Modular VTO
(Version 3.1)

Quick Start Guide

V1.0.1

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

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

2. Update Firmware

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

"Nice to have" recommendations to improve your network security

1. Change Passwords Regularly

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

2. Change Default HTTP and TCP Ports:

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

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

3. Enable HTTPS/SSL:

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

4. Enable IP Filter:

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

5. Change ONVIF Password:

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

6. Forward Only Ports You Need:

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

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

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

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

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

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

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

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

14. Physically Lock Down the Device:

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

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

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

16. Isolate NVR and IP Camera Network

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

Foreword

General

This document mainly introduces product function, structure, networking, mounting process, debugging process, WEB operation and technical parameters of modular VTO, which is matched with Version 3.12 WEB interface.

Device Upgrade

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

General Description about Keys

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

Safety Instructions

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

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

Revision History

No.	Version No.	Revision Content	Release Date
1	V1.0.0	First release	2017.10.31
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 Camera Module

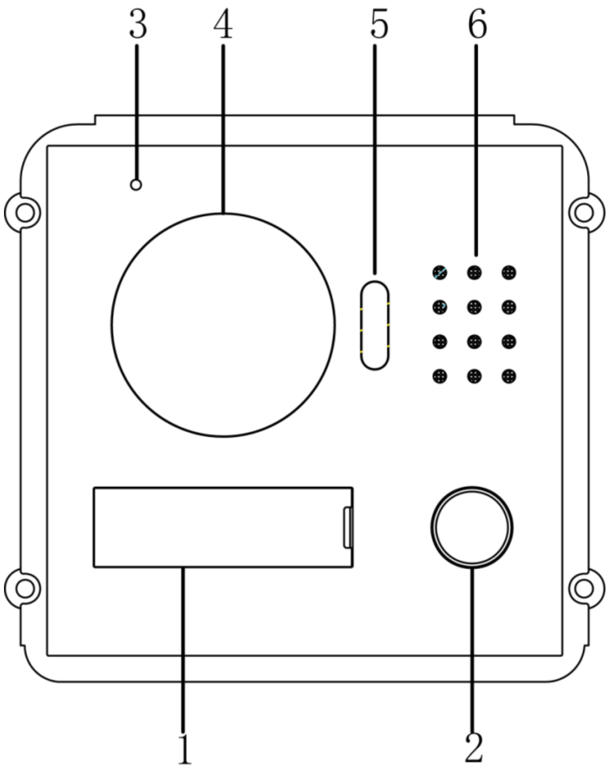


Figure 1-1

No.	Name	Description
1	User directory	Display user info.
2	Call key	Call the user or management centre.
3	Microphone	Audio input.
4	Camera	Monitor the door area, with adjustable angle.
5	Fill-in light	Provide fill-in light for camera in case of insufficient light.
6	Speaker	Audio output.

Table 1-1

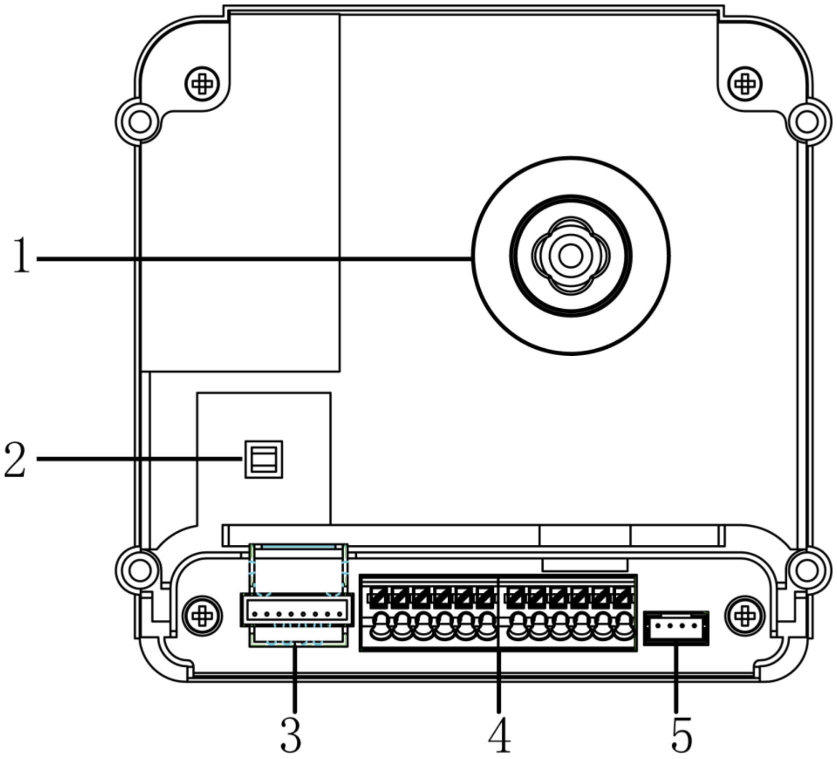


Figure 1-2

No.	Name	Description
1	Camera angle adjusting column	Adjust camera angle.
2	Tamper switch	When VTO is detached from the wall forcibly, give out alarm sound and report alarm info to management centre.
3	Network port	Connect network cable (RJ45 plug) through a connection line.
4	User port	Provide power port, lock port, door sensor feedback port and exit button port to connect power supply, electric control lock, solenoid lock and exit button. Wiring method is shown in Figure 1-3 and Figure 1-4.
5	Cascade connection port	Connect other modules. 📖 Note In case of cascade connection of multiple modules, modules shall adopt cascade connection between each other.

