

Unit VTO
(Version 3.1)
User's Manual

V1.0.0

Trademark

- VGA is the trademark of IBM.
- Windows logo and Windows are trademarks or registered trademarks of Microsoft.
- Other trademarks and company names mentioned are the properties of their respective owners.

About this Document

- This document is for reference only. Please refer to the actual product for more details.
- This document serves as a reference for multiple types of products, whose specific operations won't be enumerated. Please operate according to actual products.
- The user shall undertake any losses resulting from violation of guidance in the document.
- In case that PDF document cannot be opened, please upgrade the reading tool to the latest version or use other mainstream reading tools.
- This company reserves rights to revise any information in the document anytime; and the revised contents will be added to the new version without prior announcement. Some functions of the products may be slightly different before and after revision.
- The document may include technically inaccurate contents, inconsistencies with product functions and operations, or misprint. Final explanations of the company shall prevail.

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.

Overview

This document mainly introduces function, structure, networking, mounting process, debugging process, WEB interface operation and technical parameters of unit VTO product, matched with Version 3.1 WEB interface.

Applicable Model

VTO1220A, VTO1220BW, VTO1210B-X, VTO1210C-X and VTO1210A-X

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.

Symbol Definition

The following symbols may appear in the document. Please refer to the table below for the respective definition.

Symbol	Note
 Danger	It indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
 Warning	It indicates a moderate or low level of potential danger which, if not avoided, could result in minor or moderate injury.
 Caution	It indicates a potential risk that, if ignored, could result in damage to device, loss of data, degraded performance, or unpredictable results.
 Anti-static	It means electrostatic-sensitive device.

 Protection against electric shock	It means high-voltage danger.
 Laser radiation	It means intensive laser radiation.
 Tip	It means that it can help you to solve some problems or save your time.
 Note	It means the additional information, which is to emphasize or supplement.

Revision Record

No.	Version No.	Revision Content	Release Date
1	V1.0.0	First release	2017.11.10

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

Legal Statement.....	I
Cybersecurity Recommendations.....	II
Preface.....	V
Important Safeguards and Warnings.....	VII
1 Product Overview	1
1.1 Product Profile.....	1
1.2 Product Function.....	1
2 Product Structure	3
2.1 VTO1220A/VTO1210A-X.....	3
2.1.1 Front Panel.....	3
2.1.2 Rear Panel.....	5
2.2 VTO1220BW/VTO1210B-X.....	5
2.2.1 Front Panel.....	5
2.3 VTO1210C-X.....	8
2.3.1 Front Panel.....	8
2.3.2 Rear Panel.....	10
2.4 Port Wiring Description.....	10
2.4.1 Access Input and Output Wiring.....	10
2.4.2 Analog Signal Wiring.....	11
2.4.3 RS485/RS422 Wiring.....	12
3 Networking Diagram	14
4 Device Mounting	15
4.1 Mounting Flow Chart.....	15
4.2 Open-case Inspection.....	15
4.3 Mounting Requirement.....	16
4.4 Device Mounting.....	16
4.4.1 VTO1220A/VTO1210A-X.....	16
4.4.2 VTO1210B-X/VTO1220BW.....	17
4.4.3 VTO1210C-X.....	18
5 Device Debugging	21
5.1 Debugging Settings.....	21
5.1.1 Single Debugging.....	21
5.1.2 Batch Debugging.....	35
5.2 Debugging Verification.....	42
5.2.1 Verification with Version 3.1 VTH.....	42
5.2.2 Verification with Version 4.0 VTH.....	44
6 Basic Function.....	46
6.1 Call Function.....	46
6.1.1 Call Management Centre.....	46
6.1.2 Single Call of VTH.....	47
6.1.3 Group Call.....	47

6.2	Unlock Function.....	49
6.2.1	Remote Unlock at VTH/VTs.....	49
6.2.2	Open Door at WEB Interface.....	49
6.2.3	Unlock with IC Card.....	49
6.2.4	Unlock with Exit Button.....	49
6.2.5	Unlock with Password.....	49
6.3	Issue Card.....	50
6.3.1	Issue Card from Local VTO.....	50
6.3.2	Issue Card at Access Manager Interface.....	51
6.3.3	Issue Card at Digital Indoor Station Manager Interface.....	52
6.4	Monitoring Function.....	52
6.5	Tamper Switch.....	53
6.6	Restore Backup.....	53
7	Local Operation.....	55
7.1	Enter Project Settings.....	55
7.2	Modify IP.....	55
7.3	Modify Volume.....	55
7.4	Issue Card.....	56
7.5	View Version Info.....	56
8	WEB Config.....	57
8.1	Initialization.....	57
8.2	Reset the Password.....	58
8.3	System Login.....	60
8.4	User Manager.....	61
8.4.1	Add User.....	61
8.4.2	Modify User.....	62
8.4.3	Delete User.....	64
8.5	Network Parameter Config.....	64
8.5.1	TCP/IP.....	64
8.5.2	FTP Server.....	65
8.5.3	Port.....	65
8.5.4	DDNS Server.....	67
8.5.5	HTTPS Setting.....	68
8.5.6	UPnP.....	68
8.5.7	IP Purview.....	71
8.6	LAN Config.....	72
8.7	Local Parameter Config.....	73
8.7.1	Local Config.....	73
8.7.2	Access Manager.....	74
8.7.3	Sound Control.....	76
8.7.4	Talk Manager.....	77
8.7.5	System Time.....	78
8.7.6	Config Manager.....	79
8.8	VTO Info.....	79
8.9	Indoor Manager.....	80
8.9.1	Add VTH.....	81
8.9.2	Modify VTH.....	81

8.9.3 Delete VTH.....	82
8.9.4 Config Manager.....	82
8.9.5 Card Manager.....	83
8.10 Allocator Manager.....	85
8.11 Video Set.....	85
8.11.1 Video Set.....	85
8.11.2 Audio Set.....	87
8.12 IPC Info.....	87
8.12.1 Add One IPC.....	88
8.12.2 Delete.....	89
8.12.3 Batch Import.....	89
8.12.4 Batch Export.....	89
8.13 IP Allocate Auto.....	89
8.14 Publish Information.....	90
8.14.1 Send Info.....	90
8.14.2 History Info.....	91
8.15 Info Search.....	92
8.15.1 Call History.....	92
8.15.2 Alarm Record.....	92
8.15.3 Unlock Record.....	92
8.16 Status Statistics.....	93
8.17 Reboot Device.....	93
8.18 Logout.....	93
Appendix 1 Technical Parameters.....	95

1.1 Product Profile

Unit 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, info, video preview and record search. It is mainly applied in apartments and villas, 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, fingerprint, 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.

Info

Send info to VTH.

Record Search

Search call records, alarm records and unlock records.

Info Search

Search the info sent by Property Management Center.

2.1 VTO1220A/VTO1210A-X

2.1.1 Front Panel

Connect power supply, and the screen turns on after about 2 minutes. The system is booted and enters normal working interface.



Figure 2-1

No.	Name	Description
1	Photosensitive device	Sense ambient light and choose fill-in light or not.
2	Fill-in light	Provide fill-in light for camera in case of insufficient light.
3	Microphone	Audio input.












No.	Name	Description
4	Key area	<ul style="list-style-type: none"> • : delete previous character or end the current call. • Ten numeric keys: enter 0~9 numbers. • : to unlock with password, press , enter password and press  again to complete. • : call key. After entering room number, press this key to make a call. • : press this key to call the management center directly.
5	Speaker	Audio output.
6	Card swiping area	Unlock by swiping card.
7	Display screen	<p>Display prompt, date and time.</p> <ul style="list-style-type: none"> • “User: room no. + press  to make a call. • “Center: press  to call Video Intercom Master Station (VTS). • “Unlock:  + password + , enter unlock password and press  again for confirmation.
8	Camera	Monitor the door area.

Table 2-1

2.1.2 Rear Panel

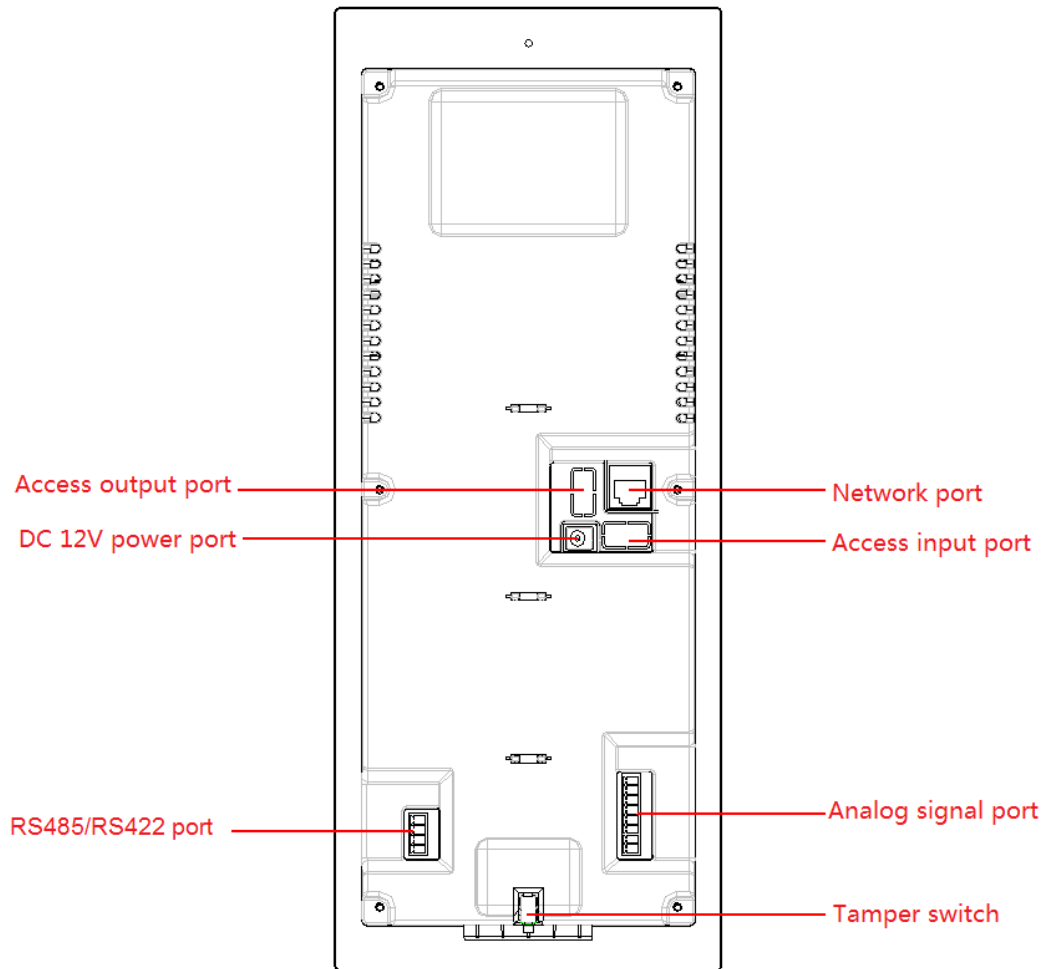


Figure 2-2

2.2 VTO1220BW/VTO1210B-X

2.2.1 Front Panel

Connect power supply, and the screen turns on after about 2 minutes. The system is booted and enters normal working interface.

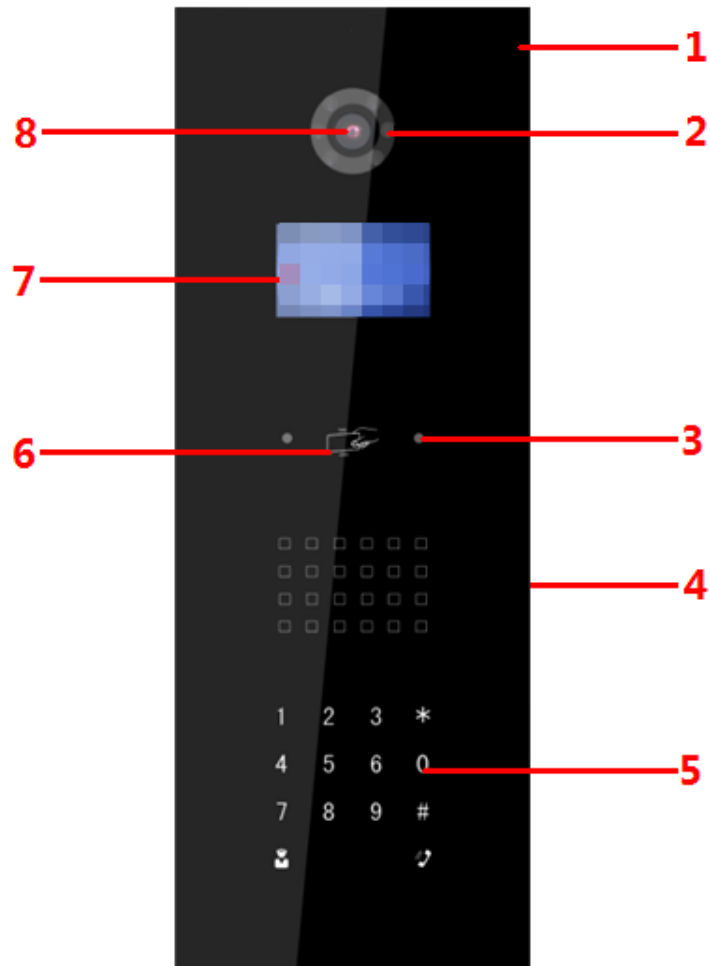




Figure 2-3

No.	Name	Description
1	Microphone	Audio input.
2	Fill-in light	Provide fill-in light for camera in case of insufficient light.
3	Proximity sensor	Trigger proximity sensing when a person or object passes by.
4	Speaker	Audio output.
5	Key area	<ul style="list-style-type: none"> • *: delete previous character or end the current call. • Ten numeric keys: enter 0~9 numbers. • #: to unlock with password, press #, enter password and press # again to complete. • : call key. After entering room number, press this key to make a call. • : press this key to call the management center directly.
6	Card swiping area	Unlock by swiping card.


No.	Name	Description		
7	Display screen	<p>Display prompt, date and time.</p> <ul style="list-style-type: none"> ● “User: room no. + press 8	Camera	Monitor the door area.

Table 2-2

2.3 VTO1210C-X

2.3.1 Front Panel



Figure 2-4

No.	Name	Description
1	Microphone	Audio input.
2	Fill-in light	Provide fill-in light for camera in case of insufficient light.
3	Speaker	Audio output.





No.	Name	Description
4	Key area	<ul style="list-style-type: none"> ● * : delete previous character or end the current call. ● Ten numeric keys: enter 0~9 numbers. ● # : to unlock with password, press # , enter password and press # again to complete. ●  : call key. After entering room number, press this key to make a call. ●  : press this key to call the management center directly. ● ^ v : at the contact interface, press these keys to page up and down.
5	Card swiping area	Unlock by swiping card.
6	Display screen	<p>Display prompt, date and time.</p> <ul style="list-style-type: none"> ● “User: room no. + press  to make a call. ● “Center: press  to call Video Intercom Master Station (VTS). ● “Unlock: # + password + #”, means that if you want to unlock with password, please press # , enter unlock password and press # again for confirmation.
7	Camera	Monitor the door area.

Table 2-3

2.3.2 Rear Panel

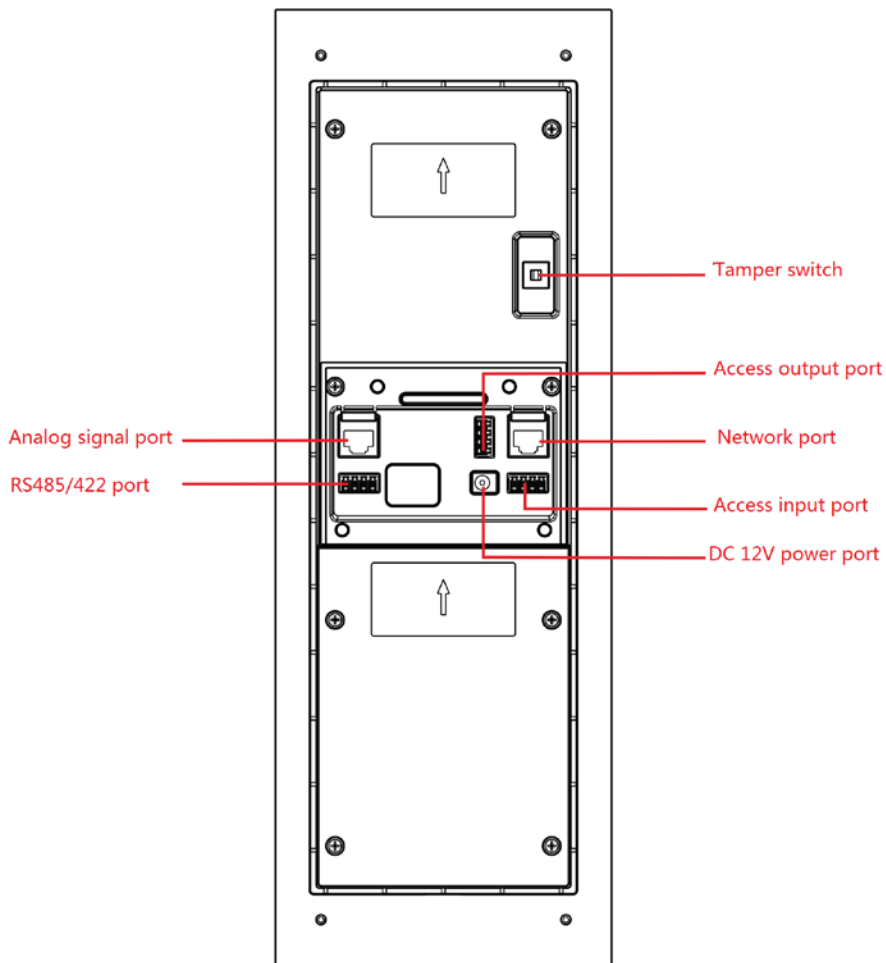


Figure 2-5

2.4 Port Wiring Description

Different models of devices may have different port positions and port types, but port functions are consistent.

2.4.1 Access Input and Output Wiring



Access input and output port of VTO1220A, VTO1210A-X, VTO1220BW, VTO1210B-X and VTO1210C-X have two terminals.

- Access input port connects exit button and door sensor signal.
- Access output port controls opening or closing of normally open (NO)/normally closed (NC) lock.

Different locks have different wiring methods, as shown in Figure 2-6, Figure 2-7 and Figure 2-8.

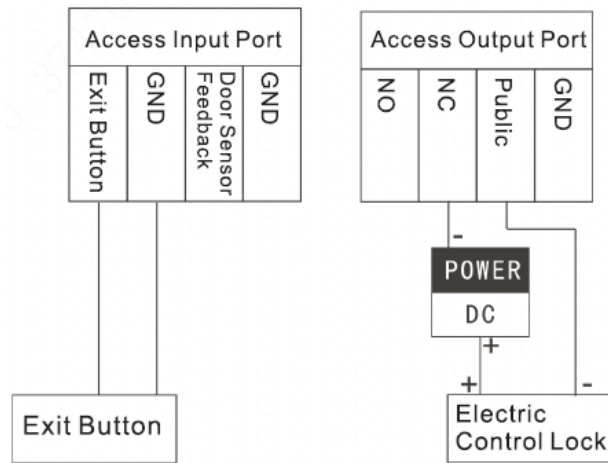


Figure 2-6

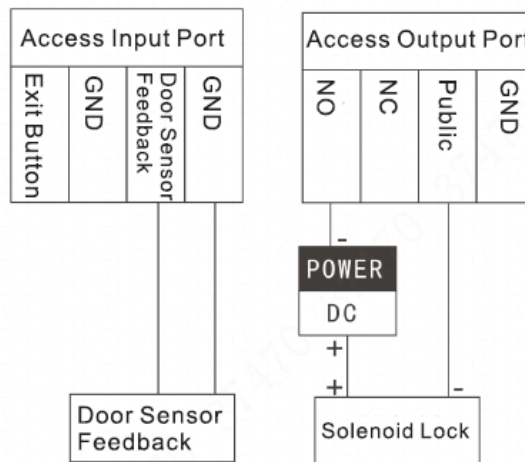


Figure 2-7

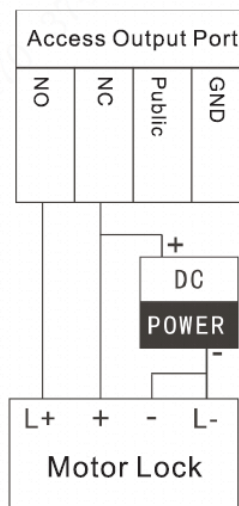


Figure 2-8

2.4.2 Analog Signal Wiring

Analog signal port connects analog signal from the distributor, which applies to –X devices only. Analog signal port type includes RJ45 Ethernet port or terminal; both functions and wirings are the same, as shown in Figure 2-9.

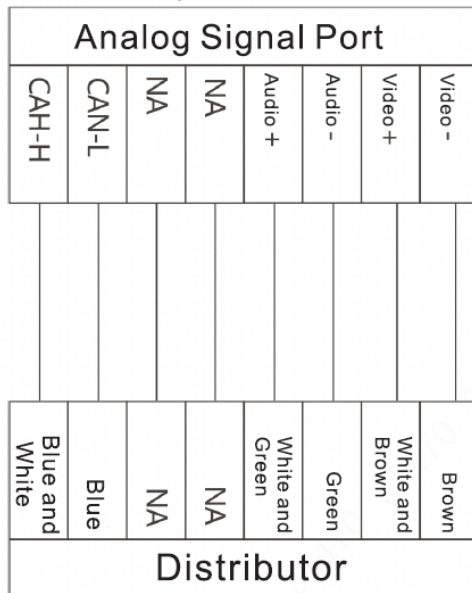


Figure 2-9

2.4.3 RS485/RS422 Wiring

Connect RS485 or RS422 communication device, as shown in Figure 2-10, Figure 2-11 and Figure 2-12.

 Note

VTO1220A, VTO1210A-X, VTO1220BW, VTO1210B-X and VTO1210C-X can connect RS485 and RS422 communication devices, with shared ports.

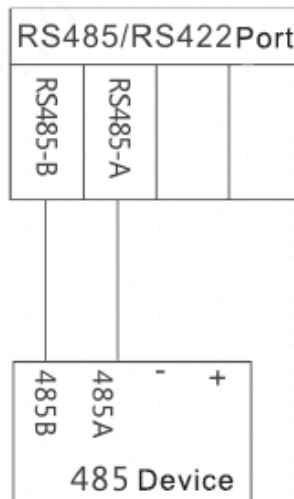


Figure 2-10

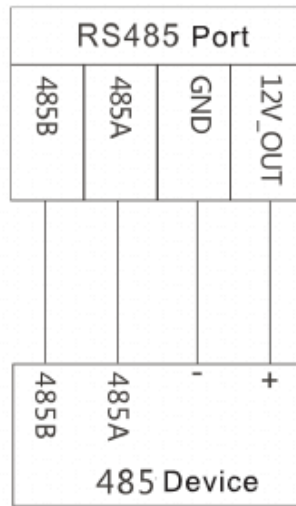


Figure 2-11

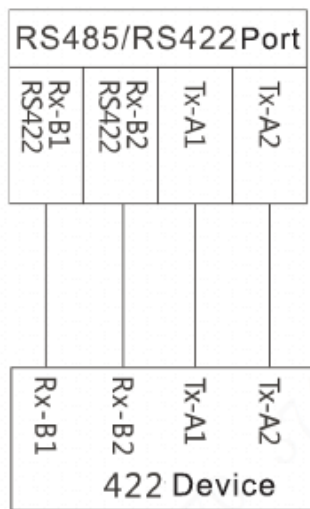


Figure 2-12

3

Networking Diagram

Networking diagram of VTO is shown in Figure 3-1.

