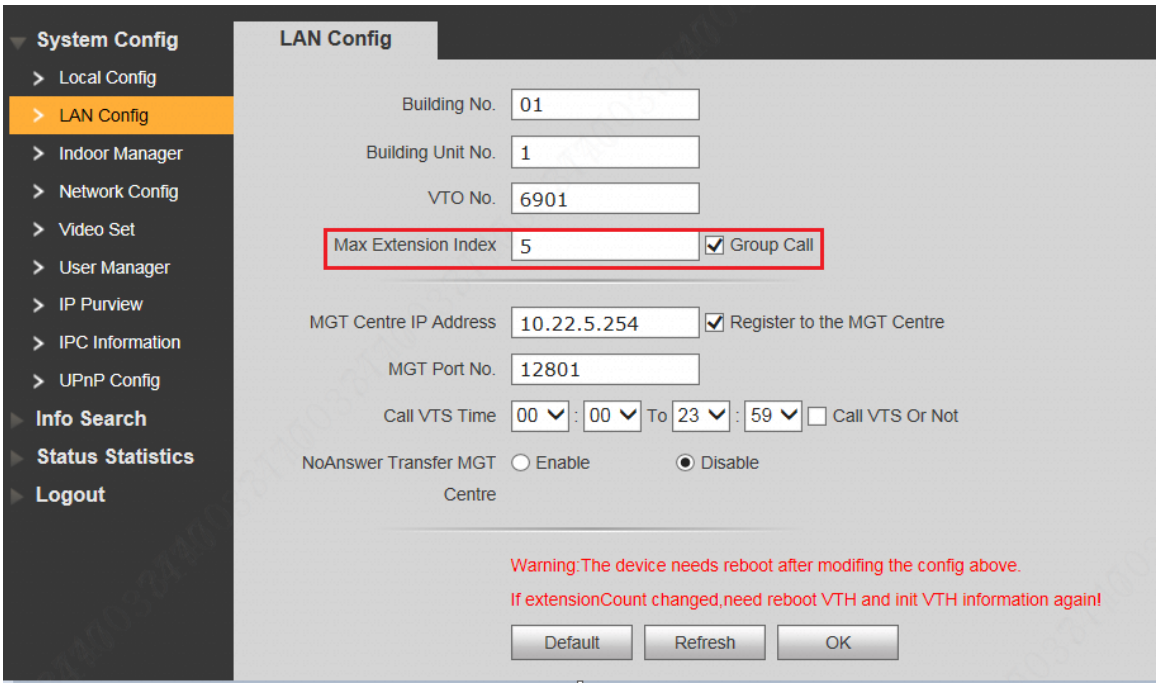

Figure 6-3

6.2 Unlock Function

6.2.1 Remote Unlock at VTH/VTS

When being called, during monitoring and calling status, the VTO will be unlocked remotely at VTS or VTH.

6.2.2 Open Door at WEB Interface

Step 1 Select “System Config >Video Set>Video Set”.
The system displays “Video Set” interface.
Step 2 Click “Open Door”, and VTO is unlocked, as shown in Figure 6-4.

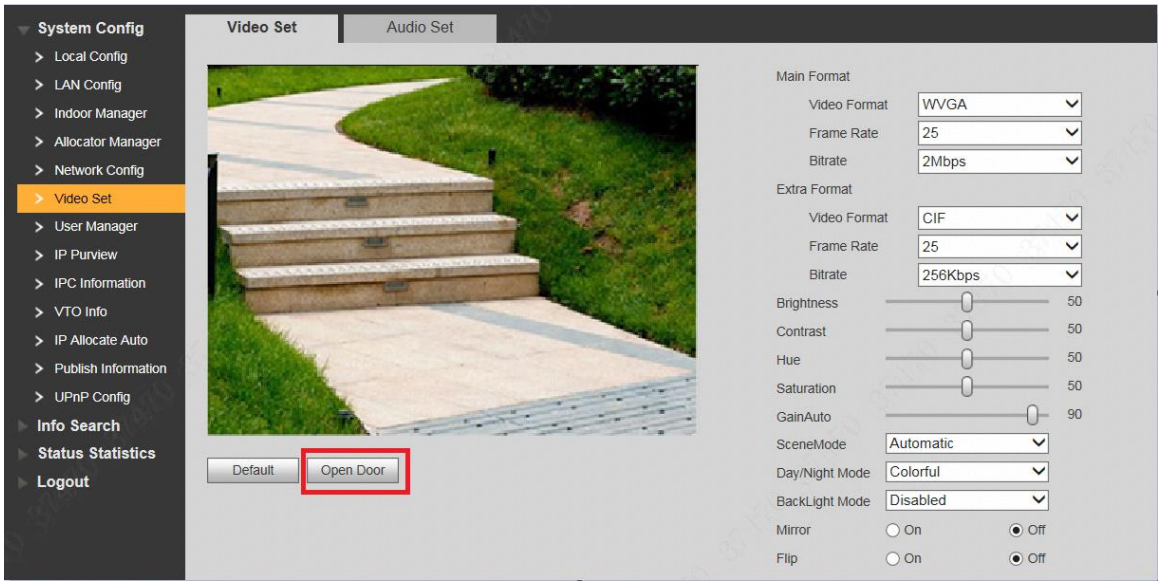

Figure 6-4

6.2.3 Unlock with IC Card

Swipe the authorized IC card at VTO, so as to open the door.

Note

- Only some models of devices support this function.
- Authorized IC card refers to a card that is issued and authorized to open the door. For card issuing operation, please refer to “6.3 Issue Card”.

6.2.4 Unlock with Exit Button

If VTO is connected with exit button, press the exit button to open the door.

6.3 Issue Card

Authorize IC card at VTO WEB interface, so the user can open door with authorized card.

Note

Some models of devices don’t support this function.

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

The system displays “A&C Manager” interface, as shown in Figure 6-5.

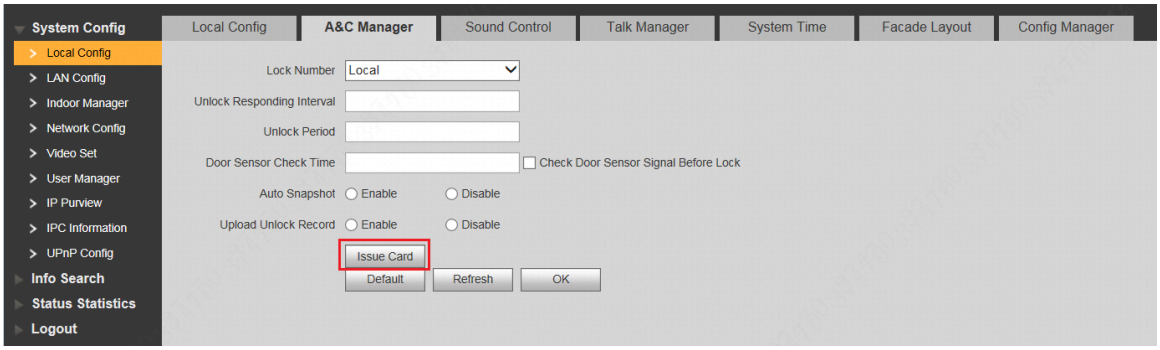

Figure 6-5

Step 2 Click “Issue Card”.

The system displays 30s countdown, as shown in Figure 6-6.

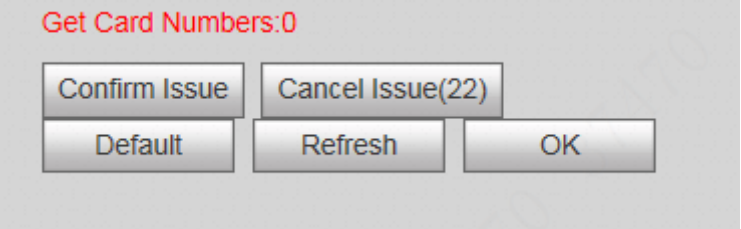

Figure 6-6

Step 3 Within 30s countdown, swipe an unauthorized card at VTO.

The system pops up “Card Info” interface, as shown in Figure 6-7.

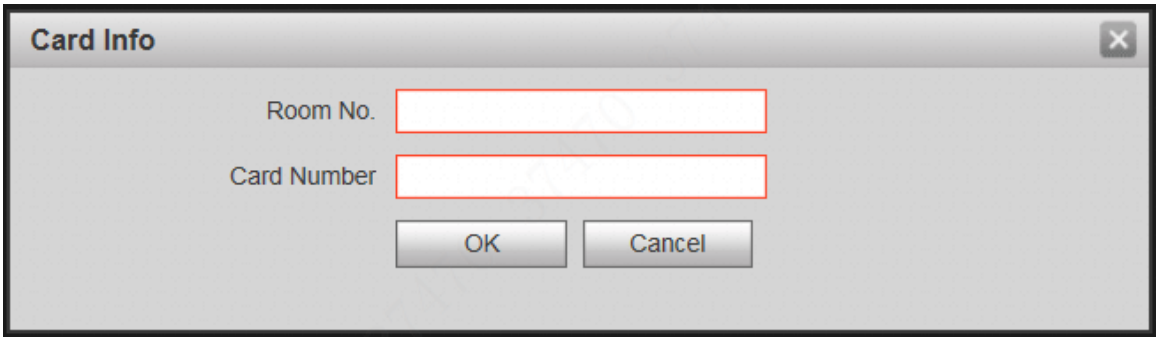

Figure 6-7

Step 4 Enter “Room No.” and “Card No.”.

Note

Cards can be swiped continuously, within a period of 30s.

Step 5 Click “OK” to finish issuing card.

Note

- Click “OK” within the countdown, so the cards will be valid. Otherwise, all card info will be invalid.
- Click “Cancel” when issuing cards, in order to stop issuing.

6.4 Monitoring Function

Both VTS and VTH can monitor the VTO.

VTO supports multi-channel stream monitoring. Available channels vary under different video formats. Support max. 4 channels with 720P, and support max. 6 channels with WVGA.

Video format is set as follows:

Step 1 At VTO WEB interface, select “System Config >Video Set>Video Set”.

The system displays “Video Set” interface.

Step 2 Select “Video Format”.

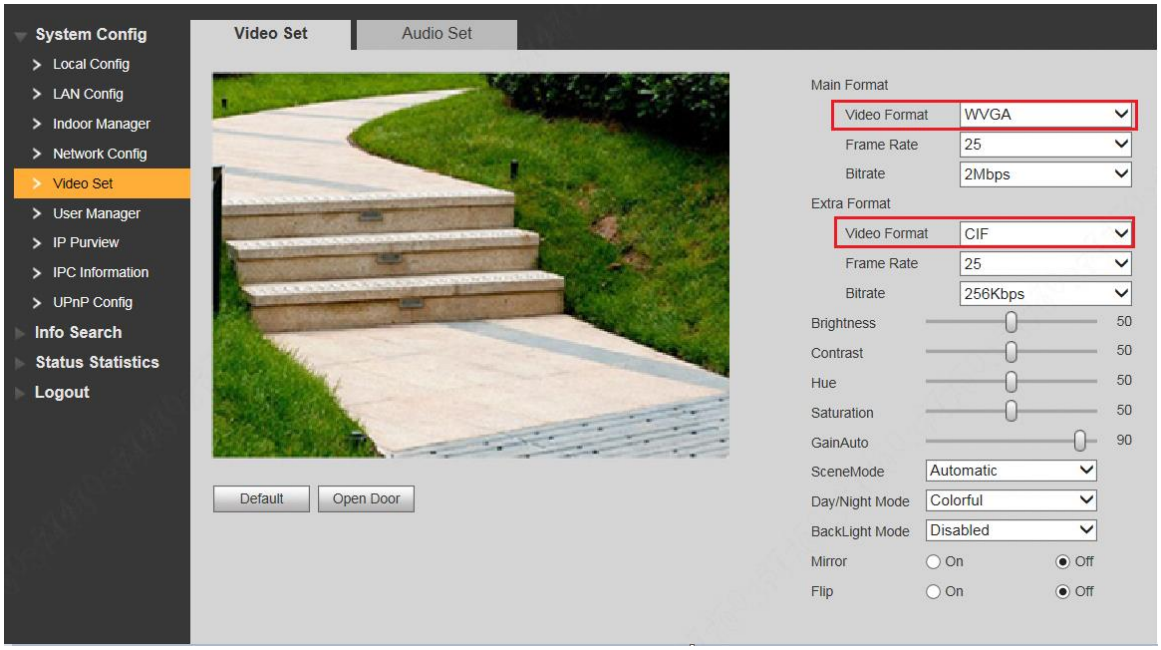

Figure 6-8

6.5 Tamper Switch

VTO is equipped with a tamper switch against the wall. In case that the device is disassembled from the wall, tamper switch will leave the wall too. The device will emit tamper alarm sound and report alarm info to management centre.

6.6 Restore Backup

If VTH info or card no. info is modified by mis-operation during use, two restoration ways are available to restore them.

Caution

VTO saves VTH info of the system automatically every half an hour. If VTH info is modified by mis-operation, please restore them timely. Otherwise, the system will automatically save mis-operation info after half an hour.

Restore from backup data in device memory

Step 1 Select “System Config >Local Config > Config Manager”.
The system displays “Config Manager” interface, as shown in Figure 6-9.

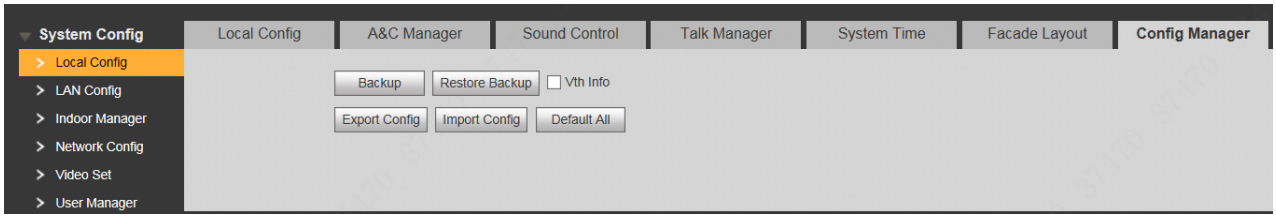

Figure 6-9

Step 2 Select “VTH Info” and click “Restore Backup”.

Backup VTH info in the device will be restored to VTO.

Restore from local backup data

Step 1 Select “System Config >Indoor Manager”.

The system displays “Digital Indoor Station Manager” interface, as shown in Figure 6-10.

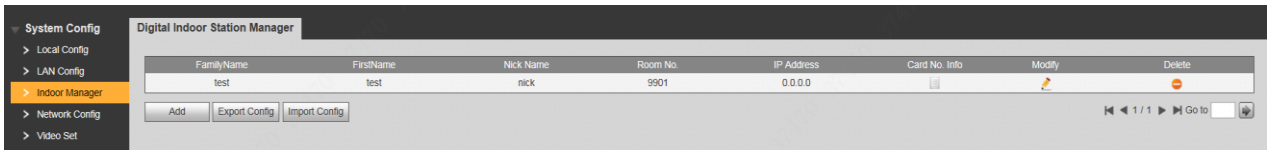

Figure 6-10

Step 2 Click “Import Config”. The system displays “Open” interface.