Table 1-2

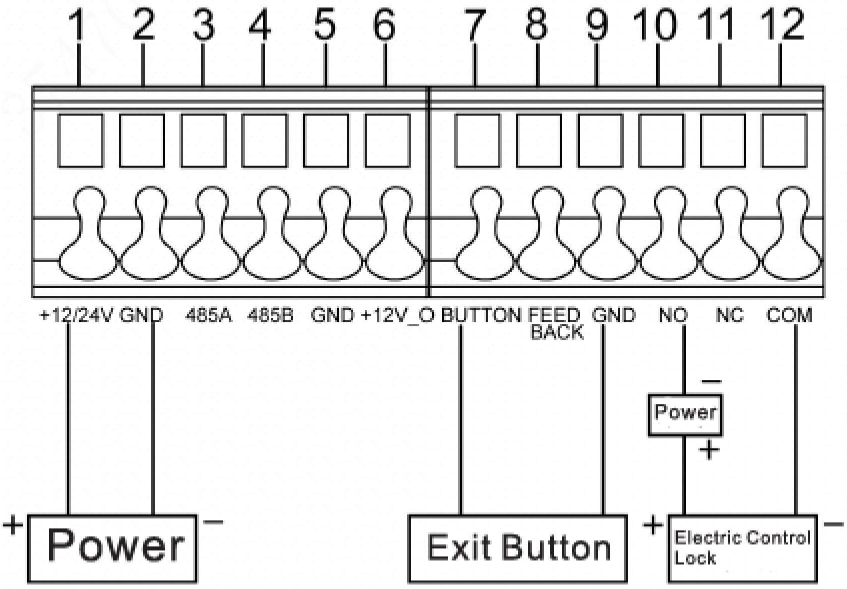


Figure 1-3

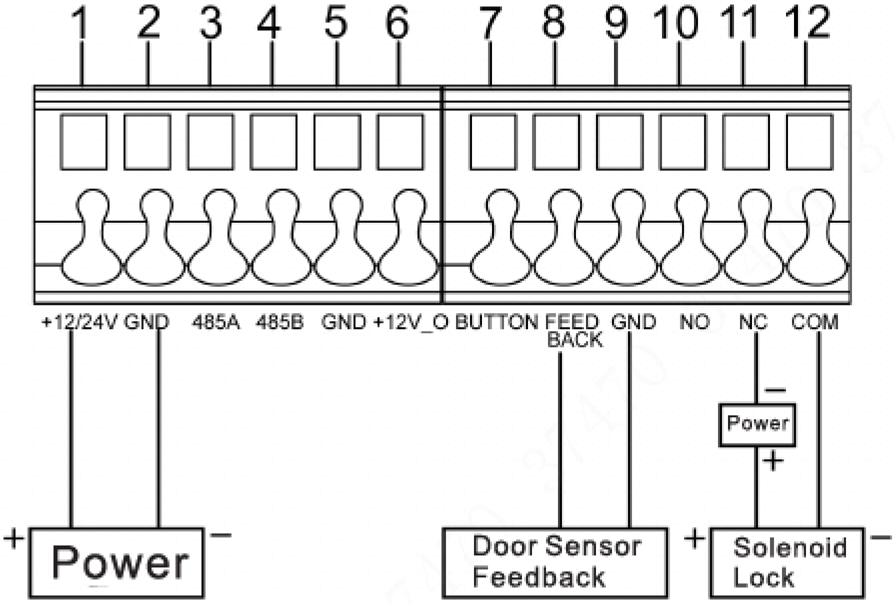


Figure 1-4

1.2 Button Module

Button module consists of one-button module, three-button module and five-button module; their functions are the same, although button quantity is different. Take “three-button module” for example.

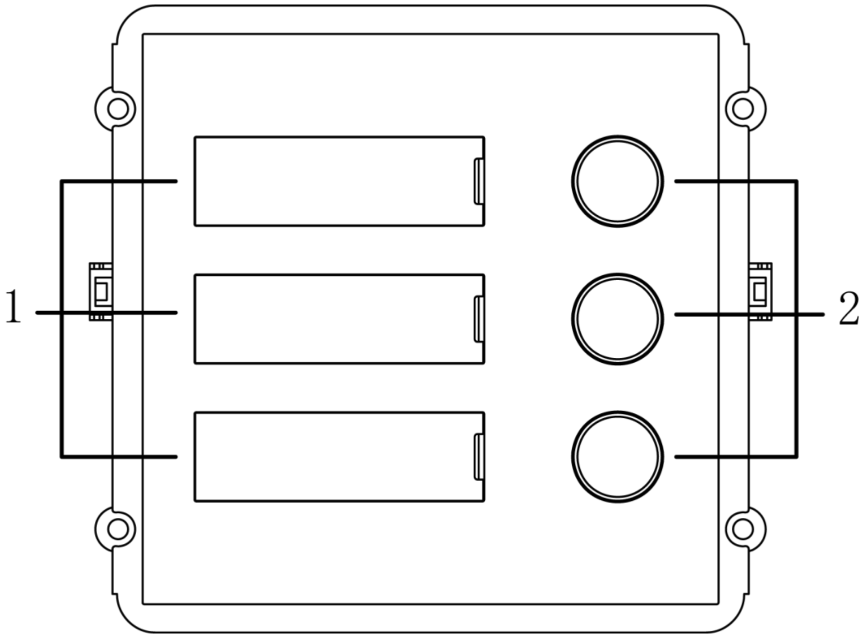


Figure 1-5

No.	Name	Description
1	User directory	Display user info according to buttons.
2	Call key	Call the VTH.

Table 1-3

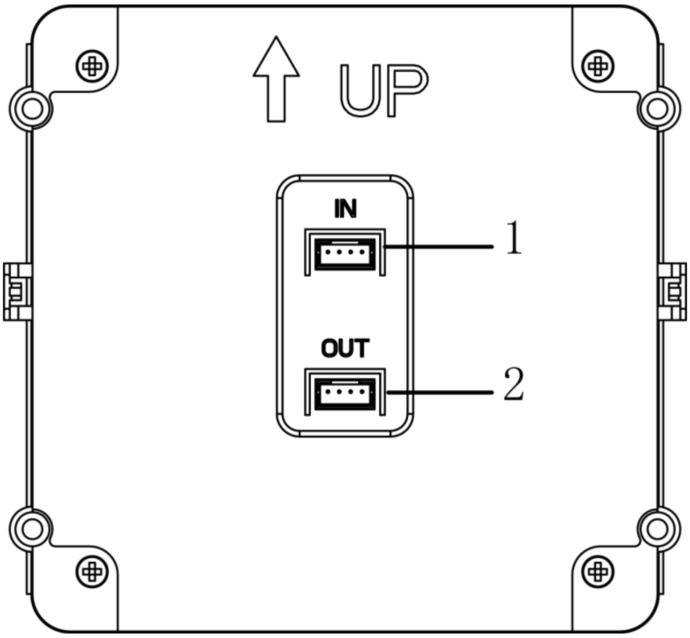


Figure 1-6

No.	Name	Description
1	Cascade input port	Connect other modules.
2	Cascade output port	

Table 1-4

1.3 Keyboard Module (with Braille)

Note

Rear panel of keyboard module is the same as rear panel of button module.

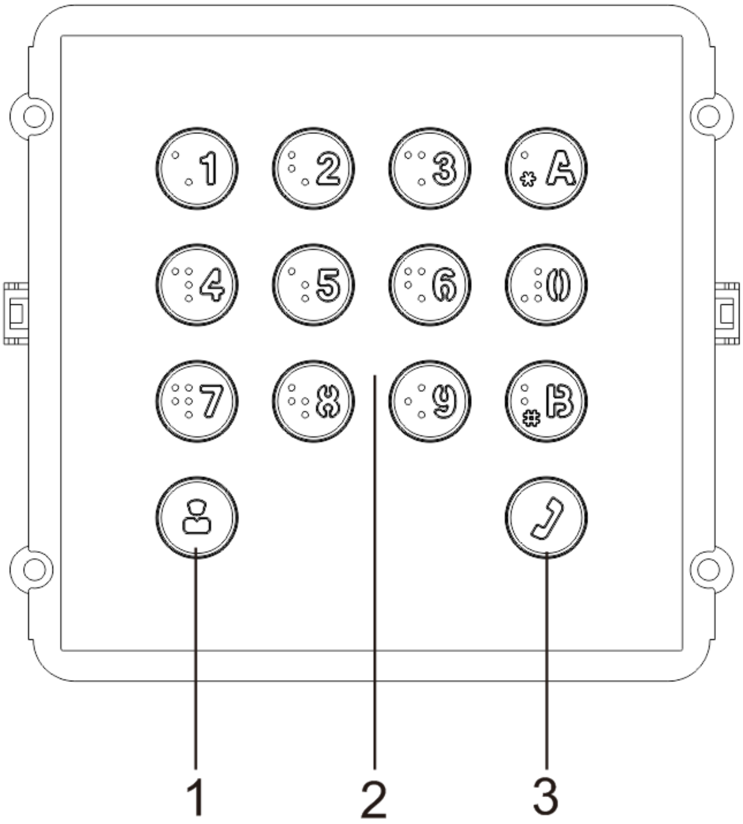


Figure 1-7

No.	Name	Description
1	Call management centre	Call management centre.
2	Numeric key	Input the password. For example, unlock password is 123456. Please input “#+ unlock password +#”.
3	Call key	Call the VTH.

Table 1-5

1.4 Card Swiping Module

Note

Rear panel of card swiping module is the same as rear panel of button module.