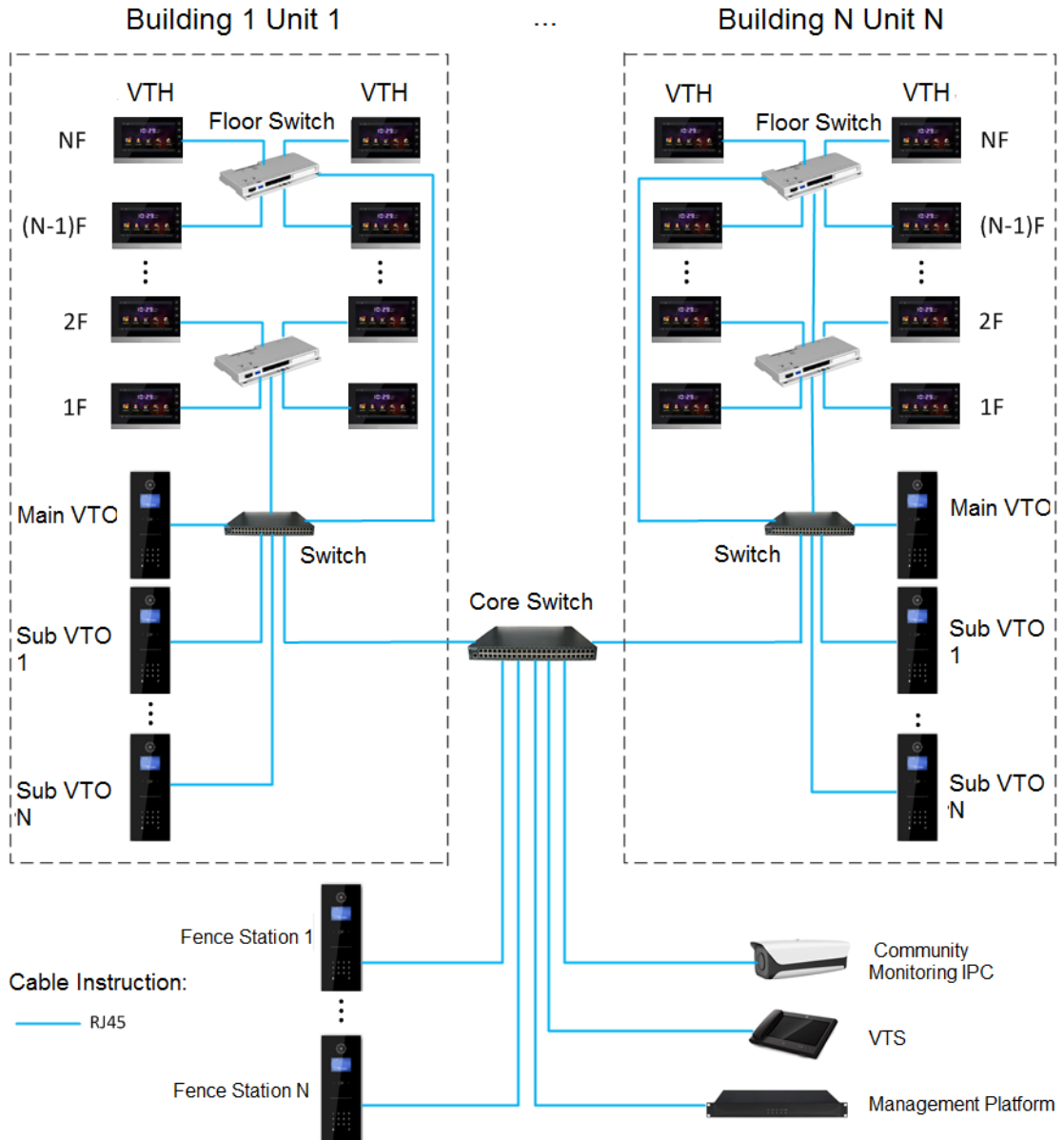


Figure 3-1

4.1 Mounting Flow Chart

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

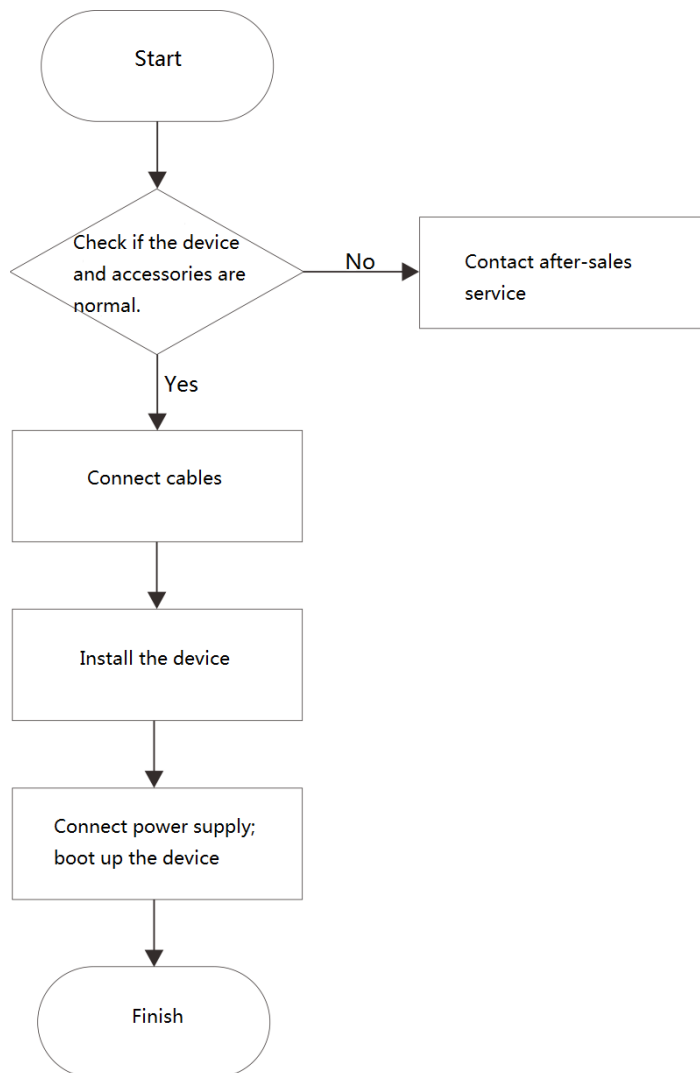


Figure 4-1

 Note

- For cable connection, please refer to “2.4 Port Wiring Description”.
- For device mounting, please refer to “4.4 Device Mounting”.

4.2 Open-case Inspection

When receiving the device, please carry out open-case inspection by reference to Table 4-1.

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 VTO1220A/VTO1210A-X

VTO1220A/VTO1210A-X devices can be mounted with metal flush mounting box.

 Note

Overall dimension of metal flush mounting box is 135mm×362.5mm×60mm.

Groove the wall according to hole positions of metal flush mounting box; then, drill holes in the grooves according to hole positions of box screws.

Mount the expansion pipes in holes.

Connect cables, pass through the box and connect the cables in walls. Please refer to "2.4 Port Wiring Description" for details.

Fix the metal flush mounting box onto the wall with ST3×18 screws.

Fix the bare device onto the metal flush mounting box with M3×16 screws.

Apply glue between bare device and the wall, in order to fix the device.

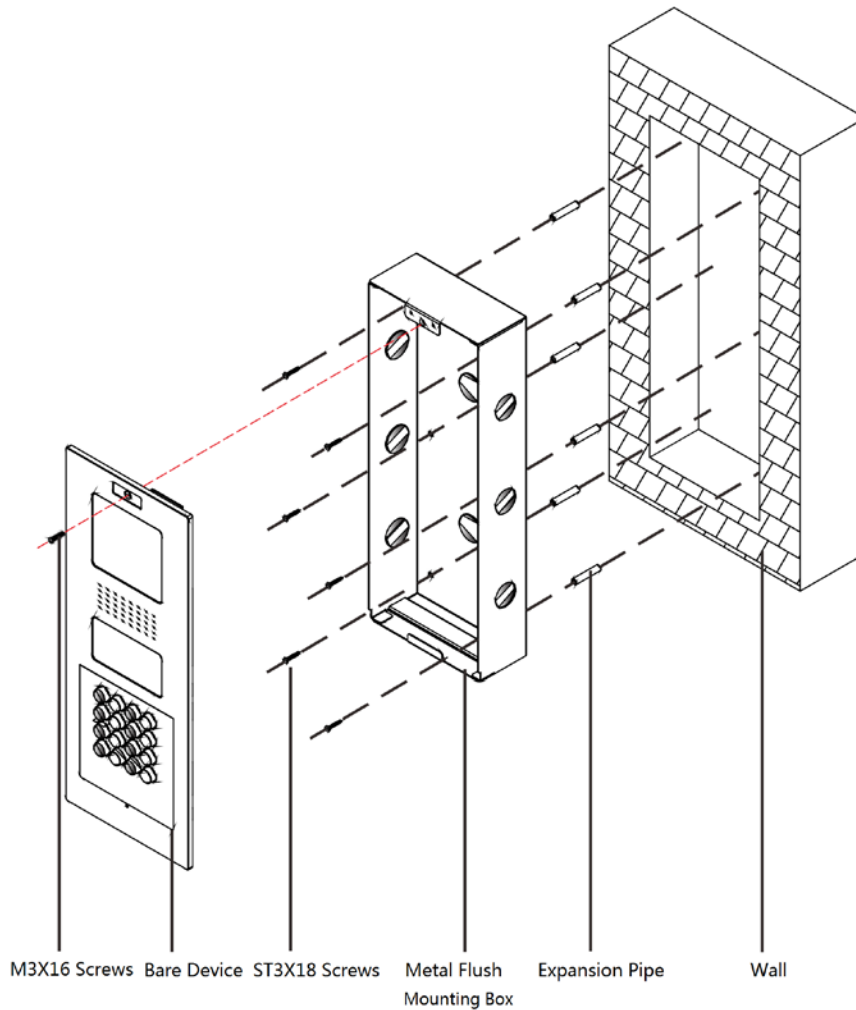


Figure 4-2

4.4.2 VTO1210B-X/VTO1220BW

4.4.2.1 Plastic Flush Mounting Box

Step 1 Embed the plastic flush mounting box into the wall.

 Note

Overall dimension of plastic flush mounting box is 149mm×400mm×63mm.

Step 2 Connect cables, pass through the bracket and connect the cables in walls. Please refer to “2.4 Port Wiring Description” for details.

Step 3 Fix the mounting bracket onto the box with ST3×18 screws.

Step 4 Fix the bare device onto mounting bracket with M3×16 screws.

Step 5 Apply glue between the bare device, box and wall.

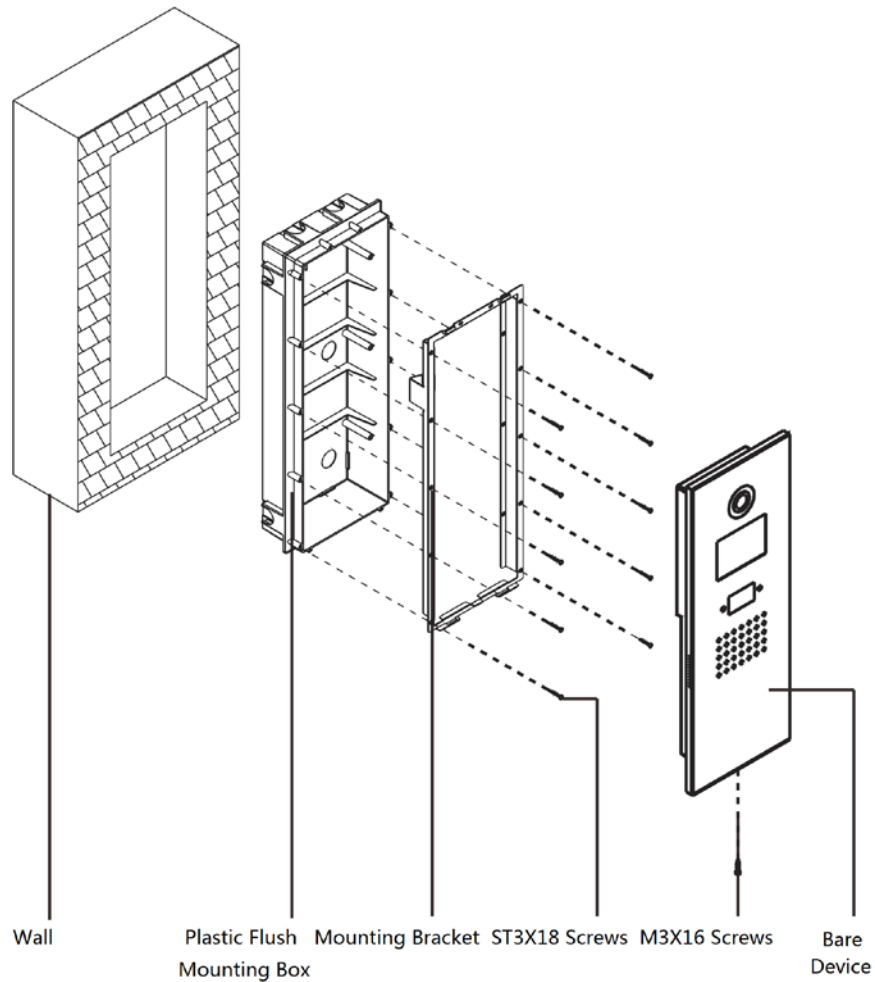


Figure 4-3

4.4.3 VTO1210C-X

4.4.3.1 Surface Mounting

- Step 1 Drill holes in the wall according to hole positions of surface mounting box; insert expansion pipes.
- Step 2 Fix surface mounting box onto the wall with ST4.2x25 screws.
- Step 3 Connect cables, and connect the cables in walls. Please refer to “2.4 Port Wiring Description” for details.
- Step 4 Fix the bare device onto the box with M4x30 screws.
- Step 5 Apply glue between the box and wall.

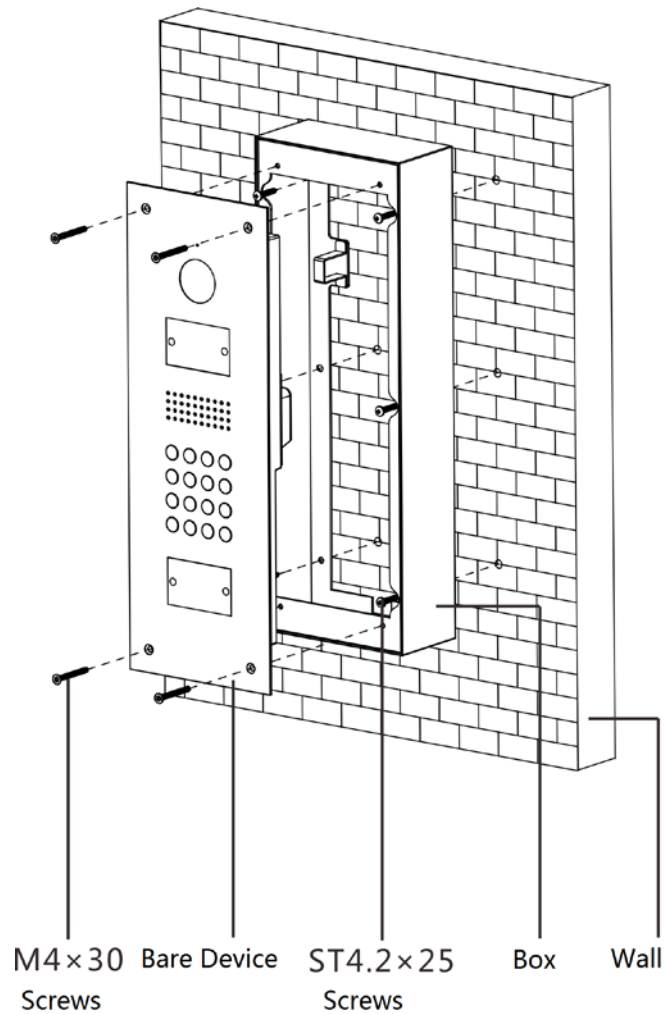



Figure 4-4

4.4.3.2 Plastic Flush Mounting Box

Step 1 Embed the plastic flush mounting box into the wall.

 Note

Overall dimension of plastic flush mounting box is 126mm×389mm×71mm.

Step 2 Connect cables, and connect the cables in walls. Please refer to “2.4 Port Wiring Description” for details.

Step 3 Fix the bare device onto the mounting bracket with M4×40 screws.

Step 4 Apply glue between the bare device, box and wall.

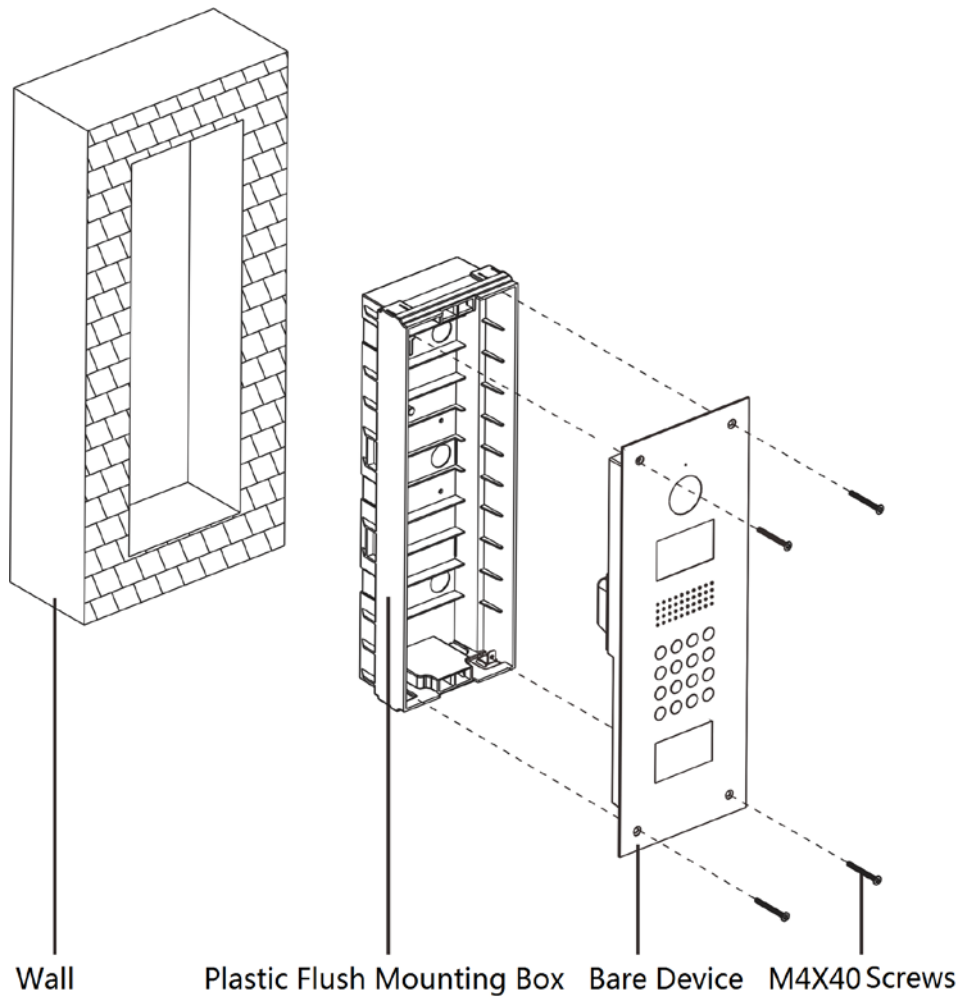


Figure 4-5

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



Debugging settings are different depending on matched VTH program.

The system provides two debugging methods. Please select according to matched VTH program.

- Single debugging
It applies to Version 3.1 and 4.0 VTH programs.
Set VTO info and VTH info at WEB interface of every VTO, set VTH info, network info and VTO info on every VTH, and thus realize video intercom function.
- Batch debugging
It only applies to Version 3.1 VTH programs.
Set VTO info and VTH info at WEB interface of every VTO, set VTH network segment and enable it at WEB interface of a unit VTO, and then add info about all VTOs. Initialize every VTH to realize video intercom function.

5.1.1 Single Debugging

5.1.1.1 VTO Settings

5.1.1.1.1 Initialization

For the first time, please initialize and modify login password.



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 supply and power on.

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.

Device

1 Setting 2 Protect 3 OK

Username admin

New Password

Weak Middle Strong

Confirm

Use a password that has 8 to 32 characters, it can be a combination of letters, numbers and symbols (please do not use special symbols like \\' \\' ; \\' \\' &)

Next

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.

Device

1 Setting 2 Protect 3 OK

Email

(To reset password, please input properly or update in time)

Next

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!"

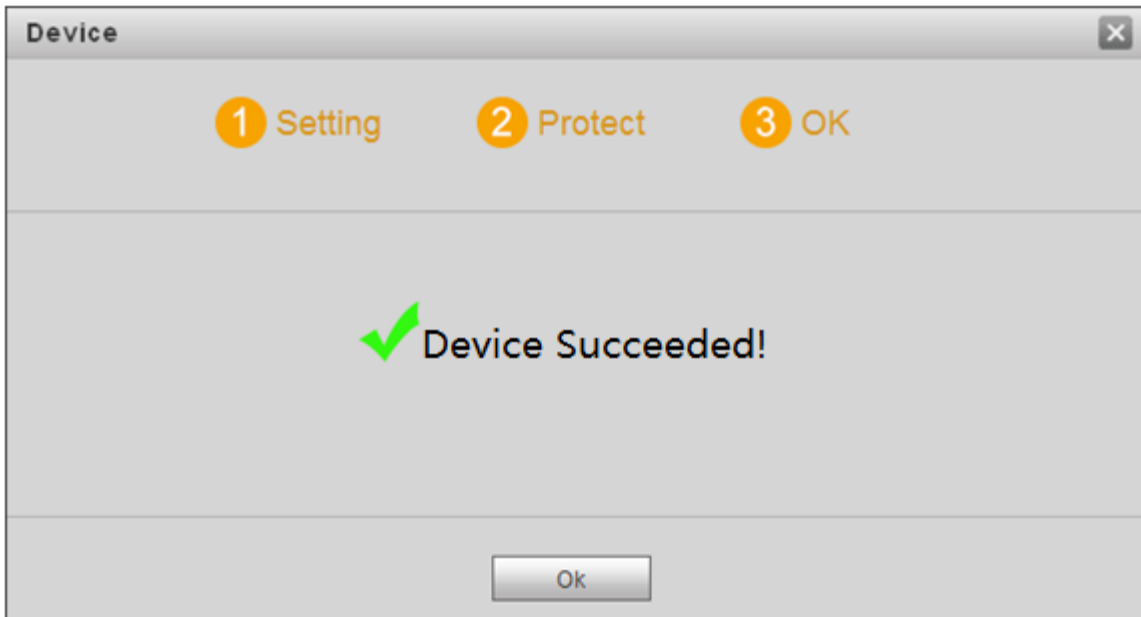


Figure 5-3

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.

5.1.1.1.2 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.

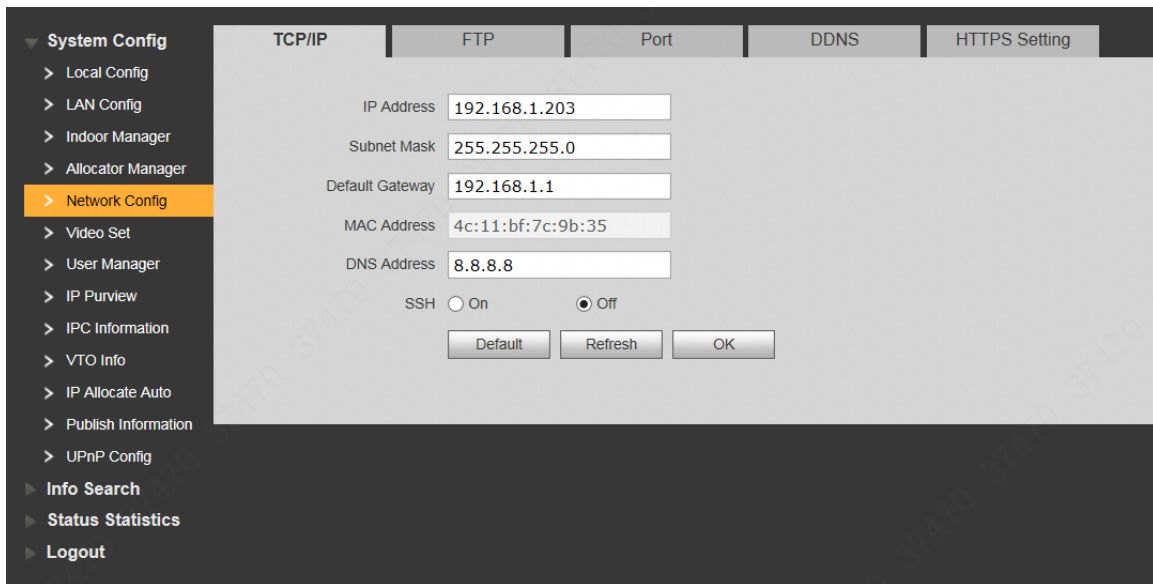


Figure 5-5

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.

5.1.1.1.3 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.

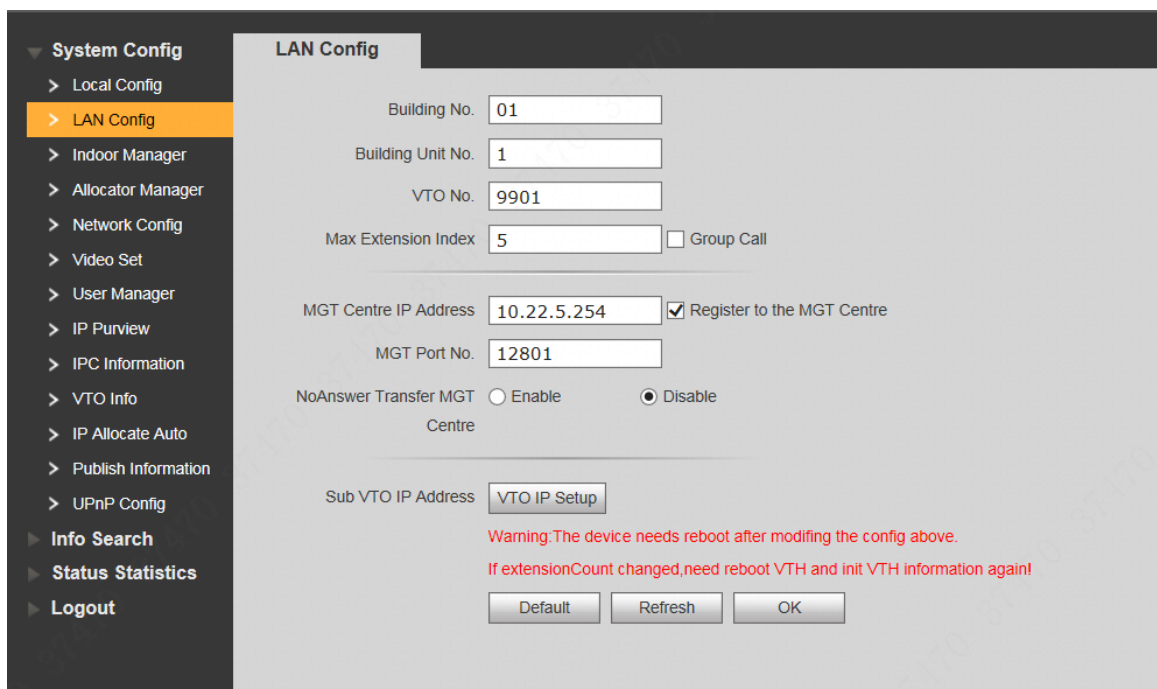


Figure 5-6

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.”.
- To provide group call, please select “Group Call” and set “Max Extension Index”.

