Unit VTO
(Version 3.1)

Quick Start Guide

V1.0.2

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

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

2. Update Firmware

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

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

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

2. Change Default HTTP and TCP Ports:

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

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

3. Enable HTTPS/SSL:

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

4. Enable IP Filter:

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

5. Change ONVIF Password:

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

6. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

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

8. Use a Different Username and Password for SmartPSS:

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

9. Limit Features of Guest Accounts:

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

10. UPnP:

● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

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

12. Multicast:

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

13. Check the Log:

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

14. Physically Lock Down the Device:

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

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

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

16. Isolate NVR and IP Camera Network

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

Foreword

General

This document mainly introduces structure, mounting process, debugging and verification process of unit VTO products.

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.

Safety Instructions

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

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
🔑 TIPS	Provides methods to help you solve a problem or save you time.
📖 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

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

Privacy Protection Notice

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

About the Manual

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

Important Safeguards and Warnings

The following description is the correct application method of the device. Please read the manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirement

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

Power Requirement

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

Table of Contents

1 Product Structure

1.1 VTO1220A/VTO1210A-X

1.1.1 Front Panel

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

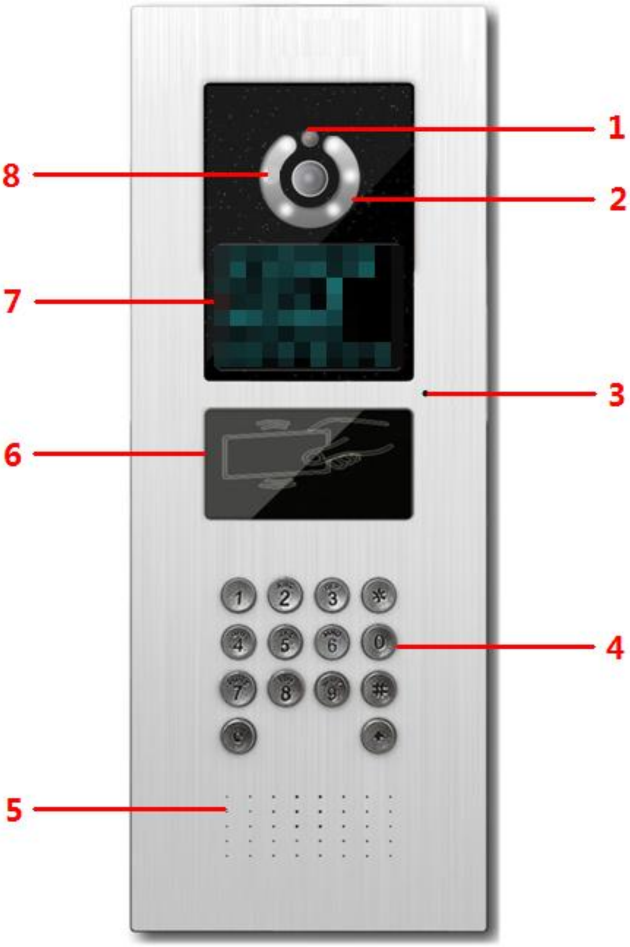


Figure 1-1

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	● ⊛: 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	Display prompt, date and time. ● "User: room no. + press ↑" means that if you want to call the user, please enter the user's room no. and press ⬆ to make a call. ● "Center: press ↻", means that if you want to call the management center, please 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.
8	Camera	Monitor the door area.

Table 1-1

1.1.2 Rear Panel

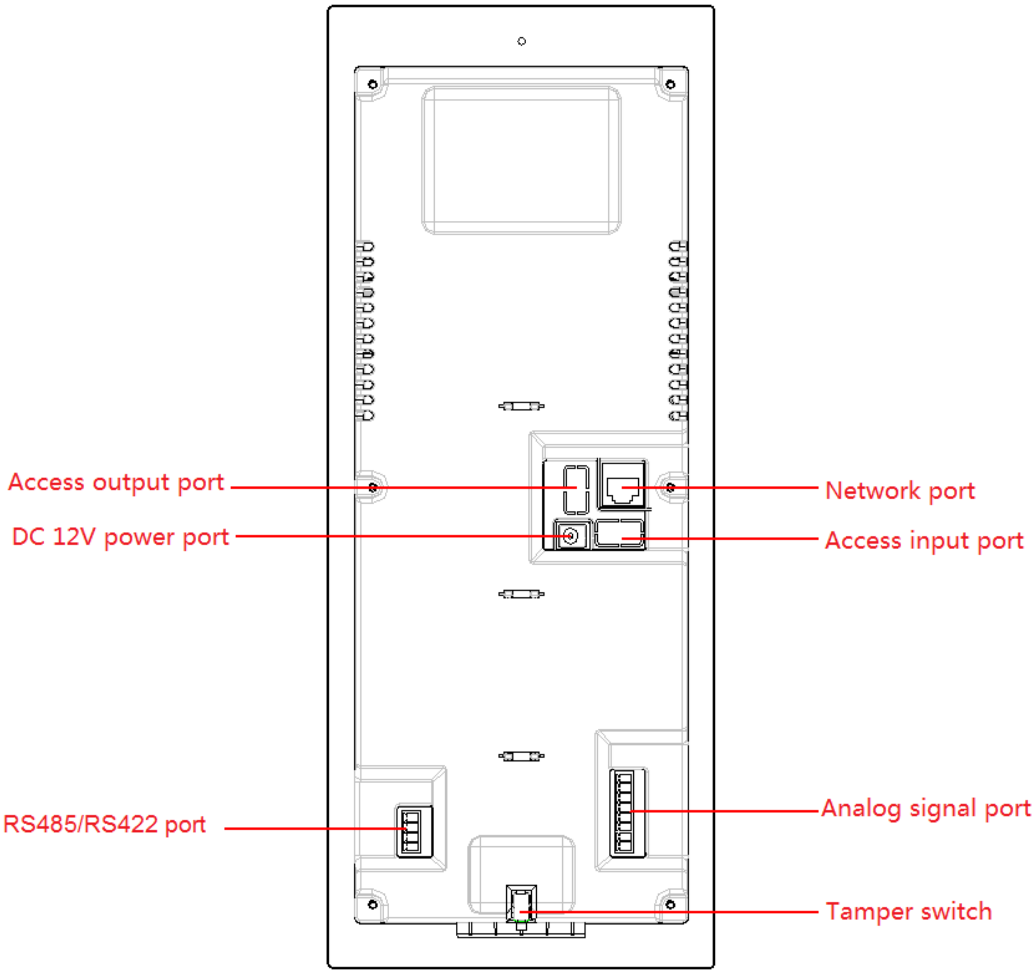


Figure 1-2

1.2 VTO1220BW/VTO1210B-X/ VTO1210C-X

1.2.1 Front Panel

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

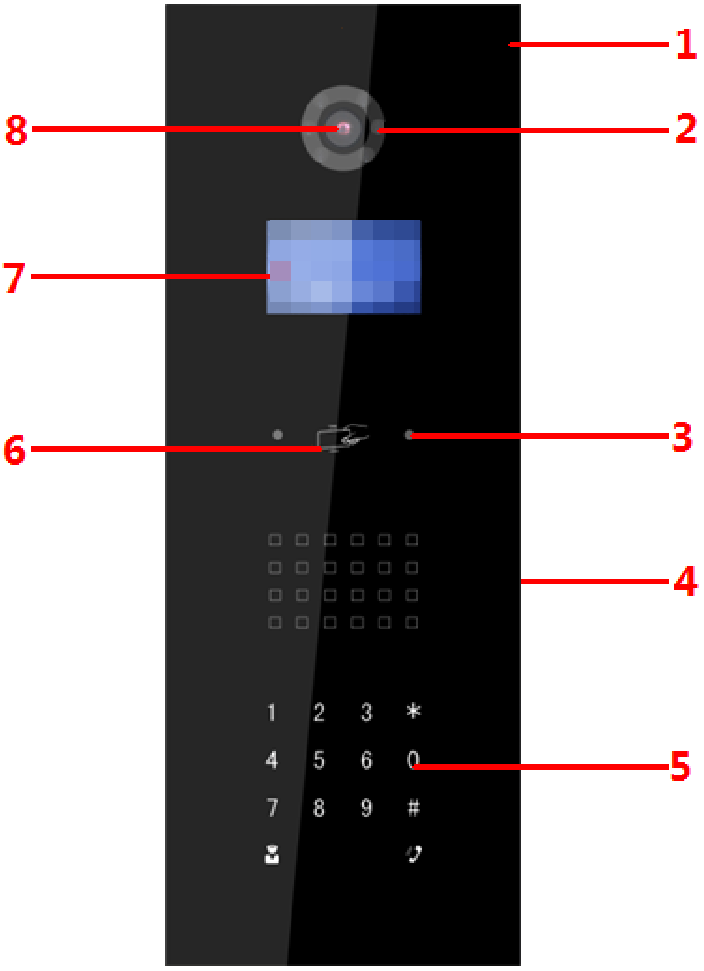


Figure 1-3

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	● *: 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	Display prompt, date and time. ● "User: room no. + press 📞" means that if you want to call the user, please enter the user's room no. and press 📞 to make a call. ● "Center: press 👤", means that if you want to call the management center, please 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.
8	Camera	Monitor the door area.

Table 1-2

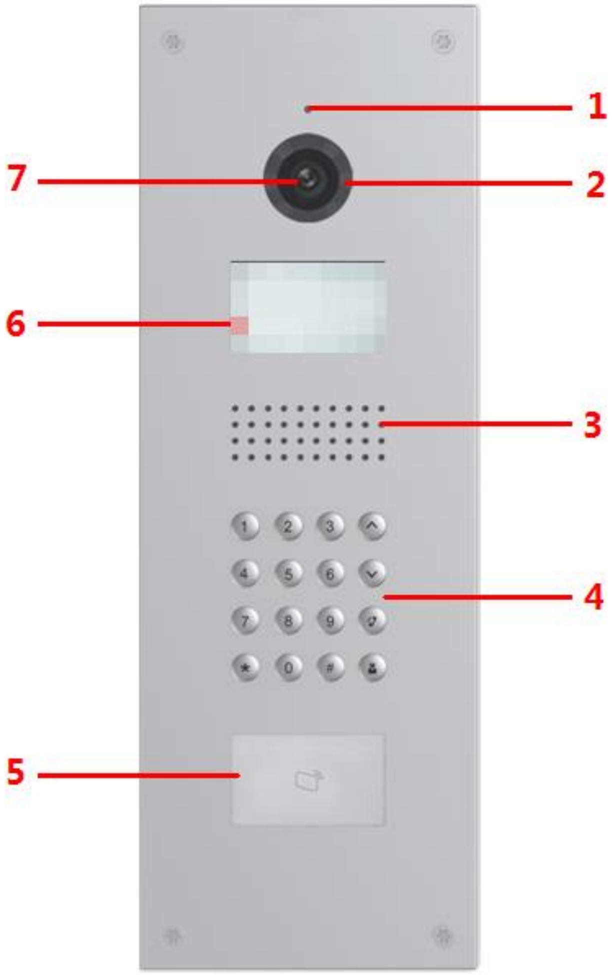


Figure 1-4

No.	Name	Description
1	Microphone	Audio input.