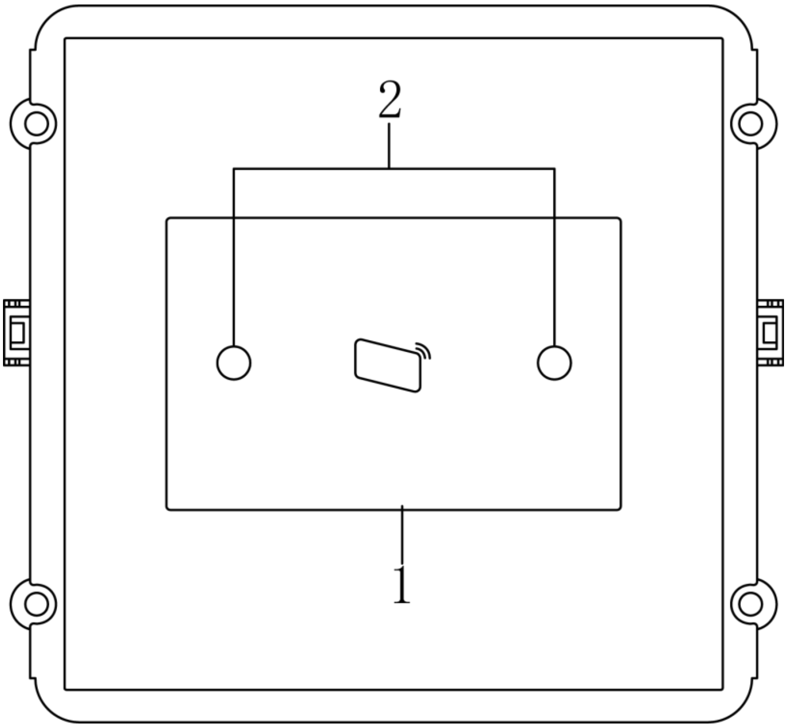


Figure 1-8

No.	Name	Description
1	Card swiping area	It is valid to swipe the card here.
2	Proximity sensor	When a person is about 1m away from the device, the device will sense the person’s approaching. Backlights of display screens of all modules and the keyboard will be turned on automatically. And they will turn off automatically after the person leaves.

Table 1-6

1.5 Fingerprint Module

Note

Rear panels of fingerprint module and button module have different port positions, but port functions are the same.

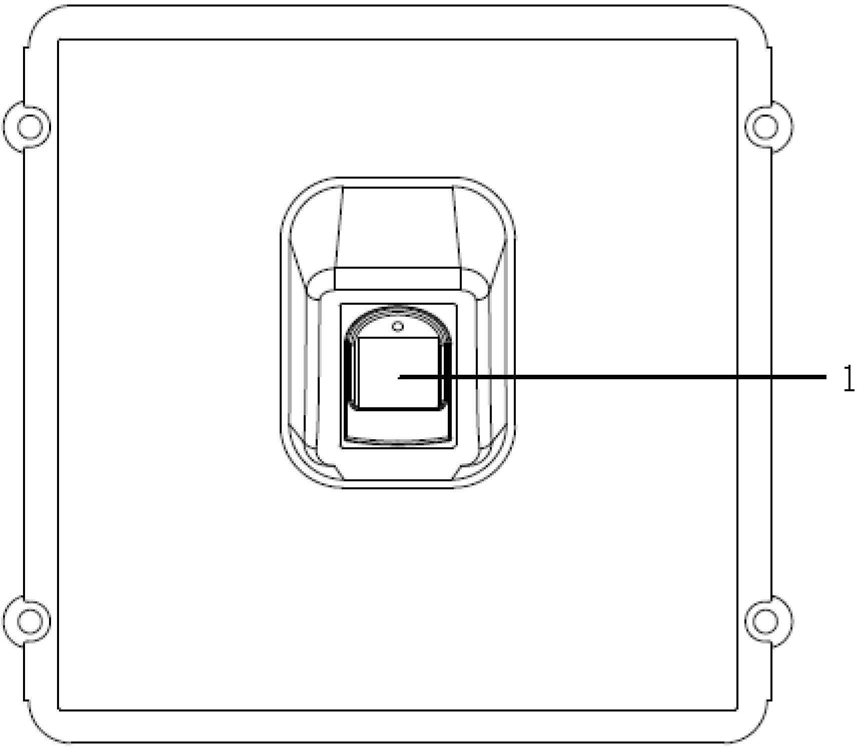


Figure 1-9

No.	Name	Description
1	Fingerprint module	The user inputs a fingerprint or unlocks with a fingerprint.

Table 1-7

1.6 Blank Module

Note

Rear panels of blank module and button module have different port positions, but port functions are the same.

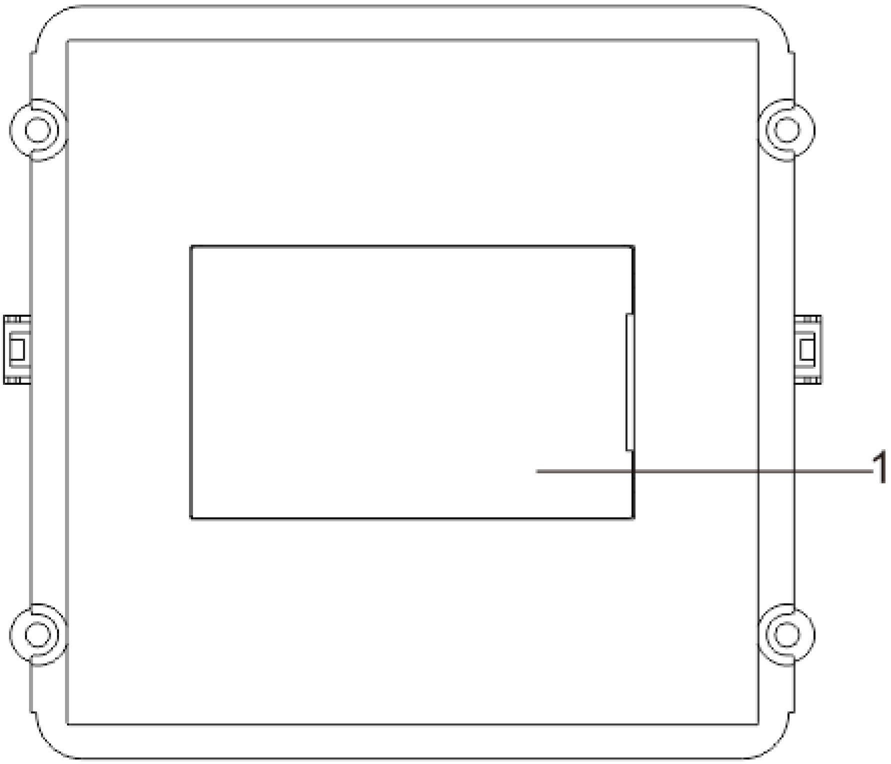


Figure 1-10

No.	Name	Description
1	User directory	Display user info according to buttons.

Table 1-8

2 Device Mounting

Modular VTO consists of single module mounting, double module mounting and 3-module mounting. Take 3-module mounting for example.

⚠ Caution

- When leaving factory by default, visiting cards and card cover have been included in the attachment.
- When power-on after mounting, please ensure that all modules have been connected; otherwise, they fail to work normally.
- Before installation of surface mounting box and flush mounting box, cables in the wall shall go through the bracket or flush mounting box.

2.1 Surface Mounting

Step 1 Drill holes according to hole positions of surface mounting box, and put expansion pipe in place.

Step 2 Fix surface mounting box onto the wall with ST3×18 screws.

Step 3 Fix every module onto front panel with M3×6 screws.

Step 4 Connect cables. Please refer to “1 Product Structure” for details.

Step 5 Fix the front panel onto surface mounting box with M4×40 screws.

Step 6 Apply glue between surface mounting box and the wall.

Step 7 Write room number or the user’s name on the visiting card, and insert it into user directory.