Step 3 Select config files (.log) and click “Open”.

The system displays “Success” to complete importing config.

7.1 Initialization

Caution

- For the first login or login after restoring factory defaults, please initialize WEB interface.
- Please ensure that default IP addresses of PC and VTO are in the same network segment. Otherwise, it fails to enter initialization interface.

Step 1 Enter default IP address of VTO at the address bar of PC browser, and press [Enter] key.
The system displays “Setting” interface, as shown in Figure 7-1.

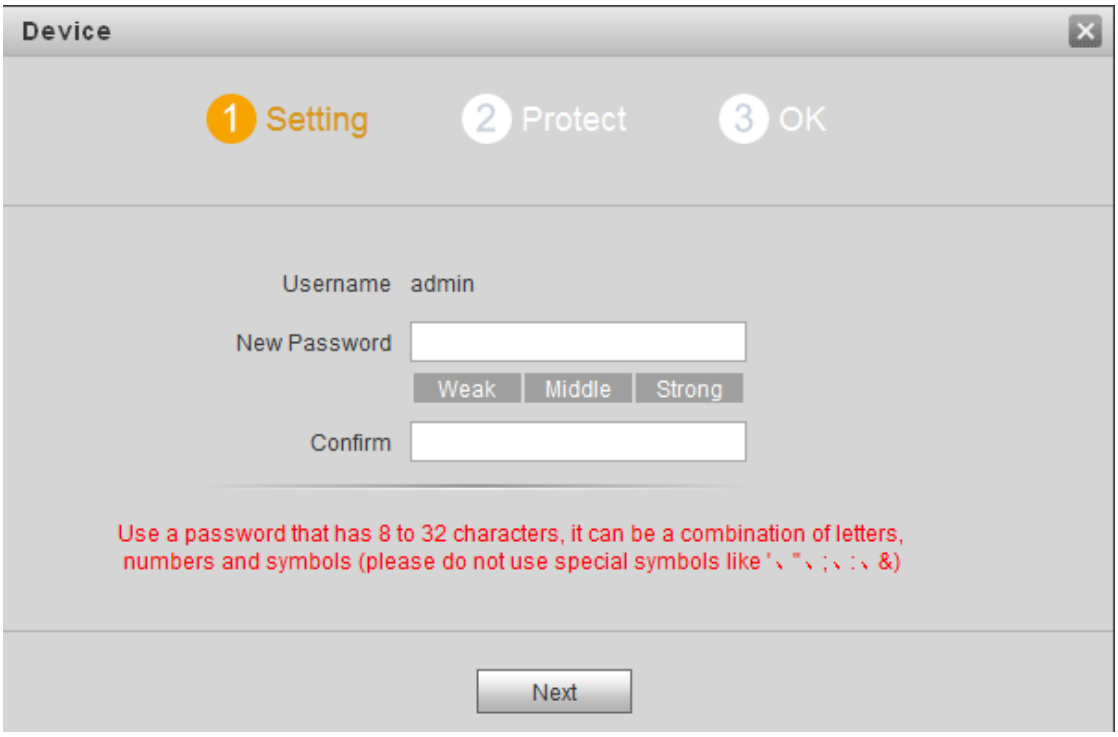

Figure 7-1

Step 2 Enter “New Password” and “Confirm”, and click “Next”.
The system displays “Protect” interface, as shown in Figure 7-2.
This password is used to login WEB interface. It shall be at least 8 characters, and shall include at least two types of number, letter and symbol.

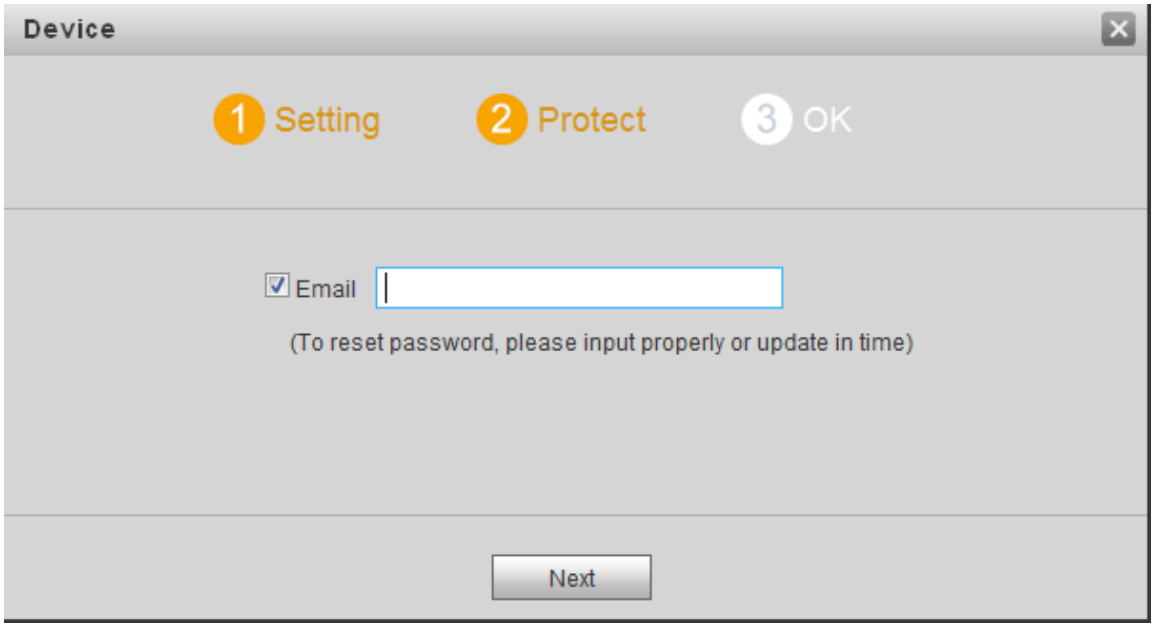

Figure 7-2

Step 3 Select “Email” and enter your Email address.

This Email address is used to reset the password, so it is recommended that it should be set.

Step 4 Click “Next”. The system displays “OK” interface, as shown in Figure 7-3, and shows “Device succeeded!”

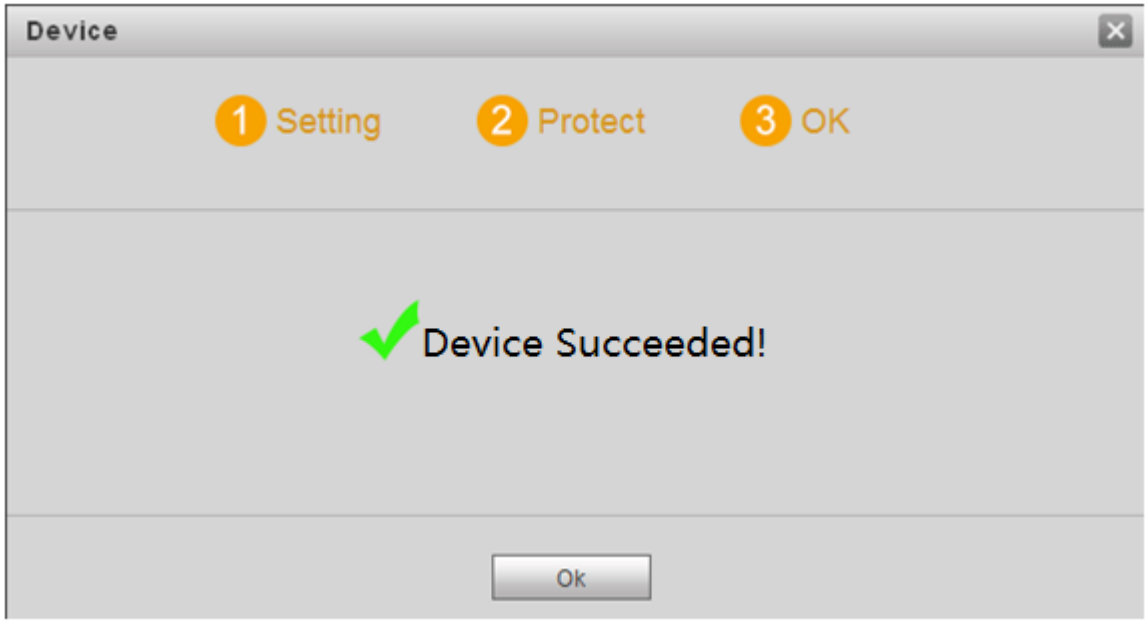

Figure 7-3

Step 5 Click “OK”.

The system displays WEB login interface.

7.2 Reset the Password

If you forget login password of admin user, please reset the login password by scanning QR code.

Step 1 Enter IP address of VTO at the address bar of PC browser, and press [Enter] key.
The system displays login interface, as shown in Figure 7-4.

Figure 7-4

Step 2 Click “Forgot Password”.
The system displays “Reset the password” dialog box, as shown in Figure 7-5.

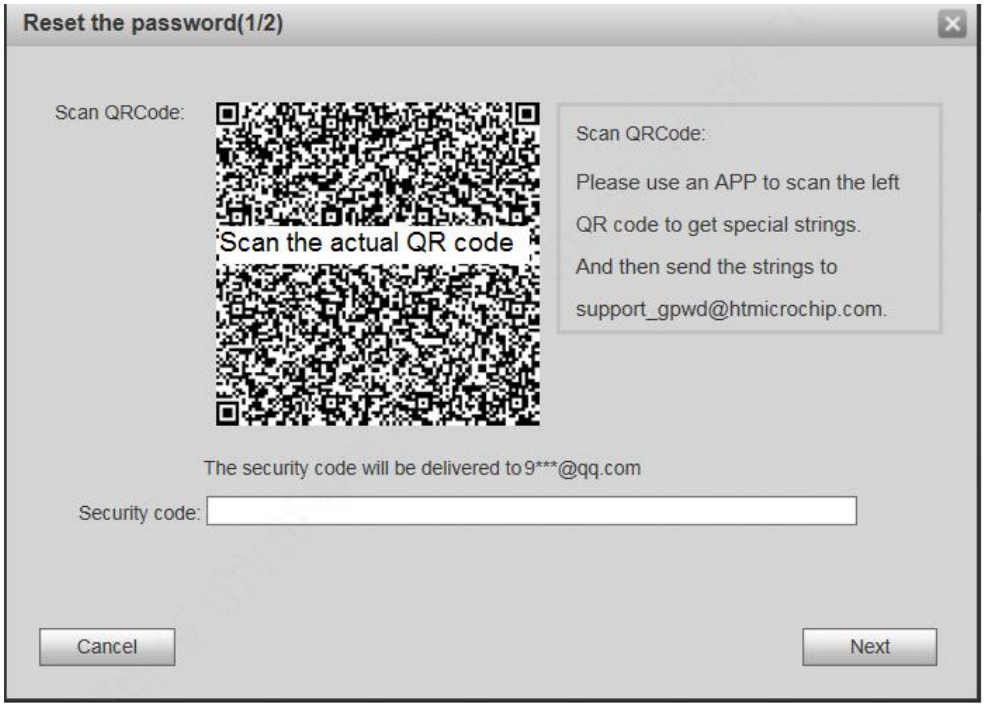

Figure 7-5

Step 3 Scan the QR code according to interface prompts and obtain security code.

Caution

- Two security codes can be obtained by scanning the same QR code. To obtain security code again, please refresh QR code.
- After receiving security code in your Email, please reset the password with the security code within 24 hours. Otherwise, the security code will become invalid.
- If wrong security code is entered for 5 times continuously, this account will be locked for 5 min.

Step 4 Please enter the received security code in the dialog box.

Step 5 Click “Next”.

The system displays new password setting interface, as shown in Figure 7-6.

Figure 7-6

Step 6 Set “New Password” and “Confirm”.

Password can be 8 to 32 non-null characters; it consists of letters, numbers and symbols (except “'”, “"”, “;”, “:” and “&”). The password shall consist of 2 types or over 2 types. Please set a high-security password according to password strength prompt.

Step 7 Click “OK” to complete resetting.

7.3 System Login

Caution

Please ensure that IP addresses of PC and VTO are in the same network segment; otherwise, it fails to enter WEB login interface.

Step 1 Enter IP address of VTO at the address bar of PC browser, and press [Enter] key.

The system displays WEB login interface, as shown in Figure 7-7.

Figure 7-7

Step 2 Enter username and password, and click “Login”.

Log in the WEB interface of the device.

Note

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

7.4 User Manager

Add, delete and modify WEB user info.

Select “System Config > User Manager”. The system displays “User Manager” interface, as shown in Figure 7-8.

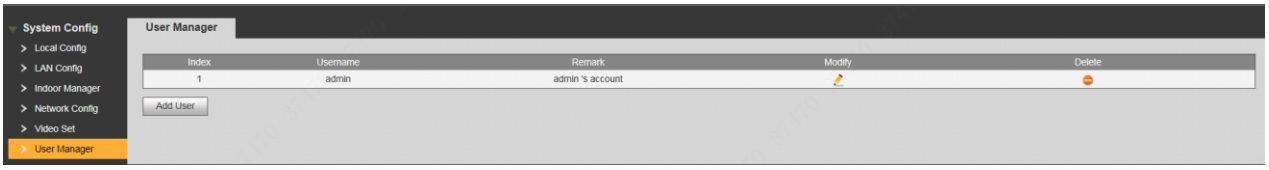

Figure 7-8

7.4.1 Add User

The added user enjoys all operating authorities except adding user and admin user management.

Step 1 Click “Add User”.

The system displays “Add User” interface, as shown in Figure 7-9.

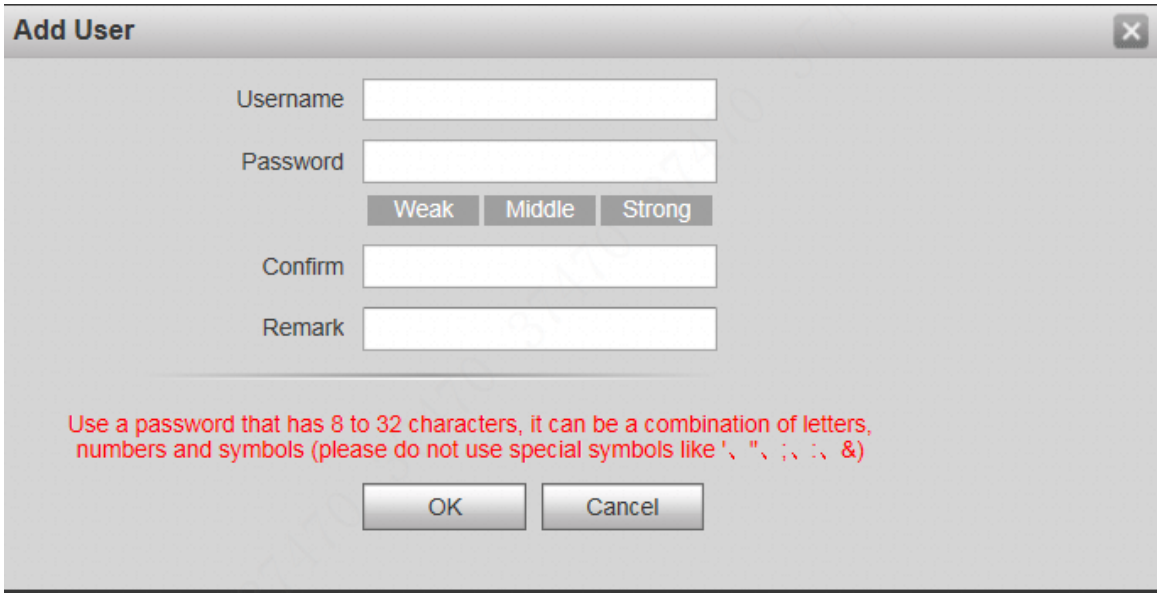

Figure 7-9

Step 2 Enter “Username”, “Password”, “Confirm” and remark.