No.	Name	Description
2	Fill-in light	Provide fill-in light for camera in case of insufficient light.
3	Speaker	Audio output.
4	Key area	● ＊: 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. ● ∧∨: at the contact interface, press these keys to page up and down.
5	Card swiping area	Unlock by swiping card.
6	Display screen	Display prompt, date and time. ● "User: room no. + press ☎" means that if you want to call the user, please enter the user's room no. and press ☎ to make a call. ● "Center: press 👮", means that if you want to call the management center, please 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 1-3

1.2.2 Rear Panel

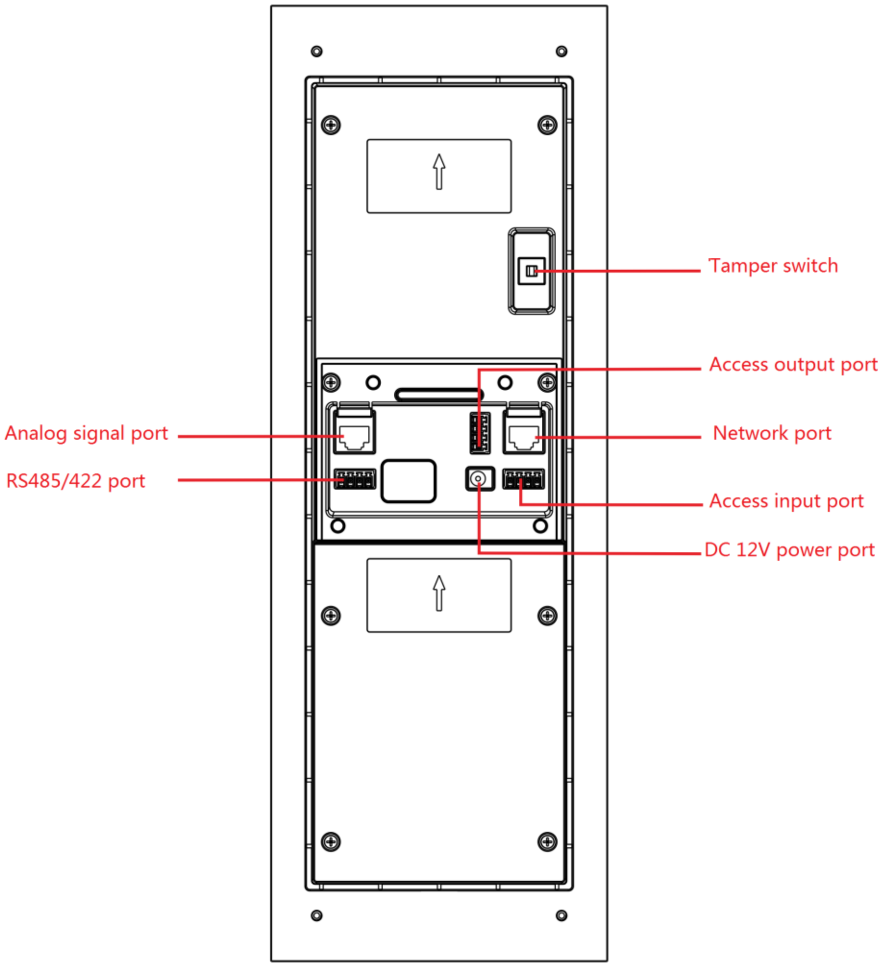


Figure 1-5

1.3 Port Wiring Description

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

1.3.1 Access Input and Output Wiring

⚠ Caution

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 1-6, Figure 1-7 and Figure 1-8.

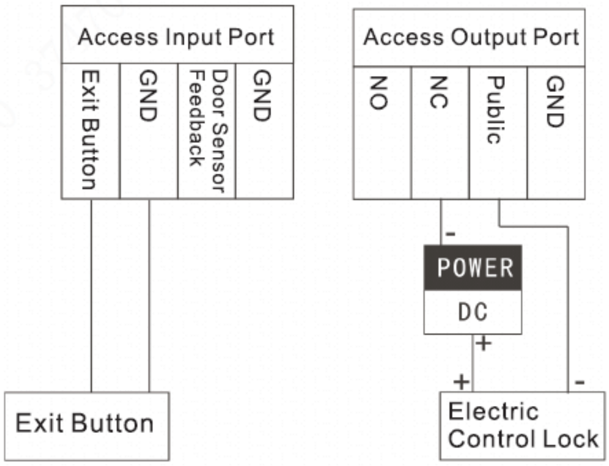


Figure 1-6

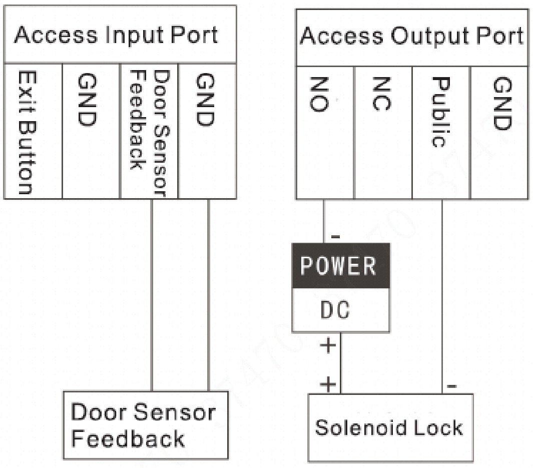


Figure 1-7

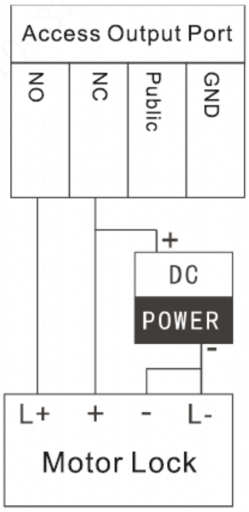


Figure 1-8

1.3.2 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 1-9.

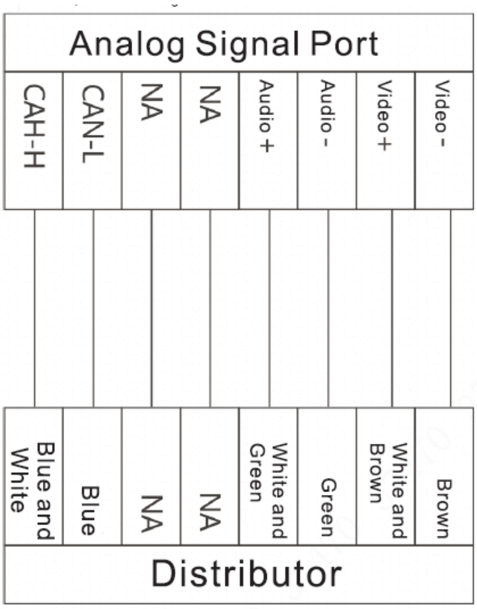


Figure 1-9

1.3.3 RS485/RS422 Wiring

Connect RS485 or RS422 communication device, as shown in Figure 1-10, Figure 1-11 and Figure 1-12.

Note

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

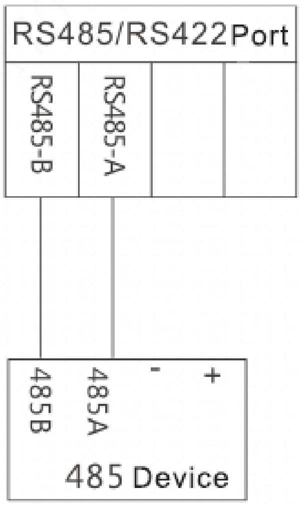


Figure 1-10

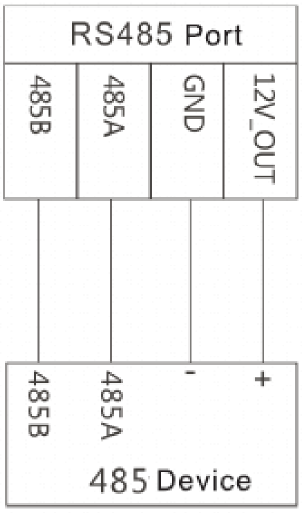


Figure 1-11

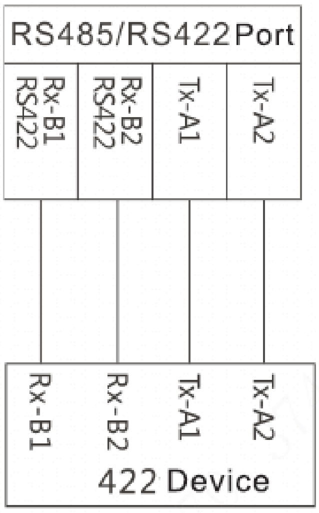


Figure 1-12

2 Mounting and Debugging

2.1 Mounting

⚠ Caution

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

2.1.1 VTO1220A/VTO1210A-X

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

📖 Note

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

Step 1 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.

Step 2 Mount the expansion pipes in holes.

Step 3 Connect cables, pass through the box and connect the cables in walls. Please refer to “1.3 Port Wiring Description” for details.

Step 4 Fix the metal box onto wall with ST3×18 screws.

Step 5 Fix the bare device onto metal box with M3×16 screws.

Step 6 Apply glue between the bare device and wall.

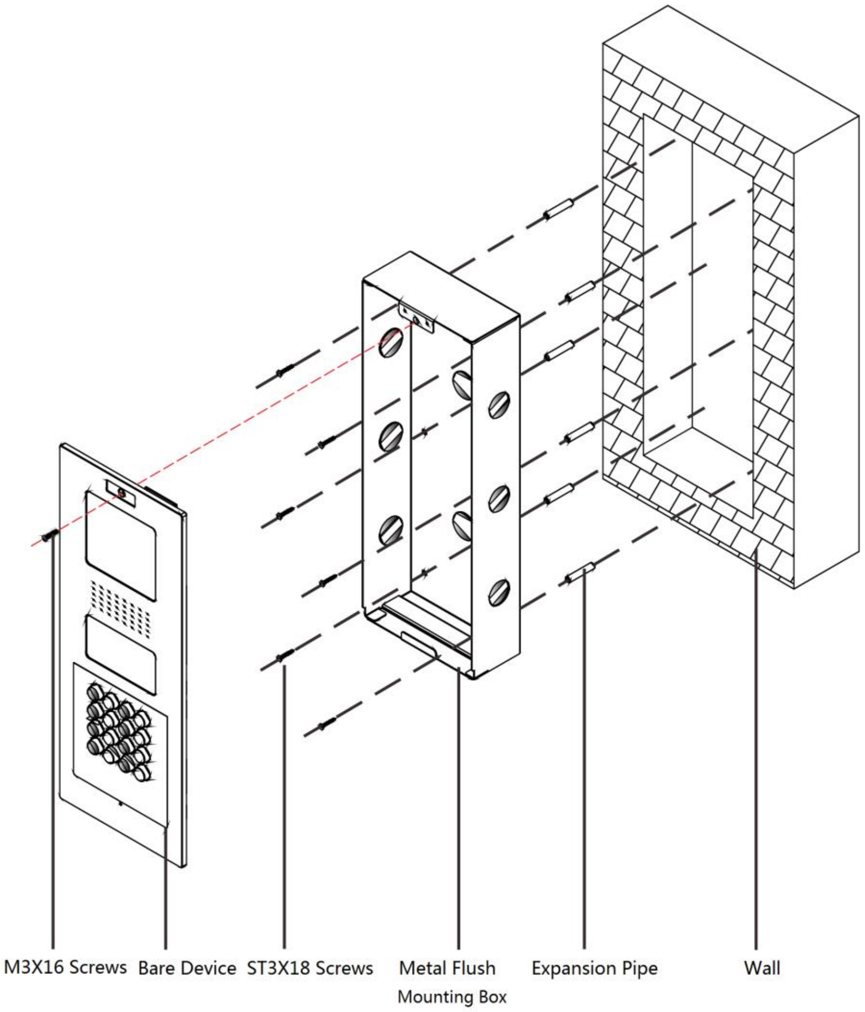


Figure 2-1

2.1.2 VTO1220BW/VTO1210B-X

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 mounting bracket and connect the cables in walls. Please refer to “1.3 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.