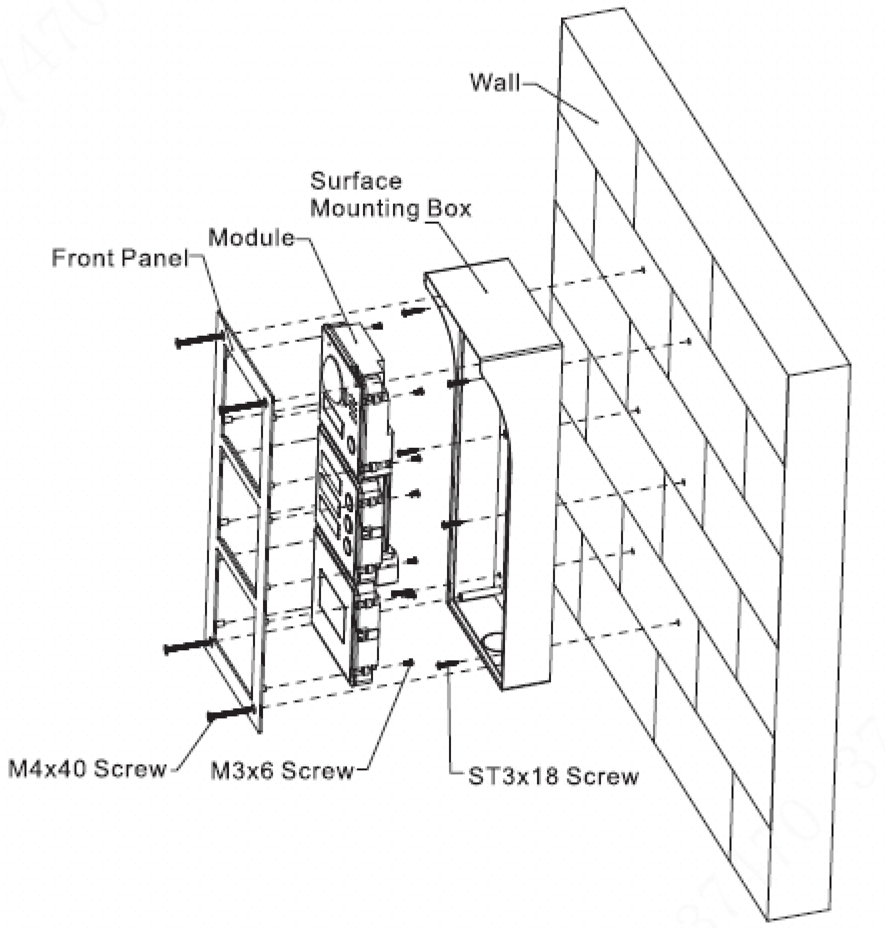


Figure 2-1

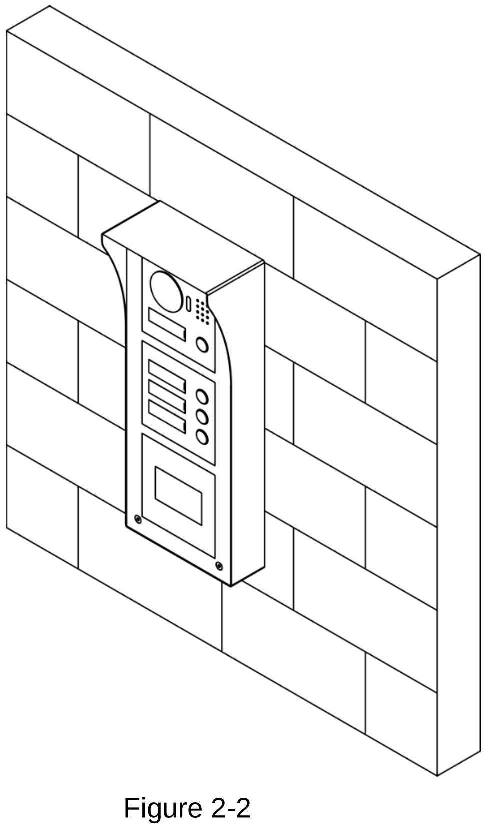


Figure 2-2

2.2 Flush Mounting

Step 1 Dig a hole in the wall.

Note

- Regarding single module mounting, hole dimension is 115mm×115mm×57mm.
- Regarding double module mounting, hole dimension is 237mm×125mm×50mm.
- Regarding 3-module mounting, hole dimension is 349mm×125mm×50mm.

Step 2 Embed flush mounting box into the wall; ensure that box edge clings to the wall.

Step 3 Fix every module onto front panel with M3×6 screws.

Step 4 Connect cables. Please refer to “1 Product Structure” for details.

Step 5 Fix the front panel onto flush mounting box with M4×40 screws.

Step 6 Apply glue among front panel, flush mounting box and the wall.

Step 7 Write room number or the user’s name on the visiting card, and insert it into user directory.

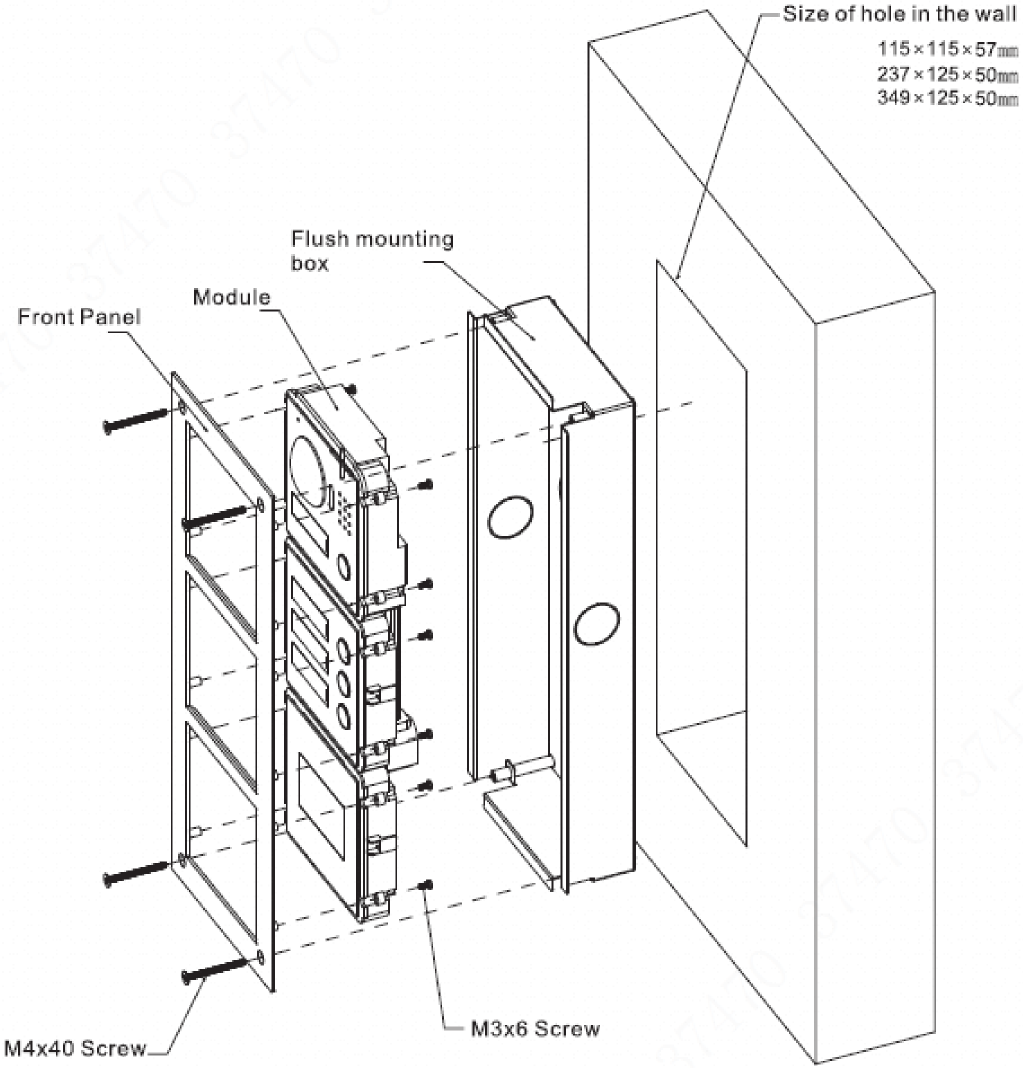


Figure 2-3

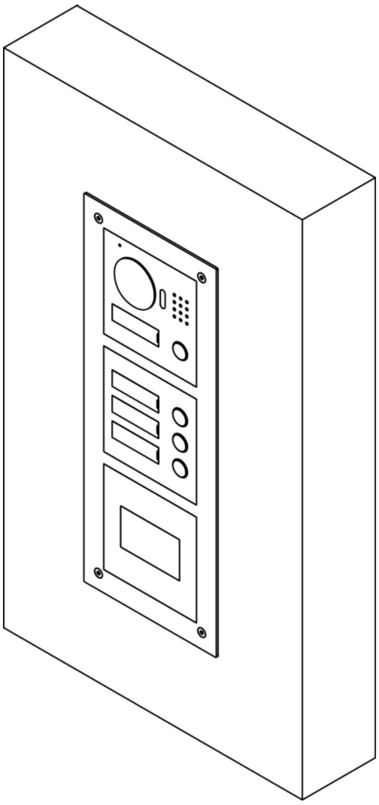


Figure 2-4

3 Device Debugging

3.1 Debugging Settings

3.1.1 VTO Settings

3.1.1.1 Initialization

For the first time, please initialize login password.