Step 3 Click “OK”.

5.1.1.1.4 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”.

5.1.1.2 VTH Config (Version 3.1)

5.1.1.2.1 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.

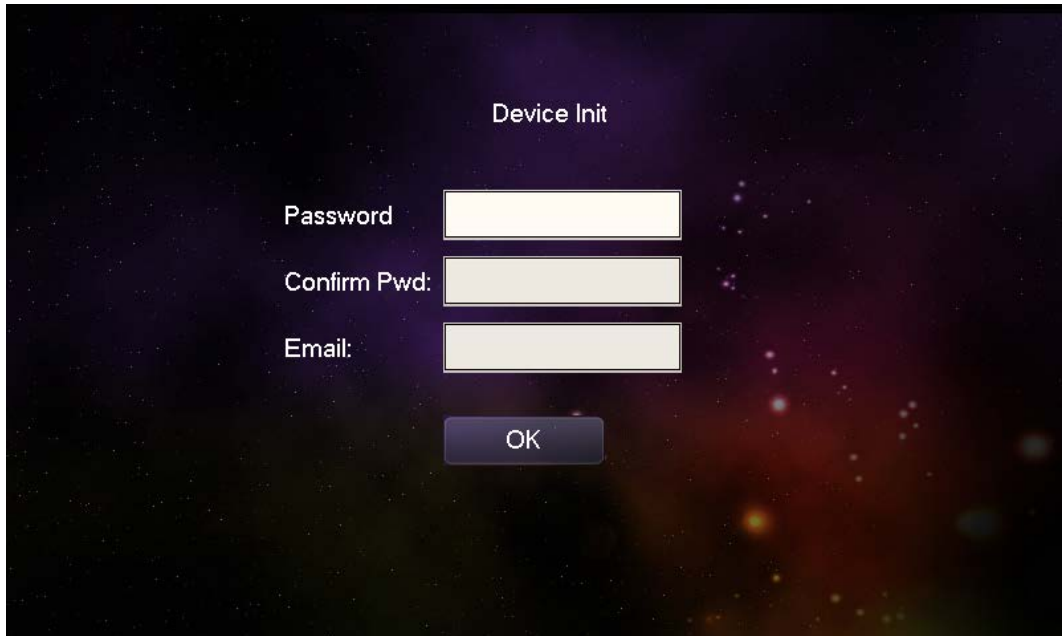



Figure 5-9

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.

5.1.1.2.2 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.

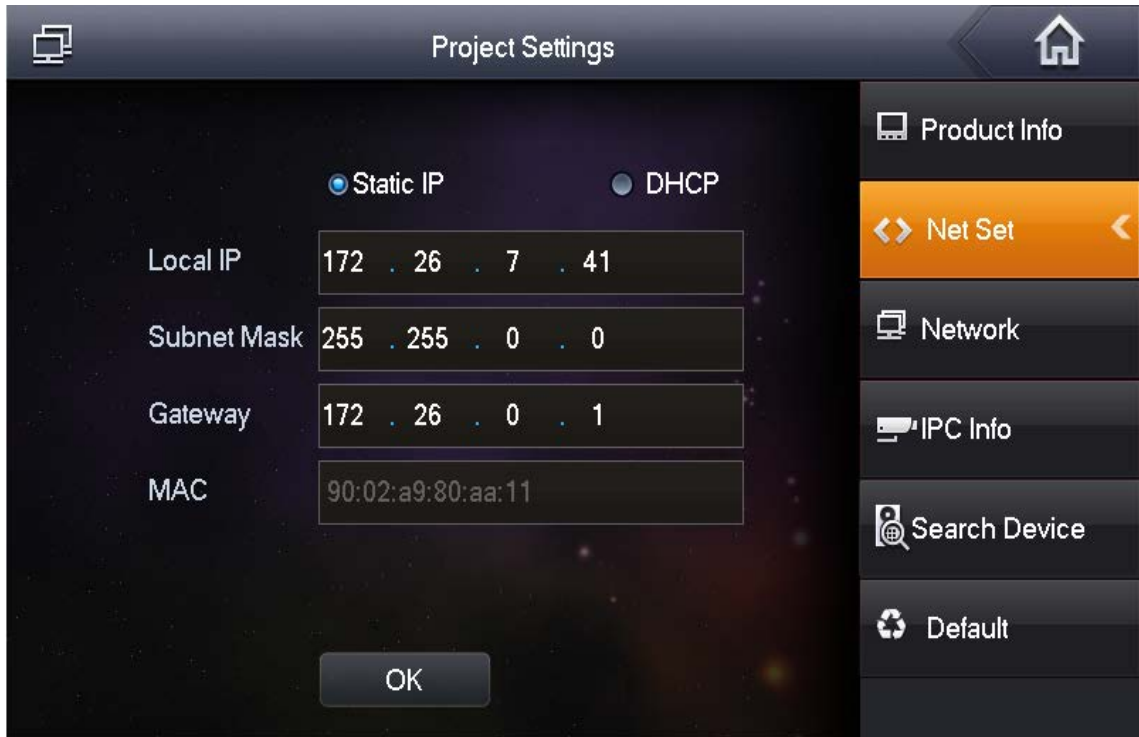


Figure 5-10

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.

5.1.1.2.3 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.

5.1.1.2.4 Set Network

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

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.

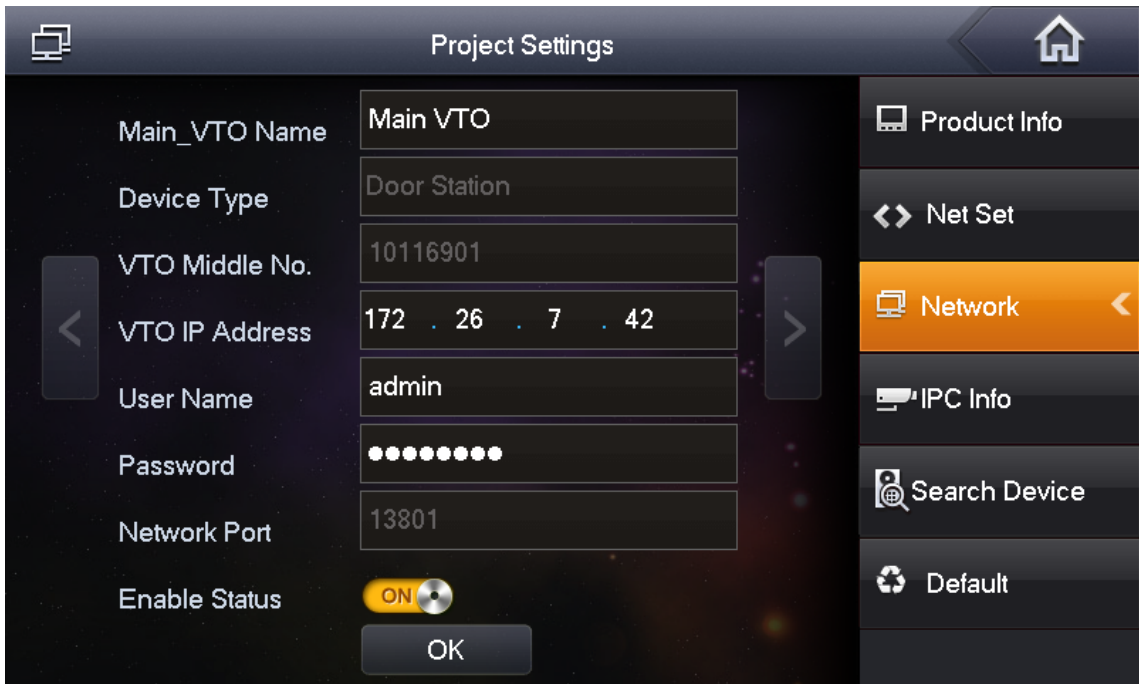







Figure 5-12

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 .

 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. Enter sub VTO name, IP address, “Username” and “Password”.
3. Switch “Enable Status” to .
- 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 no.), “Username” and “Password”.
 3. Switch “Enable Status” to .

Step 5 Click [OK] to save the settings.

5.1.1.3 VTH Settings (Version 4.0)

5.1.1.3.1 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.

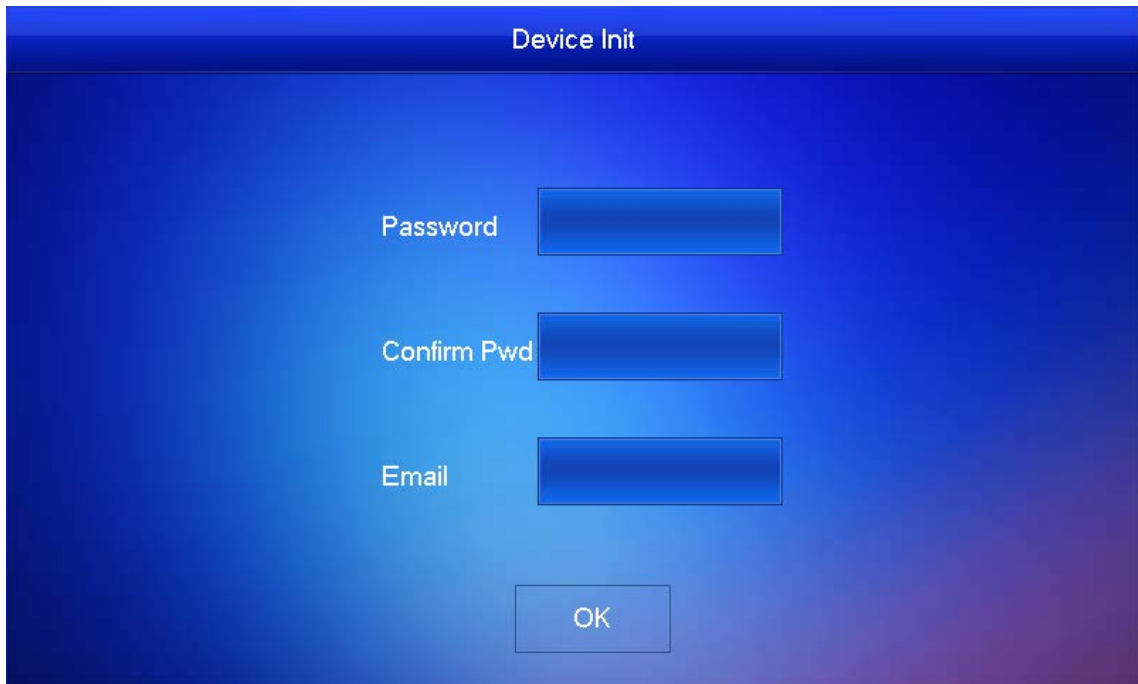


Figure 5-13

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

The system displays main interface.

5.1.1.3.2 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.

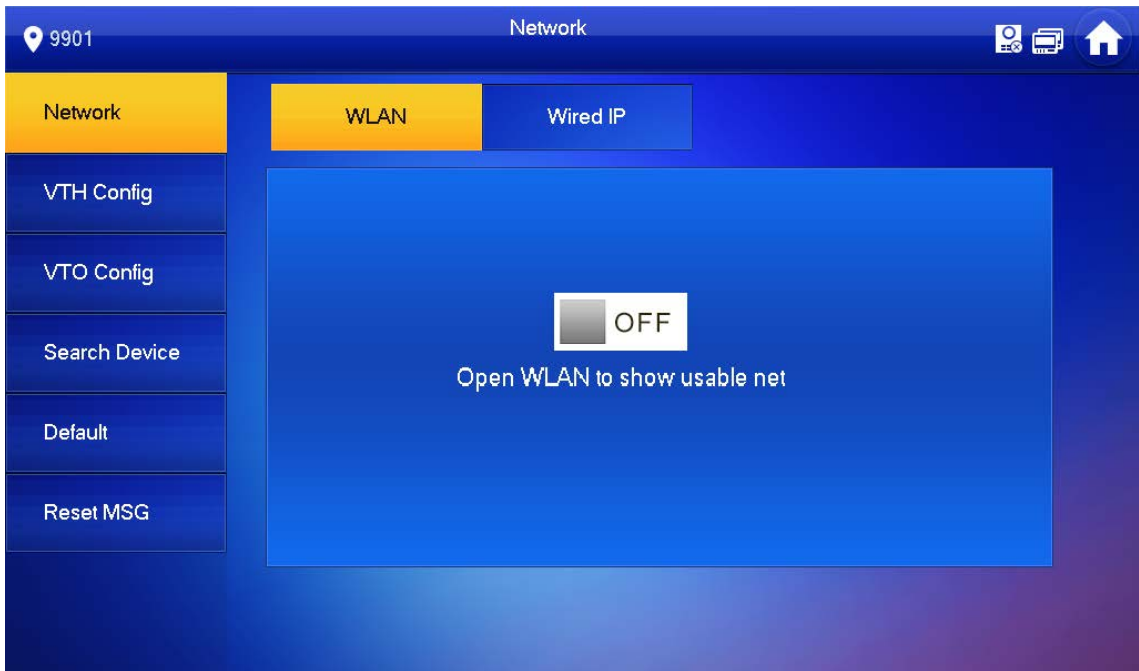


Figure 5-14



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

5.1.1.3.3 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.

Field	Value
Room No.	9901
Master	Master
Master IP	0 . 0 . 0 . 0
Master Name	
Master Pwd	
Version	V4.000.0000.0.R.20171024
SSH	ON

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.

5.1.1.3.4 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 .

 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 sub VTO.
 1. Press  to switch to sub VTO setting interface.
 2. Enter sub VTO name, IP address, “User Name” and “Password”.
 3. Switch the “Enable Status” to be .
- 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 no.), “User Name” and “Password”.
 3. Switch the “Enable Status” to be .

5.1.2 Batch Debugging

5.1.2.1 VTO Settings

5.1.2.1.1 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 5-20.

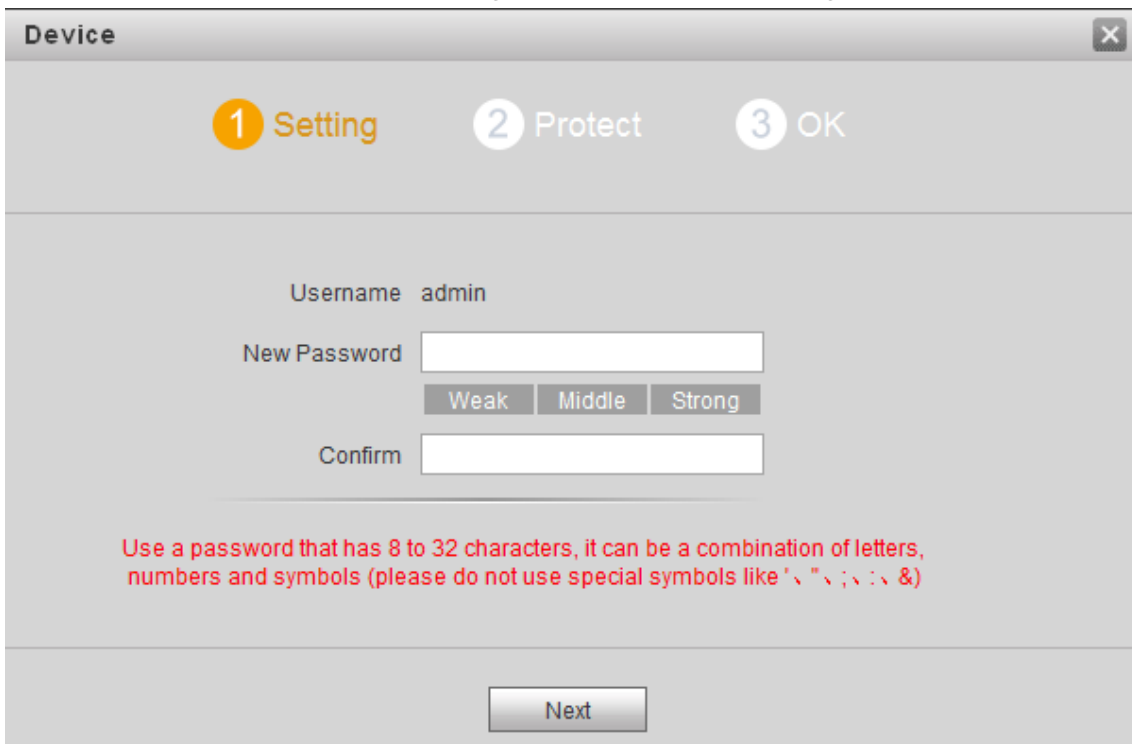


Figure 5-20

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

The system displays “Protect” interface, as shown in Figure 5-21.

 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.

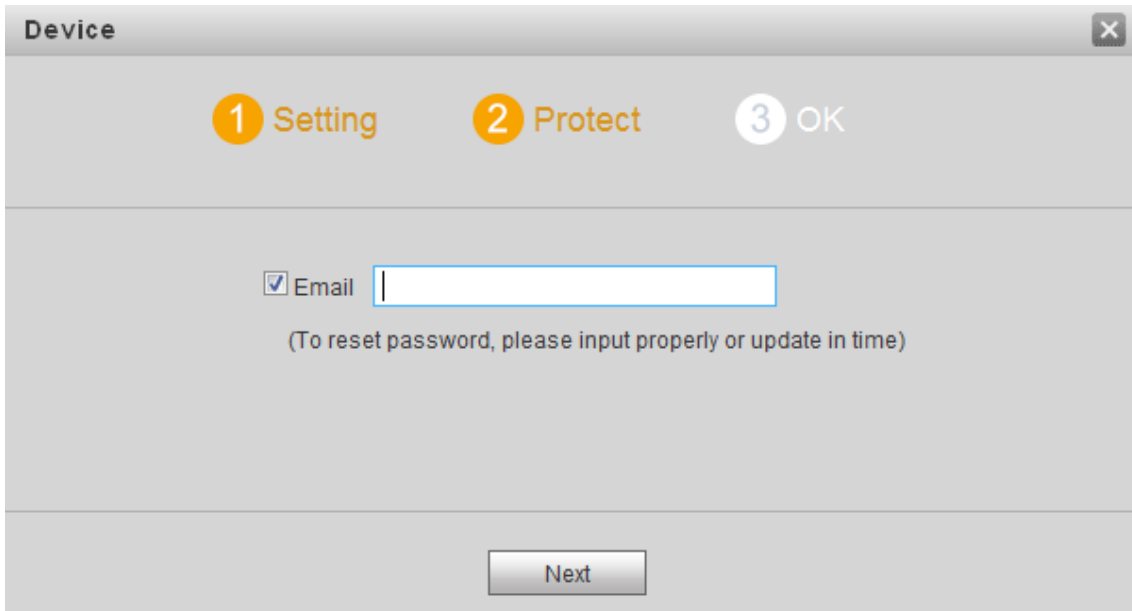


Figure 5-21

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 5-22, and shows "Device succeeded!"

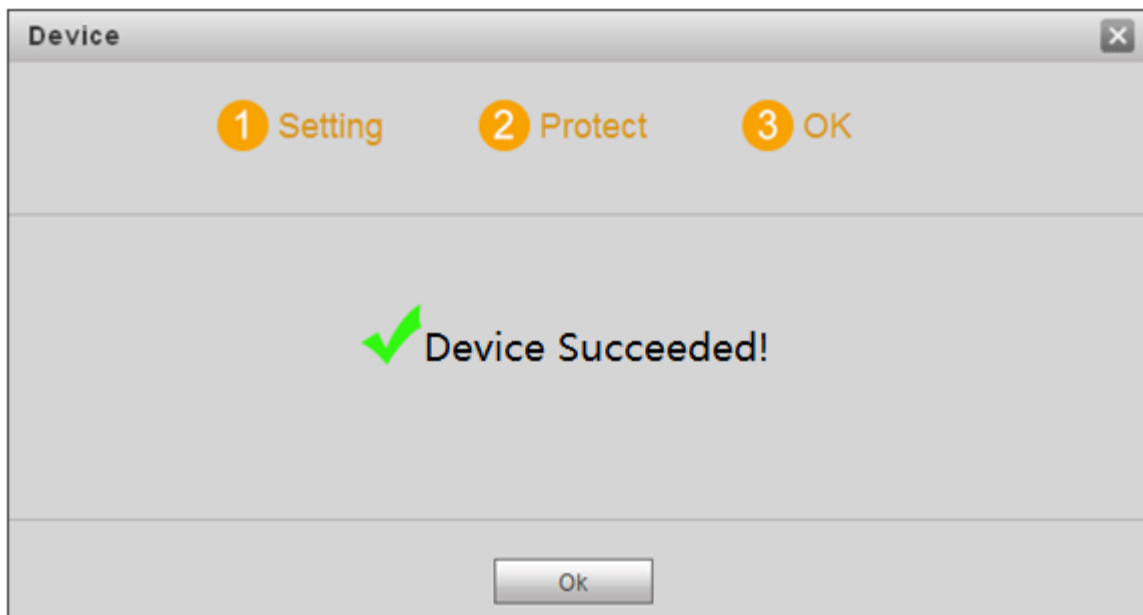


Figure 5-22

Step 6 Click "OK".

The system displays WEB login interface, as shown in Figure 5-23.

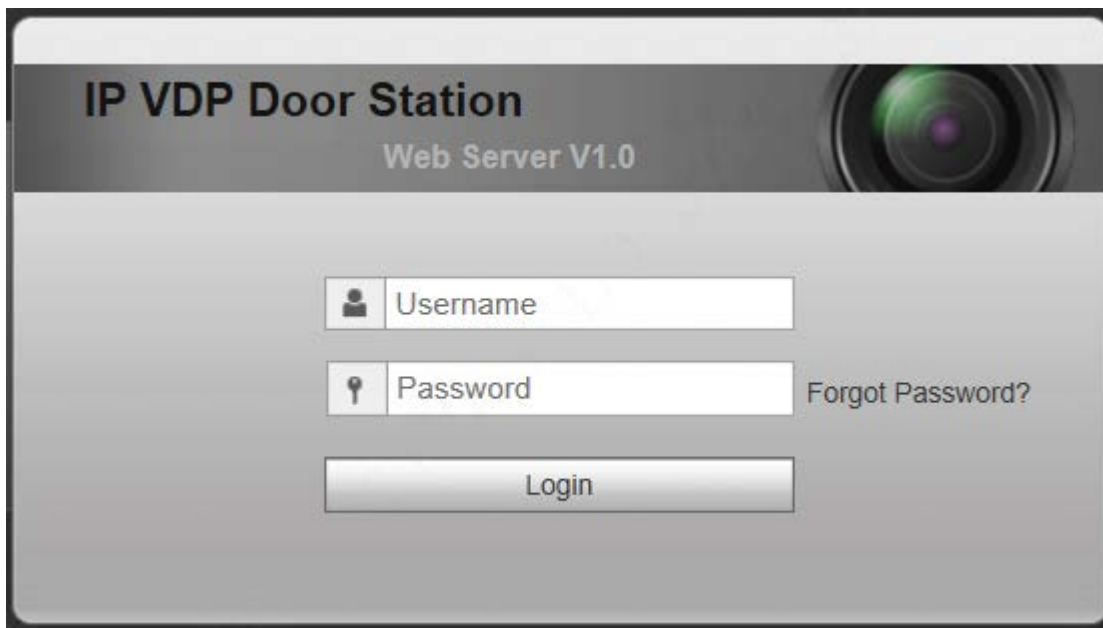


Figure 5-23

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.

5.1.2.1.2 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 5-24.

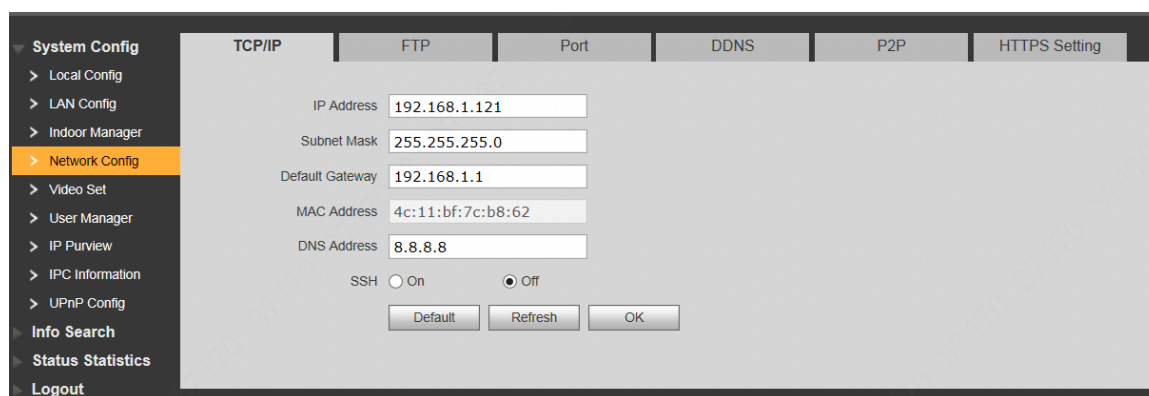


Figure 5-24

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.