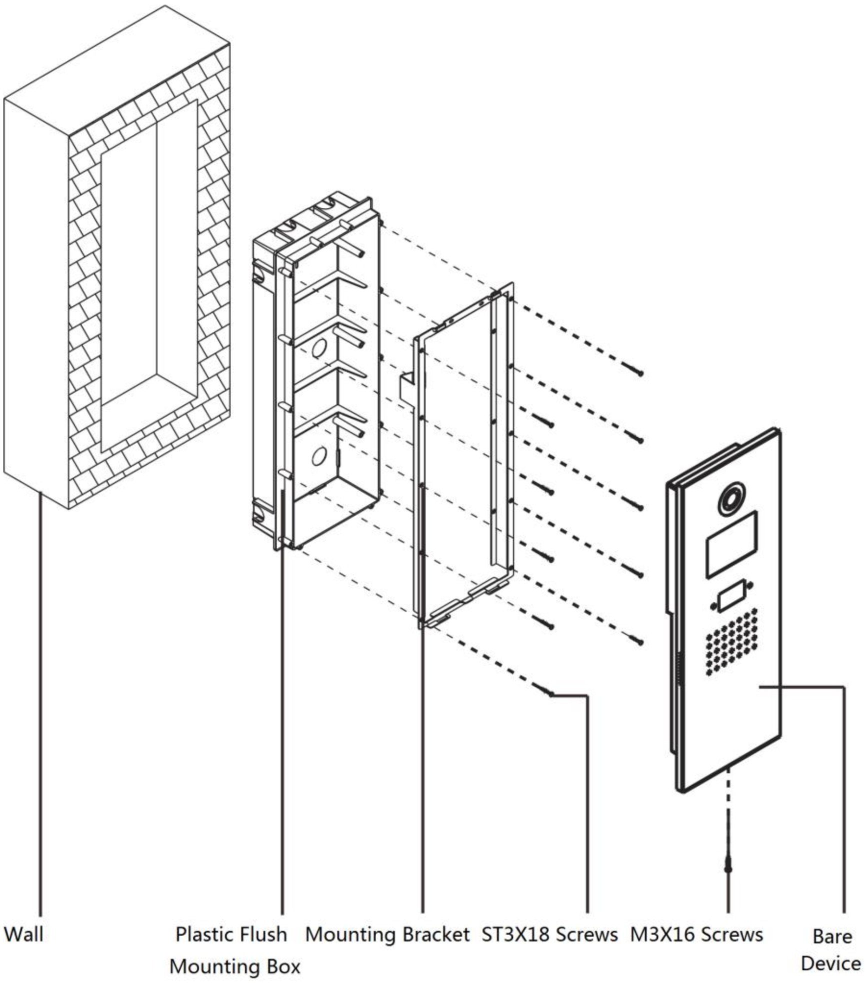


Figure 2-2

2.1.3 VTO1210C-X

2.1.3.1 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 ST4.2×25 screws.

Step 3 Connect cables and connect the cables in walls. Please refer to "1.3 Port Wiring Description" for details.

Step 4 Fix the bare device onto the box with M4×30 screws.

Step 5 Apply glue between the box and wall.

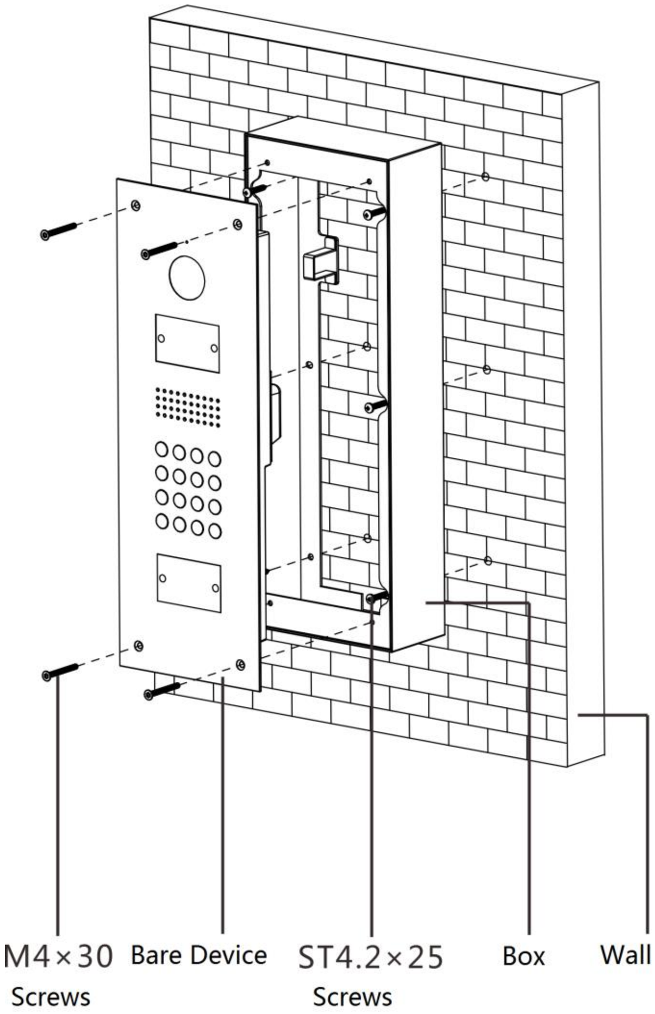


Figure 2-3

2.1.3.2 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 “1.3 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.

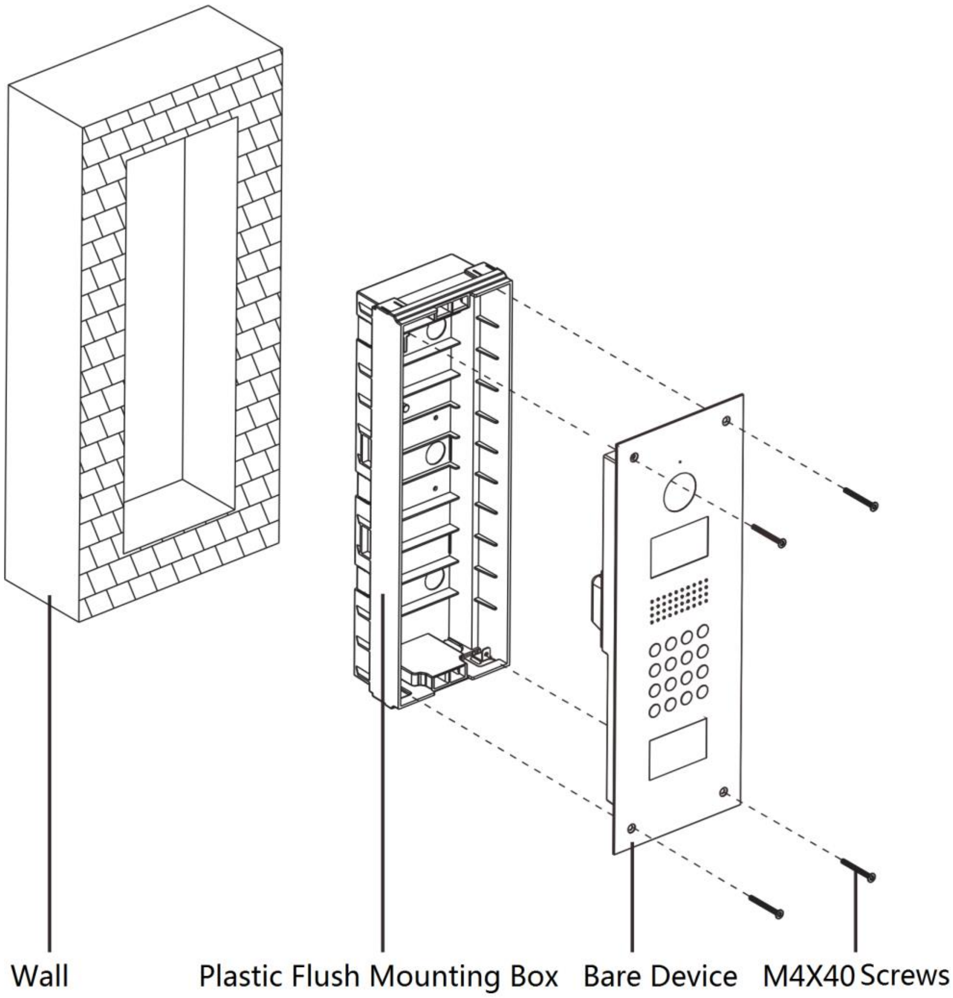


Figure 2-4

2.2 Debugging

⚠ Caution

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.

The system provides two debugging methods. Please select according to actual needs.

- 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.

2.2.1 Single Debugging

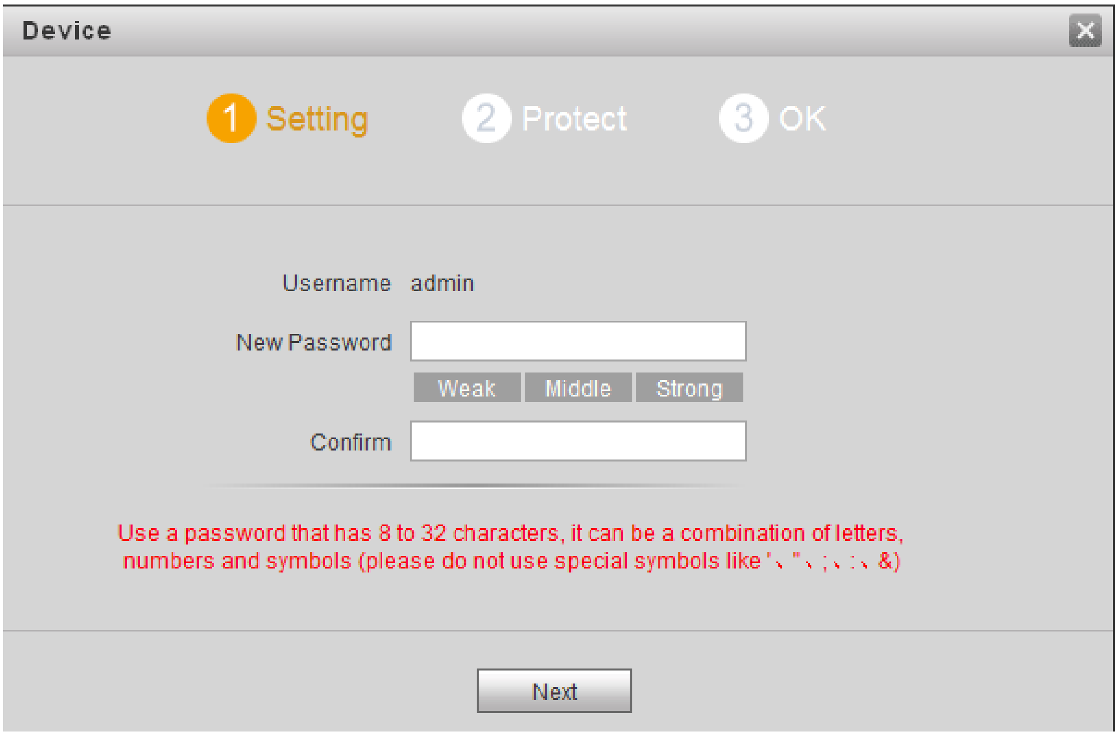
2.2.1.1 VTO Settings

For the first time, please initialize and modify 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 Power on the device, and enter default IP address of VTO at the address bar of PC browser. The system displays "Setting" interface, as shown in Figure 2-5.



Username admin

New Password

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 '、"、;、:、&)

Figure 2-5

Step 2 According to interface prompt, enter "New Password" and "Confirm", and click "Next". 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.

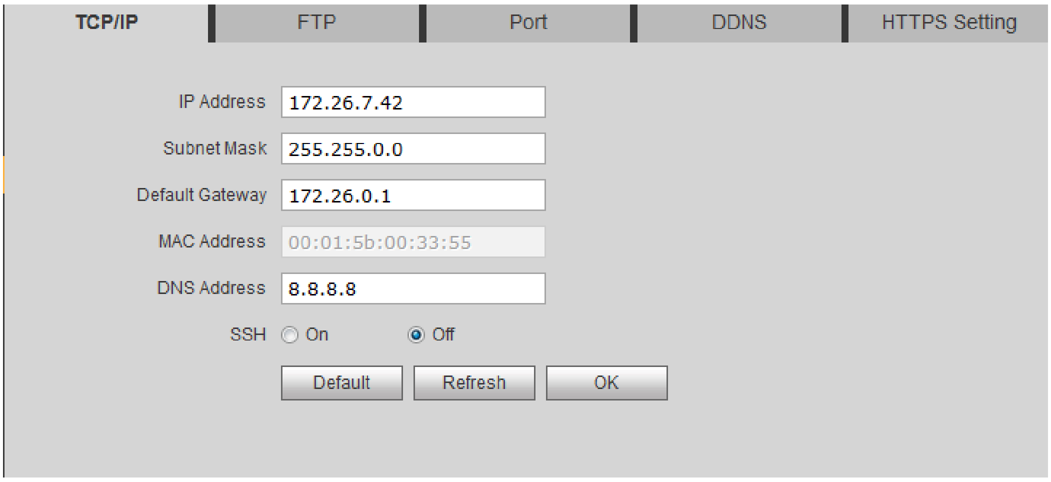
Step 3 Login WEB interface.