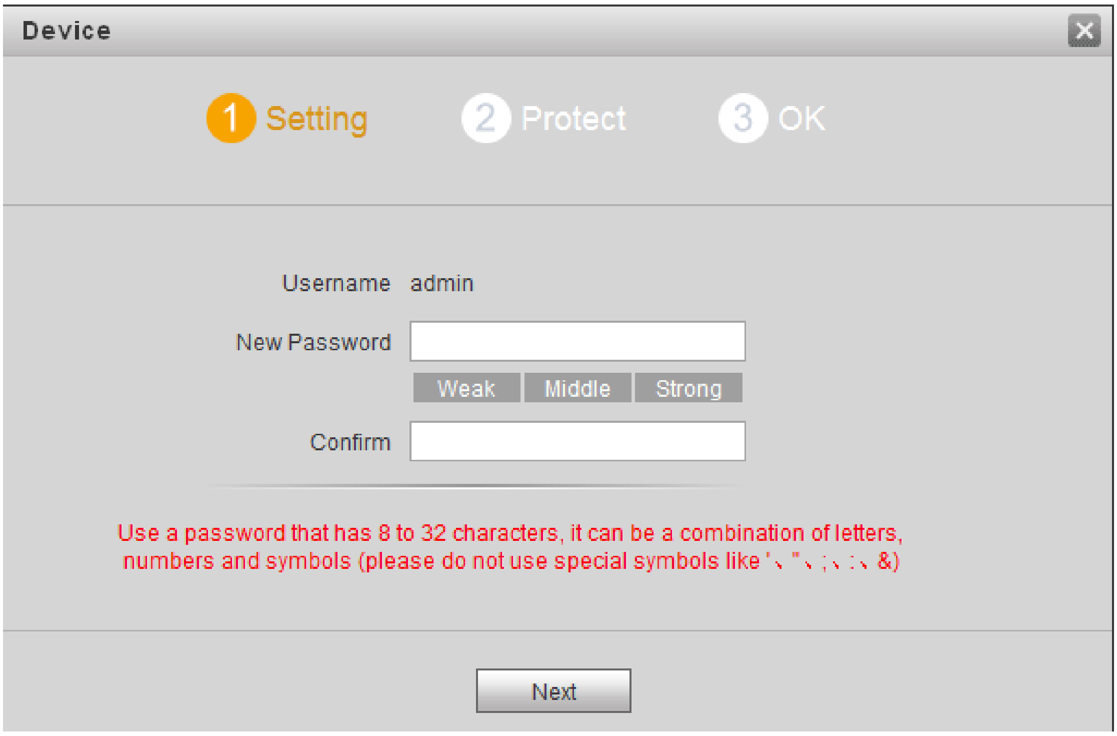
Note

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

Step 1 Connect power supply of VTO, 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 3-1.



Username admin

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 '、"、;、:、&)

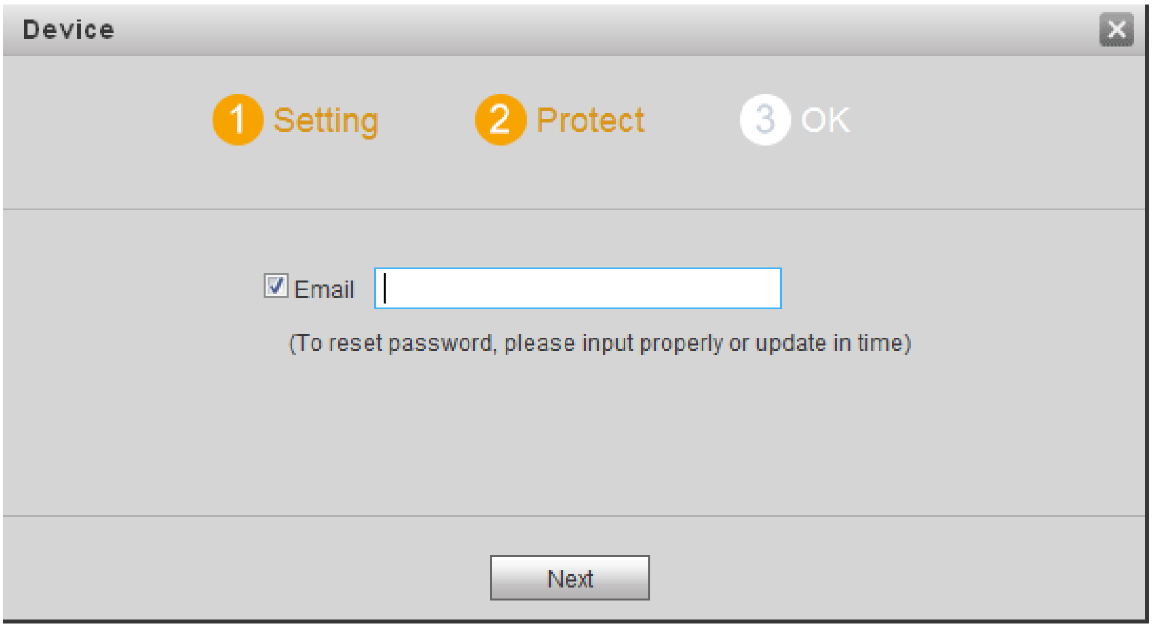
Figure 3-1

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

The system displays “Protect” interface, as shown in Figure 3-2.

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.



☑ Email

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

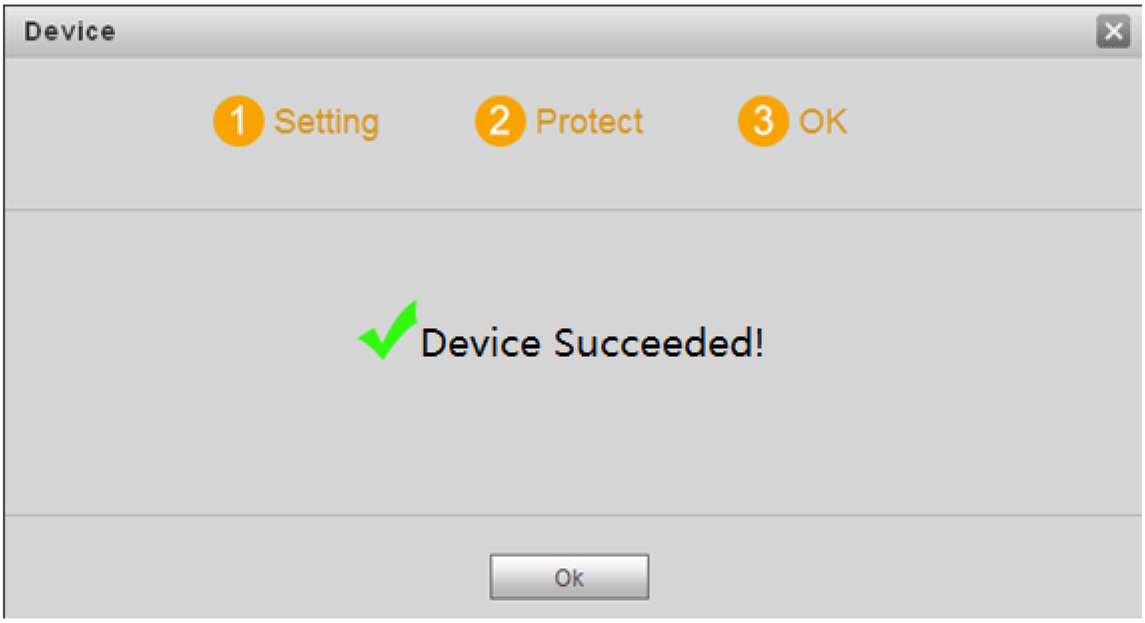
Figure 3-2

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 3-3 错误!未找到引用源。, and shows “Device succeeded!”