5.1.2.1.3 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 5-25.

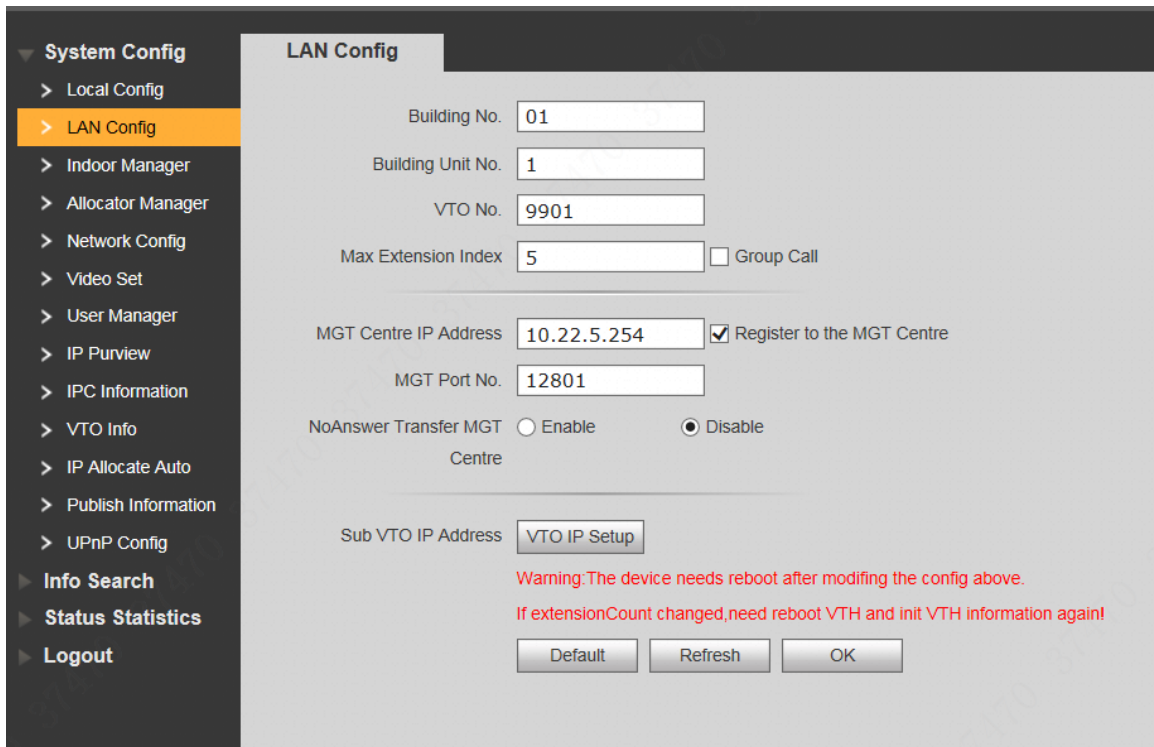


Figure 5-25

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.”.
- To provide group call, please select “Group Call” and set “Max Extension Index”.

Step 3 Click “OK”.

5.1.2.1.4 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 5-26.

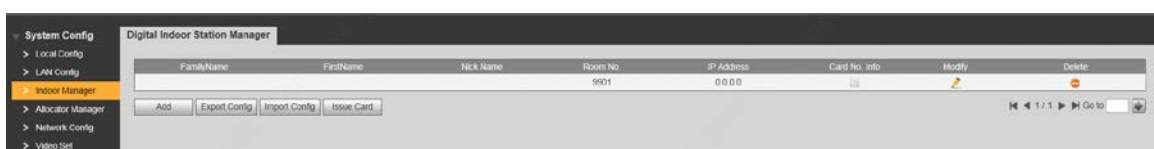


Figure 5-26

Step 2 Click “Add”.

The system displays “Add” interface, as shown in Figure 5-27.

The screenshot shows a window titled "Add" with a close button (X) in the top right corner. It contains five text input fields stacked vertically: "FamilyName", "FirstName", "Nick Name", "VTH Short No.", and "IP Address". The "VTH Short No." field has a red asterisk to its right. Below the input fields are two buttons: "OK" and "Cancel".

Figure 5-27

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

 Note

During batch debugging, VTH IP address is distributed automatically, so IP address may not be filled in. After VTH is registered to VTO successfully, VTO will obtain IP address of VTH.

Step 4 Click “OK”.

5.1.2.1.5 VTO Settings

Add all VTO and fence station info. After VTH info initialization, obtain VTO and fence station info here.

Step 1 Select “System Config >VTO Info”.

The system displays “VTO Info” interface, as shown in Figure 5-28.

The screenshot shows the "VTO Info" interface. On the left is a navigation menu with "VTO info" selected. The main area displays a table with the following columns: "VTO Name", "Device Type", "VTO Middle Number", "IP Address", "Enable", and "Modify". The table contains 14 rows of data, with the first row highlighted in yellow.

VTO Name	Device Type	VTO Middle Number	IP Address	Enable	Modify
Main VTO	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	
	vto		0.0.0	<input type="checkbox"/>	

Figure 5-28

Step 2 Click .

The system displays “Modify” interface, as shown in Figure 5-29.

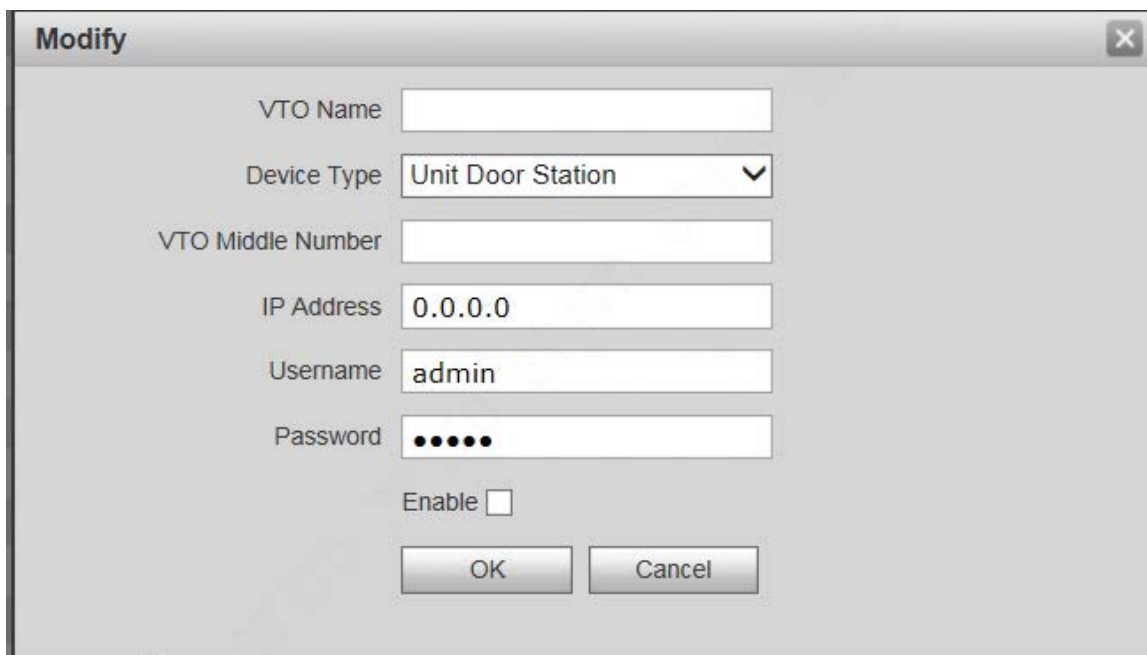


Figure 5-29

Step 3 Enter “VTO Name”, “VTO Middle Number” and “IP Address”; select “Device Type”.

Note

VTO middle no. consists of “1+building no. + unit no. + VTO no.”; building no. has 2 digits, unit no. has 1 digit and VTO no. has 4 digits, so middle no. has 8 digits in total. For example, middle no. is 10116901 for Building 01 Unit 1 Room 6901.

Step 4 Select “Enable”.

Step 5 Click “OK” to add VTO info.

5.1.2.1.6 IP Allocate Auto

Set VTH IP range. After VTH info initialization, obtain IP address from the range automatically.

Step 1 Select “System Config > IP Allocate Auto”.

The system displays “IP Allocate Auto” interface, as shown in Figure 5-30.

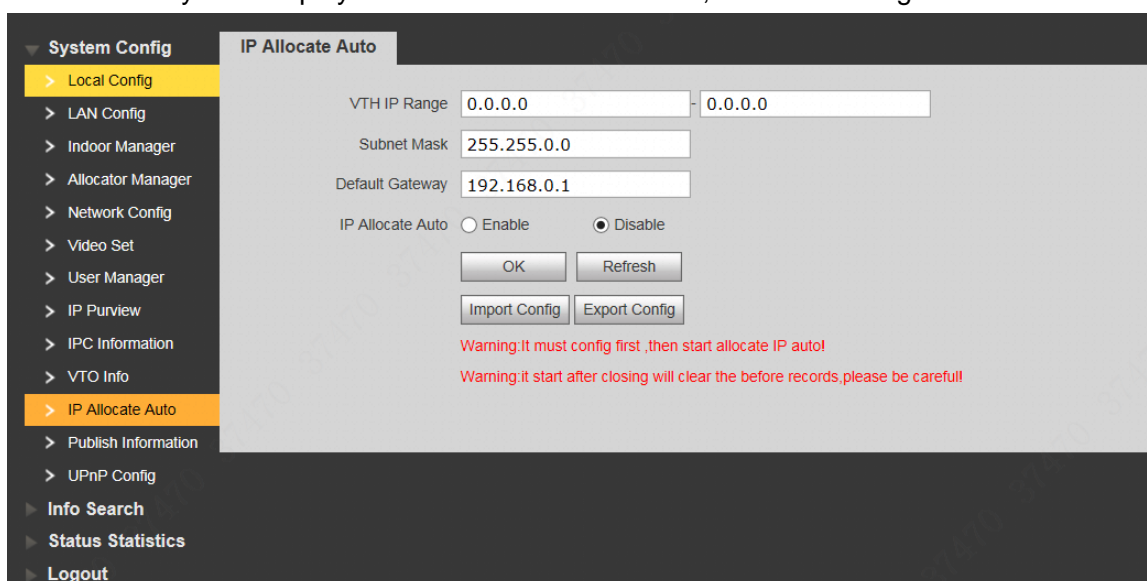


Figure 5-30

Step 2 Enter “VTH IP Range”, “Subnet Mask” and “Default Gateway”.

Step 3 “IP Allocate Auto” selects “Enable”.

Step 4 Click [OK] to save the settings.

5.1.2.2 VTH Settings (Version 3.1)

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 “Initialization” interface, as shown in Figure 5-31.

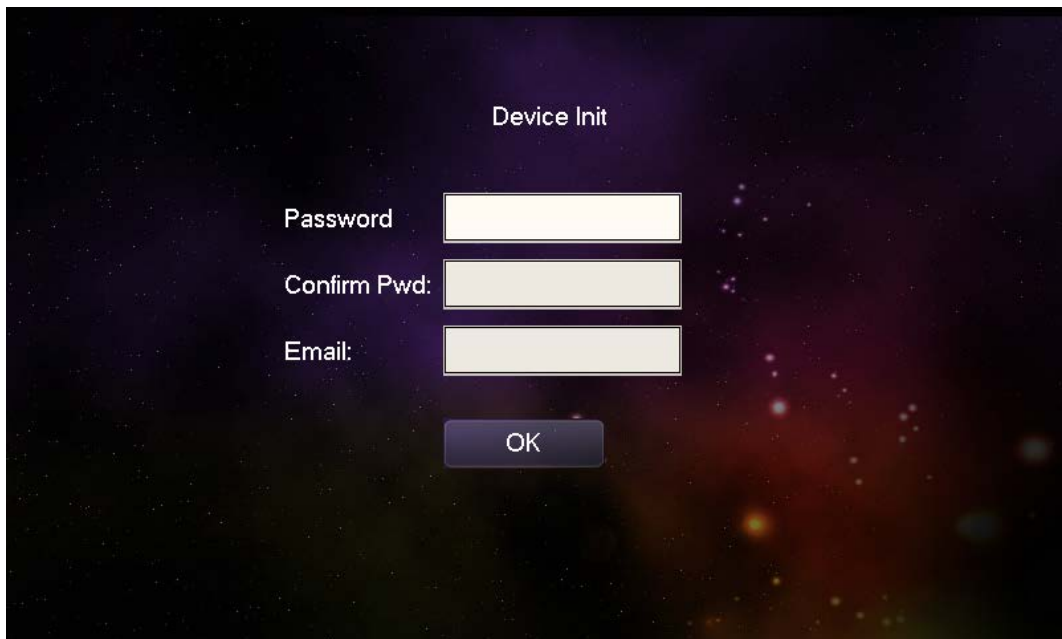


Figure 5-31

Step 2 Enter “Password”, “Confirm Pwd” and “Email”.

Step 3 Click [OK].

The system displays “Info Init” interface, as shown in Figure 5-32.

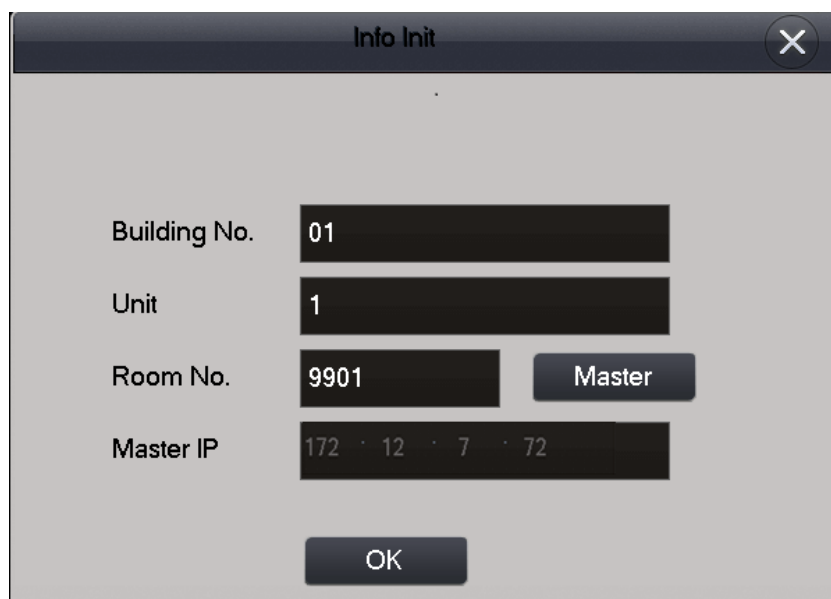


Figure 5-32

Step 4 Initialize the VTH.



Note

Please initialize the master VTH and then initialize extension VTH.

- Initialize the master VTH.

Enter “Building No.,” “Unit” and “Room No.” (such as 9901); press [OK]. After successful initialization, master VTH will obtain IP address and VTO info. At “Digital Indoor Station Manager” of VTO WEB interface, view IP address of the bound master VTH, as shown in Figure 5-33.



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.

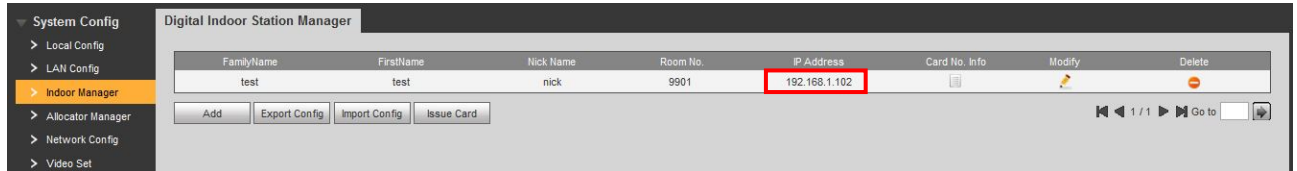


Figure 5-33

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

After successful initialization, extension VTH will obtain VTO info. At “Digital Indoor Station Manager” of VTO WEB interface, view the bound extension VTH info.

5.2 Debugging Verification

5.2.1 Verification with Version 3.1 VTH

5.2.1.1 VTO Calls VTH

Dial VTH room no. (such as 9901) at VTO, and thus call VTH. VTH pops up monitoring image and operating keys, as shown in Figure 5-34. It represents successful debugging.

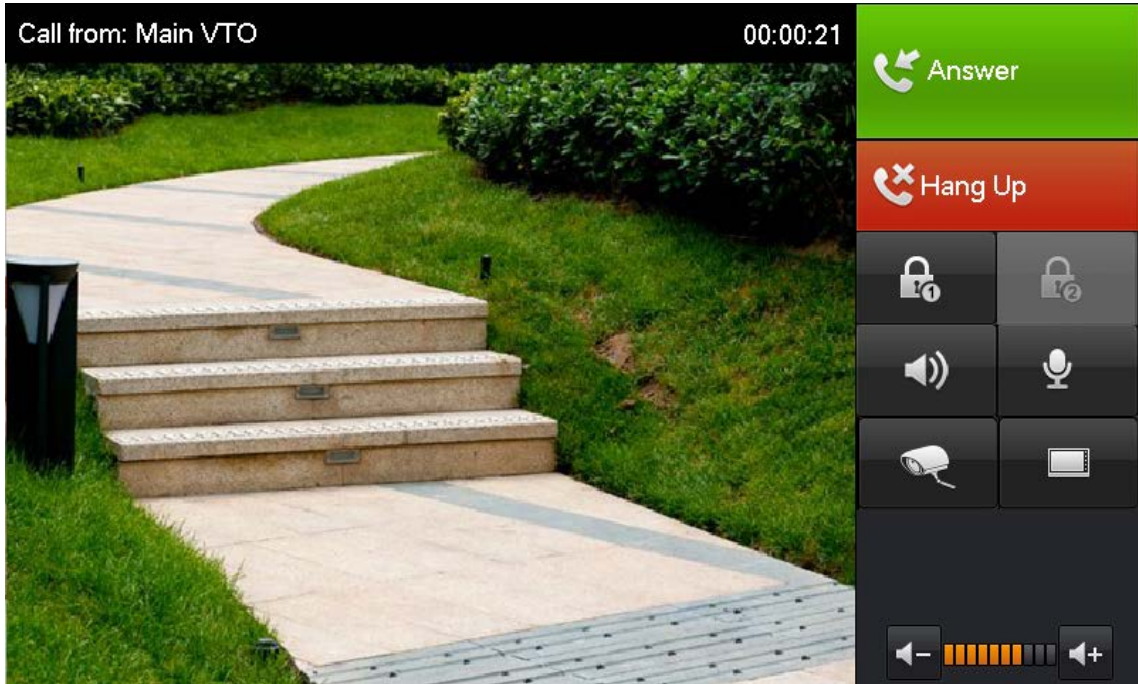


Figure 5-34

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 5-35. Select the VTO to enter monitoring image, as shown in Figure 5-36.

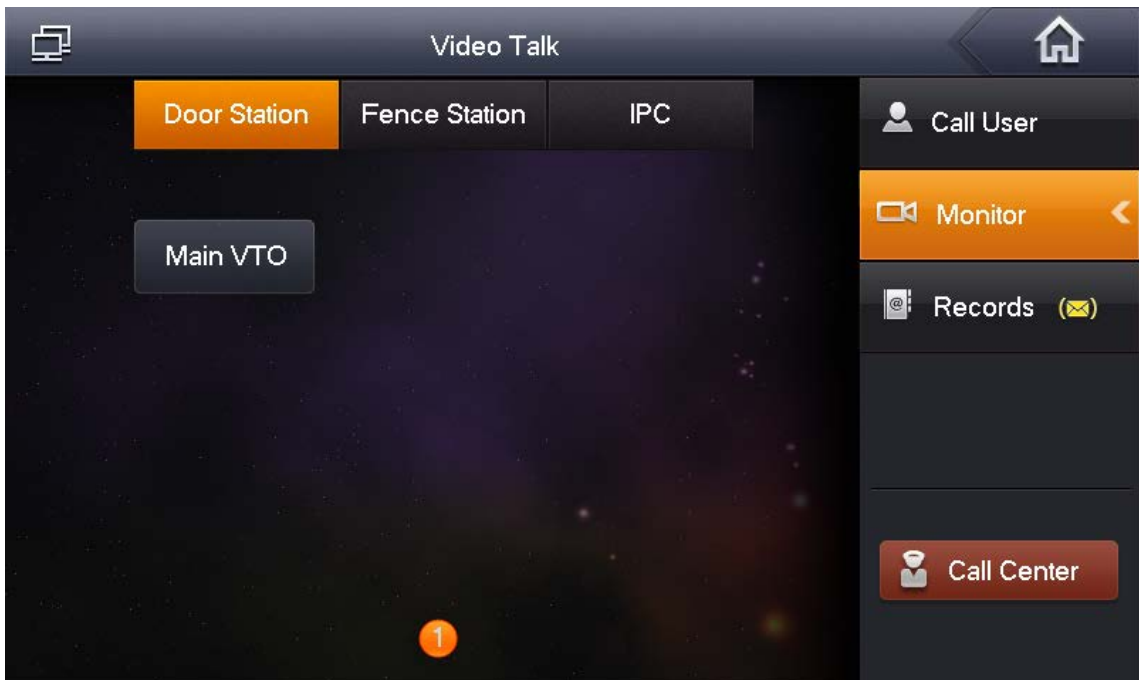


Figure 5-35

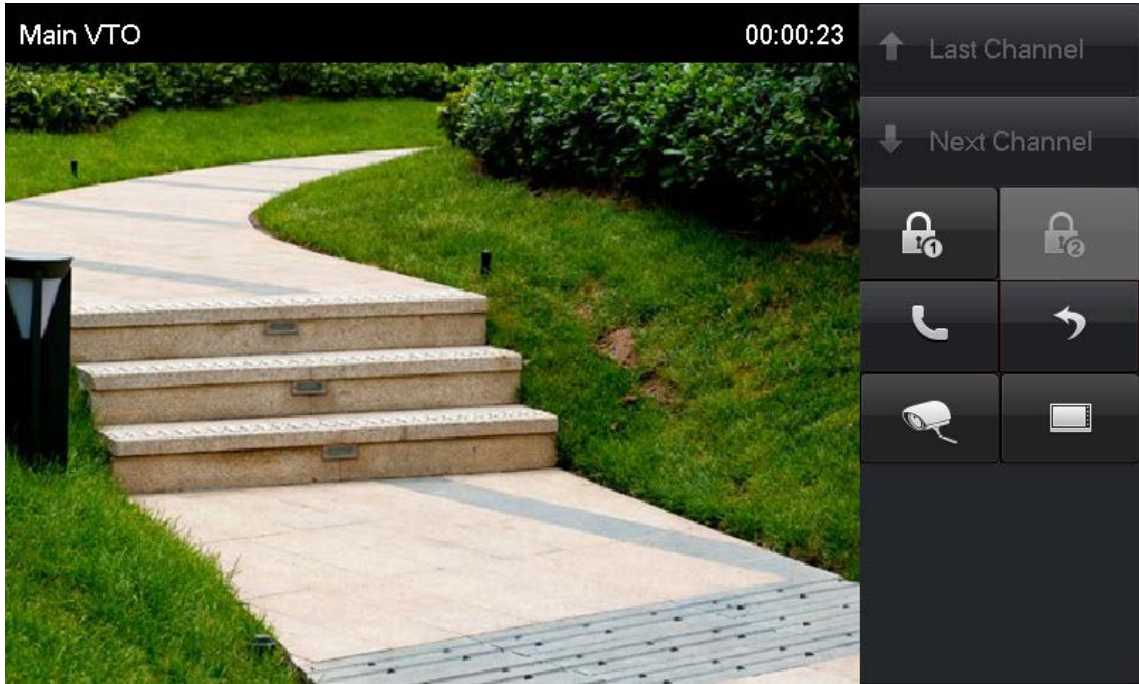


Figure 5-36

5.2.2 Verification with Version 4.0 VTH

5.2.2.1 VTO Calls VTH

Dial VTH room no. (such as 9901) at VTO, and thus call VTH. VTH pops up monitoring image and operating keys, as shown in Figure 5-37. 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.