Note

- Default user name is admin.
- Password is the new one set during initialization.

Step 4 Select "System Config > Network Config> TCP/IP".

The system displays "TCP/IP" interface, as shown in Figure 2-6.



IP Address: 172.26.7.42

Subnet Mask: 255.255.0.0

Default Gateway: 172.26.0.1

MAC Address: 00:01:5b:00:33:55

DNS Address: 8.8.8.8

SSH ○ On ● Off

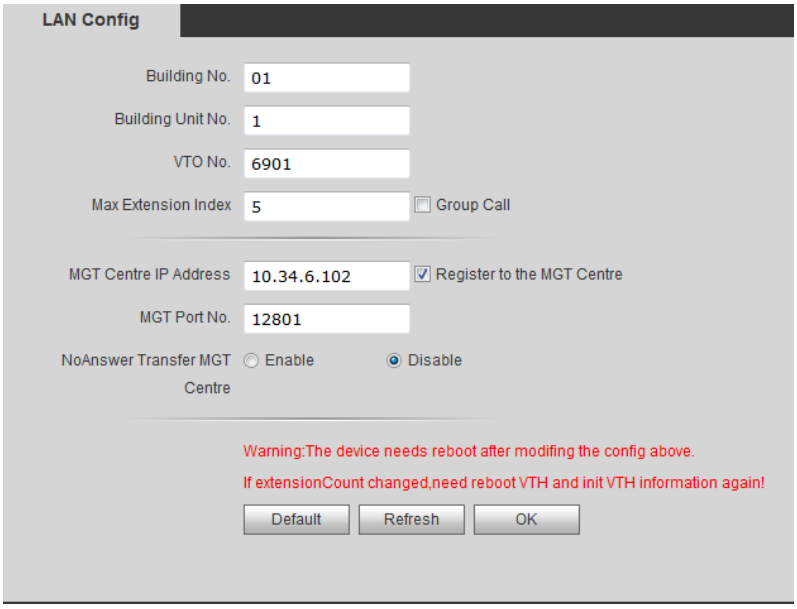
Figure 2-6

Step 5 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, login will be failed. Please add PC to the planned network segment and login WEB interface again.

Step 6 Login WEB interface again; select "System Config > LAN Config".

The system displays "LAN Config" interface, as shown in Figure 2-7.



Building No.: 01

Building Unit No.: 1

VTO No.: 6901

Max Extension Index: 5 □ Group Call

MGT Centre IP Address: 10.34.6.102 ☑ Register to the MGT Centre

MGT Port No.: 12801

NoAnswer Transfer MGT Centre ○ Enable ● Disable

Warning:The device needs reboot after modifing the config above.

If extensionCount changed,need reboot VTH and init VTH information again!

Figure 2-7

1. Enter VTO "Building No.", "Building Unit No." and "VTO No.".

   Note

   - To call the management center, please tick "Register to the MGT Center", and set "MGT Center IP Address" and "MGT Port No.".
   - To provide group call function, please tick "Group Call" and set "Max Extension Index", which is 5 at most.

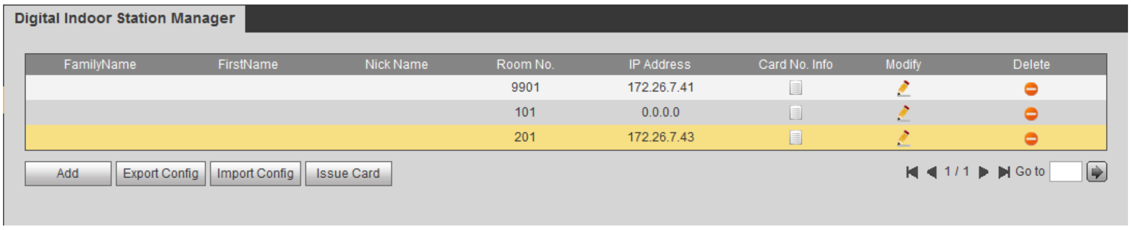
2. Click "OK".

Step 7 Select "System Config > Digital Indoor Station Manager".

The system displays "Digital Indoor Station Manager" interface, as shown in Figure 2-8.

Note

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



Digital Indoor Station Manager

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	▤	✎	⊖

Figure 2-8

1. Click “Add”.
2. 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.
3. Click “OK”.

2.2.1.2 VTH Settings (Version 3.1)

For the first time, please initialize the password and bind Email. Password is used to enter project setting interface, while Email 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 2-9.

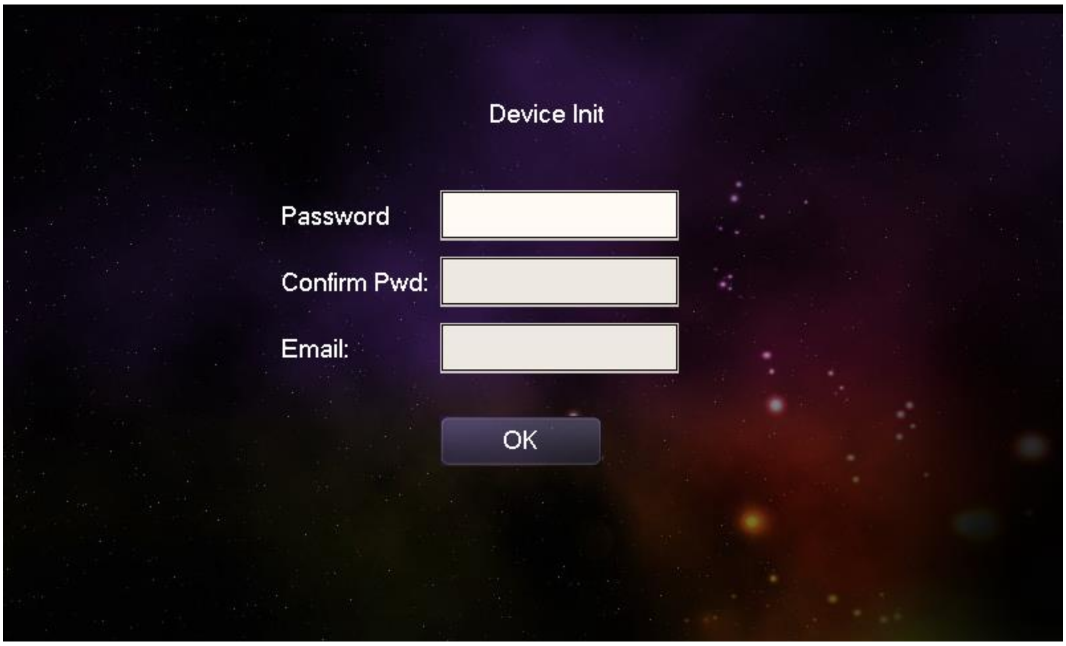


Figure 2-9

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

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

Step 3 Select “System Config >Project Settings”.

The system pops up “Password” prompt box.

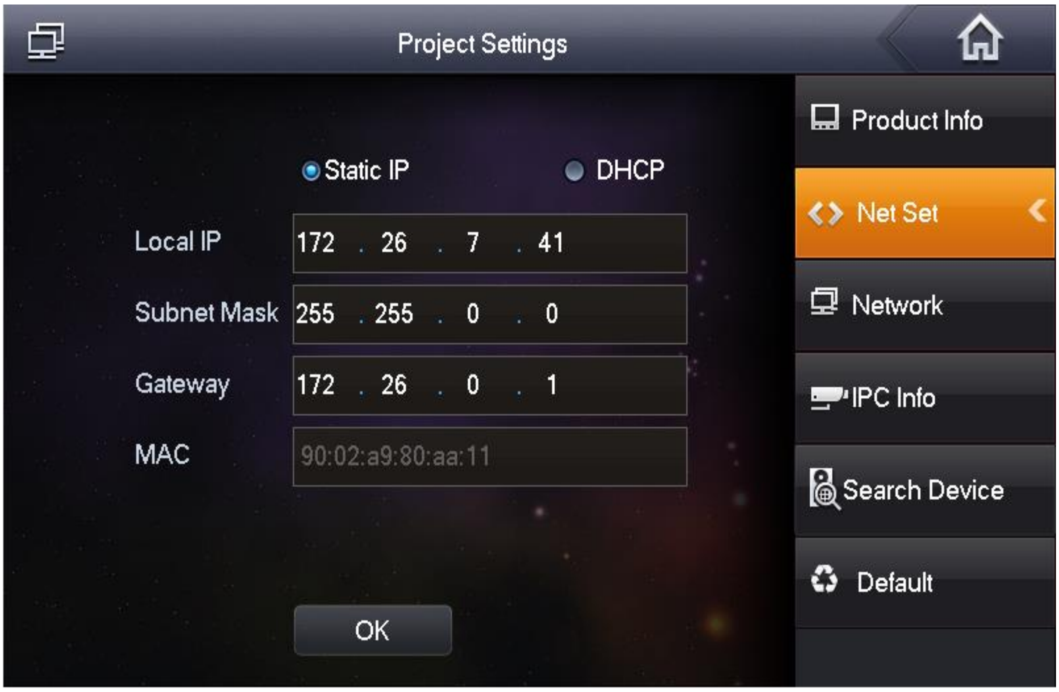
Step 4 Enter the password set during initialization, and click [OK].

Step 5 Click [Net Set].

The system displays “Net Set” interface, as shown in Figure 2-10.

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.



● Static IP ○ DHCP

Local IP 172 . 26 . 7 . 41

Subnet Mask 255 . 255 . 0 . 0

Gateway 172 . 26 . 0 . 1

MAC 90:02:a9:80:aa:11

Figure 2-10

1. Set according to actual network access mode.

- Static IP

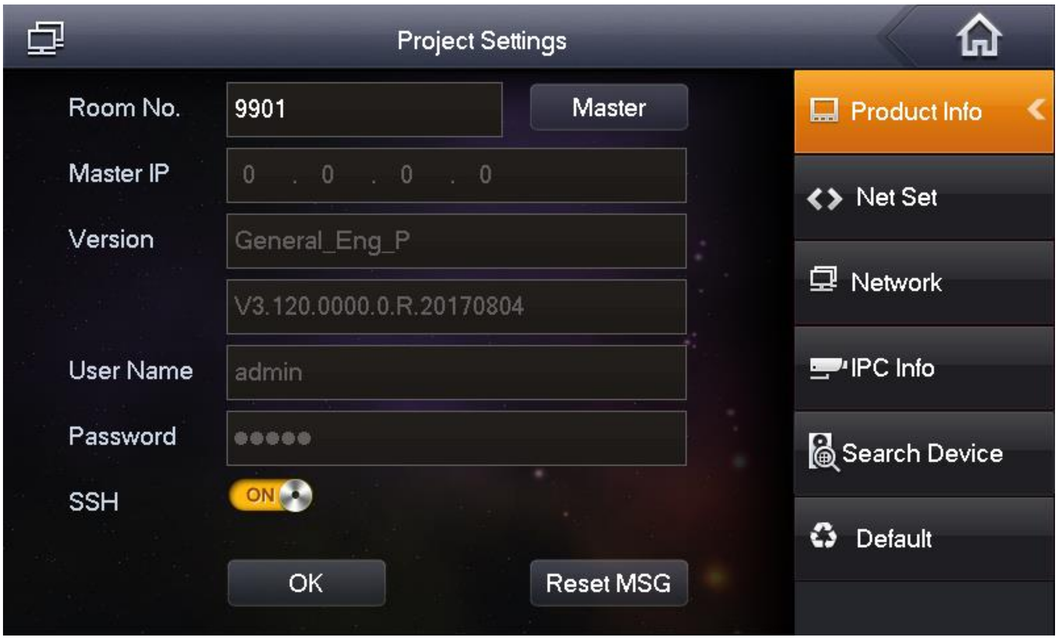
  Select “Static IP”. Enter “Local IP”, “Subnet Mask” and “Gateway”.
- DHCP

  Select “DHCP” to obtain IP address automatically.