Device Succeeded!

Figure 3-3

Step 6 Click “OK”.

The system displays WEB login interface, as shown in Figure 3-4.

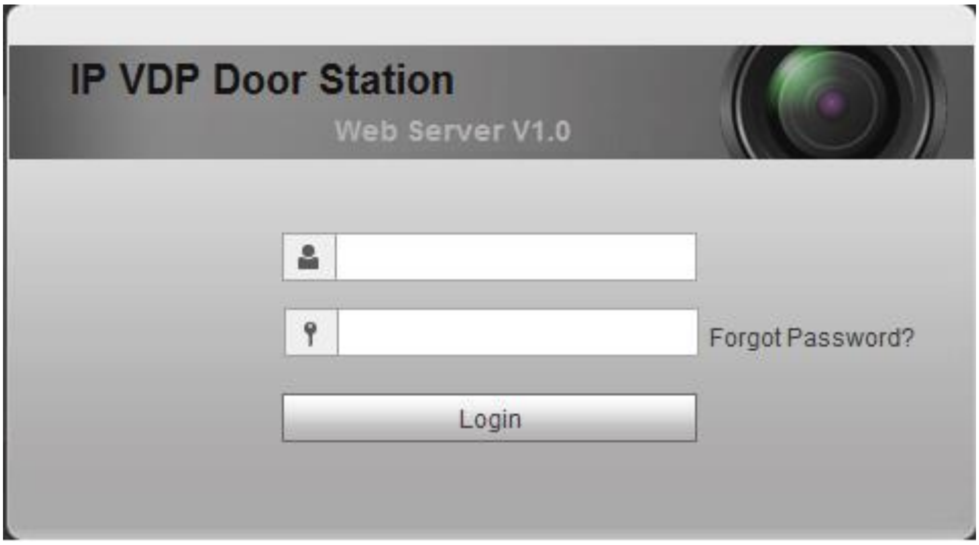


Figure 3-4

Step 7 Enter user name and password, and click “Login”.

Log in the WEB interface of the device.

Note

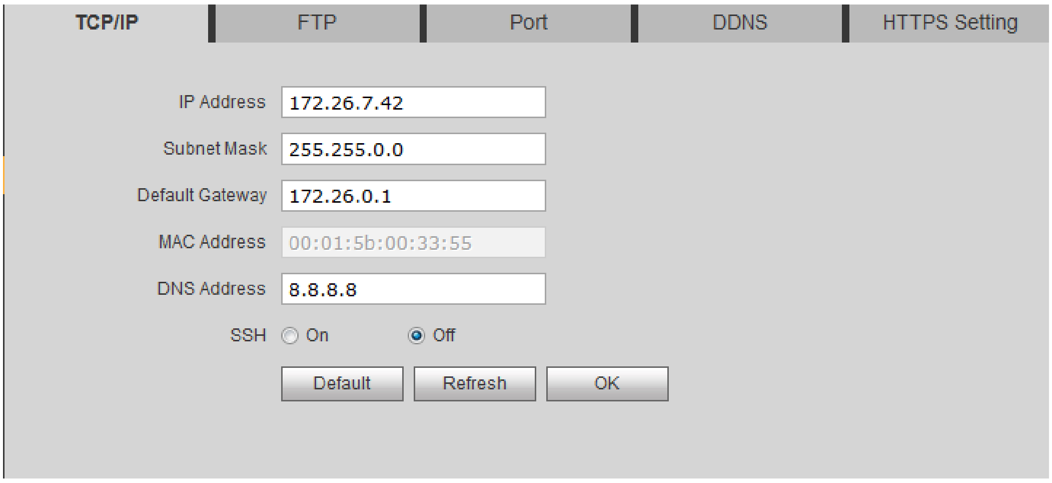
- Default user name is admin.
- Password is the one set during initialization.

3.1.1.2 Modify Device Network

Modify IP address of VTO to the planned IP address.

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

The system displays “TCP/IP” interface, as shown in Figure 3-5.



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 3-5

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.

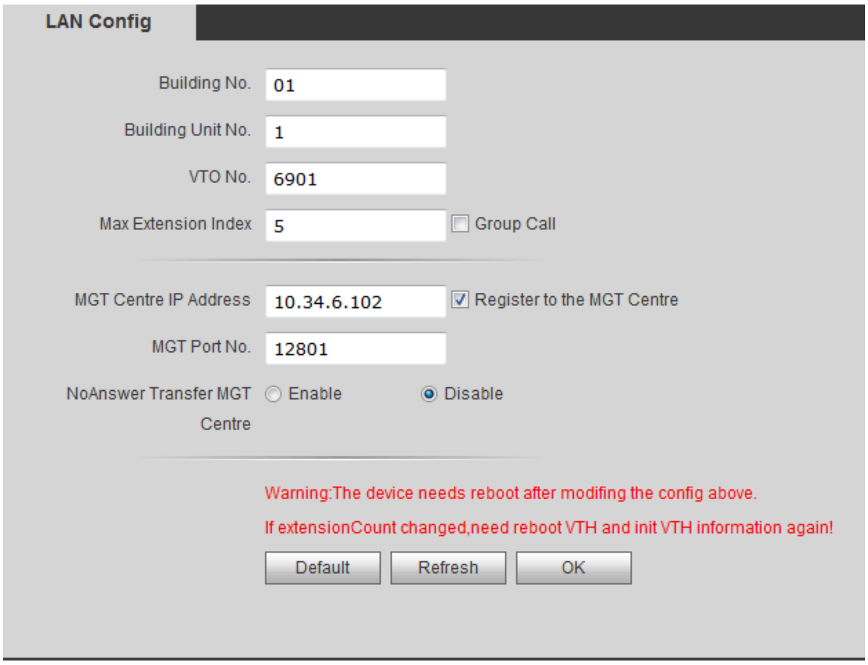
- If PC is in the planned network segment, WEB interface jumps to new IP login interface automatically.
- If PC is not in the planned network segment, login will be failed. Please add PC to the planned network segment and login WEB interface again.

3.1.1.3 LAN Config

Configure VTO building no., unit no. and VTO no. info.

Step 1 Select “System Config> LAN Config”.

The system displays “LAN Config” interface, as shown in Figure 3-6.



LAN Config

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 3-6

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

Note

- To call the management centre, please tick “Register to the MGT Centre”, and set “MGT Centre IP Address” and “MGT Port No.”. Enable or disable “No Answer Transfer MGT Centre”.
- To provide group call function, please tick “Group Call” and set “Max Extension Index”, which is 5 at most.

Step 3 Click “OK”.

3.1.1.4 Add VTH

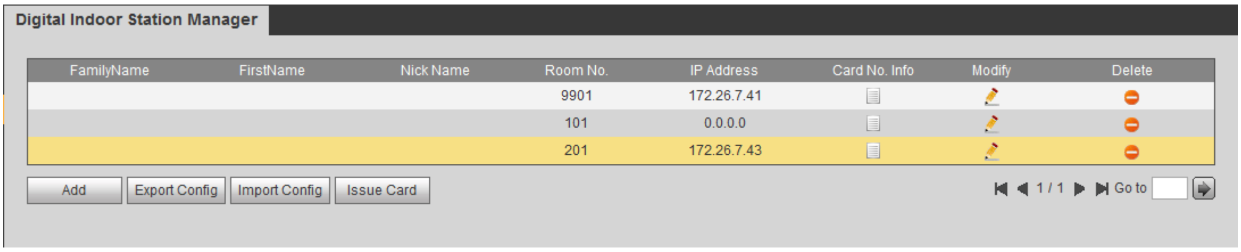
Add VTH info. After VTH and VTO have completed debugging, VTH will be registered on VTO automatically and realize bonding.