Note

Password is required to be at least 8 characters, and shall include at least two types of number, letter and symbol.

Step 3 Click “OK” to complete adding.

7.4.2 Modify User

7.4.2.1 Modify Admin User

Admin user can modify his/her own user password and Email address. Email address is used to reset the password and receive info.

Step 1 Click  in the line of admin user info.

The system displays “Modify User” interface, as shown in Figure 7-10.

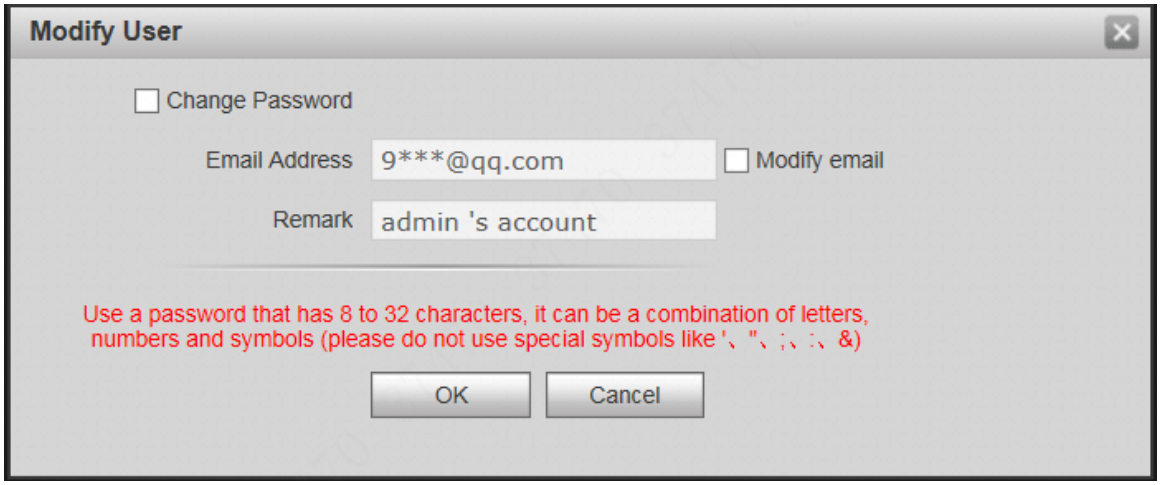

Figure 7-10

Step 2 Modify user info.

1. Tick “Change Password”.

The system displays password change interface, as shown in Figure 7-11.

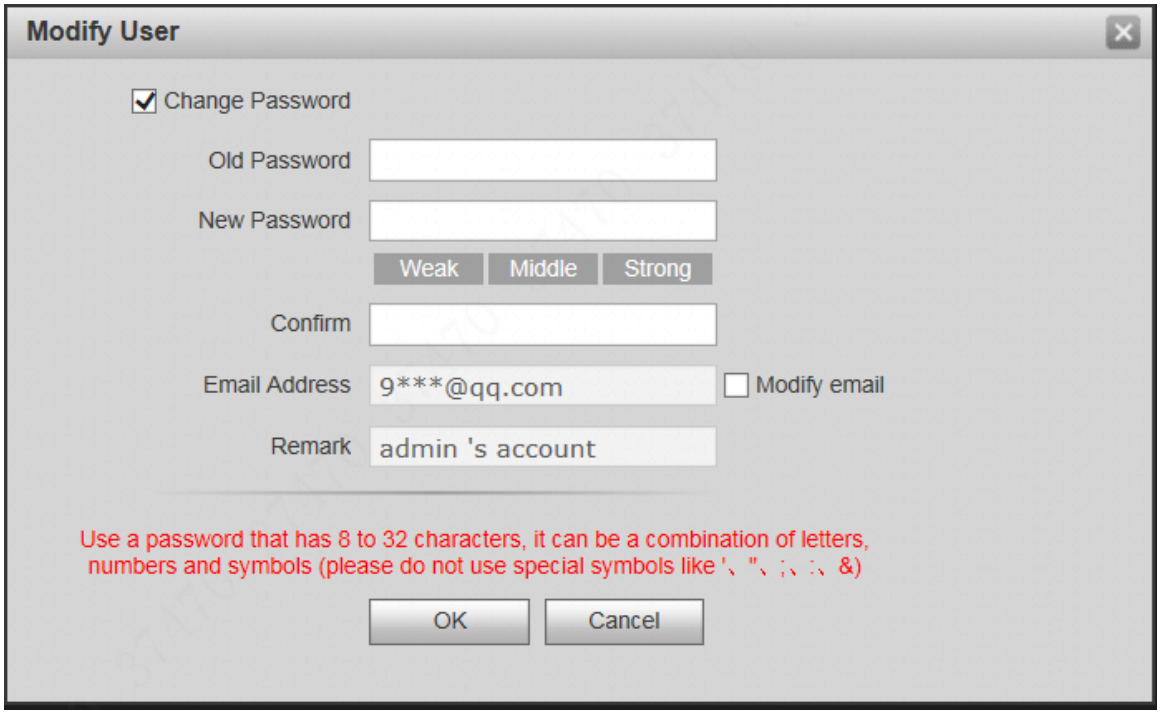

Figure 7-11

2. Enter “Old Password”, “New Password” and “Confirm”.
3. Tick “Modify Email” to enter Email address.
4. Click “OK”.

7.4.2.2 Modify Ordinary User

Ordinary user refers to other uses except admin user. Admin user can modify remark and password of all other users, while ordinary user can modify his/her own password only. Take admin user modifying ordinary user for example.

Step 1 Click  in the line of ordinary user info.

The system displays “Modify User” interface, as shown in Figure 7-12.

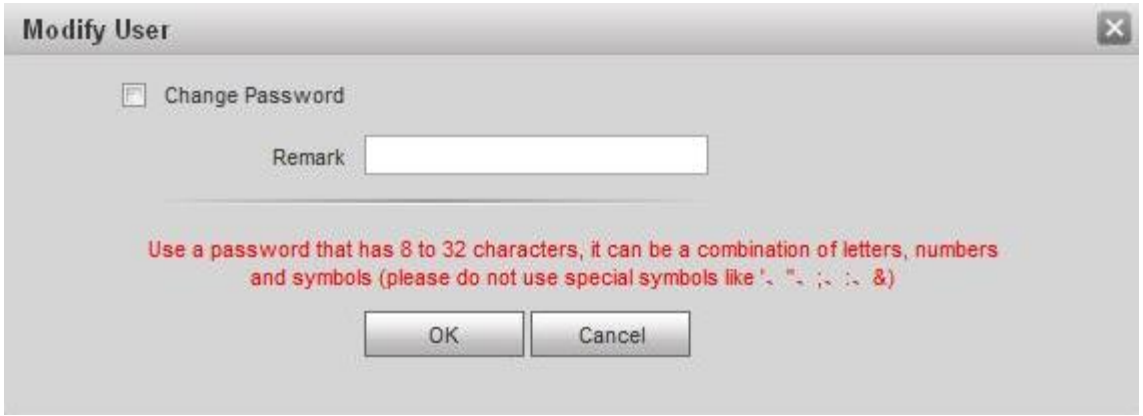

Figure 7-12

Step 2 Modify user info, as shown in Figure 7-13.

1. Tick “Change Password”.

   The system displays password change interface, as shown in Figure 7-13.

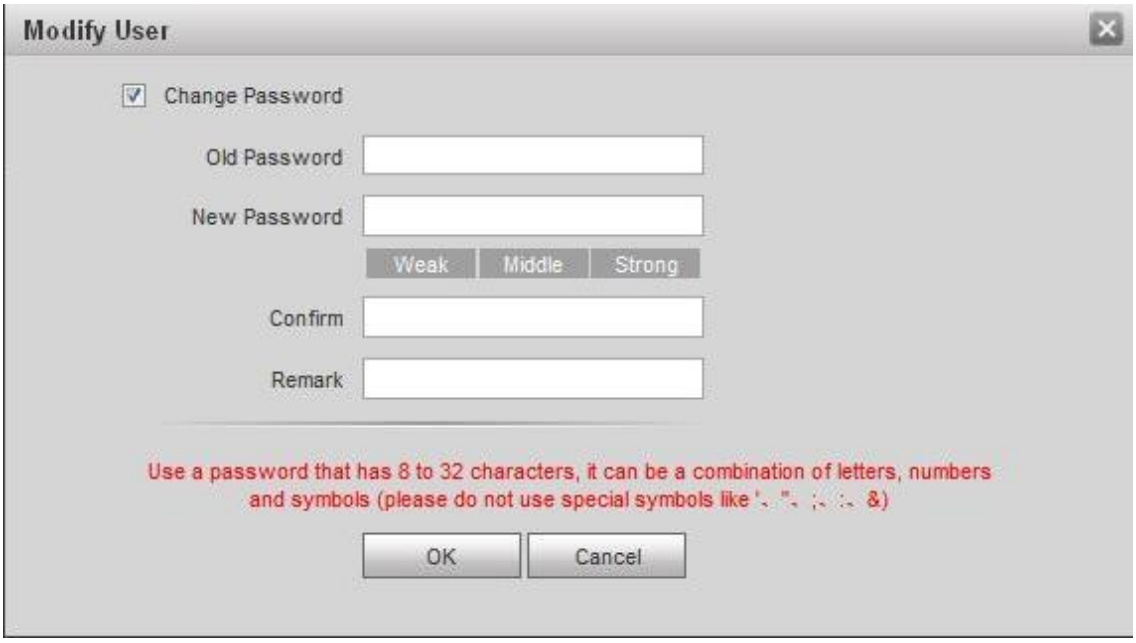

Figure 7-13

2. Enter “Old Password”, “New Password” and “Confirm”.
3. Update remark.
4. Click “OK”.

7.4.3 Delete User

Click in the line of user info that requires deletion, in order to delete this user.

7.5 Network Parameter Config

Set IP address, FTP server, application port, DDNS, HTTPS, UPnP and IP authority.

7.5.1 Network Config

Set IP address of VTO.

Step 1 Select “System Config > Network Config > TCP/IP”.

The system displays “TCP/IP” interface, as shown in Figure 7-14.

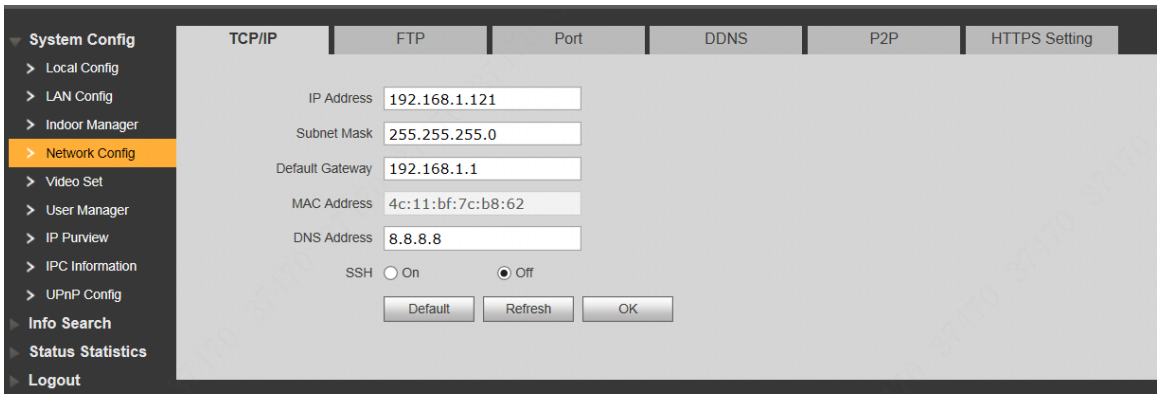

Figure 7-14

Step 2 Enter the planned “IP Address”, “Subnet Mask” and “Default Gateway”.

Step 3 Turn on SSH according to needs.

After SSH is on, Telnet and other debugging terminals can connect VTO, operate and debug it.

Step 4 Click “OK” to save the settings.

7.5.2 FTP Server

Set FTP server, so recordings and snapshots will be saved in FTP server.

Caution

Please obtain FTP server info in advance.

Step 1 Select “System Config > Network Config > FTP”.

The system displays ““FTP” interface, as shown in Figure 7-15.

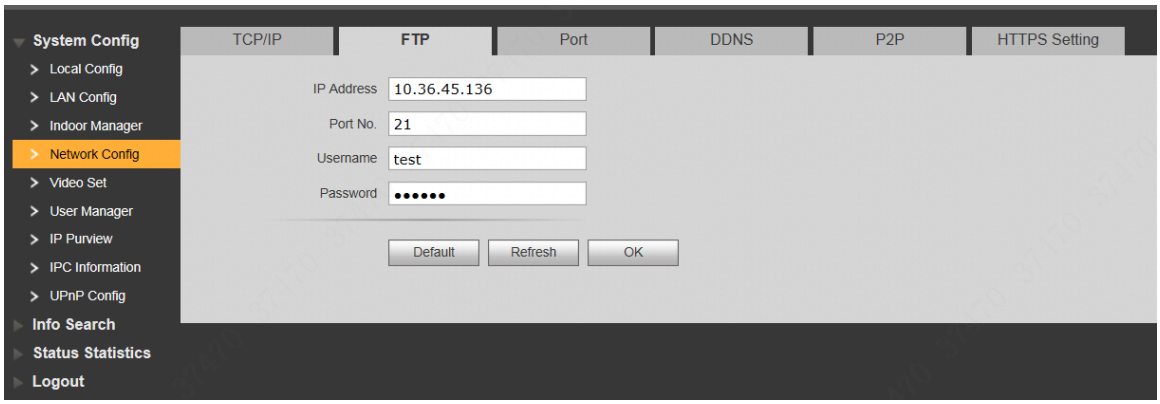

Figure 7-15

Step 2 Set the parameters and refer to Table 7-1 for details.

Parameter	Description
IP Address	IP address of the host to install FTP server.
Port No.	It is 21 by default.
Username	Username and password to visit FTP server.
Password	

Table 7-1

Step 3 Click “OK” to save the settings.

7.5.3 Port

Set the port to visit WEB interface of VTO.

Step 1 Select “System Config > Network Config > Port”.

The system displays “Port” interface, as shown in Figure 7-16.