2. Click [OK] to save the settings.

Step 6 Press [Product Info].

The system displays “Product Info” interface, as shown in Figure 2-11.



Room No. 9901

Master IP 0 . 0 . 0 . 0

Version General_Eng_P

V3.120.0000.0.R.20170804

User Name admin

Password ●●●●●

SSH ON

Figure 2-11

- Be used as a master VTH.

Enter “Room No.” (such as 9901) and click “OK”.

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.

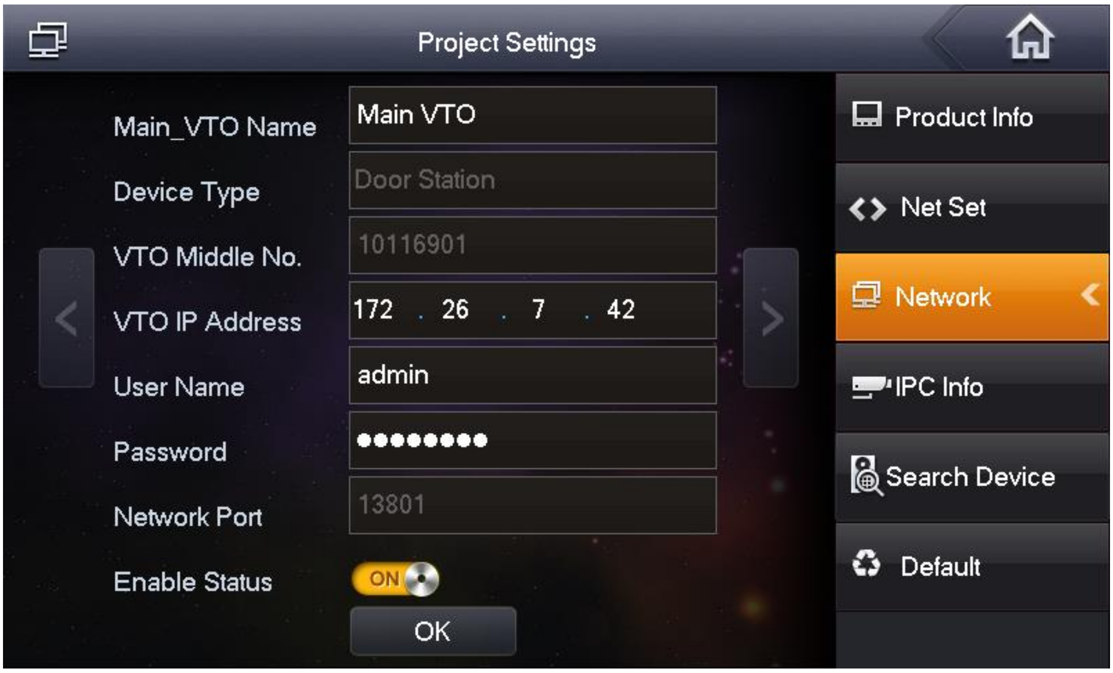
1. Press [Master] and switch to “Extension”.
2. Enter “Room No.” (such as 9901-1) and “Master IP” (IP address of master VTH).

   Note

   “User Name” and “Password” are the user name and password of master VTH. Default user name is admin, and the password is the one set during device initialization.
3. Click [OK] to save the settings.

Step 7 Press [Network].

The system displays “Network” interface, as shown in Figure 2-12.



Main_VTO Name: Main VTO

Device Type: Door Station

VTO Middle No.: 10116901

VTO IP Address: 172 . 26 . 7 . 42

User Name: admin

Password: ●●●●●●●●

Network Port: 13801

Enable Status: ON

Figure 2-12

- Add main VTO.

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

Note

- Default device type is “Door Station”. VTO middle no. will be obtained automatically. The format is “1+building no.+ unit no. + VTO no.”. Building no. has 2 digits, unit no. has 1 digit, and no. has 4 digits, so middle no. has 8 digits in total.
- “User Name” and “Password” shall be consistent with WEB login user name 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 sub VTO.

1. Press > to switch to sub VTO setting interface.
2. Enter sub VTO name, IP address, “User Name” and “Password”.
3. Switch “Enable Status” to ON.

- 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., “User Name” and “Password”.

Note

Fence station middle no. consists of “1+00+0+fence station no.”; building no. is 00, unit no. is 0 and VTO no. has 4 digits, so middle no. has 8 digits in total. For example, 10006901.

3. Switch “Enable Status” to ON.

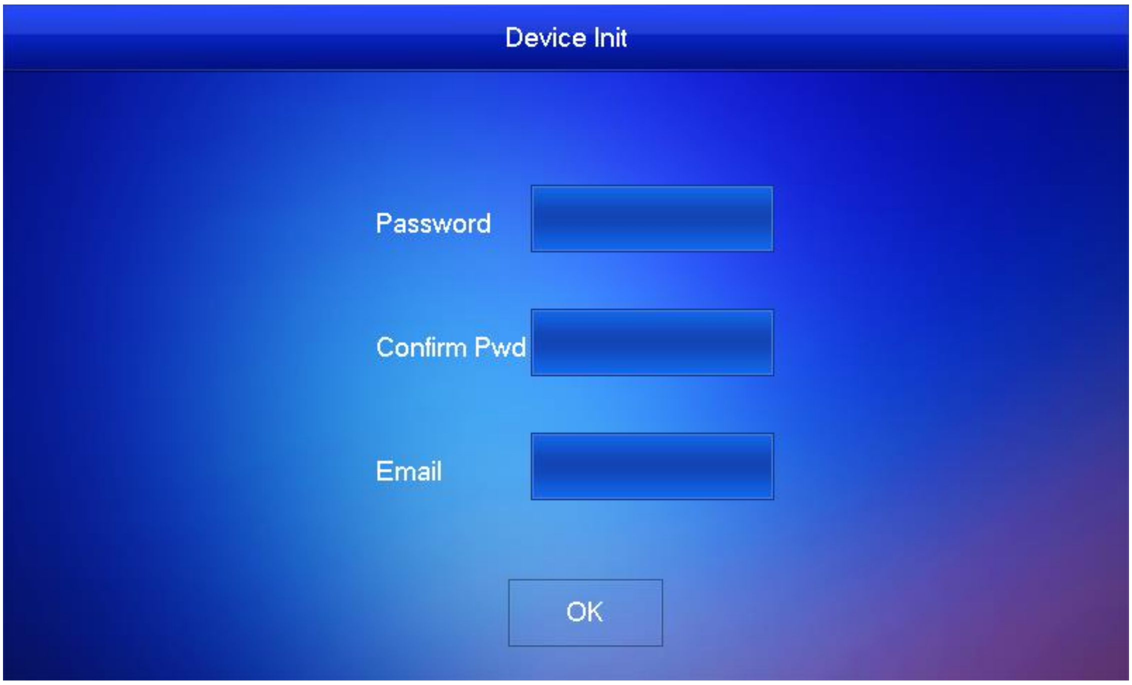
Step 8 Click [OK] to save the settings.

2.2.1.3 VTH Settings (Version 4.0)

For the first time, please initialize the password and bind Email. Password is used to enter project setting interface, while Email 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 2-13.



Device Init

Password

Confirm Pwd

Email

OK

Figure 2-13

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

Step 3 Press [Setting] for more than 6 seconds.

The system pops up “Password” prompt box.

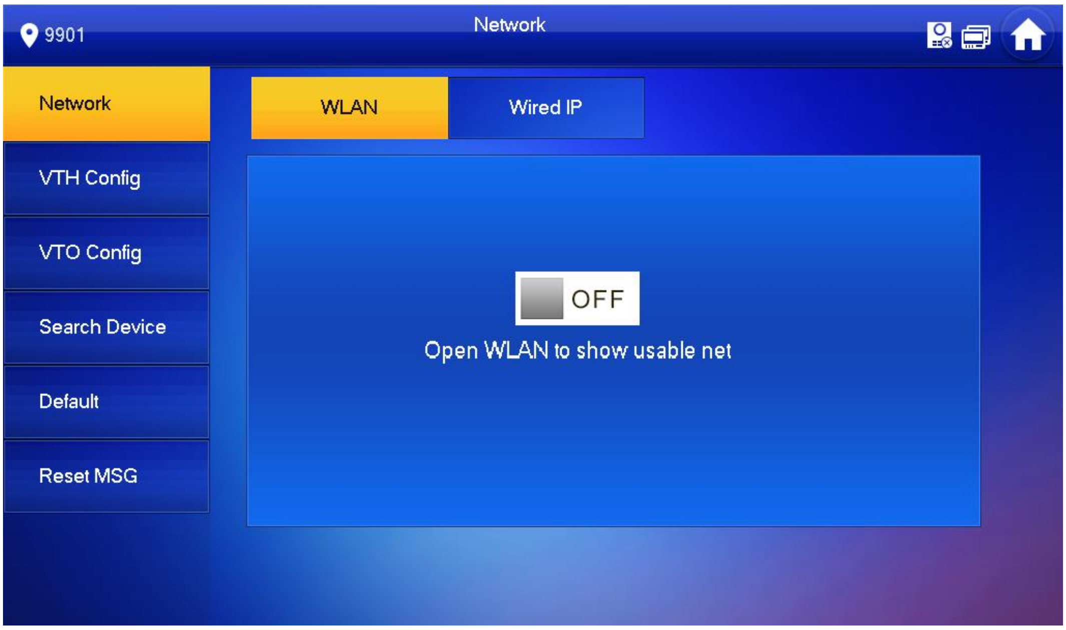
Step 4 Enter the password set during initialization, and click [OK].

Step 5 Click [Network].

The system displays “Network” interface, as shown in Figure 2-14 or Figure 2-15. Please set according to network access mode in actual application.