Note

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

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

The system displays “Digital Indoor Station Manager” interface, as shown in Figure 3-7.



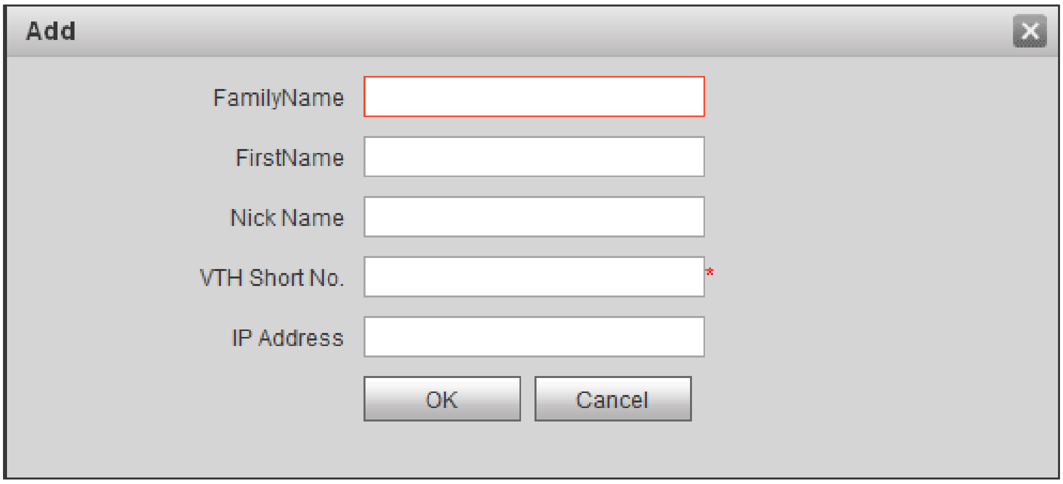
Digital Indoor Station Manager

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 3-7

Step 2 Click “Add”.

The system displays “Add” interface, as shown in Figure 3-8.



Add

FamilyName

FirstName

Nick Name

VTH Short No. *

IP Address

Figure 3-8

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”.

3.1.1.5 Set Modules

Camera module exists by default; all other modules shall be added in facade layout before use.

Caution

- At most 9 modules can be added.
- Regarding fingerprint module, card swiping module and keyboard module, only one module of each type can be added respectively. Other modules can be matched freely.

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

The system displays “Façade Layout” interface, as shown in Figure 3-9.

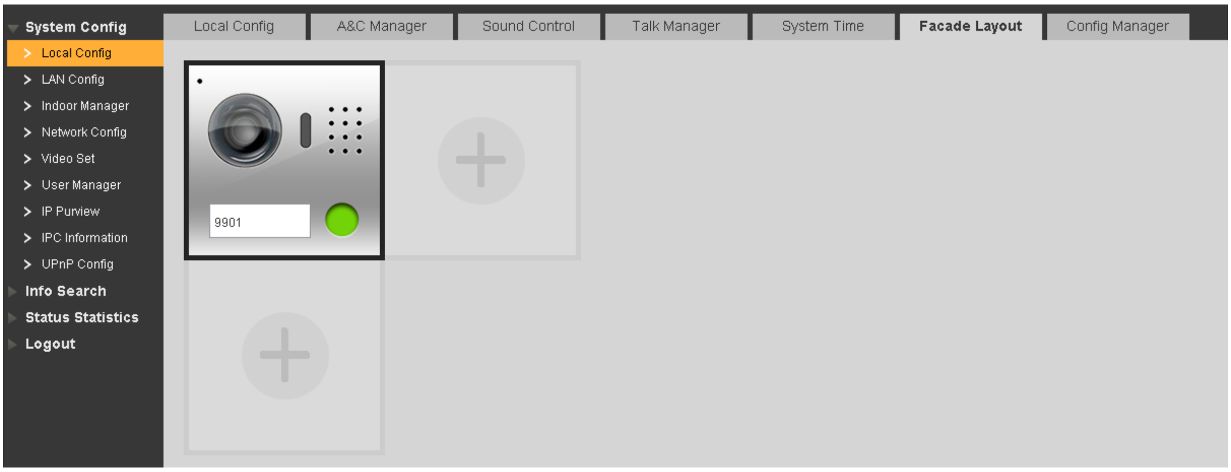


Figure 3-9

Step 2 Click +.

The system displays available modules, as shown in Figure 3-10.

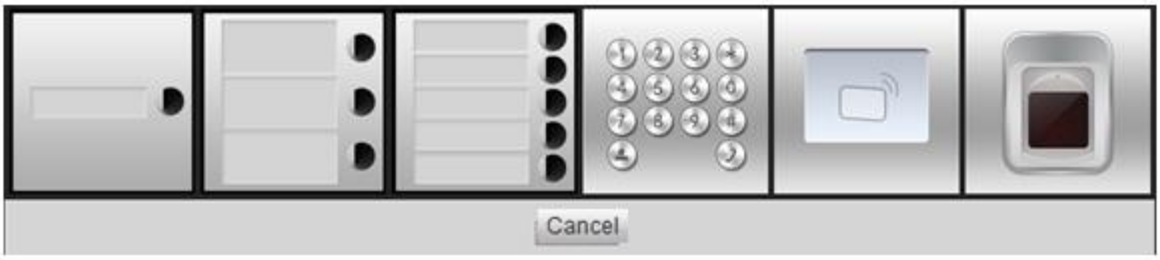


Figure 3-10

Note

If keyboard module, card swiping module and fingerprint module have been added already, they are not displayed here.

Step 3 Select modules according to actual layout of VTO.

Note

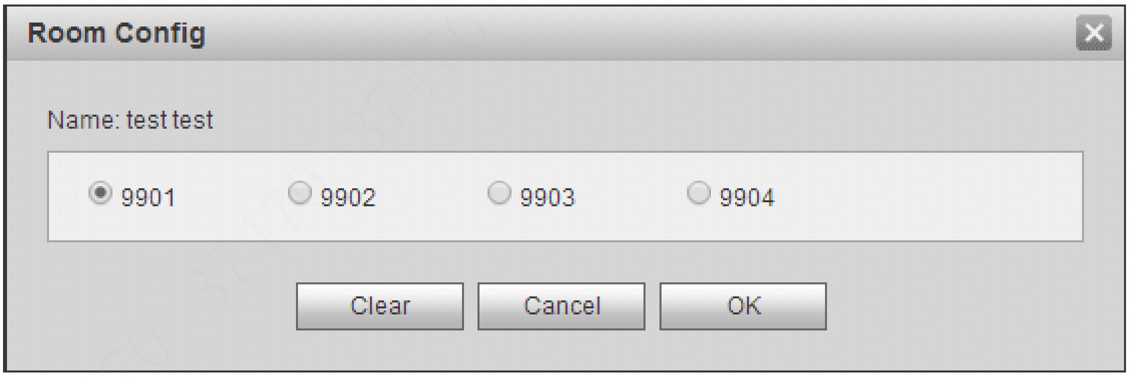
- Support continuous adding.
- Button module and camera module shall set corresponding relation of call key. For specific bonding operations, please refer to “Step 4~ Step 5”. Other modules need not to set. Click “OK” to save.

Step 4 Click Input NO. or 9901.

The system displays “Room Config”, as shown in Figure 3-11.

Note

- The displayed room no. is the added VTH.
- Click to modify the bonded buttons when necessary.



Room Config

Name: test test

● 9901 ○ 9902 ○ 9903 ○ 9904

Figure 3-11

Step 5 Select room no. and click “OK”.