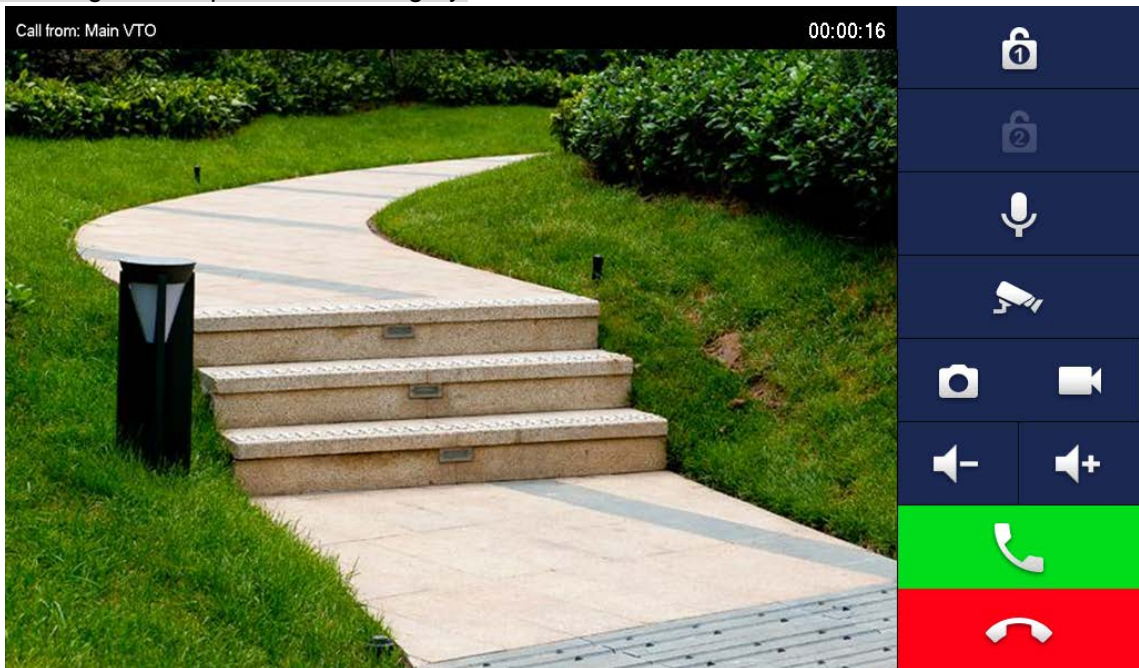



Figure 5-37

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 5-38. Select the VTO to enter monitoring image, as shown in Figure 5-39.

 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 5-38

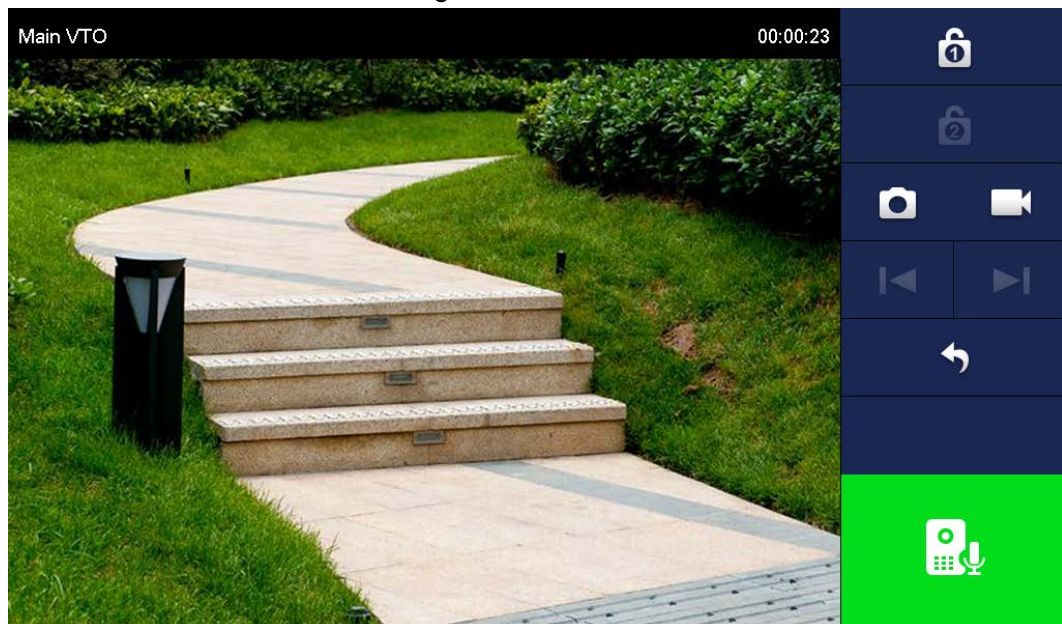




Figure 5-39

6.1 Call Function

6.1.1 Call Management Centre

In standby mode, press  to call management centre, and realize bilateral video talk after the management centre picks up. During talk, press  to end up calling and return to standby interface.

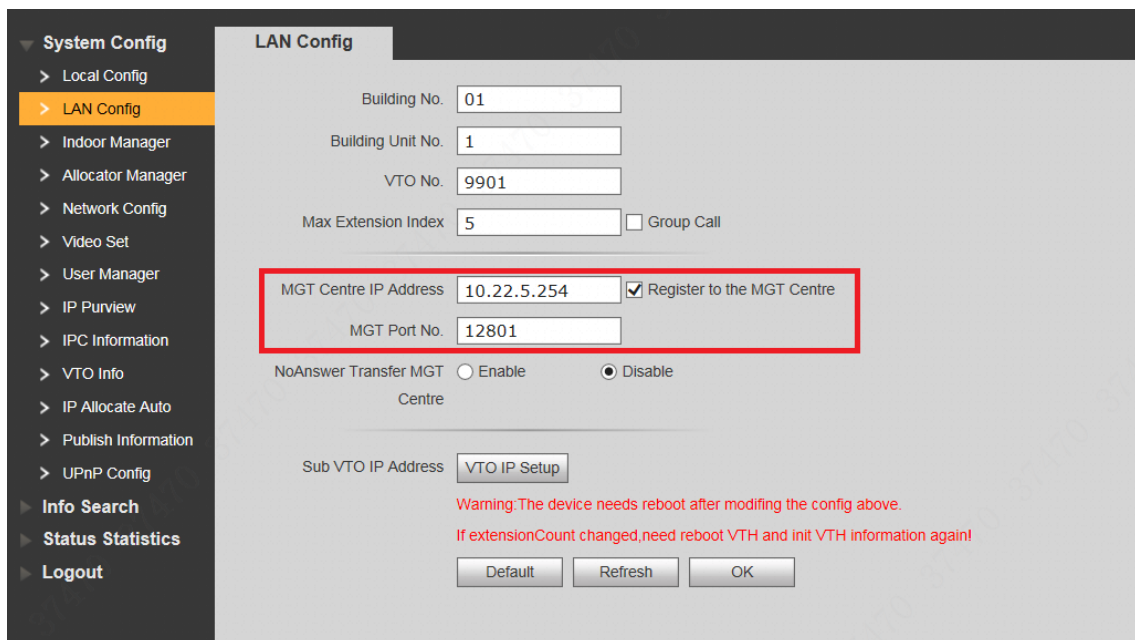
Configure the following parameters before calling.

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 Click “OK” to save the settings.



The screenshot shows the 'LAN Config' interface with a sidebar on the left containing the following menu items: System Config, Local Config, LAN Config (highlighted), Indoor Manager, Allocator Manager, Network Config, Video Set, User Manager, IP Purview, IPC Information, VTO Info, IP Allocate Auto, Publish Information, UPnP Config, Info Search, Status Statistics, and Logout. The main content area is titled 'LAN Config' and contains the following fields and options:

- Building No.: 01
- Building Unit No.: 1
- VTO No.: 9901
- Max Extension Index: 5 Group Call
- MGT Centre IP Address: 10.22.5.254 Register to the MGT Centre
- MGT Port No.: 12801
- NoAnswer Transfer MGT Centre: Enable Disable
- Sub VTO IP Address:



Warning: The device needs reboot after modifying the config above.
If extensionCount changed, need reboot VTH and init VTH information again!

Buttons: Default, Refresh, OK

Figure 6-1

6.1.2 Single Call of VTH

6.1.2.1 Dial up

In standby mode, enter VTH room no. and press  to call the VTH, and realize bilateral video talk after the VTH picks up. During talk, press  to end up calling and return to standby interface.

 Note

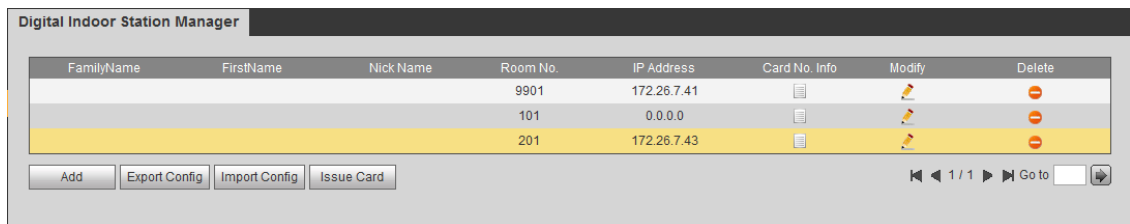
Please check settings in case of failure to call. Please refer to “5.1 Debugging Settings” for details.










6.1.2.2 Call via Contact



Caution






VTO contact obtains VTH info from “Digital Indoor Station Manager” interface. To call via contact, please select “System Config > Digital Indoor Station Manager”; check whether this VTH info exists, as shown in Figure 6-2.



FamilyName	FirstName	Nick Name	Room No.	IP Address	Card No. Info	Modify	Delete
			9901	172.26.7.41			
			101	0.0.0.0			
			201	172.26.7.43			

Buttons: Add, Export Config, Import Config, Issue Card. Page: 1 / 1. Go to:

Figure 6-2

In standby mode, press  or  to open the contact. According to interface prompt, select VTH, press  or  to call the VTH, and realize bilateral video talk after the VTH picks up. During talk, press  to end up calling and return to standby interface.

6.1.3 Group Call

Group call applies to the scene where one door corresponds to multiple VTHs. Dial up or call master VTH via contacts, and call other extension VTHs at the same time.



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.

- VTO contact obtains VTH info from “Digital Indoor Station Manager” interface. To call via contact, please select “System Config > Digital Indoor Station Manager”; check whether this VTH info exists, as shown in Figure 6-2.

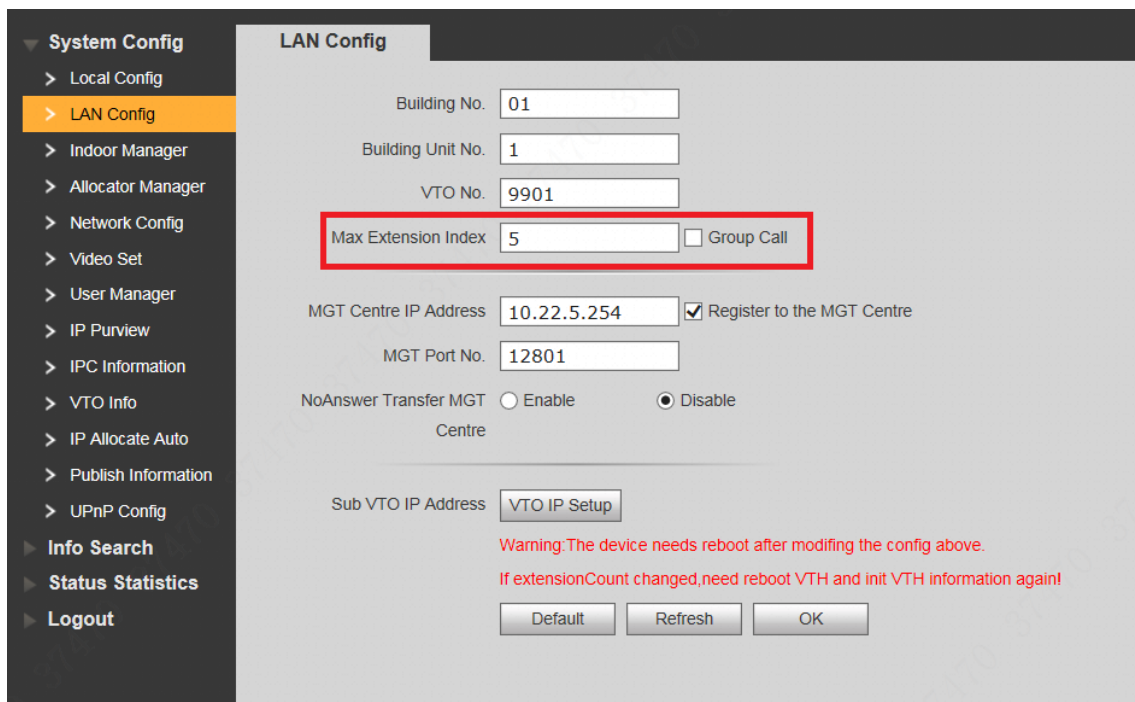


Figure 6-3

6.1.3.1 Dial up

In standby mode, enter master VTH room no. and press \uparrow / \downarrow to call the master and extension VTHs, and realize bilateral video talk after a VTH picks up. During talk, press \ast / \ast to end up calling and return to standby interface.

6.1.3.2 Call via Contact

In standby mode, press \uparrow or \downarrow to open the contact. According to interface prompt, select master VTH, press \uparrow or \downarrow to call the master and extension VTHs, and realize bilateral video talk after a VTH picks up. During talk, press \ast / \ast to end up calling and return to standby interface.

6.2 Unlock Function

6.2.1 Remote Unlock at VTH/MTS

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.

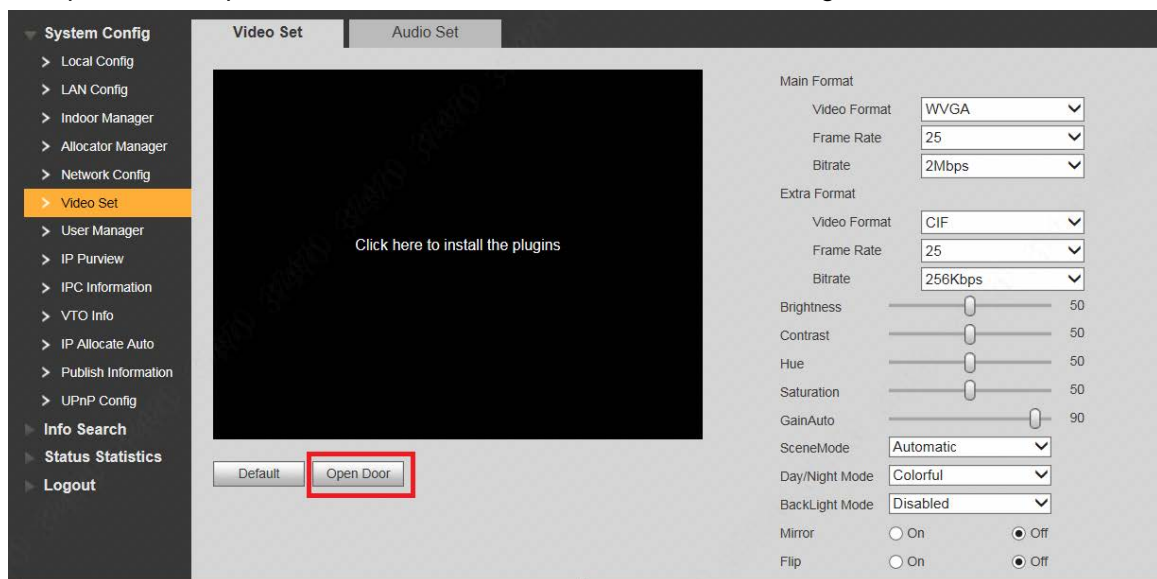



Figure 6-4

6.2.3 Unlock with IC Card

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

 Note

- Authorized IC card refers to a card that is issued and authorized to open the door.

6.2.4 Unlock with Exit Button



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

6.2.5 Unlock with Password

Support to unlock with personal password, unified password and duress password.



- Personal password is set at VTH. Please refer to matched VTH user's manual for details.
- Please refer to “8.7.2 Access Manager” for unified password and duress password setting.

6.2.5.1 Unlock with Personal Password

In standby mode, press /#, enter four-digit room no. (add 0 in front of room no. if it is less than 4 digits)+ personal password, and press /# again to unlock.



For example, 9901 user sets personal password to be 123456. Press #9901123456# to unlock.

6.2.5.2 Unlock with Unified Password

In standby mode, press /#, enter unified password (default password is 123456), and press /# to unlock.

For example, XX user presses #123456# to unlock.

6.2.5.3 Unlock with Duress Password

In case of duress, press /#, enter duress password (default password is 654321) , and press /# to unlock.

For example, XX user presses #654321# to unlock. At the time, the system sends alarm info to management centre.

6.3 Issue Card

The system issues cards in 3 ways, local VTO, access management interface and VTH management interface.

6.3.1 Issue Card from Local VTO

Issue card with main card and password.


Step 1 At project settings interface, press [2] or [8] and select “Issue Card”.

Step 2 Press /#.

- Issue card with main card

 Note

Before start, please ensure that this IC card has been set to be main card. Please refer to “8.9.5.2 Set Main Card” for details.

1. Press [2] or [8], then press /# and select “Issue Card with Main Card”.
2. Swipe the main card.

3. Enter room no. of the authorized card; press **#/#**.
4. Swipe the authorized card.
The interface displays “Issued card successfully”. Then, swipe other authorized cards continuously, or press ***/*** or ***** to exit.

- Issue card with password

1. Press [2] or [8], then press **#/#** and select “Issue Card with Password”.
2. Enter card-issuing password and press **#/#**.

 Note

Card-issuing password is 002236 by default. Please refer to “8.7.2 Access Manager” for details.

3. Enter room no. of the authorized card; press **#/#**.
4. Swipe the authorized card.
The interface displays “Issued card successfully”. Then, swipe other authorized cards continuously, or press ***/*** or ***** to exit.

6.3.2 Issue Card at Access Manager Interface

- Step 1 At VTO WEB interface, select “System Config >Local Config > A&C Manager”.
The system displays “A&C Manager” interface.
- Step 2 Click “Issue Card”.
The system displays 30s countdown, as shown in Figure 6-5.

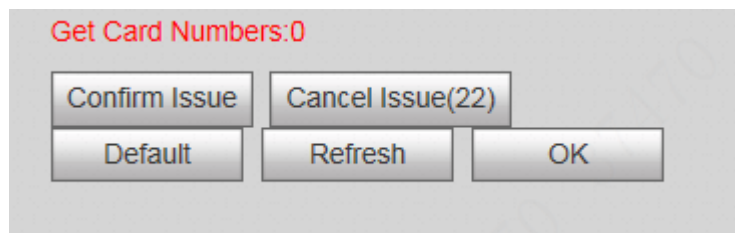


Figure 6-5

- Step 3 Within 30s countdown, swipe an unauthorized card at VTO.
The system pops up “Card Info” interface, as shown in Figure 6-6.

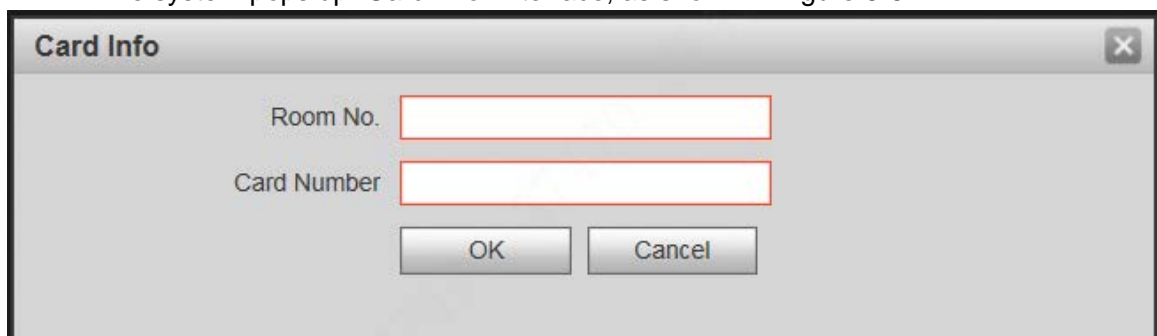


Figure 6-6

- Step 4 Enter “Room No.” and “Card No.”, and click “OK”.



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

Step 5 Click “OK” to finish issuing card.



- 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.

6.3.3 Issue Card at Digital Indoor Station Manager Interface

Step 1 Select “System Config > Indoor Manager”.

The system displays “Digital Indoor Station Manager” interface, as shown in Figure 6-7.

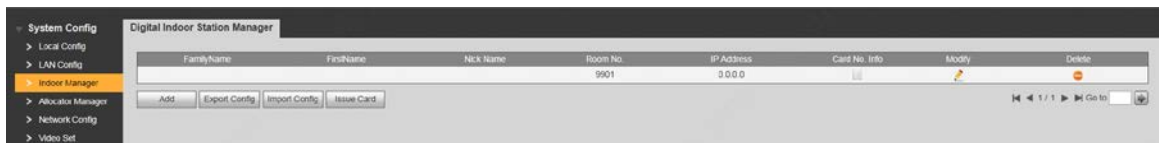


Figure 6-7

Step 2 Click “Issue Card”.

The system pops up “Card Info” interface, as shown in Figure 6-8.

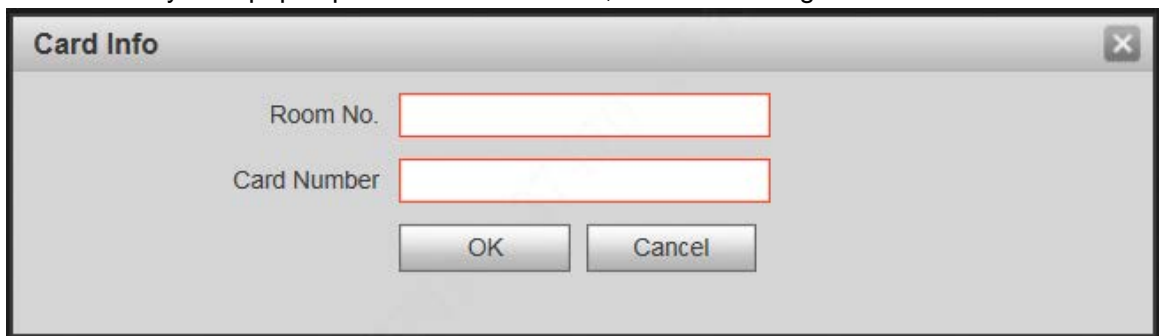


Figure 6-8

Step 3 Enter “Room No.” and “Card No.”.

Step 4 Click “OK” to save the settings.

6.4 Monitoring Function

Both VTS and VTH can monitor the VTO.

VTO supports multi-channel video 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”.

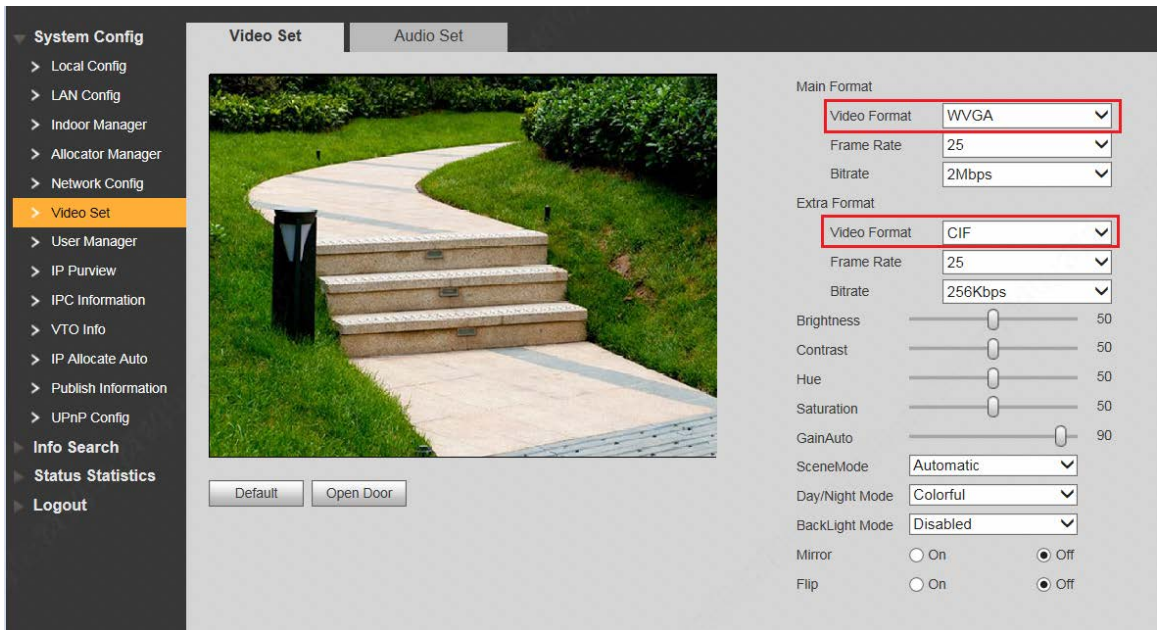


Figure 6-9

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.



VTO saves card no. and VTH info of the system automatically every half an hour. If VTH info or card no. 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 6-10.

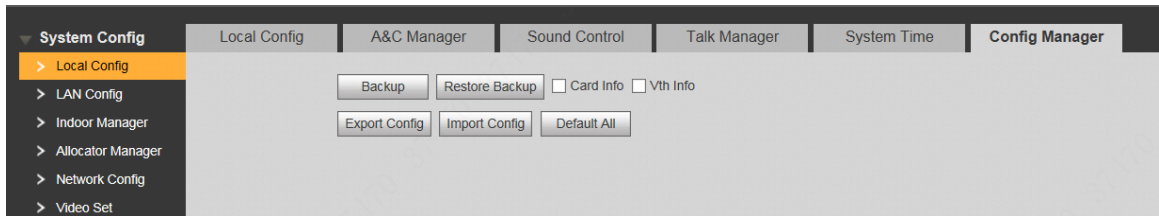


Figure 6-10

- Step 2 Select “Card Info” or “VTH Info” and click “Restore Backup”.
Backup card info or 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 6-11.