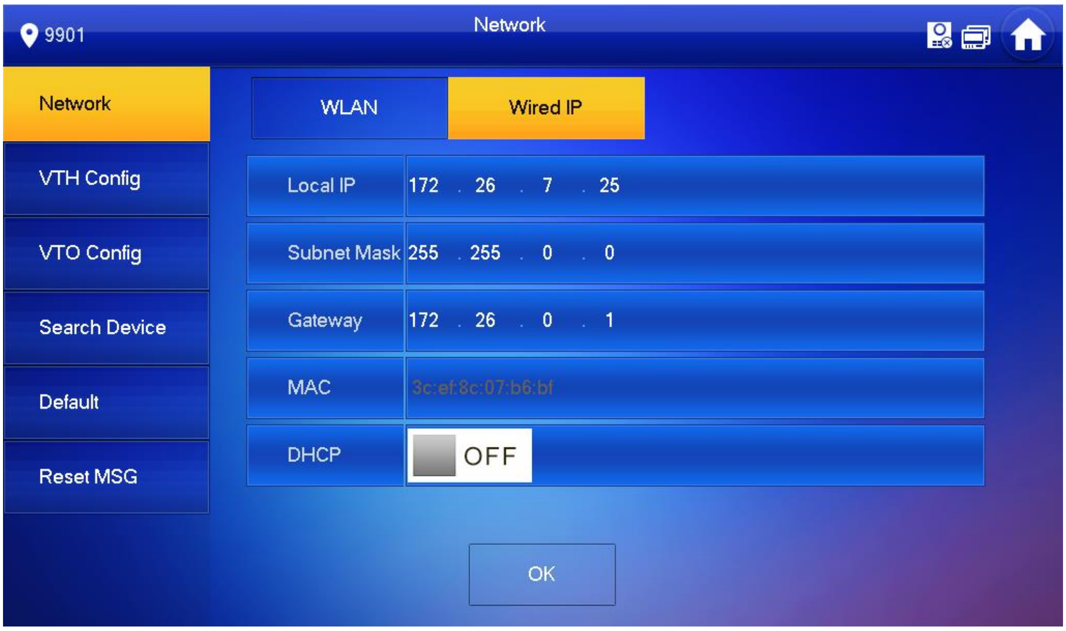
Note

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



Open WLAN to show usable net

Figure 2-14



Local IP 172 . 26 . 7 . 25

Subnet Mask 255 . 255 . 0 . 0

Gateway 172 . 26 . 0 . 1

MAC 3c:ef:8c:07:b6:bf

DHCP ■ OFF

Figure 2-15

- Wired IP

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

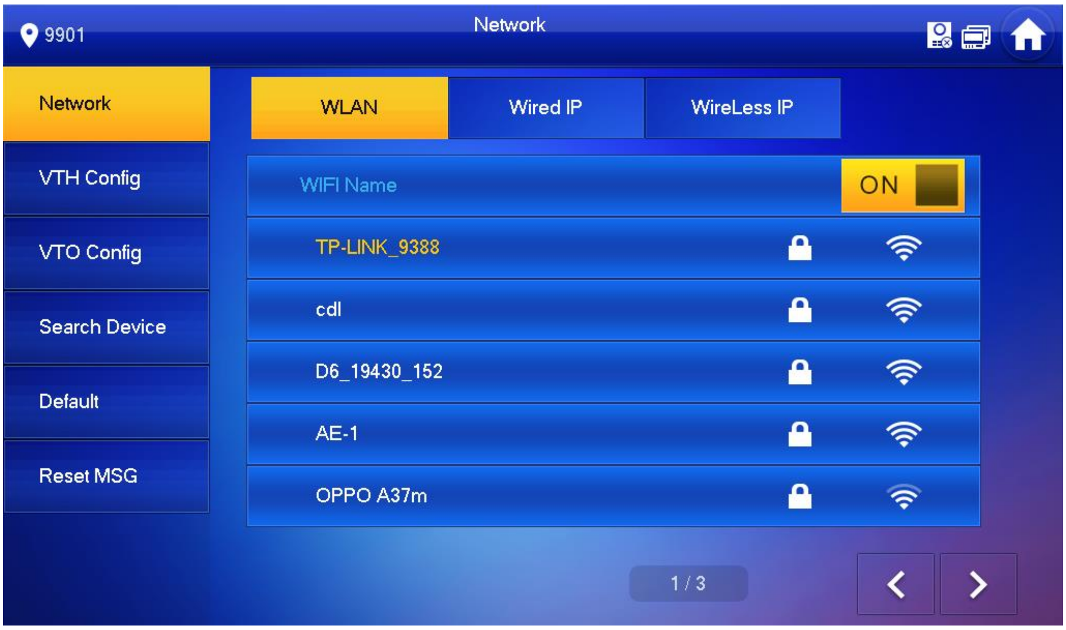
Note

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 2-16.



WIFI Name ON

TP-LINK_9388

cdl

D6_19430_152

AE-1

OPPO A37m

Figure 2-16

2. Connect WIFI.

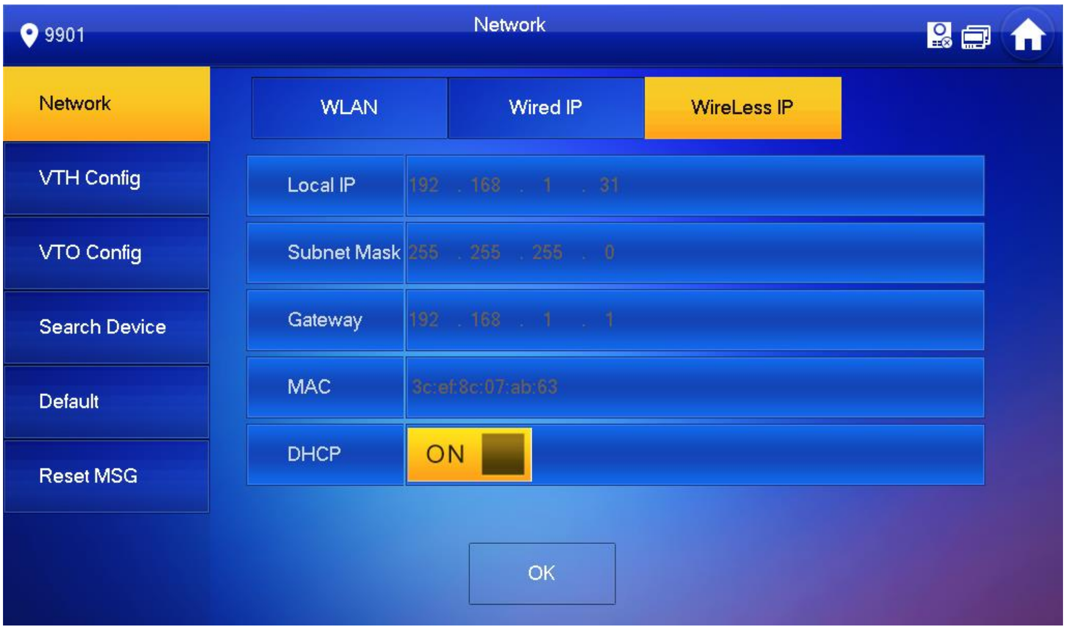
The system has 2 access ways as follows.

◇ 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 2-17.

Note

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



Local IP 192 . 168 . 1 . 31

Subnet Mask 255 . 255 . 255 . 0

Gateway 192 . 168 . 1 . 1

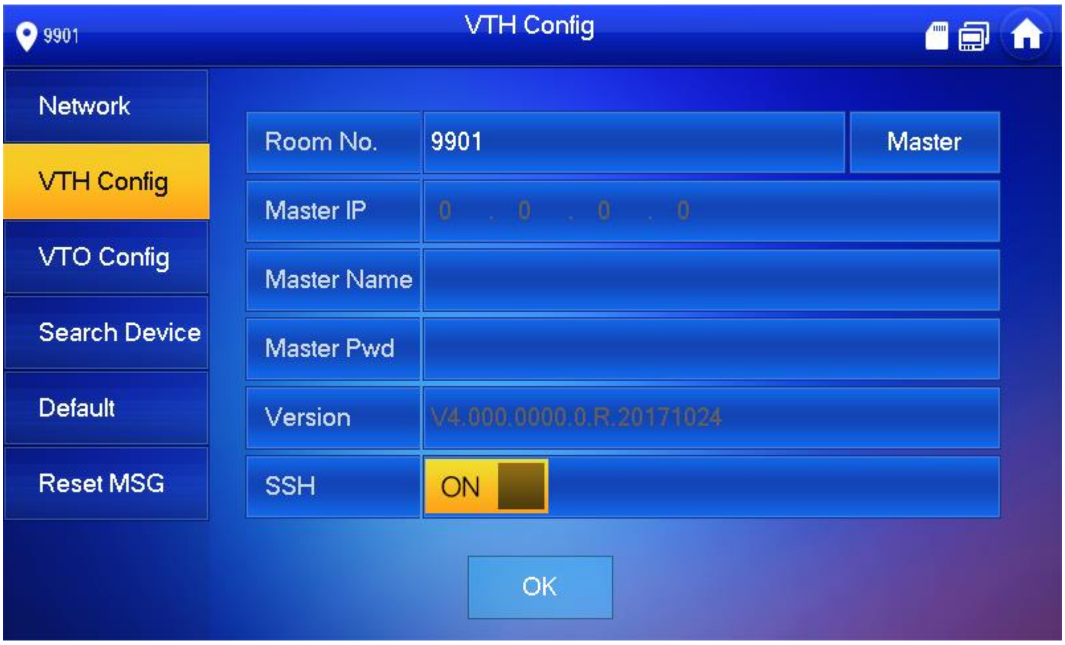
MAC 3c:ef:8c:07:ab:63

DHCP ON

Figure 2-17

Step 6 Click [VTH Config].

The system displays “VTH Config” interface, as shown in Figure 2-18.



Room No.: 9901

Master IP: 0 . 0 . 0 . 0

Master Name:

Master Pwd:

Version: V4.000.0000.0.R.20171024

SSH: ON

Figure 2-18

- Be used as a master VTH.
- Enter “Room No.” (such as 9901) and click “OK”.
- 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.

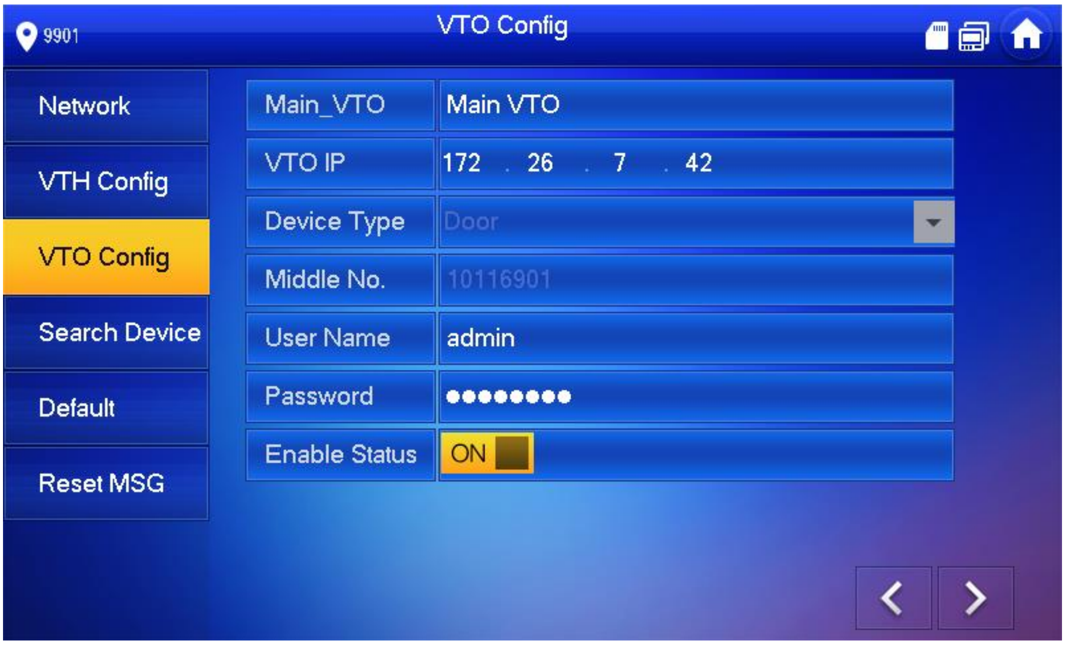
1. Press [Master] and switch to “Extension”.
2. Enter “Room No.” (such as 9901-1) and “Master IP” (IP address of master VTH).

   Note

   “Master Name” and “Master Pwd” are the user name and password of master VTH. Default user name is admin, and the password is the one set during device initialization.
3. Press [OK] to save settings.

Step 7 Click [VTO Config].

The system displays “VTO Config” interface, as shown in Figure 2-19.



Main_VTO	Main VTO
VTO IP	172 . 26 . 7 . 42
Device Type	Door
Middle No.	10116901
User Name	admin
Password	●●●●●●●●
Enable Status	ON

Figure 2-19

- Add main VTO

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

Note

- Default device type is “Door”. VTO middle no. will be obtained automatically. The format is “1+building no.+ unit no. + VTO no.”. Building no. has 2 digits, unit no. has 1 digit, and no. has 4 digits, so middle no. has 8 digits in total.
- “User Name” and “Password” shall be consistent with WEB login user name 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 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 ON.

- 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., “User Name” and “Password”.

Note

Fence station middle no. consists of “1+00+0+fence station no.”; building no. is 00, unit no. is 0 and VTO no. has 4 digits, so middle no. has 8 digits in total. For example, 10006901.