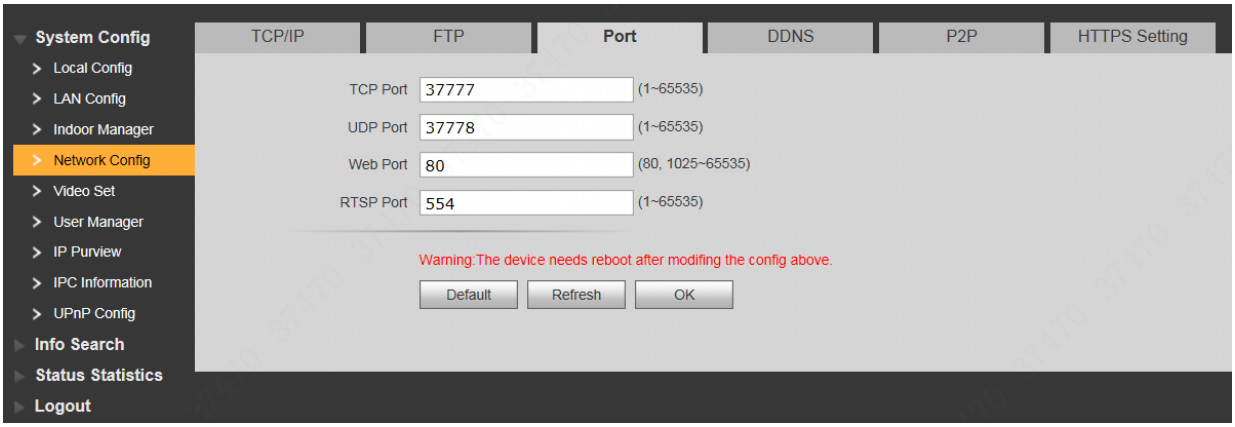

Figure 7-16

Step 2 Set port value of this device and refer to Table 7-2 for details.

Parameter	Description
TCP Port	Communication port of TCP protocol, to be set according to the user's actual needs. It is 37777 by default.
UDP Port	User datagram protocol port, to be set according to the user's actual needs. It is 37778 by default.
Web Port	Port to visit WEB interface of VTO, to be set according to the user's actual needs. It is 80 by default.
RTSP Port	● Default RTSP port no. is 554, which can be left unfilled if it is default. The user plays real-time monitoring with Apple browser QuickTime or VLC. Blackberry mobile phones also support this function. ● URL format of real-time monitoring stream: to request RTSP streaming service of real-time monitoring, please designate the requested channel no. and stream type in URL. In case of need for certification info, please provide username and password. ● To visit with Blackberry mobile phones, set stream coding mode to be H.264B and resolution to be CIF. Turn off audio. URL format is described as follows: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 ● Username: username, such as admin. ● Password: password, such as admin. ● IP: device IP, such as 10.7.8.122. ● Port: port no., which is 554 by default. It can be left unfilled if it is default. ● Channel: channel no. starting with 1. If channel is 2, channel=2. ● Subtype: stream type. Main stream is 0 (subtype=0), while extra stream is 1(subtype=1). For example, to request extra stream of channel 2 of a device, URL is as follows: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=2&subtype=1 If certification is unneeded, it is unnecessary to designated username and password. Use the following format: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0

Table 7-2

Step 3 Click "OK" to save the settings.

In case that the port is modified, enter *"http://VTO IP: WEB port no."* in the browser, to

visit WEB interface of this VTO.

7.5.4 DDNS Server

In case of frequent changes in IP address of the device, DDNS (Dynamic Domain Name Server) dynamically updates the relation between domain name and IP address on DNS server, and ensures that users are able to visit the device through domain name.

Caution

- Before configuration, please check if the device supports DDNS server; login corresponding DDNS website to register username, password and domain name info.
- After the user registers successfully on DDNS website and logins, view the registered user's all connected devices.

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

The system displays "DDNS" interface, as shown in Figure 7-17.

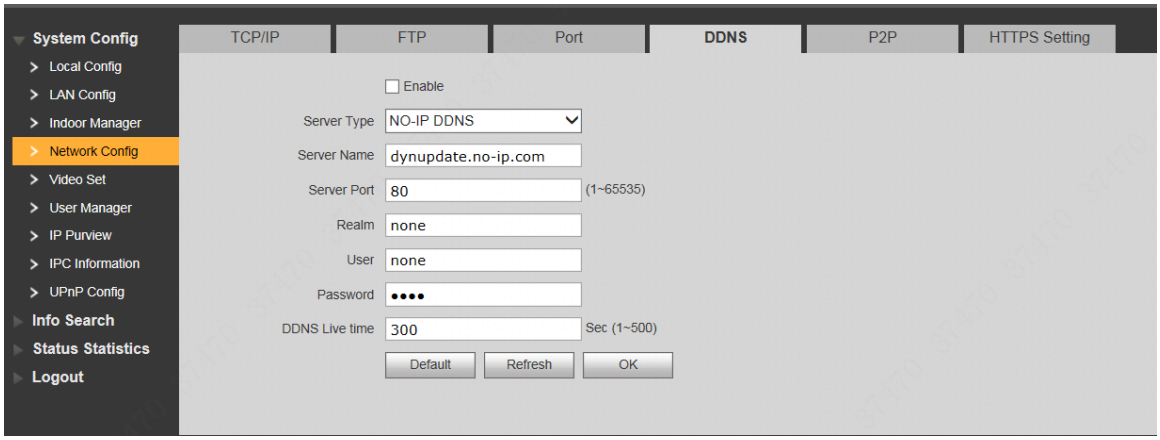

Figure 7-17

Step 2 Tick "Enable" to enable DDNS server function.

Step 3 Set parameters and refer to Table 7-3 for details.

Parameter	Description
Server Type	Server type refers to name of DDNS server provider. Relation between server type and server name is as follows. ● Dyndns DDNS address is: members.dyndns.org. ● NO-IP DDNS address is: dynupdate.no-ip.com.
Server Name	
Server Port	Port no. of DDNS server.
Realm	Domain name registered by the user at the website of DDNS server provider.
User	User name and password obtained from DDNS server provider. The user needs to register (including user name and password) at the website of DDNS server provider.
Password	
DDNS Live Time	The time interval to raise update request after designated DDNS update is enabled. The unit is second.

Table 7-3

Step 4 Click "OK" to save the settings.

Enter domain name in the browser and press [Enter] key. Configuration has succeeded if

WEB login interface of the device is displayed, and configuration has failed if WEB login interface is not displayed.

7.5.5 P2P

P2P is a private network traversal technology. After enabling P2P function, open mobile client software, enter the serial number directly or scan the QR code to obtain serial number, and thus manage multiple controllers. During easy and convenient use, it is unnecessary to apply for dynamic domain name, carry out port mapping or deploy relay server.

Caution

To use this function, the device shall be connected with Internet, in order to use it normally.

Step 1 Select “System Config > Network Config > P2P”.

The system displays “P2P” interface, as shown in Figure 7-18.

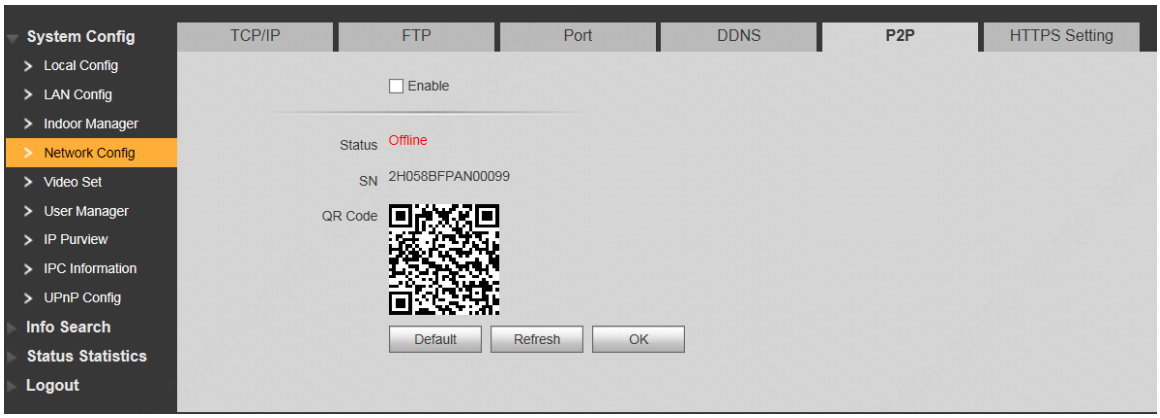

Figure 7-18

Step 2 Tick “Enable” to enable P2P function.

Step 3 Select “P2P Server”.

Step 4 Click “OK” to complete setting.

After the setting has been completed, “Status” becomes “Online”, representing successful P2P registration.

After successful P2P registration, scan QR code with mobile client or enter the serial number directly to add VTO, in order to visit and manage VTO.

7.5.6 HTTPS Setting

At HTTPS setting interface, create server certificate or download root certificate and set port number, so PC is able to login through HTTPS. In this way, ensure communication data security; guarantee user info and device security with reliable stable technology.

Step 1 Select “System Config > Network Config > HTTPS Setting”.

The system displays “HTTPS Setting” interface, as shown in Figure 7-19.

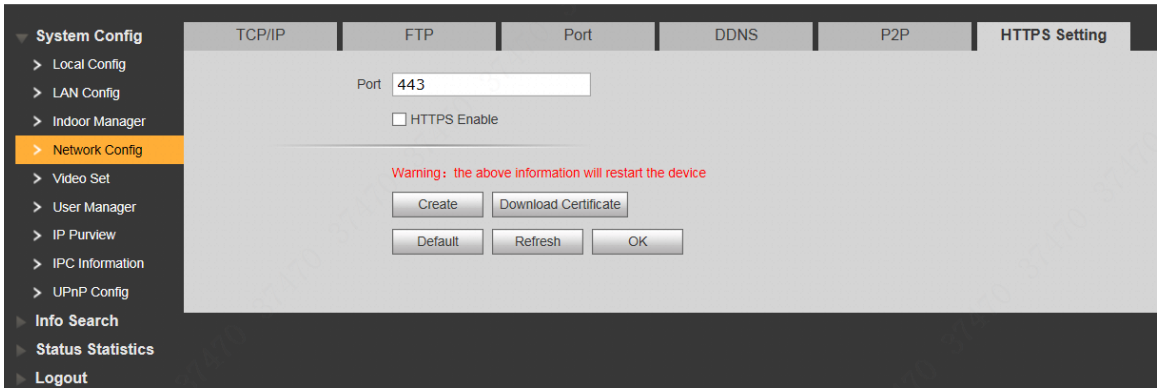

Figure 7-19

Step 2 Enter “Port”, tick “HTTPS Enable” and thus enable the HTTPS function.

Step 3 Click “OK” to save the settings.

Enter *https://VTO IP: Port No.* in the browser and WEB login interface will pop up.

Note

- If you use this function for the first time or change device IP, execute “Create” again.
- If you use HTTPS for the first time after changing computer, execute “Download Certificate” again.

7.5.7 UPnP

Via UPnP protocol, create mapping relationship between private network and WAN. WAN user can visit device in LAN via outer IP address.

Caution

Please confirm the following operation before use.

- UPnP function is used only when VTO is connected with router.
- Enable UPnP function of the router, set IP address of router WAN port (WAN IP), and connect WAN.
- Connect the device with router LAN port, and connect private network.

Select “System Config > UPnP Config”, and the system displays “UPnP” interface, as shown in Figure 7-20.

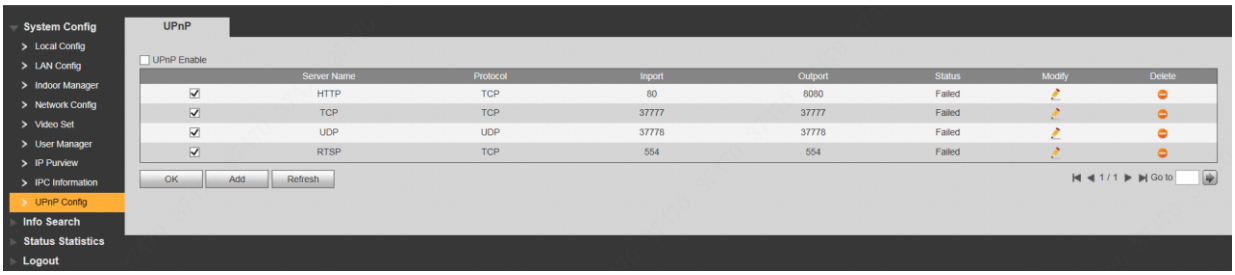

Figure 7-20

7.5.7.1 Enable Mapping

There are some mapping relations when leaving factory, which can be used after being enabled.

Step 1 Tick “UPnP Enable” to enable UPnP function.

Step 2 Select servers to enable mapping relation.

Step 3 Click “OK” to save the settings.

Enter *“http://WAN IP: External Port No.”* in the browser, to visit private network device at corresponding port in the router.

7.5.7.2 Add Server

Add new server mapping relations.

Step 1 Click “Add”.

The system displays “Add” interface, as shown in Figure 7-21.

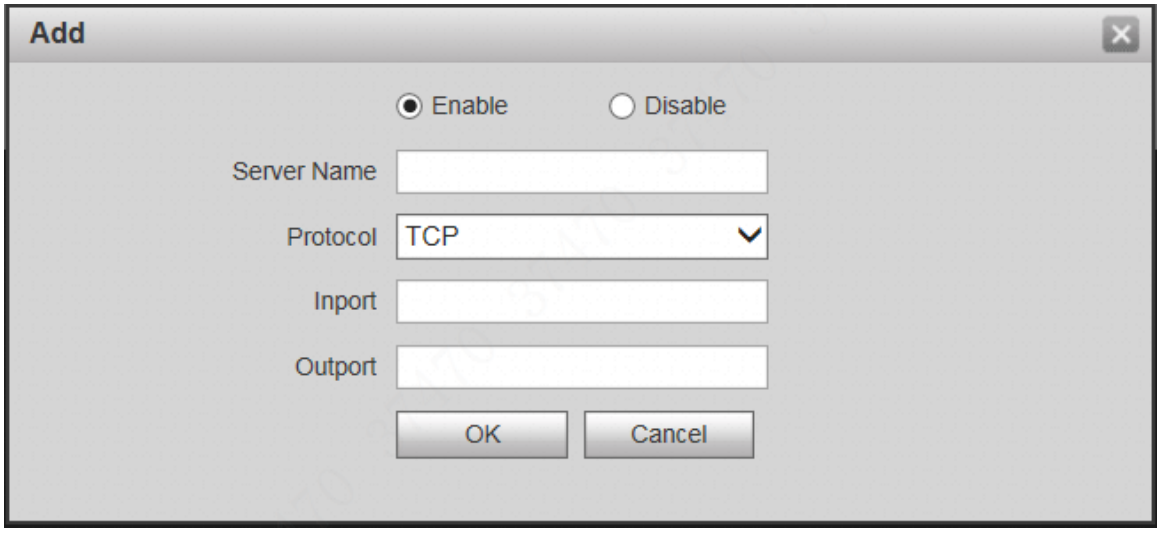

Figure 7-21

Step 2 Set parameters and refer to Table 7-4 for details.