Figure 6-11

- 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 Enter Project Settings

In standby mode, press $\text{Ⓢ}/\#$, input project settings password, and press $\text{Ⓢ}/\#$ again to enter project settings interface. Press [2] or [8] to go up and down, then press $\text{Ⓢ}/\#$ to enter sub-interface and modify.

 Note

Project settings password is 888888 by default. Please refer to “8.7.2 Access Manager” for details.

7.2 Modify IP

Step 1 At project settings interface, press [2] or [8] and select “Modify IP”.

Step 2 Press $\text{Ⓢ}/\#$ to enter IP modification interface.

Step 3 Press [2] or [8], [4] or [6] numeric keys to select IP unit, and press $\text{Ⓢ}/\#$ to enter modification.

Step 4 Press numeric keys to input numbers, and press $\text{Ⓢ}/\#$ to save.

After completing modification, press $\text{Ⓢ}/*$ to exit.

7.3 Modify Volume

Step 1 At project settings interface, press [2] or [8] and select “Audio Setting”.

Step 2 Press $\text{Ⓢ}/\#$ to enter audio modification interface.

Step 3 Press [4] or [6] to adjust VTO volume.

After completing modification, press $\text{Ⓢ}/*$ to exit.

7.4 Issue Card

Issue card with main card and password.




Step 1 At project settings interface, press [2] or [8] and select “Issue Card”.

Step 2 Press /#.



- Issue card with main card

 Note

Before start, please ensure that this IC card has been set to be main card. Please refer to “8.9.5.2 Set Main Card” for details.



1. Press [2] or [8], then press /# and select “Issue Card with Main Card”.
2. Swipe the main card.
3. Enter room no. of the authorized card; press /#.
4. Swipe the authorized card.
The interface displays “Issued card successfully”. Then, swipe other authorized cards continuously, or press  or * to exit.

- Issue card with password

1. Press [2] or [8], then press /# and select “Issue Card with Password”.
2. Enter card-issuing password and press /#.

 Note


Card-issuing password is 002236 by default. Please refer to “8.7.2 Access Manager” for details.

3. Enter room no. of the authorized card; press /#.
4. Swipe the authorized card.
The interface displays “Issued card successfully”. Then, swipe other authorized cards continuously, or press  or * to exit.

7.5 View Version Info

Step 1 At project settings interface, press [2] or [8] and select “Version Info”.

Step 2 Press /#.

Step 3 Press [2] or [8], then press /# and select “Main Program Version/SCM Version” to view version info.

8.1 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

The system displays “Setting” interface, as shown in Figure 8-1.

Device

1 Setting 2 Protect 3 OK

Username admin

New Password

Weak Middle Strong

Confirm

Use a password that has 8 to 32 characters, it can be a combination of letters, numbers and symbols (please do not use special symbols like \\' \\' ; \\' &)

Next

Figure 8-1

Step 2 Enter “New Password” and “Confirm”, and click “Next”.

The system displays “Protect” interface, as shown in Figure 8-2.

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.

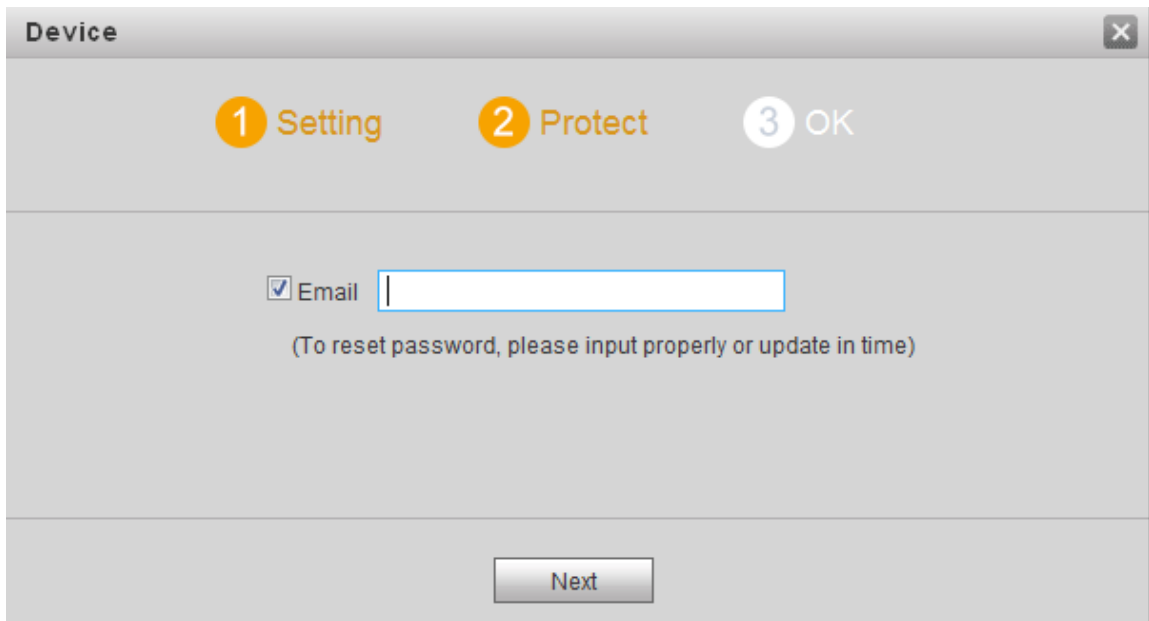


Figure 8-2

- 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 8-3, and shows “Device succeed!”

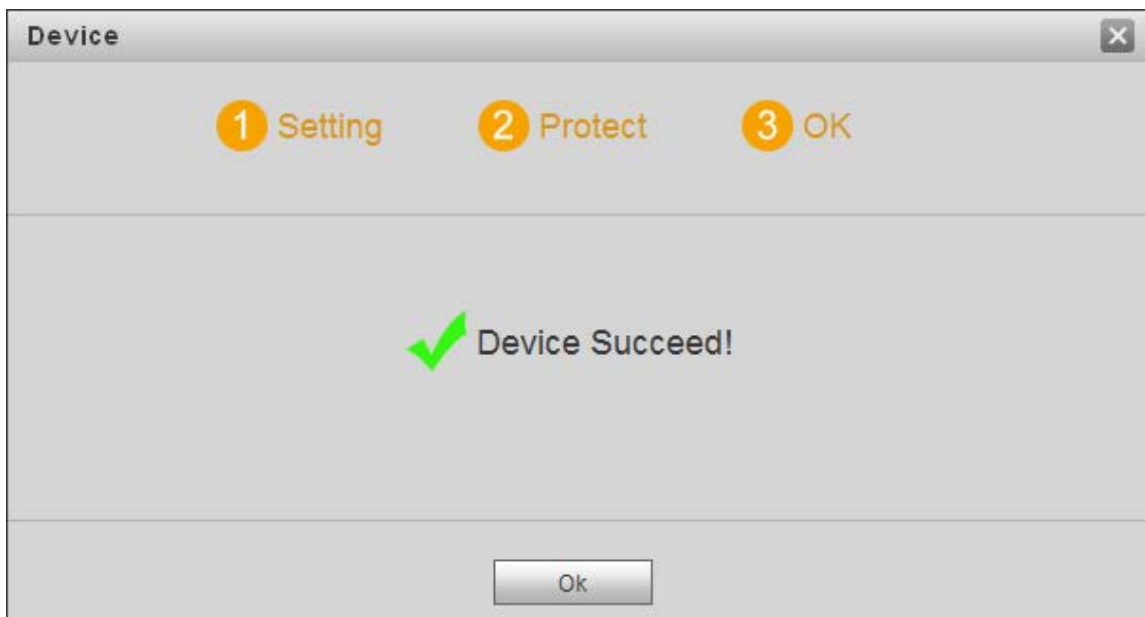


Figure 8-3

- Step 5 Click “OK”.
- The system displays WEB login interface.

8.2 Reset the Password

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

- Step 1 With the browser, enter WEB interface of the device.
- The system displays login interface, as shown in Figure 8-4.



Figure 8-4

Step 2 Click “Forgot Password”.

The system displays “Reset the password” dialog box, as shown in Figure 8-5.

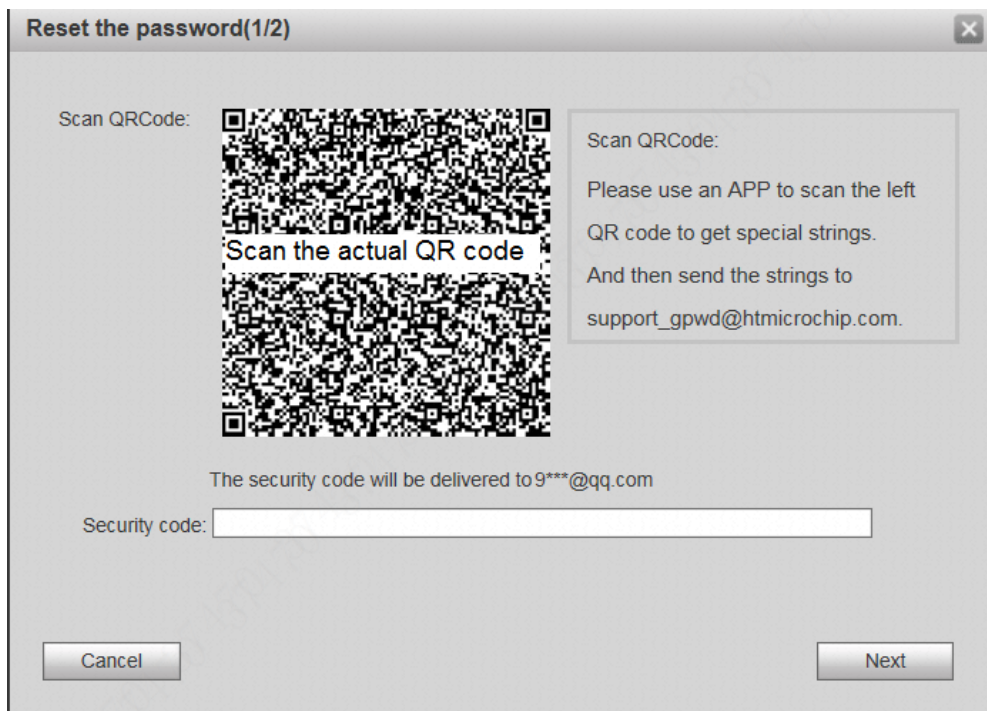


Figure 8-5

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 8-6.

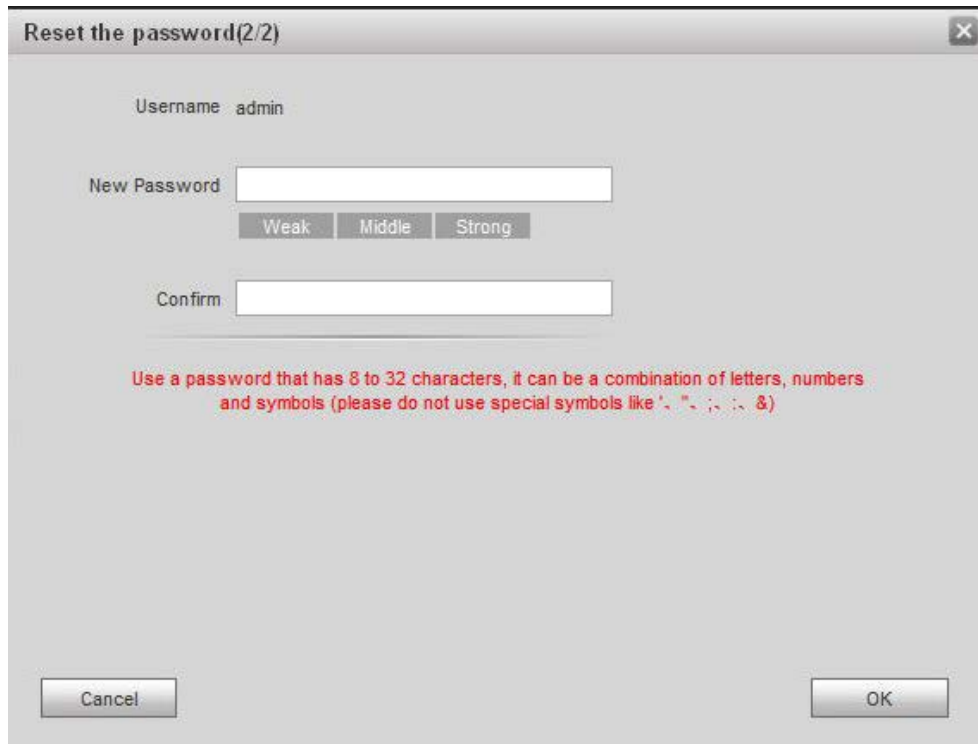


Figure 8-6

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.

8.3 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 8-7.



Figure 8-7

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.

8.4 User Manager

Add, delete and modify WEB user info.

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

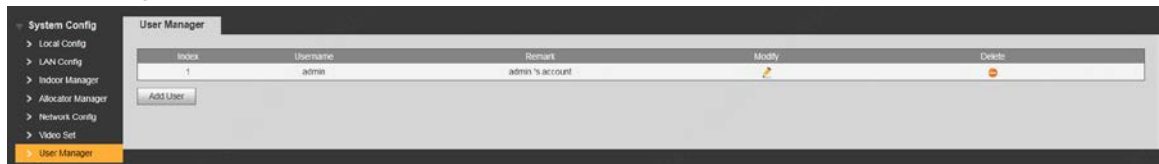


Figure 8-8

8.4.1 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 8-9.

Figure 8-9

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




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.

8.4.2 Modify User

8.4.2.1 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 8-10.

Figure 8-10

Step 2 Modify user info.

1. Tick “Change Password”.

The system displays password change interface, as shown in Figure 8-11.

Modify User

Change Password

Old Password

New Password

Weak Middle Strong

Confirm

Email Address Modify email

Remark

Use a password that has 8 to 32 characters, it can be a combination of letters, numbers and symbols (please do not use special symbols like ' , " , ; , : , &)


OK Cancel

Figure 8-11

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

8.4.2.2 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 8-12.

Modify User

Change Password

Remark

Use a password that has 8 to 32 characters, it can be a combination of letters, numbers and symbols (please do not use special symbols like ' , " , ; , : , &)

OK Cancel

Figure 8-12

Step 2 Modify user info, as shown in Figure 8-13.

1. Tick “Change Password”.

The system displays password change interface, as shown in Figure 8-13.

Figure 8-14

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.

8.5.2 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 8-15.

Figure 8-15

Step 2 Set the parameters and refer to Table 8-1 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 8-1

Step 3 Click “OK” to save the settings.

8.5.3 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 8-16.

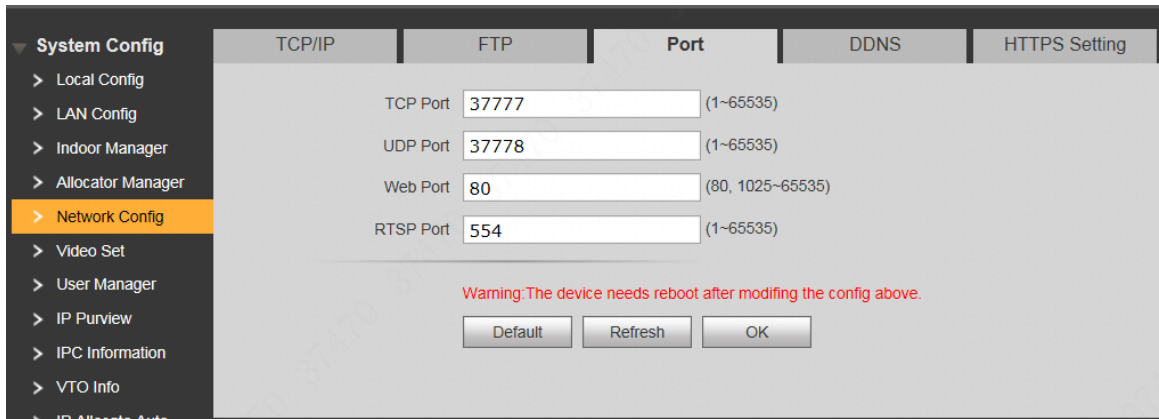


Figure 8-16

Step 2 Set port value of this device and refer to Table 8-2 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	<ul style="list-style-type: none"> 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. <p>URL format is described as follows: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</p> <ul style="list-style-type: none"> 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). <p>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</p> <p>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</p>

Table 8-2

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.

8.5.4 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 logs in, 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 8-17.

Figure 8-17

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

Step 3 Set parameters and refer to Table 8-3 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.
Server Name	<ul style="list-style-type: none"> • Dyn dns DDNS address is: members.dyndns.org. • NO-IP DDNS address is: dynupdate.no-ip.com.
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 8-3

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.

8.5.5 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 8-18.

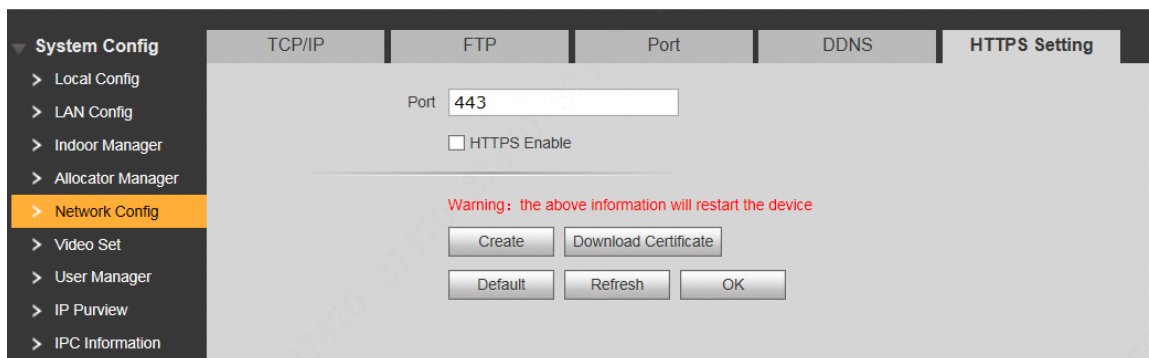


Figure 8-18

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.

8.5.6 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 8-19.

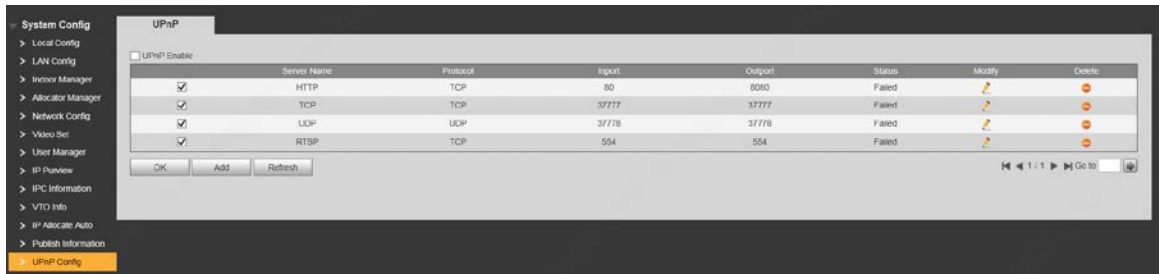


Figure 8-19

8.5.6.1 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.

8.5.6.2 Add Server

Add new server mapping relations.

Step 1 Click “Add”.

The system displays “Add” interface, as shown in Figure 8-20.

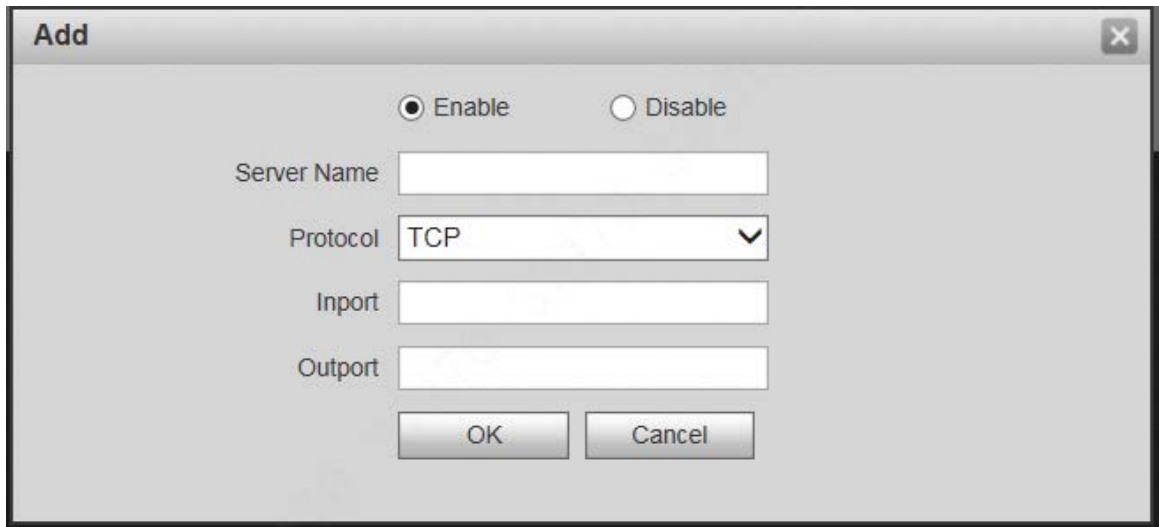



Figure 8-20

Step 2 Set parameters and refer to Table 8-4 for details.

Parameter	Description
Enable/ Disable	<ul style="list-style-type: none"> • 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	Support TCP and UDP.

Parameter	Description
Inport	Port that this device needs to map.
Outport	Port that is mapped on the router.

 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.

Table 8-4

Step 3 Click “OK” to save the settings.

8.5.6.3 Modify Server

Modify server mapping relation in the list.

Step 1 Click .

The system displays “Add” interface, as shown in Figure 8-21.

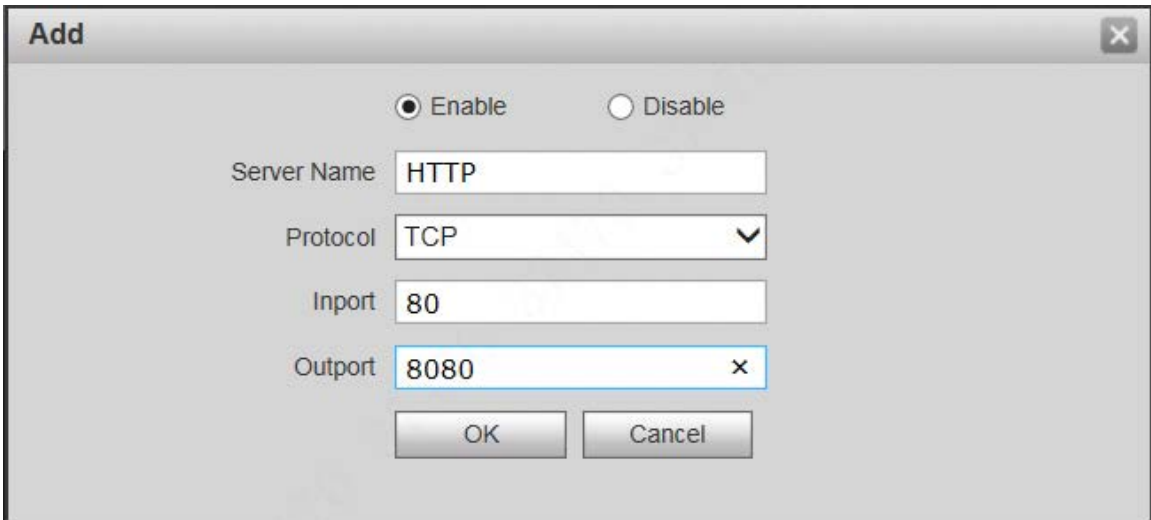



Figure 8-21

Step 2 Set parameters and refer to Table 8-4 for details.

Step 3 Click “OK” to save the settings.

8.5.6.4 Delete Server

Delete server mapping relation in the list.

Click  to delete mapping relation.

8.5.7 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 8-22.



Figure 8-22

Step 2 Tick “Enable”.

The system displays white/black list checkbox, as shown in Figure 8-23.



Figure 8-23

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

The system displays “Add” interface, as shown in Figure 8-24.

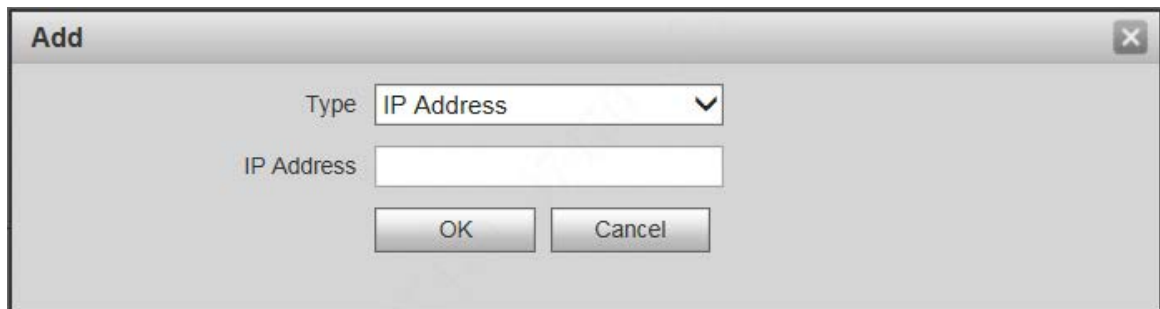


Figure 8-24

3. Set IP address and refer to Table 8-5 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.

Type	Description
IP Network Segment	Enter the start address and end address of network segment to be added.