3. Switch the “Enable Status” to be ON.

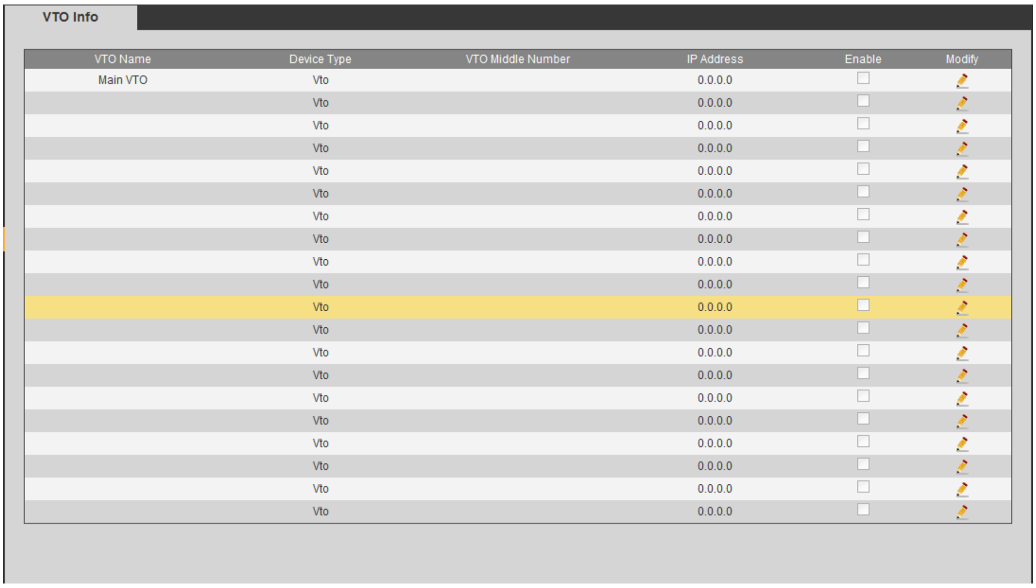
2.2.2 Batch Debugging

2.2.2.1 VTO Settings

Step 1 Refer to Step 1~ Step 7 in “2.2.1.1 VTO Settings”; configure some VTO parameters.

Step 2 Select “System Config >VTO Info”.

The system displays “VTO Info” interface, as shown in Figure 2-20.



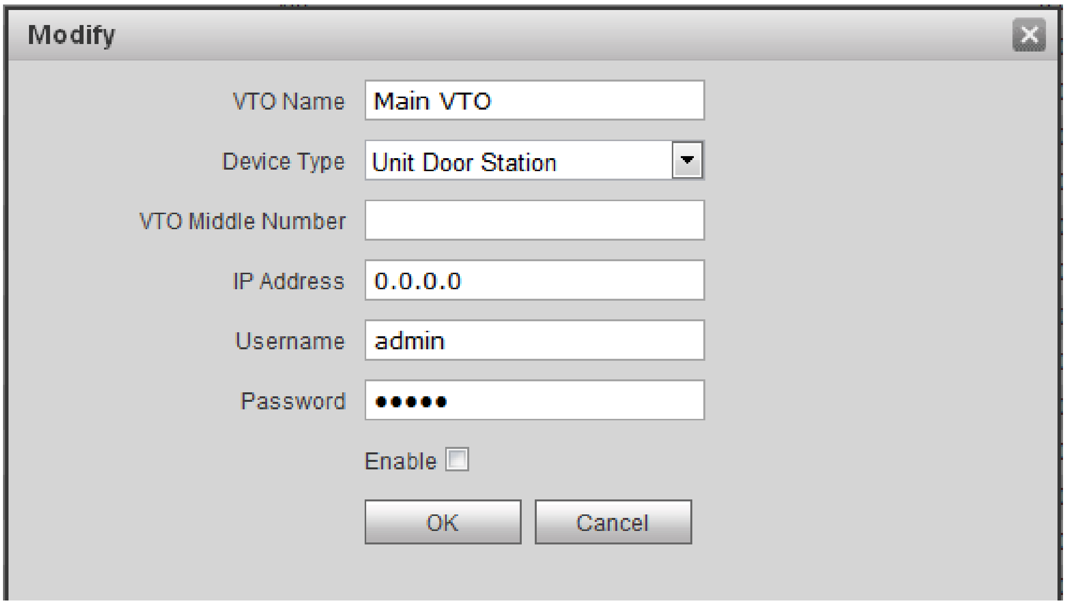
VTO Info

VTO Name	Device Type	VTO Middle Number	IP Address	Enable	Modify
Main VTO	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎
	Vto		0.0.0.0	☐	✎

Figure 2-20

1. Click ✎.

The system displays “Modify” interface, as shown in Figure 2-21.



Modify

VTO Name	Main VTO
Device Type	Unit Door Station
VTO Middle Number	
IP Address	0.0.0.0
Username	admin
Password	●●●●●

Enable ☐

Figure 2-21

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

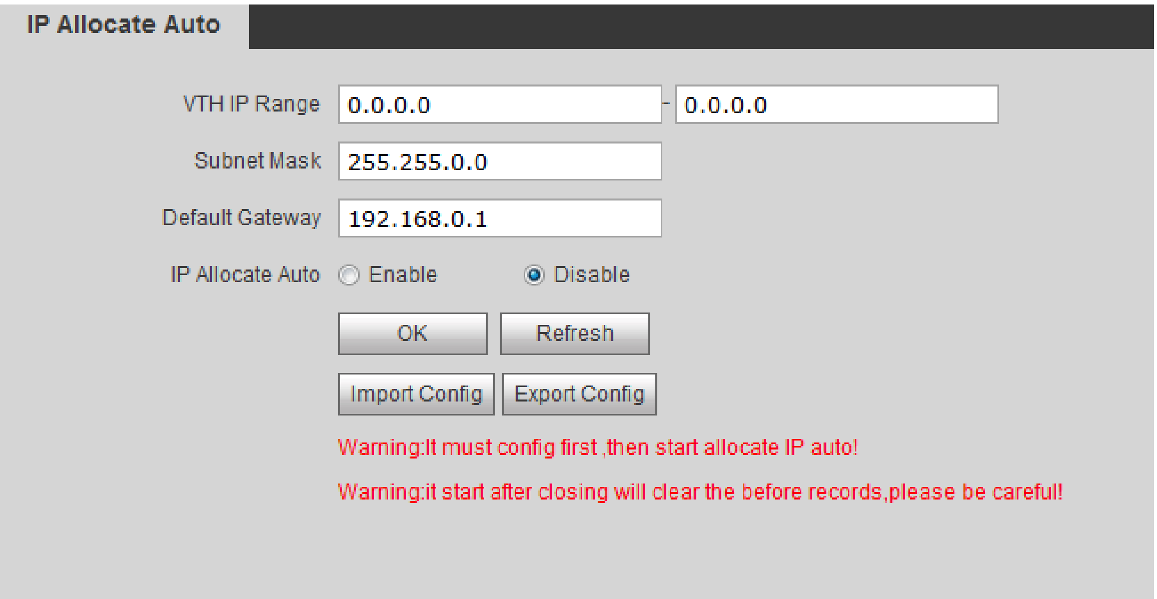
Note

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.

3. Select “Enable”.
4. Click “OK” to add VTO info.

Step 3 Select “System Config > IP Allocate Auto”.

The system displays “IP Allocate Auto” interface, as shown in Figure 2-22.



IP Allocate Auto

VTH IP Range 0.0.0.0 - 0.0.0.0

Subnet Mask 255.255.0.0

Default Gateway 192.168.0.1

IP Allocate Auto ○ Enable ● Disable

Warning:It must config first ,then start allocate IP auto!

Warning:it start after closing will clear the before records,please be careful!

Figure 2-22

1. Enter “VTH IP Range”, “Subnet Mask” and “Default Gateway”.
2. “IP Allocate Auto” selects “Enable”.
3. Click [OK] to save the settings.

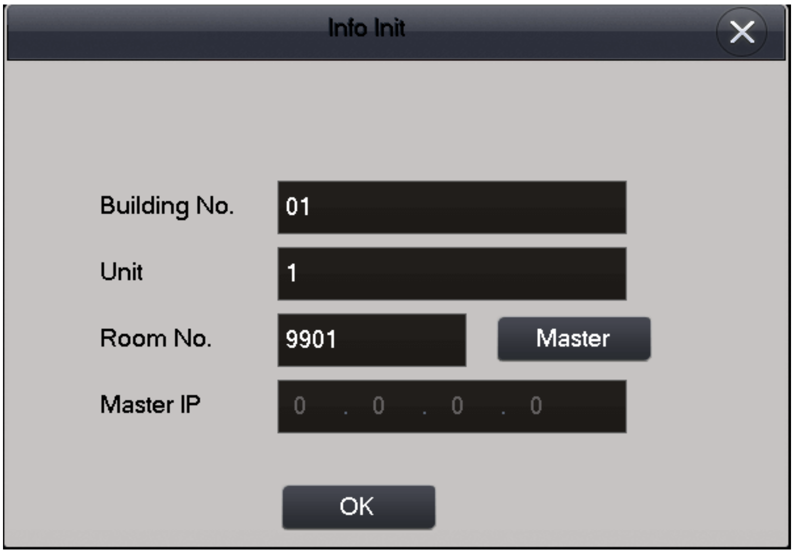
2.2.2.2 VTH Settings (Version 3.1)

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

Step 1 Power on the device, set the password and bind your Email, and then initialize the device.

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

The system displays “Info Init” interface, as shown in Figure 2-23.



Building No. 01

Unit 1

Room No. 9901

Master IP 0 . 0 . 0 . 0

Figure 2-23

Step 2 Initialize the VTH.

Note

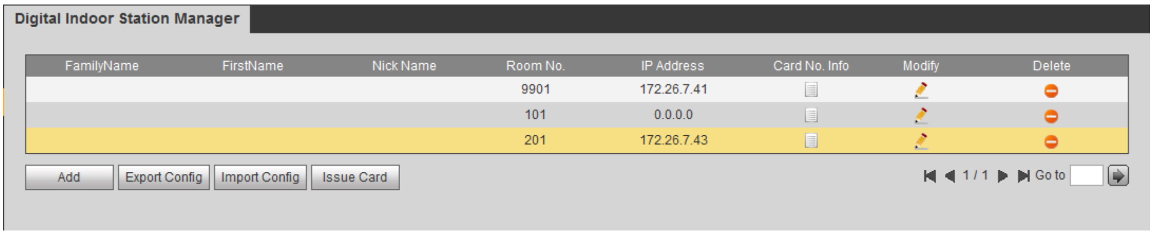
Please initialize the master VTH and then initialize extension VTH.

- 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 2-24.

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.



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	□	✎	⊖

Figure 2-24

- 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.

2.3 Debugging Verification

2.3.1 Verification with Version 3.1 VTH

2.3.1.1 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 2-25. It represents successful debugging.

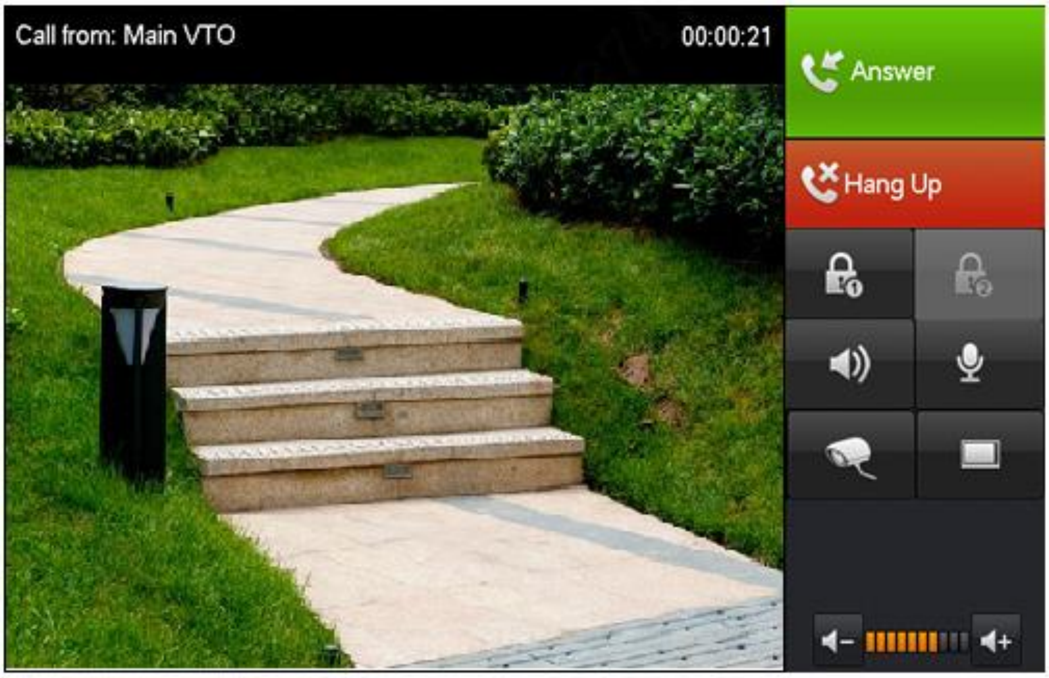


Figure 2-25

2.3.1.2 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 2-26. Select the VTO to enter monitoring image, as shown in Figure 2-27.