Parameter	Description	
Enable/ Disable	● Tick “Enable” to enable the mapping relation. ● Tick “Disable”, meaning that mapping relation is not enabled. Choose to enable it in the external list.	
Server Name	Name of network server.	
Protocol	Protocol type.	
Inport	Port that this device needs to map.	Note ● When you set router mapping outer port, try to use port within 1024~5000, avoid using well-known port 1~255 and system port 256~1023, in order to prevent conflicts. ● When there are multiple devices in the same LAN, please plan port mapping, to prevent multiple device mapping to one outer port. ● For port mapping in progress, please make sure mapping port is not occupied or limited. ● TCP/UDP inports and outports must be identical, and they cannot be modified.
Outport	Port that is mapped on the router.	

Table 7-4

Step 3 Click “OK” to save the settings.

7.5.7.3 Modify Server

Modify server mapping relation in the list.

Step 1 Click .

The system displays “Add” interface, as shown in Figure 7-22.

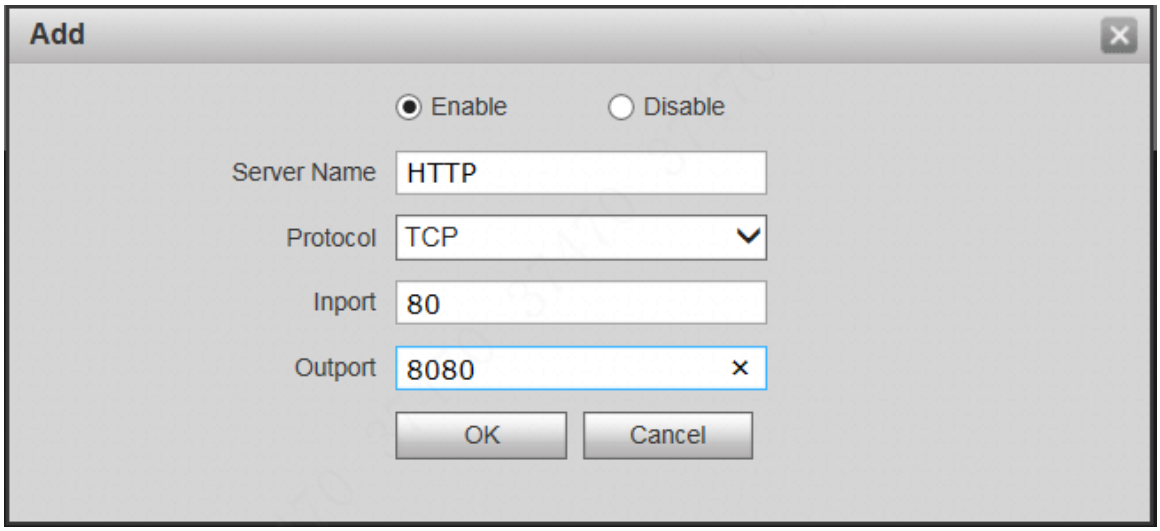

Figure 7-22

Step 2 Set parameters and refer to Table 7-4 for details.

Step 3 Click “OK” to save the settings.

7.5.7.4 Delete Server

Delete server mapping relation in the list.

Click to delete mapping relation.

7.5.8 IP Purview

In order to strengthen device network security and protect device data, set access purview of IP host (IP host refers to personal computer or server with IP).

- White list allows designated IP host to visit the device.
- Black list prohibits designated IP host from visiting the device.

Note

If white list is enabled and set, other IP address, except those in the white list, cannot login the device.

Step 1 Select “System Config > IP Purview”.

The system displays “IP Purview” interface, as shown in Figure 7-23.

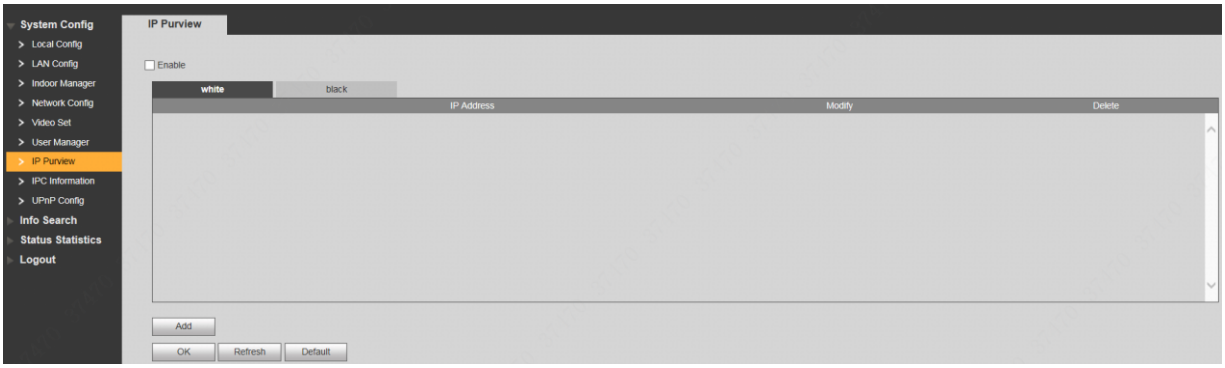

Figure 7-23

Step 2 Tick “Enable”.

The system displays white/black list checkbox, as shown in Figure 7-24.

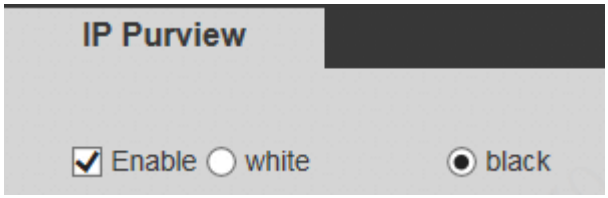

Figure 7-24

1. Add “White” or “Black”.
2. Click “Add”.

   The system displays “Add” interface, as shown in Figure 7-25.

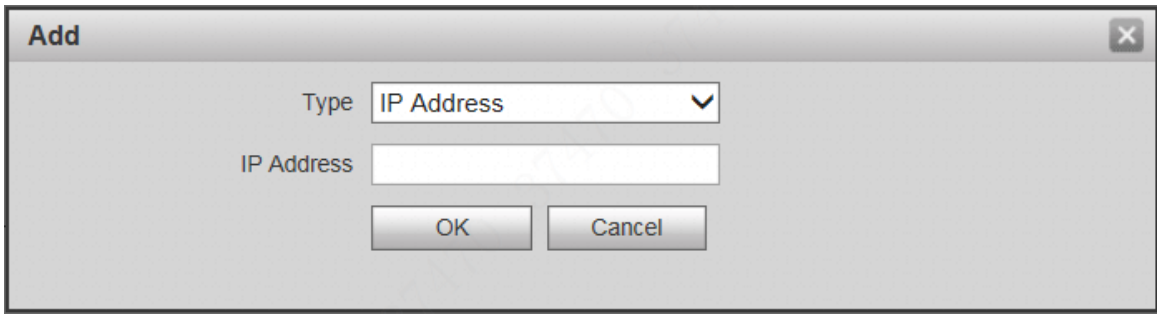

Figure 7-25

3. Set IP address and refer to Table 7-5 for details.

   The system supports to set maximum 64 IP addresses.

Type	Description
IP Address	Add host IP address to be added; adopt IPv4 format, such as 192.168.1.120.
IP Network Segment	Enter the start address and end address of network segment to be added.

Table 7-5

4. Click “OK”.

   Return to IP purview interface.

Step 3 Click “OK” to save the settings.

IP host in the white list can login WEB interface of the device successfully. The system displays “Login Failed” if IP host in the black list logins the WEB interface.

7.6 LAN Config

Set VTO building no., unit no., no., management centre and group call function.

Step 1 Select “System Config > LAN Config”.

The system displays “LAN Config” interface, as shown in Figure 7-26.

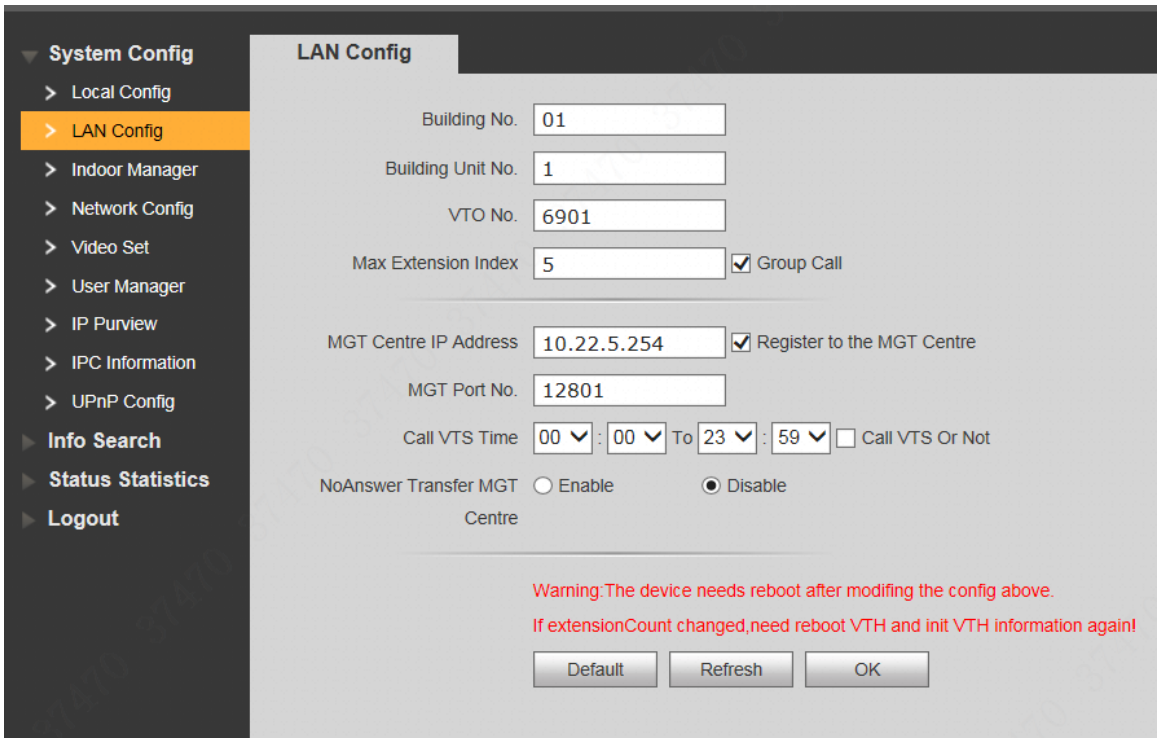

Figure 7-26

Step 2 Set parameters and refer to Table 7-6 for details.

Parameter	Description
Building No.	Set building no. of VTO.
Building Unit No.	Set unit no. of VTO.
VTO No.	Set no. of VTO.
Max. Extension Index	Tick “Group Call” to enable VTO group call function; press the call key on the VTO, to call master VTH and extension VTH simultaneously. Max. quantity of group call extension VTH shall not exceed “Max. Extension Index”.
Group Call	Note ● After group call function is enabled or disabled, the device reboots automatically, so the configuration takes effect. ● To realize group call, VTH and VTO shall be set. Please refer to “6.1.3 Group Call” for details.
MGT Centre IP Address	Set “MGT Centre IP Address” and “MGT Port No.”; tick “Register to the MGT Centre”. VTO is registered to management centre, so management centre can manage the VTO and VTH, and call VTH. Note Please obtain management centre info in advance.
MGT Port No.	
Register to the MGT Centre	
Call VTS Time	

Parameter	Description
Call VTS or Not	Ensure that VTO has been registered at management centre. Set “Call VTS Time” and tick “Call VTS or Not”. Press the call key on the VTO within the set time period, to call the management centre only.
No Answer Transfer MGT Centre	Tick “Enable” to enable transferring to management centre in case of no answer. In the following cases when VTO calls VTH, the system will transfer the call to management centre automatically. ● SD card has not been inserted into VTH. ● SD card has been inserted into VTH, but VTO message time is set to be 0 on the VTH.

Table 7-6

Step 3 Click “OK” to save the settings.

7.7 Local Parameter Config

7.7.1 Local Config

Set info about the device, such as device type and reboot date.

Step 1 Select “System Config >Local Config> Local Config”.

The system displays “Local Config” interface, as shown in Figure 7-27.

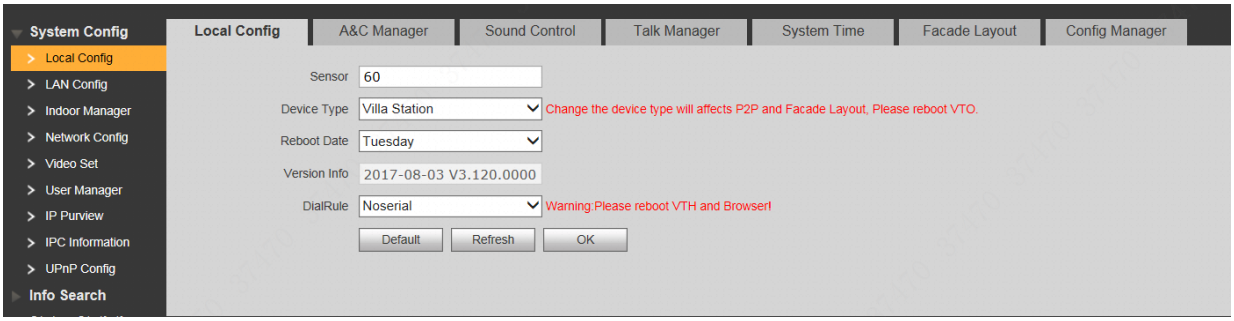

Figure 7-27

Step 2 Set parameters and refer to Table 7-7 for details.

Parameter	Description
Sensor	If it is dark during video intercom, turn on the fill-in light automatically. The larger the value is, the higher sensitivity becomes.
Device Type	It is villa station by default.
Reboot Date	Set auto reboot time of VTO. It is 2 a.m. on Tuesday by default.
Version Info	Display software version number.
Dial Rule	Set the user’s dial rule, including “Non-serial” and “Serial”.

Table 7-7

Step 3 Click “OK” to save the settings.

7.7.2 Access Manager

Set unlock responding interval, unlock period and door sensor check time.

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

The system displays “A&C Manager” interface, as shown in Figure 7-28.