Table 8-5

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.

8.6 LAN Config

Set VTO building no., unit no., no., management centre, group call function, transfer and VTO management function under analog system.

Step 1 Select “System Config > LAN Config”.

The system displays “LAN Config” interface, as shown in Figure 8-25.

The screenshot shows the 'LAN Config' interface. On the left is a navigation menu with 'System Config' expanded to 'LAN Config'. The main area contains the following fields and options:

- Building No.: 01
- Building Unit No.: 1
- VTO No.: 9901
- Max Extension Index: 5
- Group Call:
- MGT Centre IP Address: 10.22.5.254
- Register to the MGT Centre:
- MGT Port No.: 12801
- NoAnswer Transfer MGT Centre: Enable, Disable
- Sub VTO IP Address: VTO IP Setup

Warning: The device needs reboot after modifying the config above.
If extensionCount changed, need reboot VTH and init VTH information again!

Buttons: Default, Refresh, OK

Figure 8-25

Step 2 Set parameters and refer to Table 8-6 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




Parameter	Description
Group Call	<p>Index”.</p> <p> Note</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p> Note</p> <p>Please obtain management centre info in advance.</p>
MGT Port No.	
Register to the MGT Centre	
No Answer Transfer MGT Centre	<p>Tick “Enable” to enable transferring to management centre in case of no answer.</p> <p>In the following cases when VTO calls VTH, the system will transfer the call to management centre automatically.</p> <ul style="list-style-type: none"> • 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.
Sub VTO IP Address	<p>Click “VTO IP Setup”, enter sub VTO IP address and port no. and click “Enable”.</p> <p> Note</p> <p>This function is valid only when it is matched with analog VTH.</p>

Table 8-6

Step 3 Click “OK” to save the settings.

8.7 Local Parameter Config

8.7.1 Local Config

Set info about the device, such as system type, sensor, storage point, device type and reboot date.

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

The system displays “Local Config” interface, as shown in Figure 8-26.

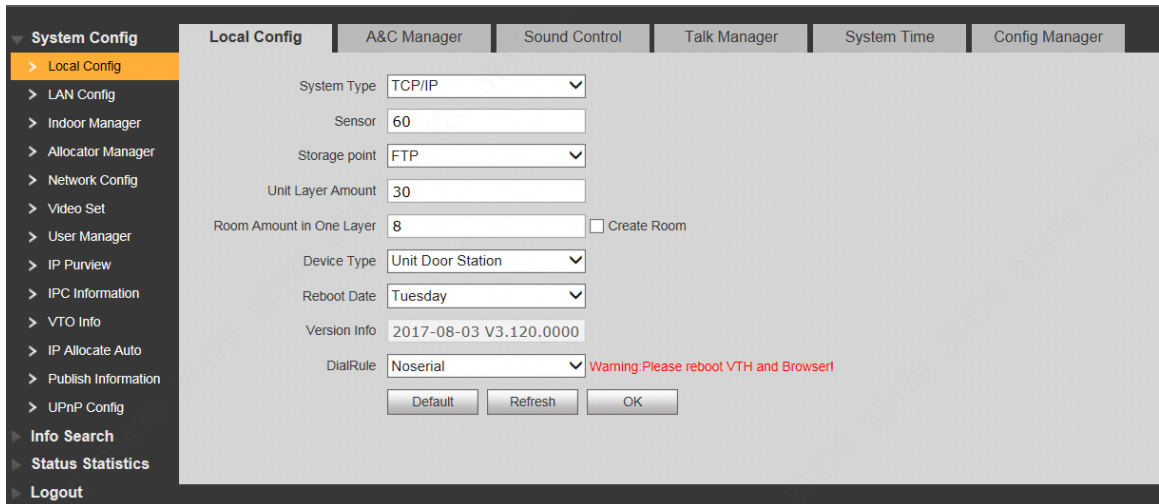


Figure 8-26

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


Parameter	Description
System Type	It is TCP/IP by default.
Sensor	If it is dark during video intercom, turn on the fill-in light automatically. The larger the value is, the higher sensitivity becomes.
Storage Point	Set storage point of recordings and snapshots. Select FTP or SD card.  Note <ul style="list-style-type: none"> When it is set to be FTP, set FTP server according to “8.5.2 FTP Server”. When it is set to be SD card, please confirm whether VTH supports SD card or whether SD card has been inserted.
Unit Layer Amount	Set layer amount of the unit building.
Room Amount in One Layer	Set total amount of rooms in one layer.
Create Room	Tick “Create Room”. The system adds VTH in batches.
Device Type	It is unit door 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 8-7

Step 3 Click “OK” to save the settings.

8.7.2 Access Manager

Set lock time, unlock command, issue card password, project password, lift control, Baud rate, unlock password, menace password and auto snapshot.

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

The system displays “A&C Manager” interface, as shown in Figure 8-27.

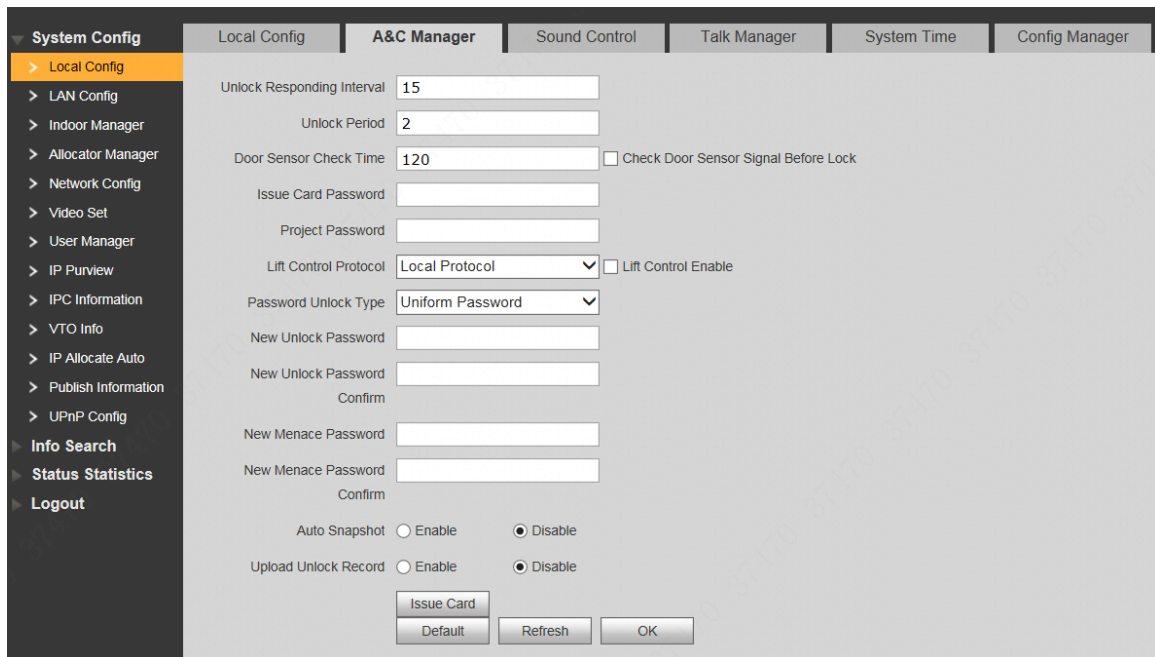




Figure 8-27

Step 2 Set parameters and refer to Table 8-8 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.
Door Sensor Check Time	However, after opening time exceeds the door sensor check time, give door sensor alarm and report the alarm info to management centre automatically.
Issue Card Password	After setting the password, issue card with this password at VTO.  Note <ul style="list-style-type: none"> This password is used by admin or engineering personnel only. Default password is 002236.
Project Password	Enter project settings interface at local VTO. Default project password is 888888.  Note <p>Project password is used by admin or engineering personnel only.</p>
Lift Control Protocol	Tick "Lift Control Protocol" and "Lift Control Enable" to enable the lift control function, and set the floor where the user can go after entering the lift.
Lift Control Enable	



Parameter	Description
Password Unlock Type	Support the following two ways: <ul style="list-style-type: none"> Personal password: it can be set at VTH. Unified password: after setting, every user of the unit can unlock with this password.
New Unlock Password	
New Unlock Password Confirm	
New Menace Password	Tick "Menace Password Enable" to enable this function. In case of menace, input the menace password to unlock; the device uploads the alarm info to management center automatically.
New Menace Password Confirm	
Auto Snapshot	Tick "Enable". 2 pictures will be snapshot automatically when the door is opened, and uploaded to FTP.
Upload Unlock Record	Reserved function.
Issue Card	<ol style="list-style-type: none"> Click "Issue Card". Swipe the unauthorized card at VTO. Pop up "Card Info" interface. Enter "Room No." and "Card No.", and click "OK". <p> Note Cards can be swiped continuously, within a period of 30s.</p> <ol style="list-style-type: none"> Click "OK" to finish issuing card. <p> Note</p> <ul style="list-style-type: none"> 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 8-8

Step 3 Click "OK" to save the settings.

8.7.3 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 8-28.

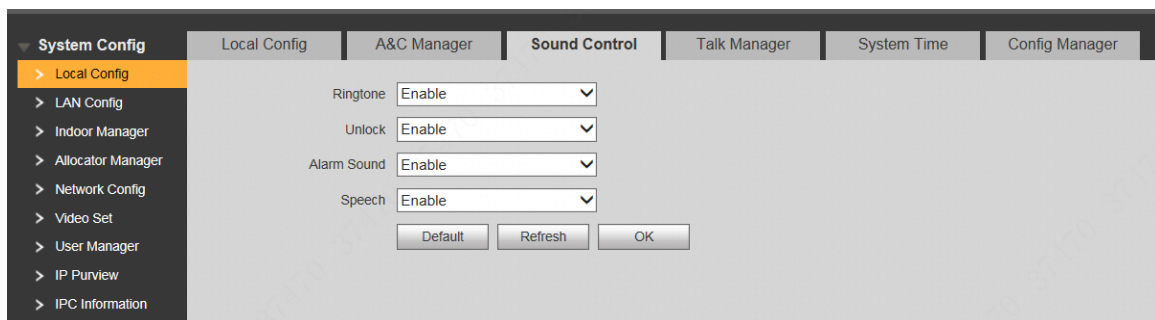


Figure 8-28

Step 2 Enable or disable corresponding sound.

Step 3 Click "OK" to save the settings.

8.7.4 Talk Manager



Caution

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

Set the auto snapshot, message and record upload functions during talk.

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

The system displays “Talk Manager” interface, as shown in Figure 8-29.

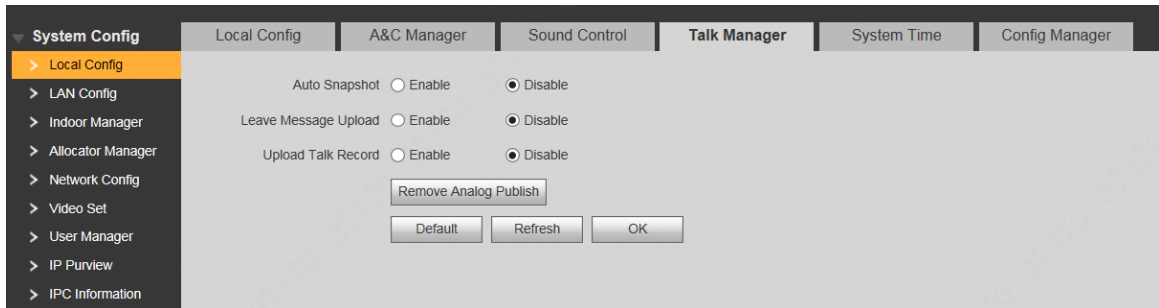


Figure 8-29

Step 2 Set parameters and refer to Table 8-9 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	 <p>Caution</p> <ul style="list-style-type: none"> 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. <p>Tick “Enable” to enable the function. VTH info interface has “Visitors' Message” tab. When VTO calls VTH and gets no response, the system 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.</p>
Upload Talk Record	Reserved function.
Remove Analog Publish	 <p>Caution</p> <p>It is valid only in analog system.</p> <p>Click “Remove Analog Publish” to remove publishes on analog VTH after confirmation.</p>

Table 8-9

Step 3 Click “OK” to save the settings.

8.7.5 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 8-30.

The screenshot shows the 'System Time' configuration page. On the left is a navigation menu with options like 'Local Config', 'LAN Config', 'Indoor Manager', etc. The main area contains the following settings:

- Date Format: Year-Month-Day
- Time Format: 24-Hour Standard
- System Time: 2017 - 11 - 20 7 : 58 : 44 (with a 'Sync PC' button)
- DST Enable:
- DST Type: Date Week
- Start Time: Jan 1 0 : 0
- End Time: Jan 2 0 : 0
- NTP Enable:
- NTP Server: 200.160.0.8
- Zone: GMT+00:00
- Port No.: 123 (1-65535)
- Update Period: 5 Minute (1-30)

Buttons at the bottom include 'Default', 'Refresh', and 'OK'.

Figure 8-30

Step 2 Set parameters and refer to Table 8-10 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 or release info. 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	Some countries or regions follow daylight-saving time (DST). Choose to enable DST or not according to actual needs:
DST Type	
Start Time	
End Time	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.
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 8-10

Step 3 Click “OK” to save the settings.

8.7.6 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 8-31.

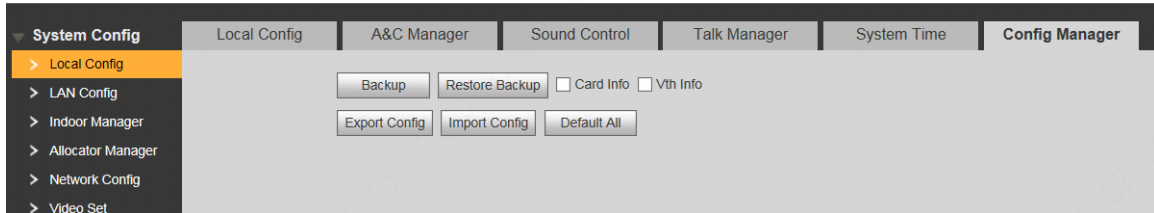


Figure 8-31

- **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.

8.8 VTO Info


Mange main VTO, sub VTO and fence station info; automatically read VTO and fence station info during VTH initialization.

Step 1 Select “System Config >VTO Info”.

The system displays “VTO Info” interface, as shown in Figure 8-32.

VTO Name	Device Type	VTO Middle Number	IP Address	Enable	Modify
Main VTO	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	
	Vto		0.0.0.0	<input type="checkbox"/>	

Figure 8-32

Step 2 Click .

The system displays “Modify” interface, as shown in Figure 8-33.

 Note

VTO under use cannot be modified.

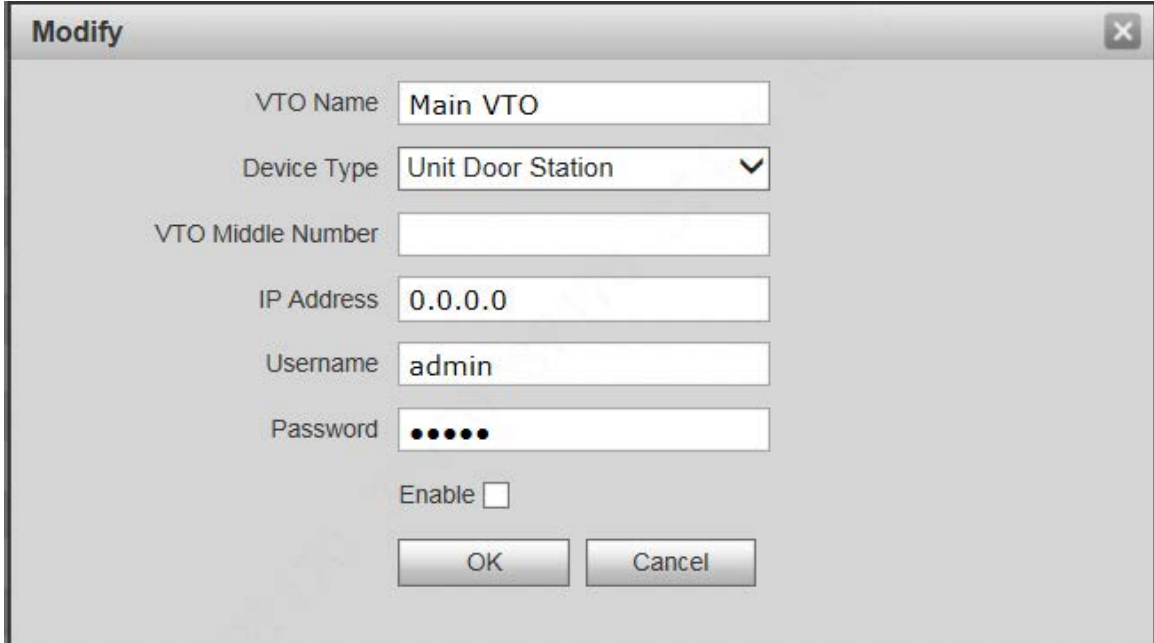


Figure 8-33

Step 3 Set parameters and refer to Table 8-11 for details.

Parameter	Description
VTO Name	Identify VTO.
Device Type	Select device type, including “Unit Door Station” and “Fence Station”.
VTO Middle Number	VTO number.
IP Address	VTO IP address.
Username	Username and password to login WEB interface of the VTO.
Password	
Enable	Tick “Select” and enable to use it after adding.

Table 8-11

Step 4 Click “OK” to save the settings.

VTO info is displayed in the list.

8.9 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 8-34.



Figure 8-34

8.9.1 Add VTH



- 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 8-35.

Figure 8-35

Step 2 Set parameters and refer to Table 8-12 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 8-12

Step 3 Click “OK” to save the settings.

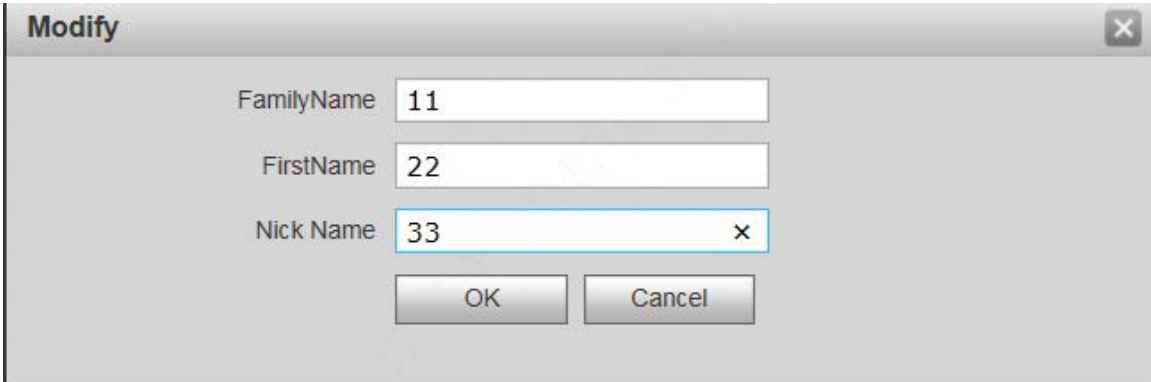
8.9.2 Modify VTH



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 8-36.



The screenshot shows a dialog box titled "Modify" with a close button (X) in the top right corner. It contains three text input fields: "FamilyName" with the value "11", "FirstName" with the value "22", and "Nick Name" with the value "33". Below the input fields are two buttons: "OK" and "Cancel".

Figure 8-36

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

Step 3 Click “OK” to save the settings.

8.9.3 Delete VTH

Click  to delete VTH info one by one.

8.9.4 Config Manager

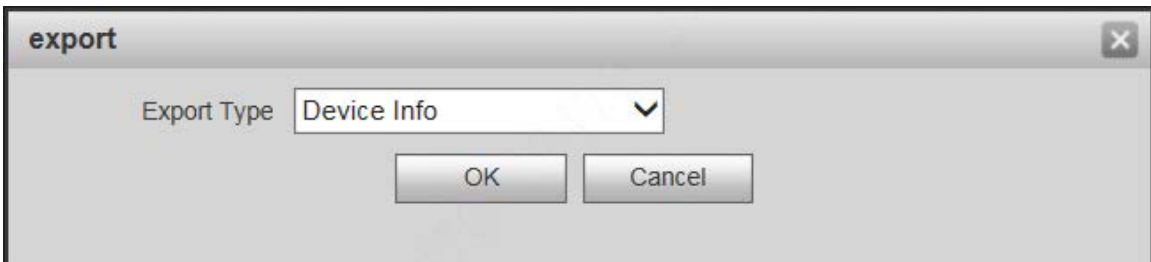
Import or export device info, password info, card no. info and login info of the device.

8.9.4.1 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 8-37.



The screenshot shows a dialog box titled "export" with a close button (X) in the top right corner. It contains a dropdown menu labeled "Export Type" with "Device Info" selected. Below the dropdown are two buttons: "OK" and "Cancel".

Figure 8-37

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.

8.9.4.2 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.

8.9.5 Card Manager

Issue card, set main card, report loss and cancel, modify card ID and delete card.

8.9.5.1 Issue Card

Step 1 Select “System Config > Indoor Manager”.

The system displays “Digital Indoor Station Manager” interface, as shown in Figure 8-38.

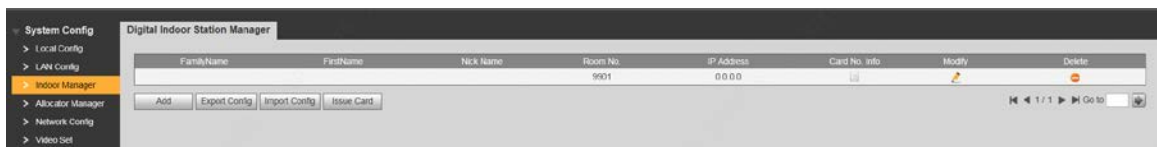


Figure 8-38

Step 2 Click “Issue Card”.

The system displays “Card Info” interface, as shown in Figure 8-39.

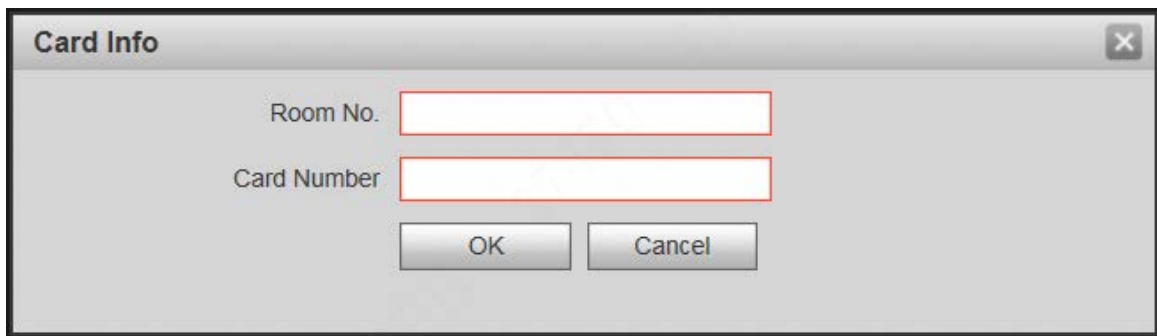


Figure 8-39

Step 3 Enter “Room No.” and “Card Number”.

Step 4 Click “OK” to save the settings.

8.9.5.2 Set Main Card

Local VTO supports to issue main card and authorize other cards.

Step 1 Click .

The system displays “Card Info” interface, as shown in Figure 8-40.

Card Info						
Card ID	Card Number	Username	Main Card	ReportLoss	Modify	Delete
9901	94BE4604		<input type="checkbox"/>			
9901	4568944B		<input type="checkbox"/>			

Figure 8-40

Step 2 Select “Main Card” and the card is set to be a main card.

Step 3 Click to close config interface.

8.9.5.3 Report Loss

If one card is lost, report loss of the card. The card doesn’t have authority to unlock the door, until the report is cancelled.

Step 1 Click .

The system displays “Card Info” interface, as shown in Figure 8-40.

Step 2 Click to report loss, and the icon is switched to .

Note

Click to cancel the report and restore unlock function.

Step 3 Click to close config interface.

8.9.5.4 Modify

Modify username of the card.

Step 1 Click .

The system displays “Card Info” interface, as shown in Figure 8-40.

Step 2 Click .

The system displays “Modify” interface, as shown in Figure 8-41.

Figure 8-41

Step 3 Modify username of the card.

Step 4 Click “OK”.

Step 5 Click to close config interface.


8.9.5.5 Delete

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

Step 1 Click .

The system displays “Card Info” interface, as shown in Figure 8-40.

Step 2 Click  to delete card info.

Step 3 Click  to close config interface.