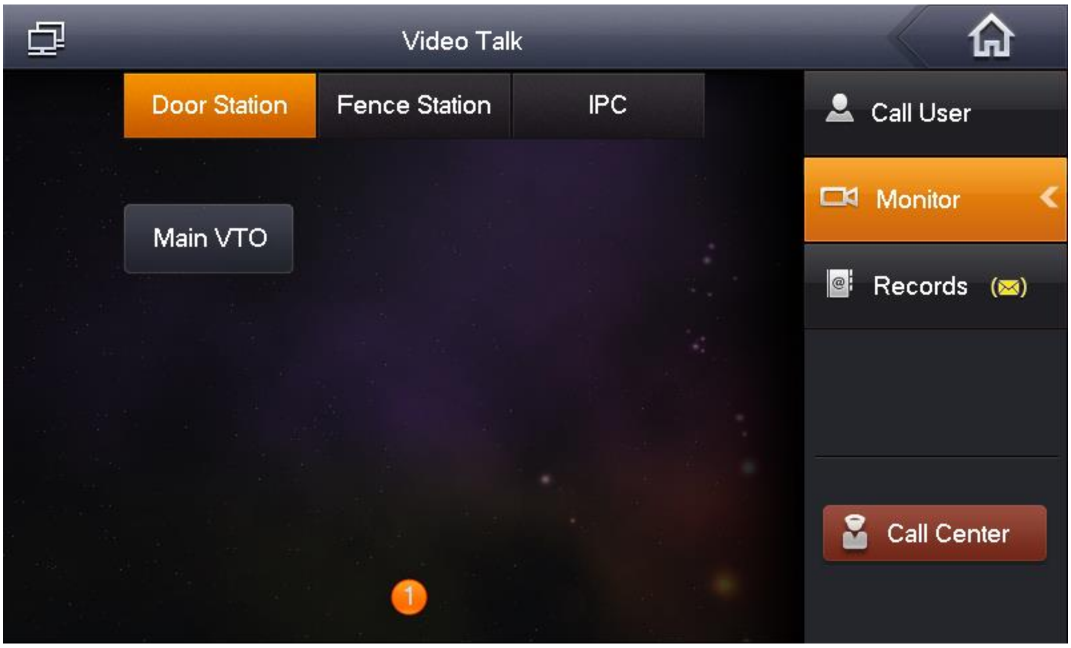


Figure 2-26

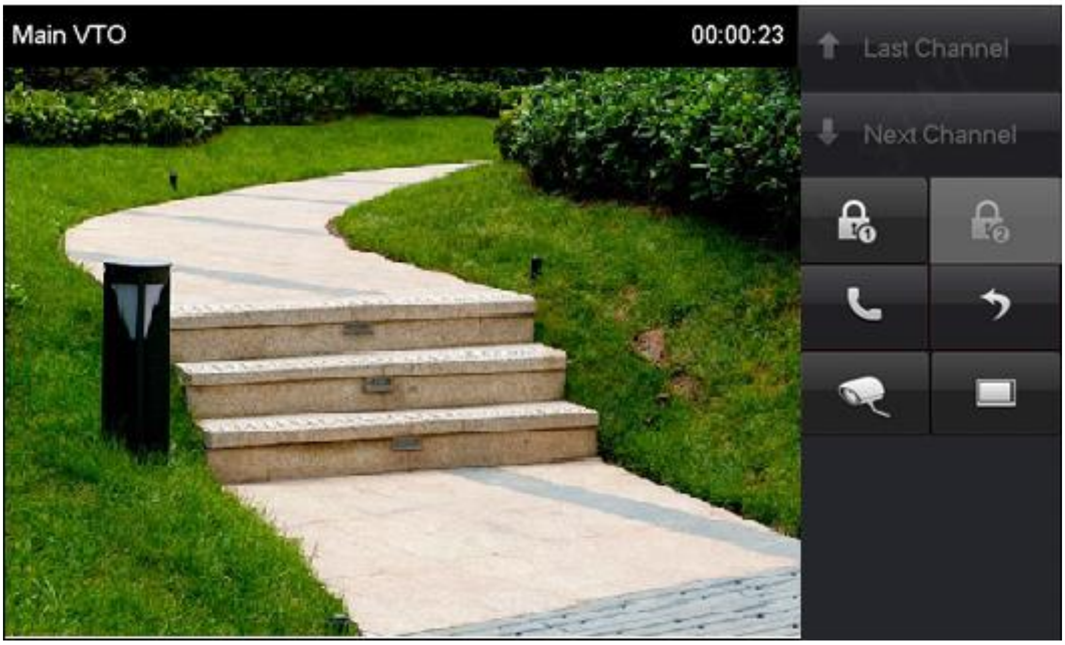


Figure 2-27

2.3.2 Verification with Version 4.0 VTH

2.3.2.1 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 2-28. 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.

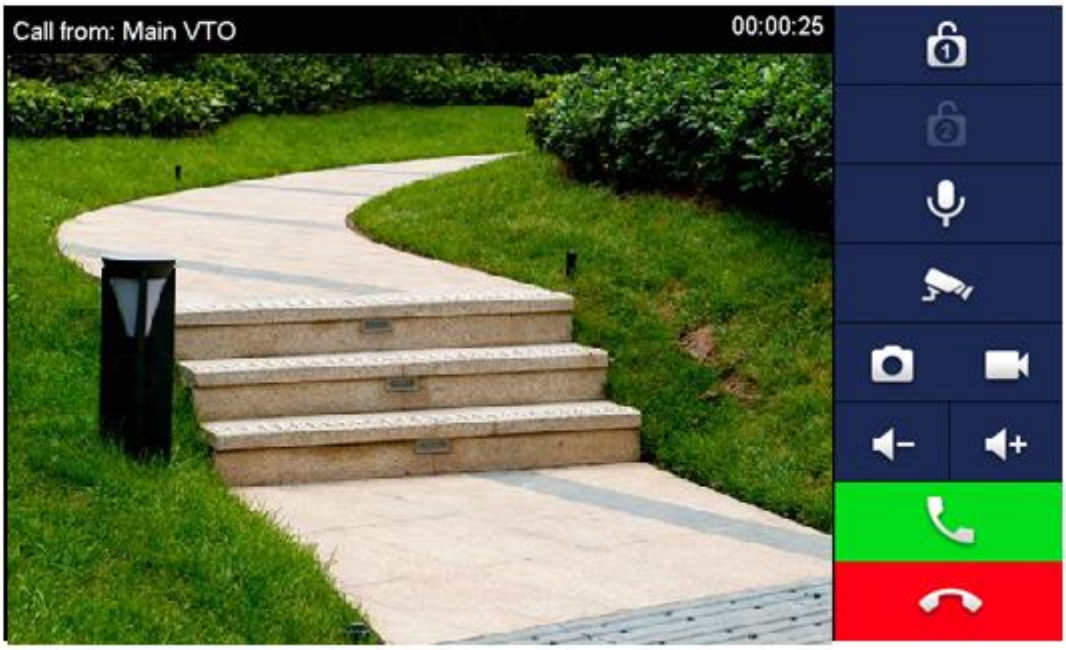


Figure 2-28

2.3.2.2 VTH Monitors VTO

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

Select “Monitor > Door”, as shown in Figure 2-29. Select the VTO to enter monitoring image, as shown in Figure 2-30.

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.

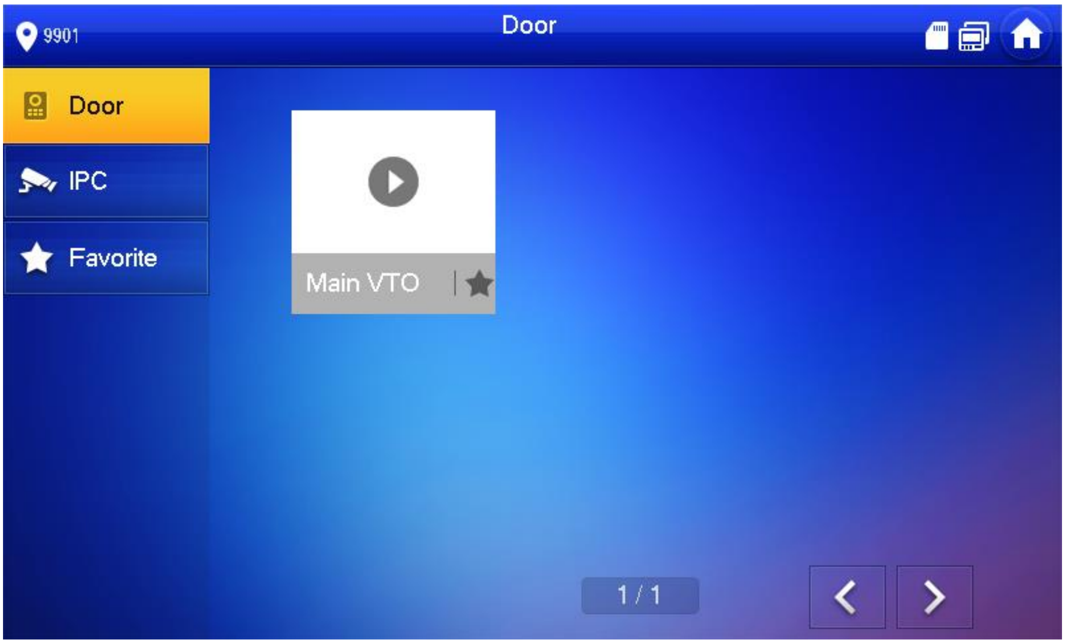


Figure 2-29

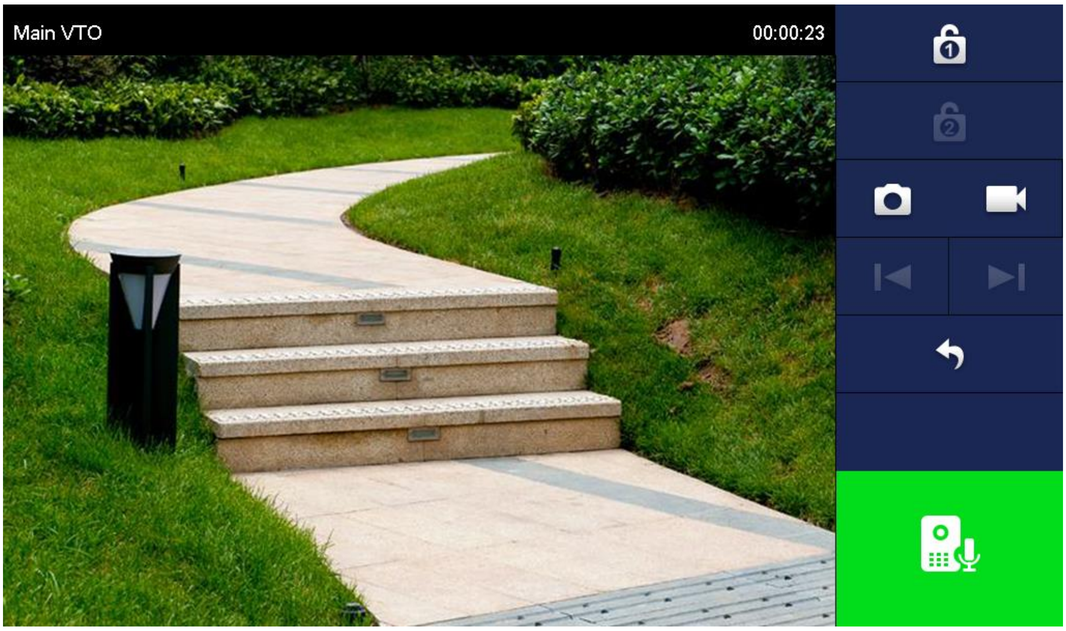


Figure 2-30