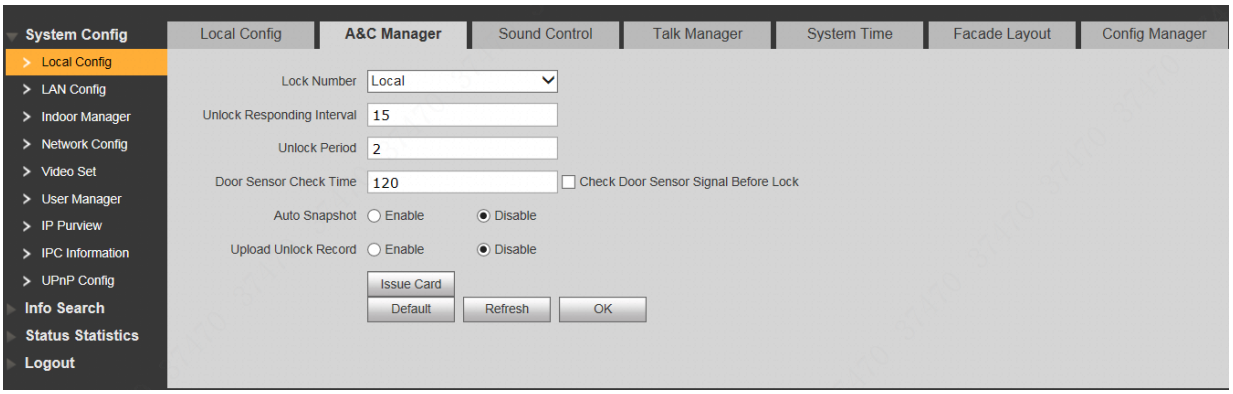

Figure 7-28

Step 2 Set parameters and refer to Table 7-8 for details.

Parameter	Description
Unlock Responding Interval	After unlock, the interval that the device responds to the next unlock. The unit is “second”.
Unlock Period	After unlock, the period that it remains unlocked. The unit is “second”.
Check Door Sensor Signal Before Lock	Tick “Check Door Sensor Signal Before Lock” to enable the function. If door sensor signal exists, it will not be locked. However, after opening time exceeds the door sensor check time, give door sensor alarm and report the alarm info to management centre automatically.
Door Sensor Check Time	
Auto Snapshot	Tick “Enable”. 2 pictures will be snapshot automatically when the door is opened, and uploaded to FTP or SD card.
Upload Unlock Record	Reserved function.
Issue Card	● Click “Issue Card”. ● Swipe an unauthorized card at VTO. The system pops up “Card Info” interface. ● Enter “Room No.” and “Card No.” and click “OK”. Note Cards can be swiped continuously, within a period of 30s. ● Click “OK” to finish issuing card. Note ● Click “OK” within the countdown, so the cards will be valid. Otherwise, all card info will be invalid. ● Click “Cancel” when issuing cards, in order to stop issuing.

Table 7-8

Step 3 Click “OK” to save the settings.

7.7.3 Sound Control

Enable and disable unlock sound, ringtone, alarm sound and speech sound.

Step 1 Select “System Config >Local Config > Sound Control”.

The system displays “Sound Control” interface, as shown in Figure 7-29.

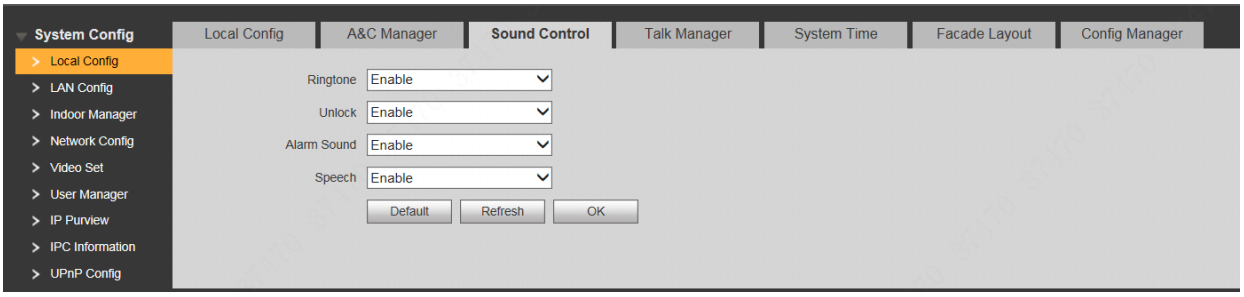

Figure 7-29

Step 2 Enable or disable corresponding sound.

Step 3 Click “OK” to save the settings.

7.7.4 Talk Manager

Set auto snapshot, message and talk record.

Caution

Auto snapshot, message and record are uploaded to FTP. Please confirm that FTP server has been configured.

Step 1 Select “System Config >Local Config > Talk Manager”.

The system displays “Talk Manager” interface, as shown in Figure 7-30.

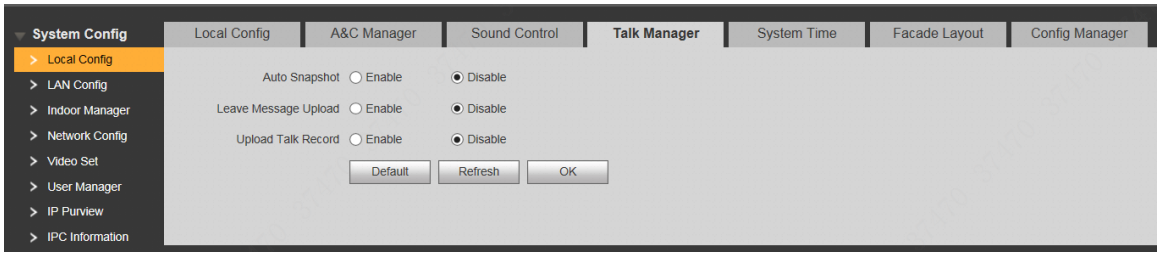

Figure 7-30

Step 2 Set parameters and refer to Table 7-8 for details.

Parameter	Description
Auto Snapshot	Tick “Enable”. 2 pictures will be snapshot automatically during calling, and 1 picture will be snapshot automatically when pickup, and then uploaded to FTP.
Leave Message Upload	Caution ● If VTH doesn’t have SD card or SD card isn’t inserted, enable this function and set FTP server to realize this function. ● If VTH has SD card, the messages and records will be saved on the VTH automatically. This function is invalid. Tick “Enable” to enable the function. VTH info interface has “Visitors’ Message” tab. When VTO calls VTH and gets no response, the system

Parameter	Description
	prompts that “No one answers. Please press 1 to leave a message”. Press [1] to leave a picture/message. The system will upload the contents to FTP and messages are available at “Visitors’ Message” tab.
Upload Talk Record	Reserved function.

Table 7-9

Step 3 Click “OK” to save the settings.

7.7.5 System Time

Set system date format, time format, system time and NTP server.

Step 1 Select “System Config >Local Config > System Time”.

The system displays “System Time” interface, as shown in Figure 7-31.

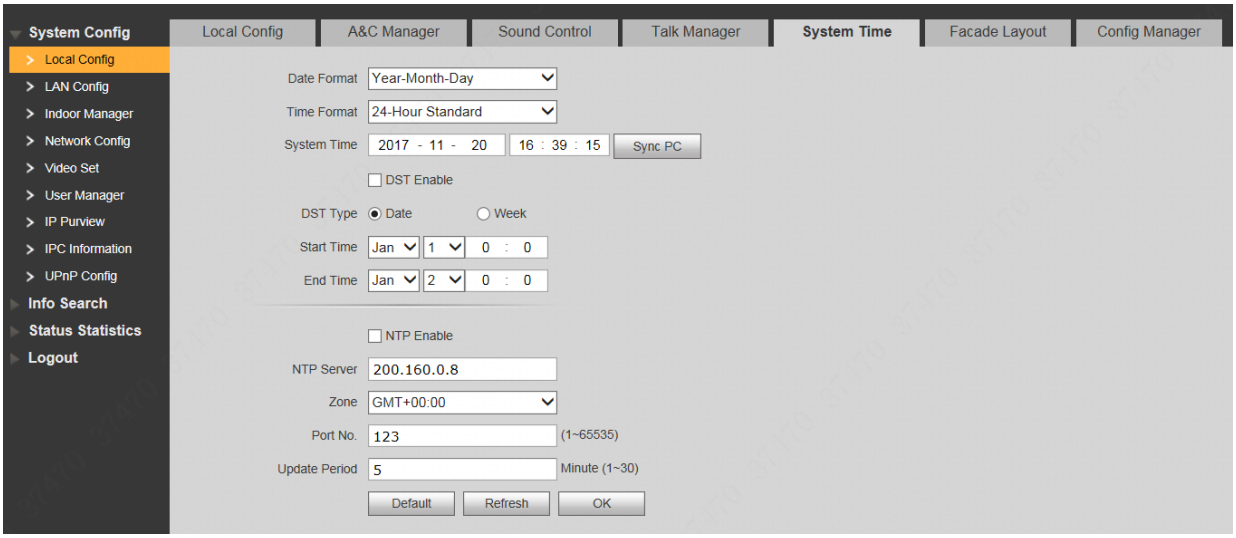

Figure 7-31

Step 2 Set parameters and refer to Table 7-10 for details.

Parameter	Description
Date Format	Set date display format, including Year-Month-Day, Month-Day-Year and Day-Month-Year.
Time Format	Set time display format, including 12-hour standard and 24-hour standard.
System Time	Set present system date and time of VTO. Caution System time shall not be changed arbitrarily; otherwise, it may fail to inquire records and snapshots. Before changing system time, please stop recording or disable auto snapshot.
Sync PC	Click “Sync PC”, so system time and local PC time are consistent.
DST Enable DST Type Start Time End Time	Some countries or regions follow daylight-saving time (DST). Choose to enable DST or not according to actual needs: 1. Tick “DST Enable” to enable DST function. 2. Select “DST Type”, including “Date” and “Week”. 3. Set the start time and end time of DST.

Parameter	Description
NTP Enable	Tick “NTP Enable” to enable this function.
NTP Server	Enter domain name or IP address of NTP server.
Zone	Select time zone of the device.
Port No.	Set port no. of NTP server.
Update Period	The time interval of updating time between device and NTP server. Maximum update period is 30 minutes.

Table 7-10

Step 3 Click “OK” to save the settings.

7.7.6 Config Manager

Realize backup or restore backup, VTH info, local config, networked config and video config; restore all default configurations.

Select “System Config >Local Config > Config Manager”. The system displays “Config Manager” interface, as shown in Figure 7-32.

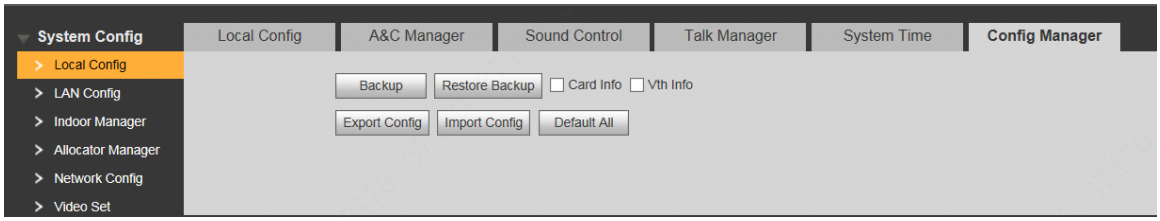

Figure 7-32

- Backup
  Select “Card Info” or “VTH Info” (supporting multiple choice), and click “Backup”, so card info and VTH info will make a backup in VTO.
- Restore Backup
  Click “Restore Backup”, so card info and VTH info is restored to backup info.
- Export Config
  Click “Export Config” to export config info and save it at local device, so as to restore config or import into other devices.
- Import Config
  Click “Import Config” to import local config files to the device, so as to restore data or synchronize data.
- Default All
  Click “Default All”. After confirmation, the device will reboot, and restore all info to default status, except IP address.

7.8 Indoor Manager

Manage VTH info and card info in the system.

Select “System Config > Indoor Manager”, and the system displays “Digital Indoor Station Manager” interface, as shown in Figure 7-33.

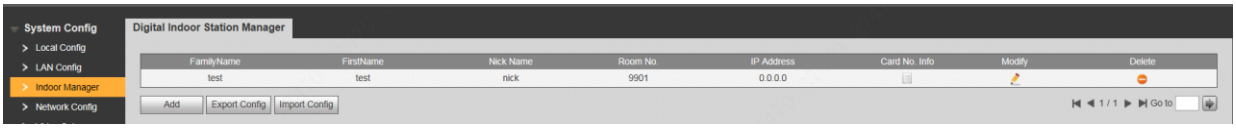

Figure 7-33

7.8.1 Add VTH

Note

- Add master VTH.
- After “Network” interface of extension VTH has added and enabled master VTH, VTO interface will obtain extension VTH info automatically.

Step 1 Click “Add”.

The system displays “Add” interface, as shown in Figure 7-34.

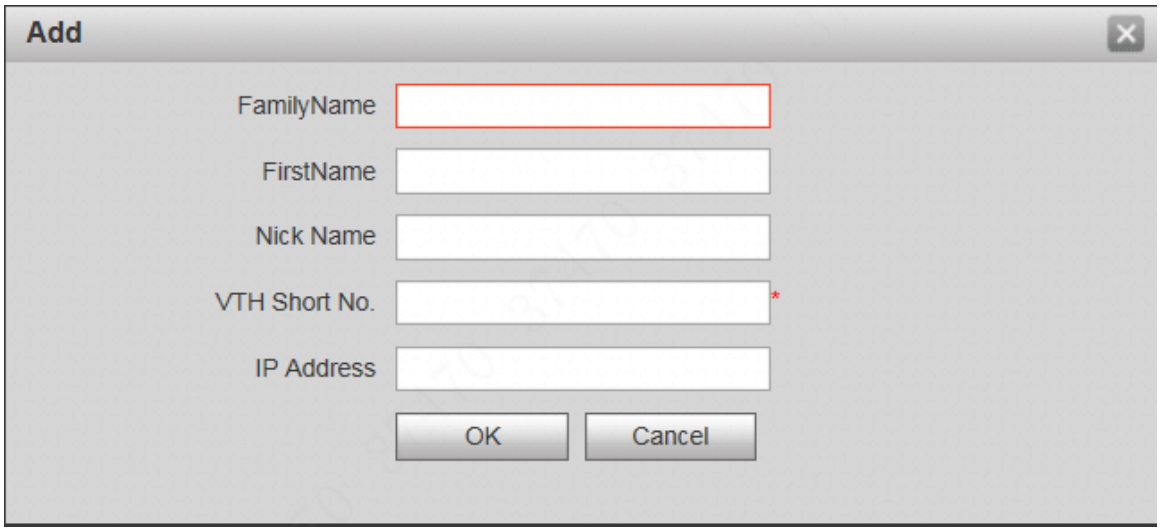

Figure 7-34

Step 2 Set parameters and refer to Table 7-11 for details.

Parameter	Description
Family Name	Set VTH user name and nick name, in order to identify VTH.
First Name	
Nick Name	
VTH Short No.	Set VTH room no.. Note VTH short no. is the same as room no. configured at VTH.
IP Address	VTH IP address.

Table 7-11

Step 3 Click “OK” to save the settings.

7.8.2 Modify VTH

Note

Only family name, first name and nick name of VTH can be modified.

Step 1 Click  .

The system displays “Modify” interface, as shown in Figure 7-35.