8.10 Allocator Manager



Caution

It is valid only in analog system.

View info about the allocator that is connected with VTO.

Select “System Config >Allocator Manager”. The system displays “Allocator Manager” interface, as shown in Figure 8-42, to view info about all connected allocator.



Figure 8-42

8.11 Video Set

Set video picture and audio volume of VTO with camera.

8.11.1 Video Set

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

The system displays “Video Set” interface, as shown in Figure 8-43. Click “Open Door”, and VTO is unlocked.

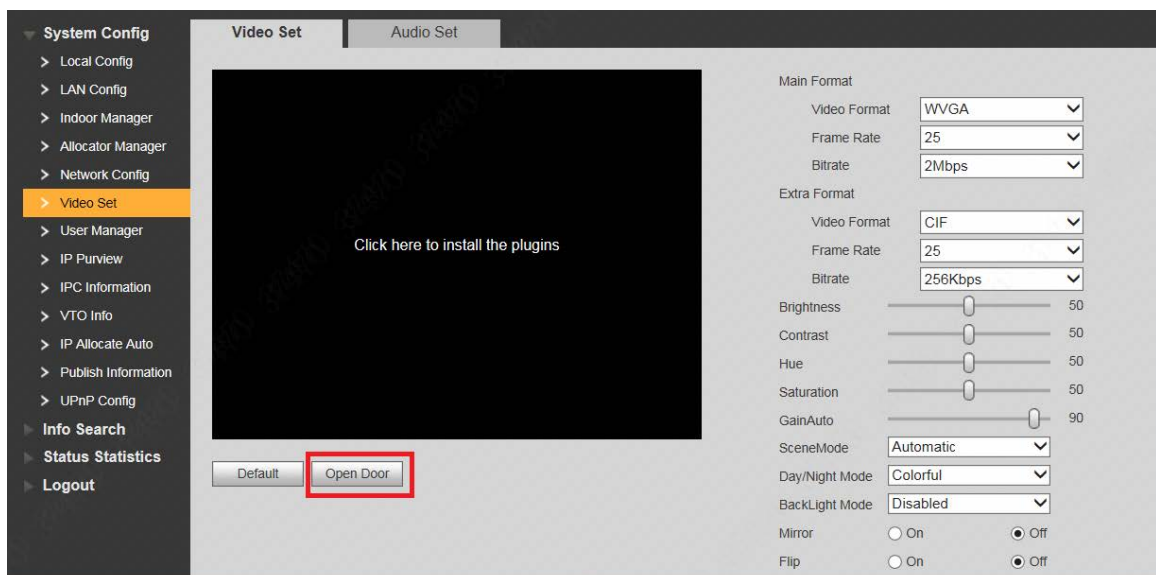


Figure 8-43

Step 2 Set parameters and refer to Table 8-13 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.
	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. <ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ● Disabled: no backlight. ● Backlight: prevent silhouette appearing in dark part of the subject against the light.

Parameter	Description
	<ul style="list-style-type: none"> 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 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 8-13

8.11.2 Audio Set

Step 1 Select "System Config >Video Set>Audio Set".

The system displays "Audio Set" interface, as shown in Figure 8-44.

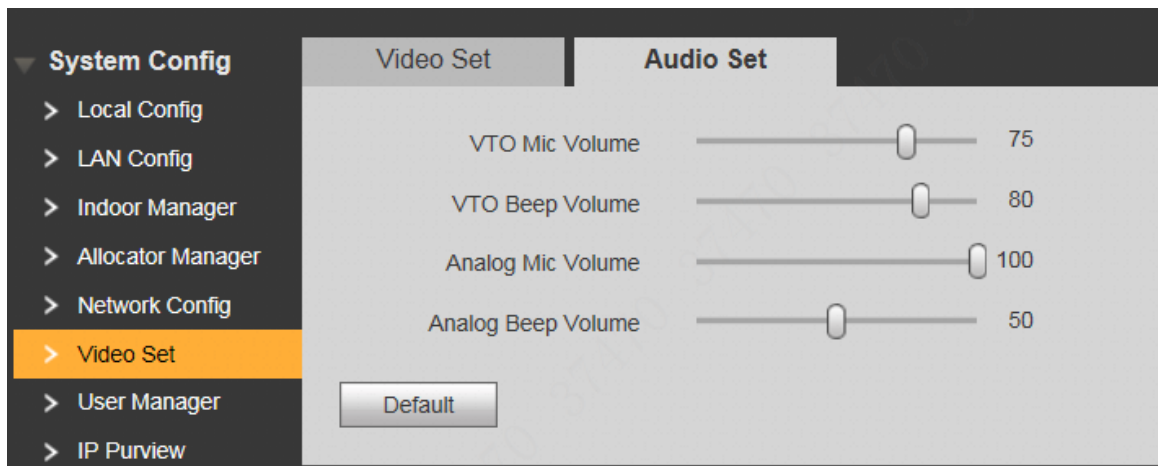


Figure 8-44

Step 2 Adjust mic volume and beep volume of VTO and analog device.

8.12 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 8-45.

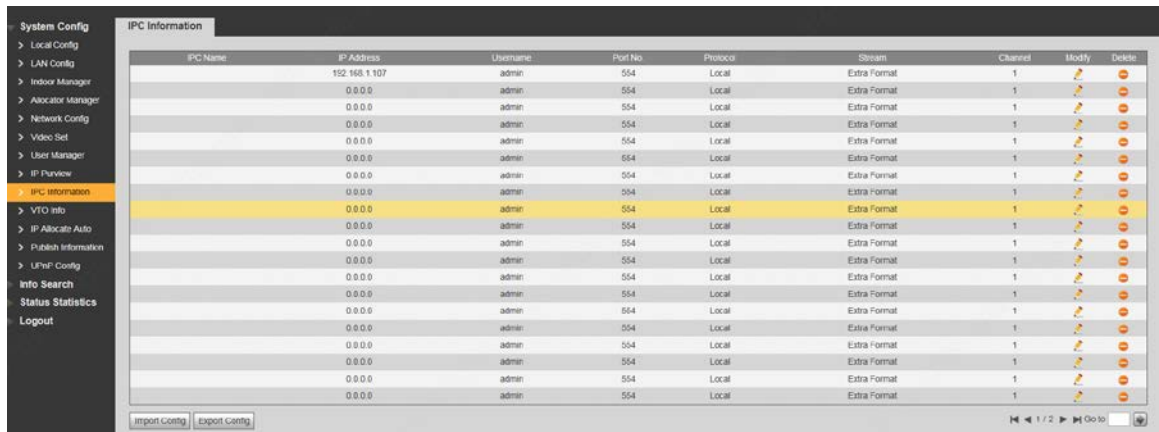


Figure 8-45

8.12.1 Add One IPC

Add IPC info one by one.



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 8-46.

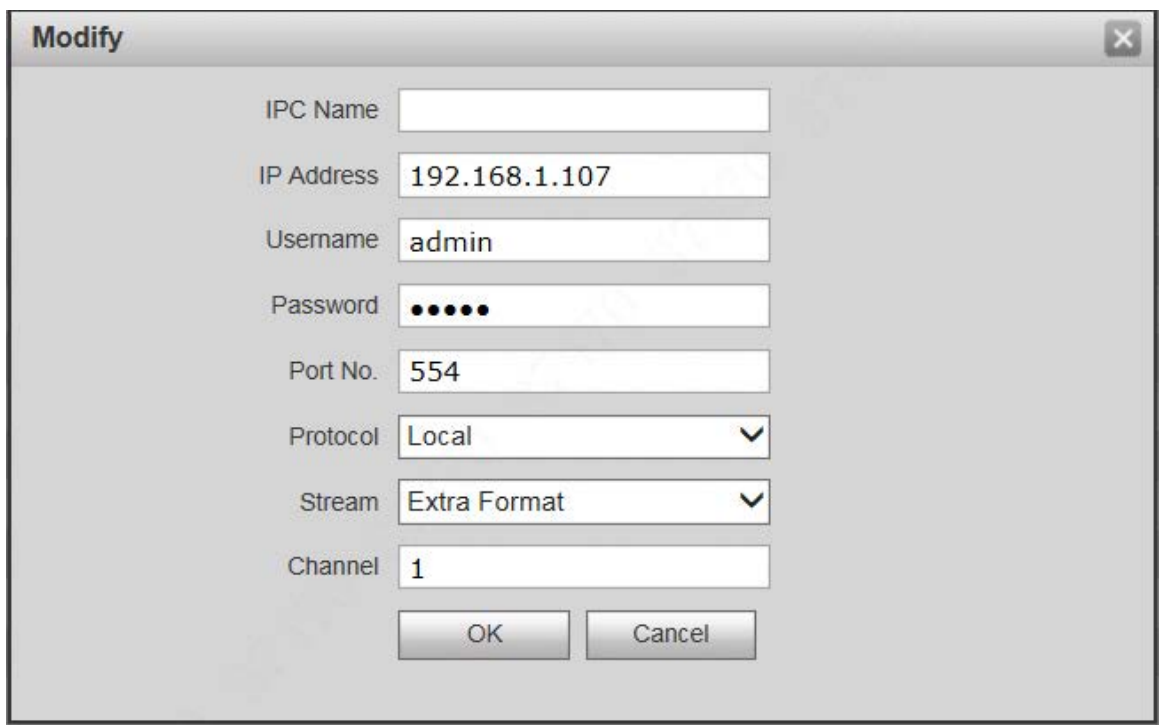


Figure 8-46

Step 2 Set parameters and refer to Table 8-14 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

Parameter	Description
Password	IPC/NVR/XVR/HCVR.
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. <ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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 8-14

Step 3 Click “OK” to complete adding.

8.12.2 Delete

Click  to delete camera info.

8.12.3 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.

8.12.4 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.

8.13 IP Allocate Auto

Set IP range and enable “IP Allocate Auto”. Obtain IP address automatically through info initialization function at VTH interface.

Step 1 Select “System Config > IP Allocate Auto”.

The system displays “IP Allocate Auto” interface, as shown in Figure 8-47.

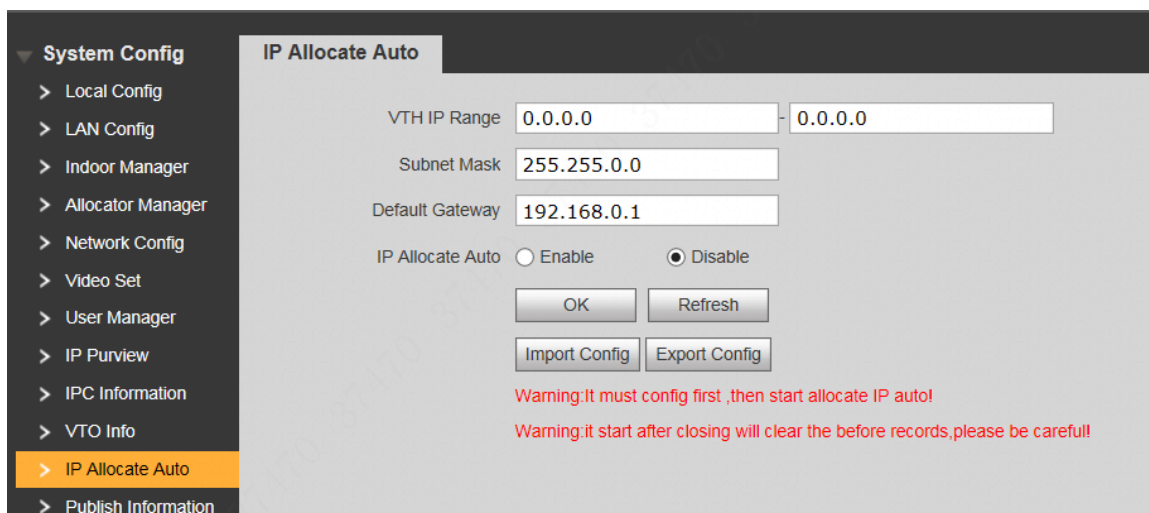


Figure 8-47

Step 2 Set parameters and refer to Table 8-15 for details.

Parameter	Description
VTH IP Range	According to network planning, set VTH start IP, end IP, subnet mask and default gateway.
Subnet Mask	
Default Gateway	
IP Allocate Auto	Set to enable “IP Allocate Auto” function or not.

Table 8-15

Step 3 Click “OK” to save the settings.

Export Config

Export info about allocated VTH IP.

Click “Export Config” to save info about allocated VTH IP to local device. To keep them unchanged in the next allocation, please import this allocation info before enabling automatic allocation.

Import Config

Prevent allocated VTH IP address from being covered.

After setting “VTH IP Range”, “Subnet Mask” and “Default Gateway”, click “Import Config” to select and import previous allocation info file, tick “IP Allocate Auto”, so previously allocated VTH IP remains unchanged, while other VTH IP is allocated automatically.

8.14 Publish Information

Send info to VTH and view history info. It is suitable for property management center to send info.

8.14.1 Send Info

Step 1 Select “System Config > Publish Information > Send Info”.

The system displays “Send Info” interface, as shown in Figure 8-48.

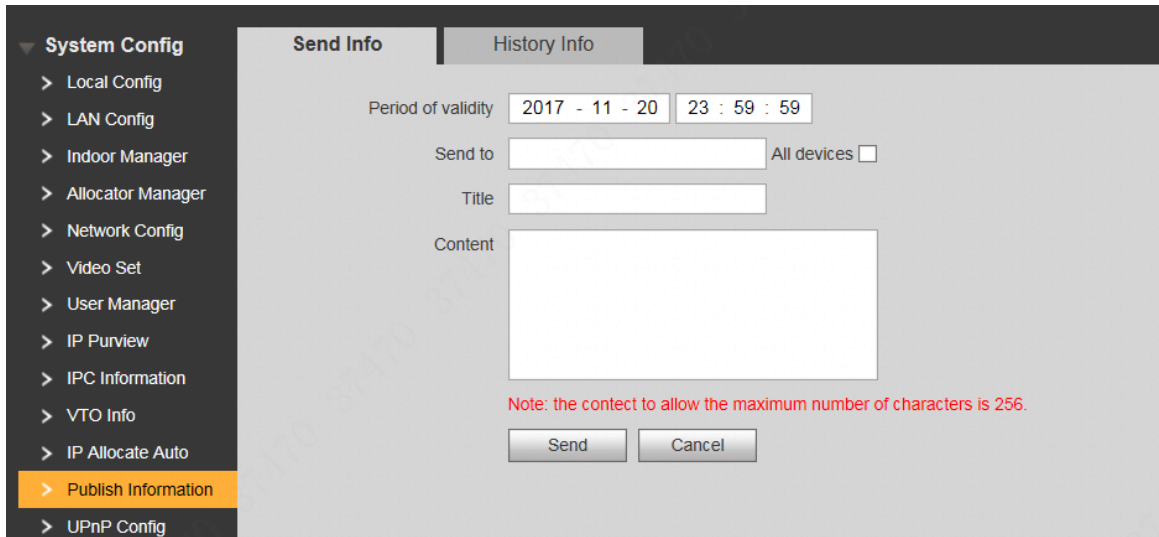


Figure 8-48

Step 2 Set parameters and refer to Table 8-16 for details.


Parameter	Description
Period of Validity	After period of validity is set, info shall be sent within period of validity, so VTH can receive the info. Otherwise, VTH fails to receive the info.  Note All info sent by VTO will be displayed in the history info, whether they are received by VTH or not.
Send to	Set info receiver.
All Devices	<ul style="list-style-type: none"> Send to one VTH: enter the receiver's room number. Send to all VTHs: tick "All Devices".
Title	Title of the info.
Content	Content of the info. Max. 256 characters can be sent.

Table 8-16

Step 3 Click "Send".

The system sends content to VTH.

8.14.2 History Info

Select "System Config > Publish Information > History Info". The system displays "History Info" interface, as shown in Figure 8-49, to view history info.

Click  to delete history info.

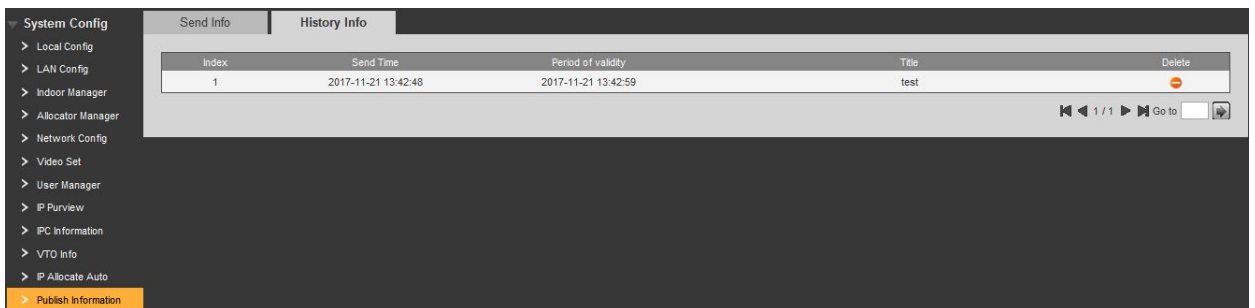


Figure 8-49

8.15 Info Search

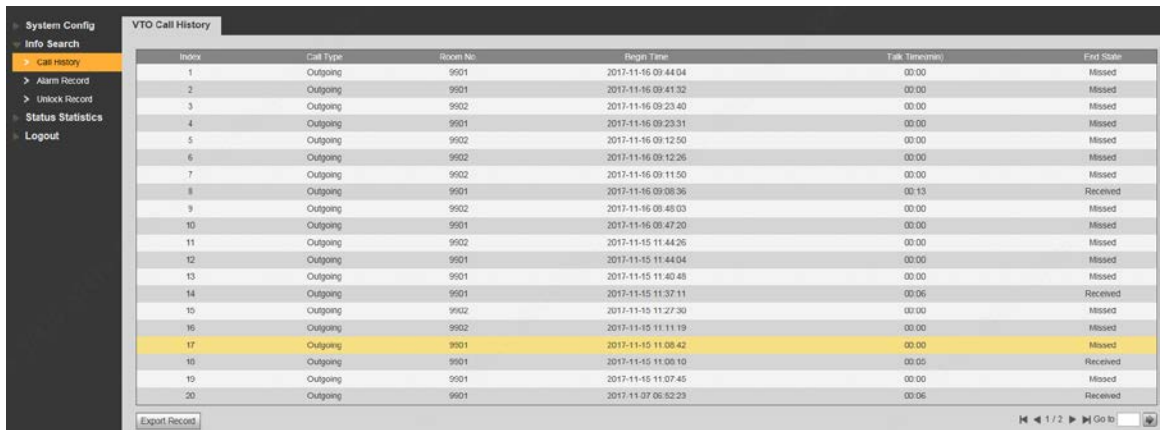
Search VTO call history, alarm record and unlock record.

8.15.1 Call History

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

Select “Info Search> VTO Call History”. The system displays “VTO Call History” interface, as shown in Figure 8-50.

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




Index	Call Type	Room No	Begin Time	Talk Time(min)	End State
1	Outgoing	9901	2017-11-16 09:44:04	00:00	Missed
2	Outgoing	9901	2017-11-16 09:41:32	00:00	Missed
3	Outgoing	9902	2017-11-16 09:23:40	00:00	Missed
4	Outgoing	9901	2017-11-16 09:23:31	00:00	Missed
5	Outgoing	9902	2017-11-16 09:12:50	00:00	Missed
6	Outgoing	9902	2017-11-16 09:12:26	00:00	Missed
7	Outgoing	9902	2017-11-16 09:11:50	00:00	Missed
8	Outgoing	9901	2017-11-16 09:08:36	00:13	Received
9	Outgoing	9902	2017-11-16 09:48:03	00:00	Missed
10	Outgoing	9901	2017-11-16 09:47:20	00:00	Missed
11	Outgoing	9902	2017-11-15 11:44:26	00:00	Missed
12	Outgoing	9901	2017-11-15 11:44:04	00:00	Missed
13	Outgoing	9901	2017-11-15 11:40:48	00:00	Missed
14	Outgoing	9901	2017-11-15 11:37:11	00:06	Received
15	Outgoing	9902	2017-11-15 11:27:30	00:00	Missed
16	Outgoing	9902	2017-11-15 11:11:19	00:00	Missed
17	Outgoing	9901	2017-11-15 11:08:42	00:00	Missed
18	Outgoing	9901	2017-11-15 11:00:10	00:05	Received
19	Outgoing	9901	2017-11-15 11:07:45	00:00	Missed
20	Outgoing	9901	2017-11-07 06:52:23	00:06	Received

Figure 8-50

8.15.2 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 8-51. Click “Export Record” to export the VTO alarm record.



Index	Room No	Event State	Channel	Begin Time
-------	---------	-------------	---------	------------

Figure 8-51

8.15.3 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 8-52. Click “Export Record” to export the VTO unlock

record.



Index	Unlock Type	Room No.	Username	Card Number	Unlock Result	Unlock Time
1	Password Unlock				Success	2017-11-20 06:42:46
2	Password Unlock				Failed	2017-11-27 03:42:27
3	Password Unlock				Success	2017-11-27 03:41:22
4	Password Unlock				Failed	2017-11-27 03:41:13

Figure 8-52

8.16 Status Statistics

View online and offline status of VTH and VTO.

Select “Status Statistics > VTH Status”. The system displays “VTH Status” interface, as shown in Figure 8-53.

- Offline: VTO is disconnected from VTH, and it cannot call, monitor and talk.
- Online: VTO is connected with VTH, and it can call, monitor and talk.



VTH	Status	MON	IP Port	Reg Time	Off Time
-----	--------	-----	---------	----------	----------

Figure 8-53

8.17 Reboot Device

Reboot the device at WEB interface.

Step 1 Select “Logout > Reboot Device”.

The system displays “Reboot Device” interface, as shown in Figure 8-54.

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

WEB interface is switched to WEB login interface.



Figure 8-54

8.18 Logout

Log out the WEB interface.

Step 1 Select “Logout > Logout”.

The system displays “Logout” interface, as shown in Figure 8-55.

Step 2 Click “Logout”.

Log out the WEB interface and return to login interface.

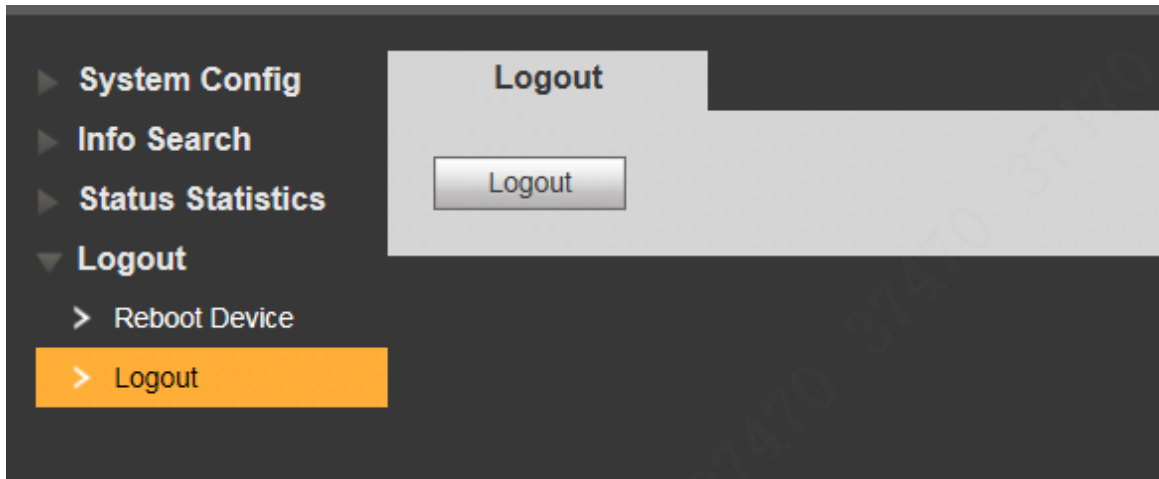


Figure 8-55

Appendix 1 Technical Parameters

Model		VTO1220A	VTO1220 BW	VTO121 0A-X	VTO12 10B-X	VTO1210 C-X
System	Main Processor	Embedded microcontroller				
	Operating System	Embedded LINUX Operating System				
Video	Video Compression Standard	H.264				
	Input/ Proximity Sensor	1.30 megapixel HD camera				
	Backlight	Support				
	Auto Fill-in Light	Support				
Audio	Input	Omnidirectional microphone				
	Output	Built-in speaker				
	Talk	Support two-way audio talk				
Display	Screen	3.5-inch TFT screen	3-inch STN screen			
	Resolution	320x240	128x64			
Operating Mode	Input	Numeric key	Touch key	Numeric key	Touch key	Numeric key
	Swiping Card	Built-in IC card induction read head				
Proximity Sensor		Infrared, about 1 meter				
Tamper Alarm		Support				
Access Control	NO/NC Output	Support				
	Exit Button	Support				
	Door Status Detection	Support				
Network	Ethernet	10M/100Mbps self-adaptive				
	Network Protocol	TCP/IP				
Storage	Memory	128MB				
	SD Card	None				
Specification	Power Supply	DC 12V				
	Power Consumption	Standby $\leq 1W$; working $\leq 10W$				
	Working Temperature	$-40^{\circ}C \sim +60^{\circ}C$; 10%RH \sim 95%RH				
	Waterproof	IP53	IP65	IP53	IP65	IP53