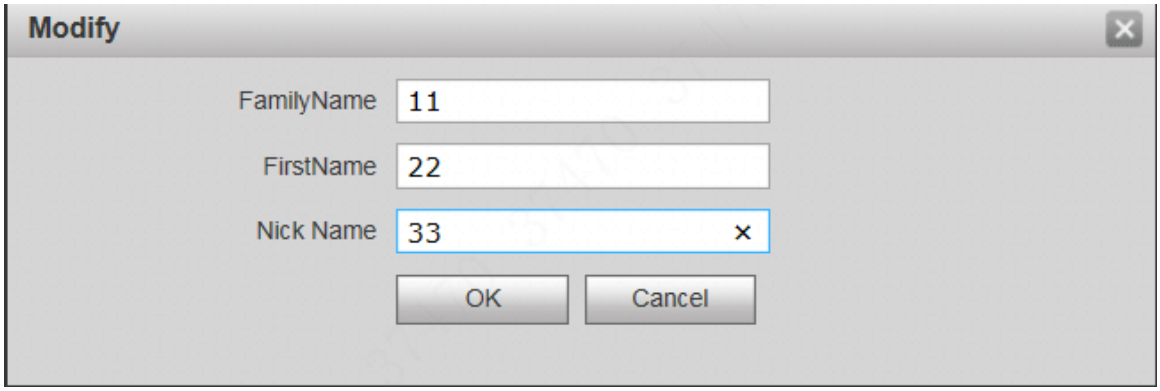

Figure 7-35

Step 2 Modify VTH “Family Name”, “First Name” and “Nick Name”.

Step 3 Click “OK” to save the settings.

7.8.3 Delete VTH

Click to delete VTH info one by one.

7.8.4 Config Manager

Import or export device info, password info, card no. info and login info of the device.

7.8.4.1 Export Config

Export and save config in the local device. When other devices need to configure the same parameters, the config file can be imported.

Step 1 Click “Export Config”.

The system displays “Export” interface, as shown in Figure 7-36.

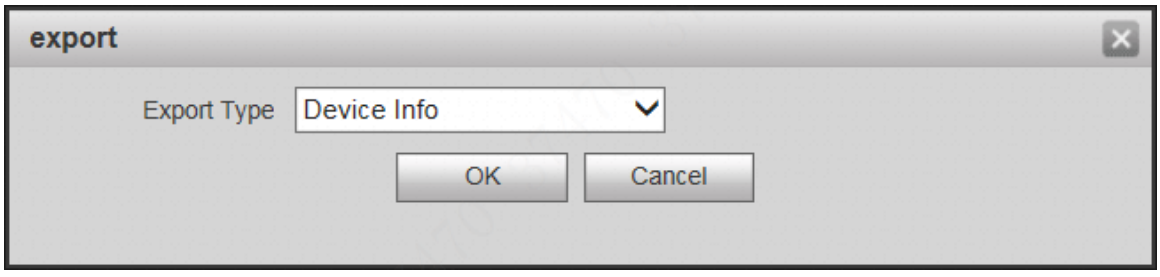

Figure 7-36

Step 2 Select “Export Type” and click “OK”.

Step 3 Select a location to save it.

Step 4 Click “Save”.

The system prompts “Operation Succeeded”, representing successful export.

7.8.4.2 Import Config

Import local config file into the device, so as to realize configuration.

Step 1 Click “Import Config”.

The system displays “Open” interface.

Step 2 Select config file (.log) to be imported and click “Open”.

The system prompts “Operation Succeeded”, representing successful import.

7.8.5 Card Manager

Report loss and cancel; modify card ID and delete card.

7.8.5.1 Report Loss

If a card is lost, please report loss, so the card is deprived of unlock authority temporarily, until report of loss is cancelled.

Step 1 Click  .

The system displays “Card Info” interface, as shown in Figure 7-37.

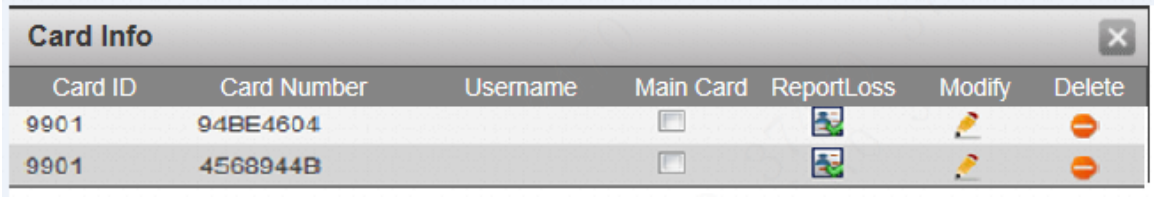

Figure 7-37

Note

Villa VTO doesn’t support mother card function.

Step 2 Click  to report loss. The icon is switched to  .

Note

Click  to cancel the report of loss, and recover unlock function.

Step 3 Click  to close config interface.

7.8.5.2 Modify

Modify username of the card.

Step 1 Click  .

The system displays “Card Info” interface, as shown in Figure 7-37.

Step 2 Click  .

The system displays “Modify” interface, as shown in Figure 7-38.

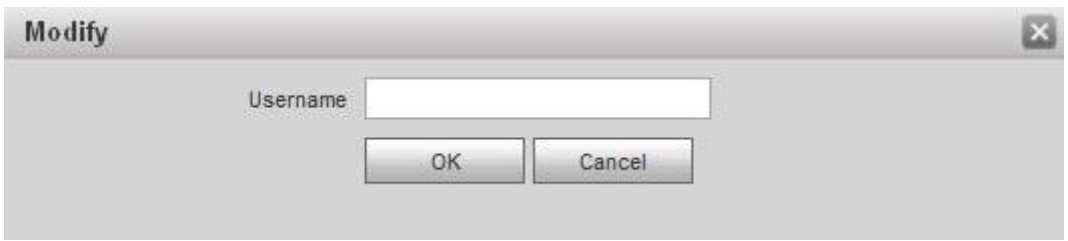

Figure 7-38

Step 3 Modify the username.

Step 4 Click “OK”.

Step 5 Click to close config interface.

7.8.5.3 Delete

After deletion, the card doesn’t own unlock authority.

Step 1 Click .

The system displays “Card Info” interface, as shown in Figure 7-37.

Step 2 Click to delete card info.

Step 3 Click to close config interface.

7.9 Video Set

Set video picture and audio volume of VTO with camera.

7.9.1 Video Set

Step 1 Select “System Config >Video Set>Video Set”.

The system displays “Video Set” interface, as shown in Figure 7-39. Click “Open Door”, and VTO is unlocked.

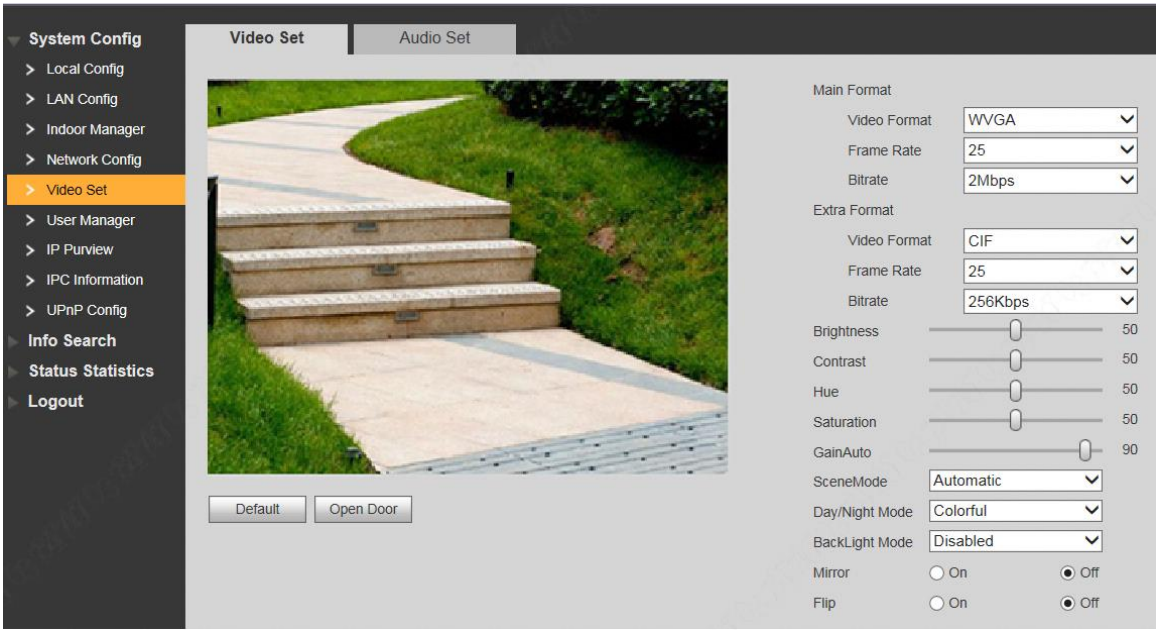

Figure 7-39

Step 2 Set parameters and refer to Table 7-12 for details.

Parameter		Description
Main Format	Video Format	Adjust resolution of video, including 720P, WVGA and D1.
	Frame Rate	Adjust transmission speed, including 3, 25 and 30 frames.

Parameter		Description
	Bitrate	Select according to actual access network, including 256Kbps, 512Kbps, 1Mbps, 2Mbps and 3Mbps.
Extra Format	Video Format	Adjust resolution of video, including WVGA, D1, QVGA and CIF.
	Frame Rate	Adjust transmission speed, including 3, 25 and 30 frames.
	Bitrate	Select according to actual access network, including 256Kbps, 512Kbps, 1Mbps, 2Mbps and 3Mbps.
Brightness		Adjust overall brightness in a linear way. The larger the value is, the brighter the image becomes; and vice versa. When this value is large, the image dims easily.
Contrast		Adjust image contrast. The larger the value is, the more contrasted the image becomes; and vice versa. When this value is large, dark part of the image is too dark, while bright part overexposes easily. When this value is small, the image dims.
Hue		Adjust image hue. There is a default value according to sensitometric feature of the sensor. Generally, it is unnecessary to adjust this value greatly.
Saturation		Adjust image shade. The larger the value is, the deeper the color becomes, and vice versa. This value doesn't affect overall brightness of the image.
Gain Auto		Adjust image noise. The less the value is, the smaller the noise becomes, but image brightness is very dark in dark scene. The larger the value is, the more brightness will be obtained in dark scene, but image noise becomes more obvious.
Scene Mode		Set white balance mode, mainly affecting overall hue. It is automatic mode by default. ● Disabled: any mode is not set. ● Automatic: set white balance automatically, compensate white balance of different color temperature automatically, and ensure normal image color. ● Sunny: threshold value of white balance is set to sunny day mode. ● Night: threshold value of white balance is set to night mode.
Day/Night Mode		Camera image display is set to colorful or black and white mode. ● Colorful: display colorful image. ● Automatic: automatically choose to display colorful image or black white image according to ambient brightness. ● Black white: display black and white image.
Backlight Mode		There are several modes: ● Disabled: no backlight. ● Backlight: prevent silhouette appearing in dark part of the subject against the light. ● Wide dynamic: according to ambient brightness, the system reduces brightness of high-brightness area, increases brightness of low-brightness area, and thus displays both areas clearly. ● Inhibition: the system inhibits brightness of high-brightness

Parameter	Description
	area of the image, reduces halo size and thus reduces brightness of the entire image.
Mirror	Select “On”; the image will be turned over from left to right.
Flip	Select “On”; the image will be turned over from top to bottom.

Table 7-12

7.9.2 Audio Set

Step 1 Select “System Config >Video Set>Audio Set”.

The system displays “Audio Set” interface, as shown in Figure 7-40.

Figure 7-40

Step 2 Adjust VTO mic volume and beep volume.

7.10 IPC Info

Add IP camera (IPC) info and support max. 32 channels. IPC info will be synchronized with VTH automatically, in order to facilitate VTH monitoring.

Select “System Config > IPC Info”. The system displays “IPC Info” interface, as shown in Figure 7-41.

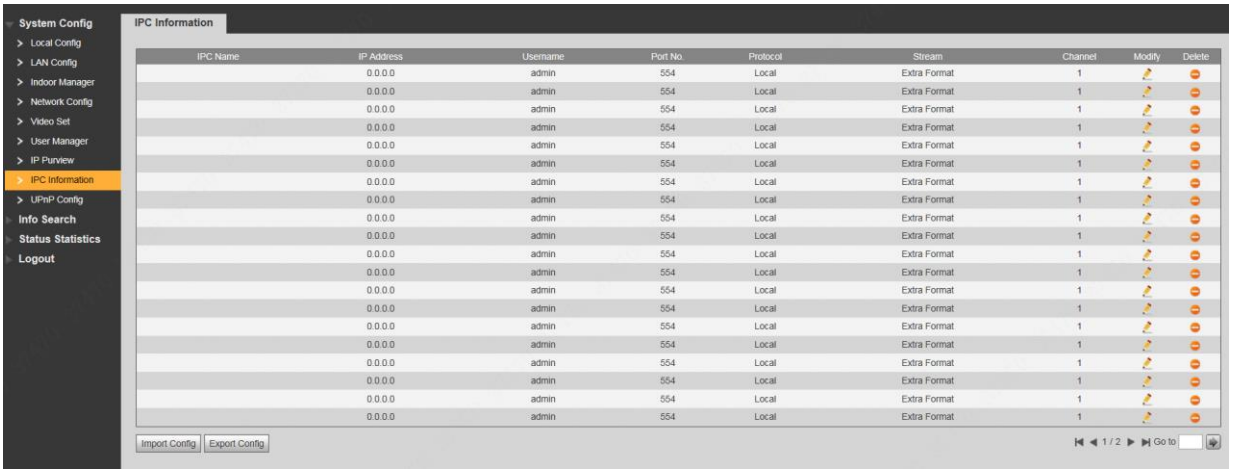

Figure 7-41

7.10.1 Add One IPC

Add IPC info one by one.

Caution

Add IPC directly, or add NVR/XVR/HCVR devices to obtain info about the added IPC.

Step 1 Click .

The system displays “Modify” interface, as shown in Figure 7-42.

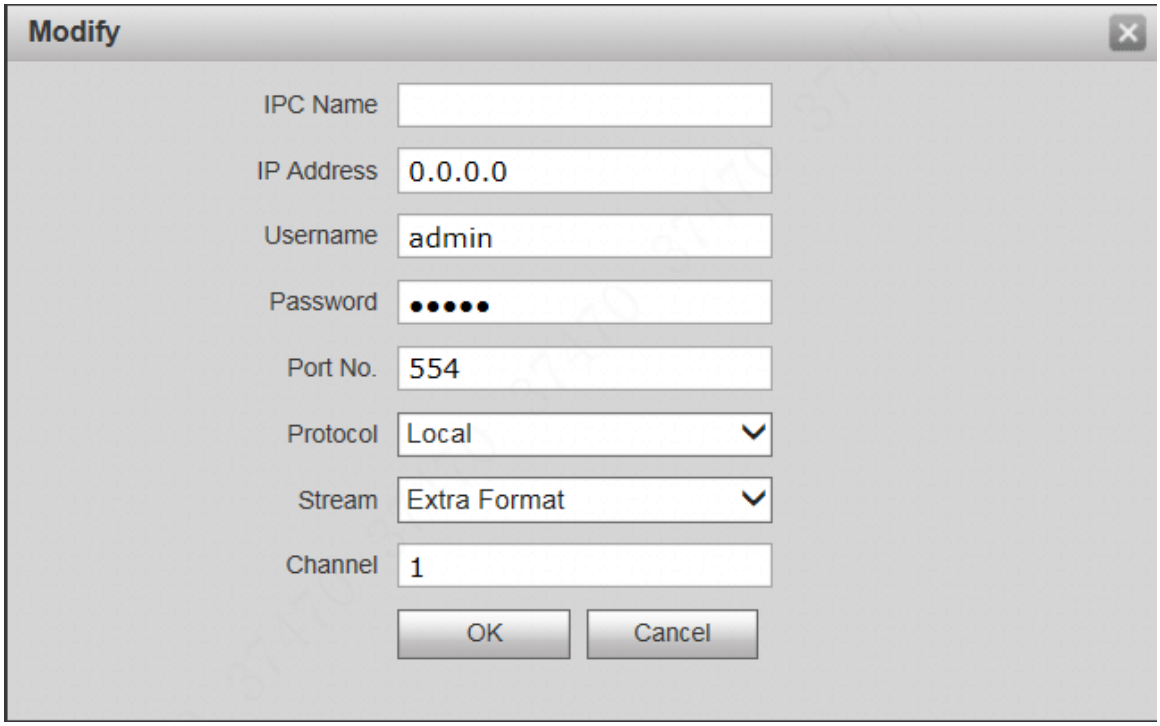

Figure 7-42

Step 2 Set parameters and refer to Table 7-13 for details.

Parameter	Description
IPC Name	Enter IPC/NVR/XVR/HCVR name.
IP Address	Enter IP address of the connected IPC/NVR/XVR/HCVR.
Username	Enter the username and password to login WEB interface of IPC/NVR/XVR/HCVR.
Password	
Port No.	It is 554 by default.
Protocol	It consists of local protocol and Onvif protocol. Please select according to the protocol supported by the connected device.
Stream	Select from main format and extra format according to needs. ● Main format: large stream, high definition, large occupied bandwidth, suitable for local storage. ● Extra format: smooth image, small occupied bandwidth, suitable for low bandwidth network transmission.
Channel	● To connect IPC, it is 1 by default. ● To connect NVR/XVR/HCVR, it is set to channel no. of IPC on NVR/XVR/HCVR.

Table 7-13

Step 3 Click “OK” to complete adding.

7.10.2 Delete

Click to delete camera info.

7.10.3 Batch Import

With batch import function, import IPC info into the system.

Click “Import Config”, select config file (.csv) and import the file info into the system.

7.10.4 Batch Export

Export and save the present IPC info to the local device, for the sake of future use.

Click “Export Config”; select the path to save config file.

7.11 Info Search

Search VTO call history, alarm record and unlock record.

7.11.1 Call History

View VTO call and talk record. Max. 1,024 records can be saved.

Select “Info Search> Call History”. The system displays “VTO Call History” interface, as shown in Figure 7-43.

Click “Export Record” to export the VTO call record.

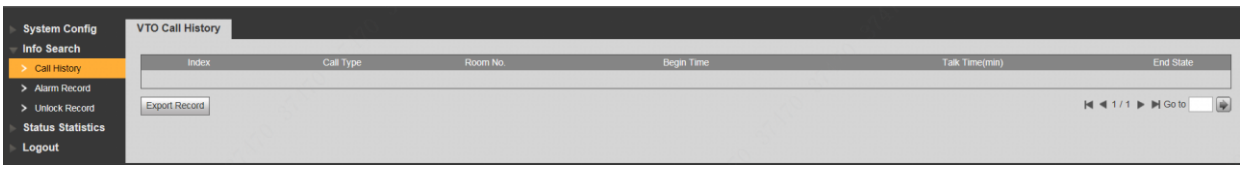

Figure 7-43

7.11.2 Alarm Record

View VTH 8-channel alarm, duress alarm and other alarm records. Max. 1,024 records can be saved.

Select “Info Search> Alarm Record”. The system displays “Alarm Record” interface, as shown in Figure 7-44. Click “Export Record” to export the VTO alarm record.

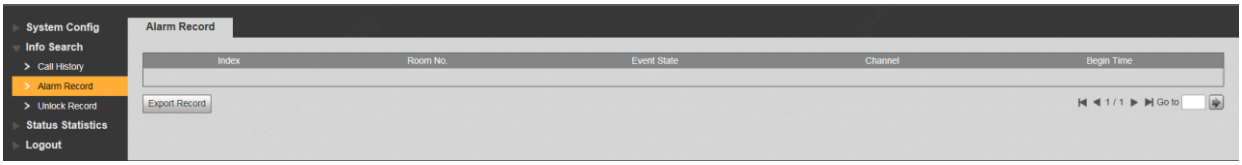

Figure 7-44

7.11.3 Unlock Record

View unlock records with card, password, remote way and button. Max. 1,000 records can be saved.

Select “Info Search> Unlock Record> VTO Unlock Record”. The system displays “VTO Unlock Record” interface, as shown in Figure 7-45.

Click “Export Record” to export the VTO unlock record.

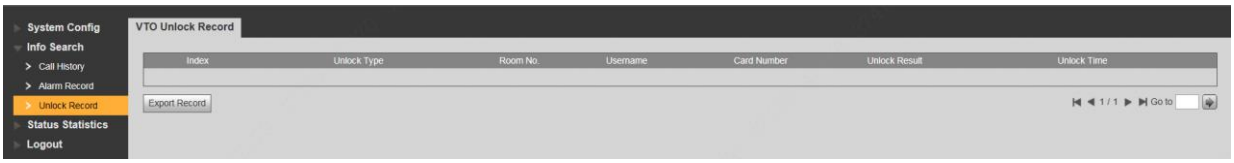

Figure 7-45

7.12 Reboot Device

Reboot the device at WEB interface.

Step 1 Select “Logout > Reboot Device”.

The system displays “Reboot Device” interface, as shown in Figure 7-46.

Step 2 Click “Reboot Device”, so the device reboots automatically.

WEB interface is switched to WEB login interface.

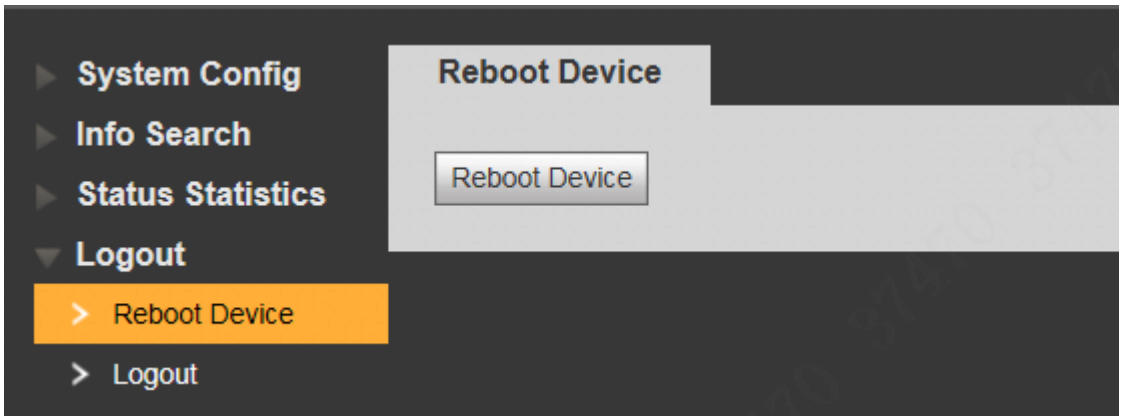

Figure 7-46

7.13 Logout

Log out the WEB interface.

Step 1 Select “Logout > Logout”.

The system displays “Logout” interface, as shown in Figure 7-47.

Step 2 Click “Logout”.

Log out the WEB interface and return to login interface.

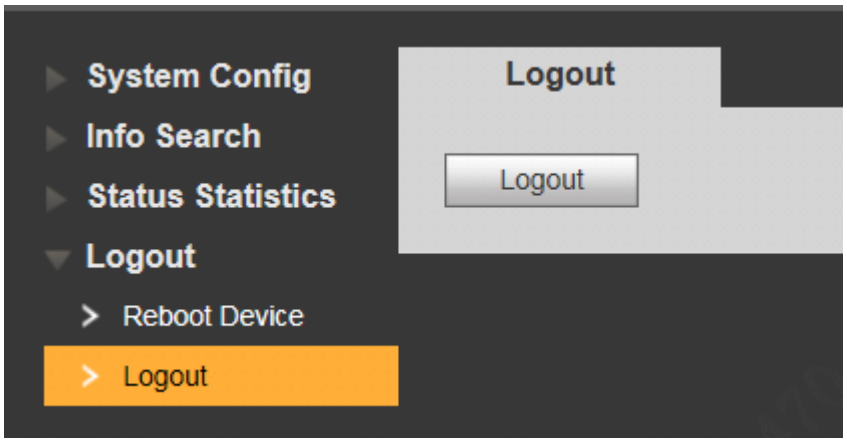

Figure 7-47

8 FAQ

1. Question: Press the call key; the indicator light turns on, but VTO doesn't call?

   Answer: Please confirm validity of this call again.

2. Question: How can I hang up?

   Answer: Please press buttons on the VTO, and VTO will send corresponding prompt tone.

3. Question: There is no sound or light, and it doesn't start. How can I deal with it?

   Answer: Check whether power supply is normal, and whether socket is in good contact.

4. Question: It prompts that the call is unreachable. How can I deal with it?

   Answer: Network failure. Please check whether network cable between this device and extension is inserted in place.

5. Question: After swiping a card, there is no response?

   Answer: Please check whether your card is IC card or whether your VTO supports card swiping.

6. Question: After swiping card, it prompts that card number is invalid. How can I deal with it?

   Answer: The card status is abnormal. Please contact the administrator to inspect and confirm.

7. Question: After swiping card, it beeps once, but the door is not opened?

   Answer: Please confirm whether the card has been authorized.

8. Question: How can I deal with problems that are not confirmed or cannot be solved?

   Answer: Please consult professional technical support.

Appendix 1 Technical Parameters

Appendix 1.1 VTO6210B

Model		VTO6210B
System	Main Processor	Embedded microcontroller
	Operating System	Embedded LINUX operating system
Video	Video Compression Standard	H.264
	Input/ Proximity Sensor	1.30 megapixel CMOS HD camera
	Night Vision	Support
Audio	Input	Omnidirectional microphone
	Output	Built-in speaker
	Talk	Support two-way audio talk
Operating Mode	Input	Touch key (with backlight)
	Swiping Card	Built-in IC card induction read head
Alarm	Tamper Alarm	Support
	Lock Status Detection	Support
Network	Ethernet	10M/100Mbps self-adaptive
	Network Protocol	TCP/IP
Specification	Power Supply	DC 10V–15V
	Power Consumption	Standby ≤1W; working ≤10W
	Working Temperature	－10℃～+60℃
	Relative Humidity	10%RH～95%RH
	Size (Length× Width × Height)	114.2mm×43mm×154.2mm
	Weight	0.5kg

Appendix 1.2 VTO6000CM and VTO6100C

Model		VTO6000CM and VTO6100C
System	Main Processor	Embedded microcontroller
	Operating System	Embedded LINUX Operating System
Video	Video Compression Standard	H.264
	Input/ Proximity Sensor	1.30 megapixel CMOS HD camera
	Night Vision	Support
Audio	Input	Omnidirectional microphone
	Output	Built-in speaker
	Talk	Support two-way audio talk
Operating Mode	Input	Input with single key (with backlight)
	Swiping Card	Only VTO6100C supports
Alarm	Tamper Alarm	Support

	Lock Status Detection	Support
Network	Ethernet	10M/100Mbps self-adaptive
	Network Protocol	TCP/IP
	Power Supply	DC 10V–15V
	Power Consumption	Standby≤1W; working≤10W
	Working Temperature	－10℃～+60℃
	Relative Humidity	10%RH～95%RH
	Size (Length× Width × Height)	100mm×42mm×141mm
	Weight	0.5kg

Appendix 1.3 VTO2000A

Model		**VTO2000A**
System	Main Processor	Embedded microcontroller
	Operating System	Embedded LINUX Operating System
Video	Video Compression Standard	H.264
	Input/ Proximity Sensor	1 megapixel CMOS HD camera
	Night Vision	Support
Audio	Input	Omnidirectional microphone
	Output	Built-in speaker
	Talk	Support two-way audio talk
Operating Mode	Input	Input with single key
	Lock Status Detection	Support (optional)
Network	Ethernet	10M/100Mbps self-adaptive
	Network Protocol	TCP/IP
Specification	Power Supply	DC 10V–15V
	Power Consumption	Standby≤1W; working≤10W
	Working Temperature	－30℃～+70℃
	Relative Humidity	10%RH～90%RH
	Size (Length× Width × Height)	129.9mm×32.2mm×140mm
	Weight	0.8kg

Appendix 1.4 VTO2000A-2

Model		**VTO2000A-2**
System	Main Processor	Embedded microcontroller
	Operating System	Embedded LINUX Operating System
Video	Video Compression Standard	H.264
	Input/ Proximity Sensor	1 megapixel CMOS HD camera
	Night Vision	Support
Audio	Input	Omnidirectional microphone
	Output	Built-in speaker
	Talk	Support two-way audio talk
Operating	Input	Input with single key

Mode	Lock Status Detection	Support (optional)
Network	Ethernet	10M/100Mbps self-adaptive
	Network Protocol	TCP/IP
Specification	Power Supply	DC 24V
	Power Consumption	Standby ≤1W; working≤7W
	Working Temperature	－30℃～+60℃
	Relative Humidity	10%RH～90%RH
	Size (Length× Width × Height)	129.9mm×32.2mm×140mm
	Weight	0.8kg

Appendix 2 Accessory Specification

Appendix 2.1 Specification of Network Cable


Caution

Please try to ensure that wiring length L_N doesn't exceed 100m.

Please select network cable reasonably according to wiring length L_N between VTO and VTH.

Specification of Network Cable	$0<L_N\leq 50m$	$50<L_N\leq 100m$
UTP Cat5e/Cat6: 10 Ohm/100m	Yes	Yes
UTP Cat5e/Cat6: 18.8 Ohm/100m	Yes	No

Appendix 2.2 Specification of Extension Power Cord


Caution

Before power on, please check whether positive and negative poles of extension power cord are wired correctly; avoid reverse connection.

Please select suitable extension power cord according to distance L_C between adapter and VTO.

Specification of Extension Power Cord	$0<L_C\leq 30m$	$30<L_C\leq 100m$
20AWG	Yes	No
18AWG	Yes	Yes
17AWG	Yes	Yes

Appendix 2.3 Specification of Embedded Box

Model	Specification of Embedded Box
VTO6000C, VTO6100C, VTO6000CM	86 box
VTO6110B, VTO6210B, VTO6110BW	86 box, 120 box
VTO2000A	Flush mounting box 126mm×115mm
VTO2000A-2	Flush mounting box 126 mm×115mm