The interface displays room no. info and corresponding button turns green, as shown in Figure 3-12.

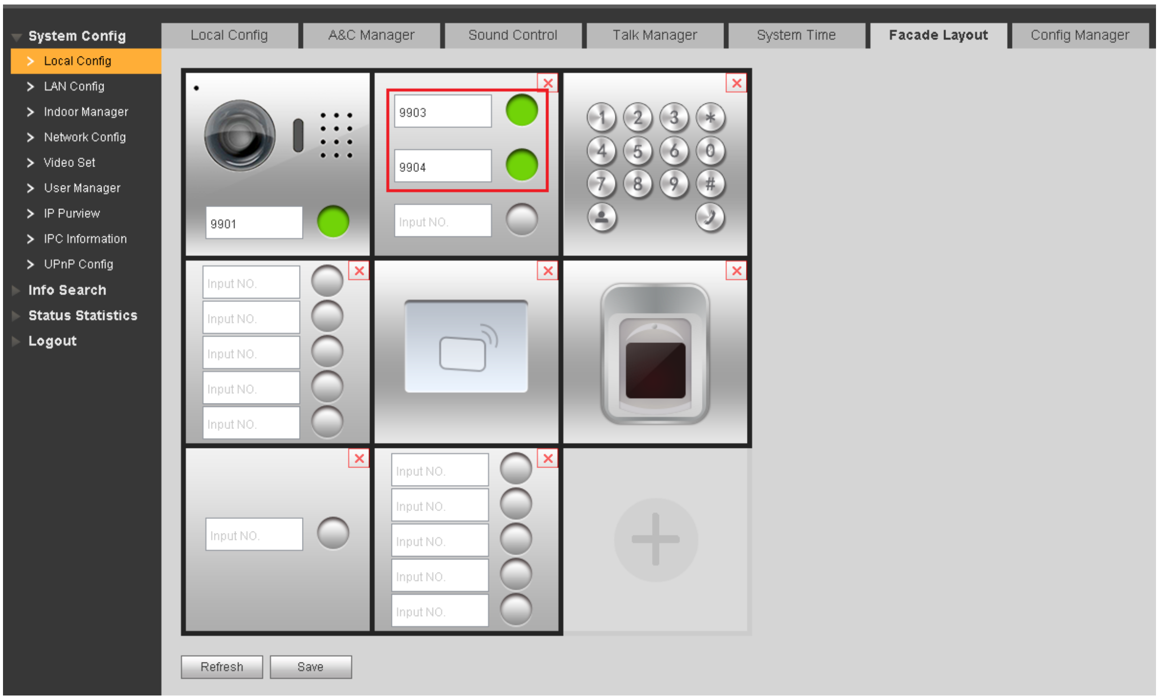


Figure 3-12

Step 6 Click “Save” to save the settings.

After saving, reboot the device to take effect.

3.1.2 VTH Settings (Version 3.1)

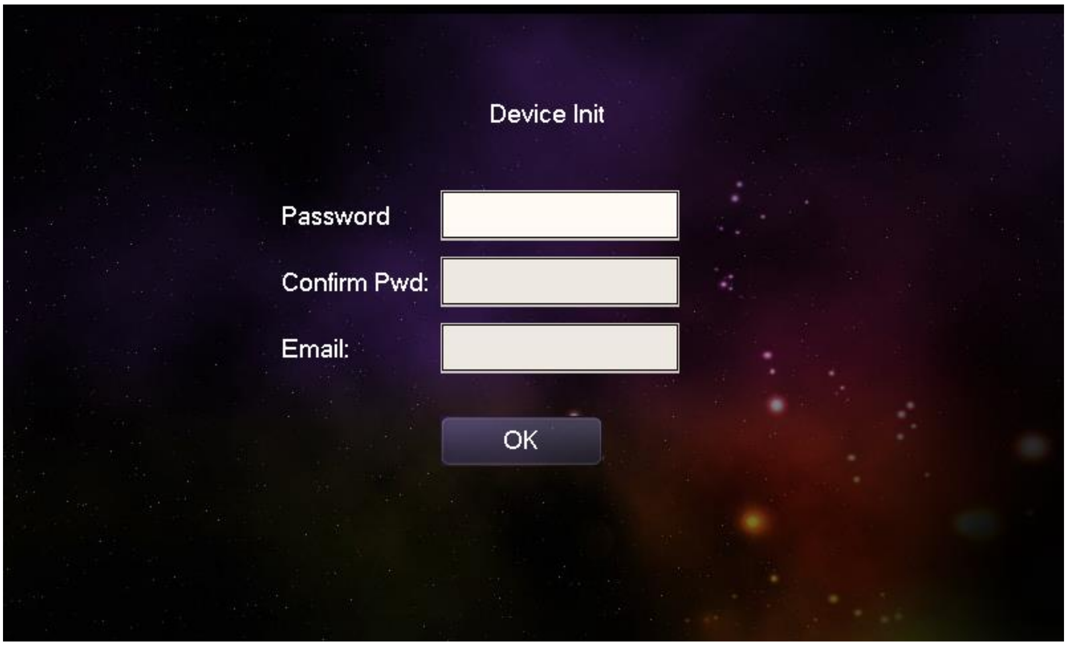
3.1.2.1 Initialization

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 3-13.


Device Init

Password

Confirm Pwd:

Email:

Figure 3-13

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

Step 3 Click [OK].

The system displays “Info Init” interface, and click ✕ to turn off the interface.

3.1.2.2 Network Settings

Set VTH network info, which supports 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.

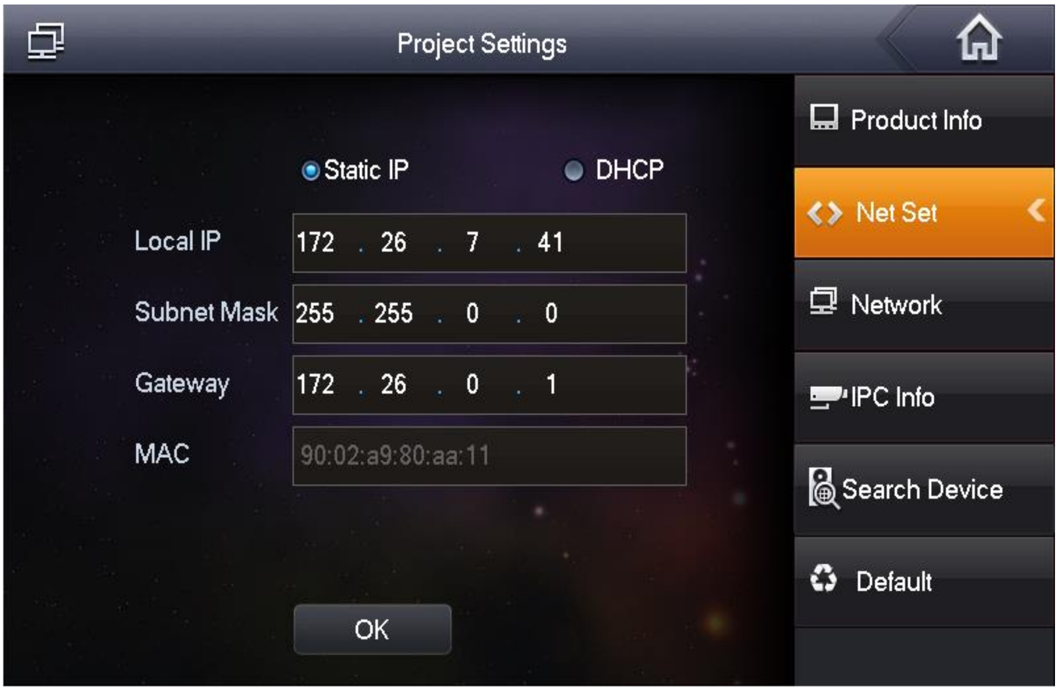
Step 1 Select “System Config>Project Settings”.

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 3-14.



● 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 3-14

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.

3.1.2.3 Product Info Settings

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

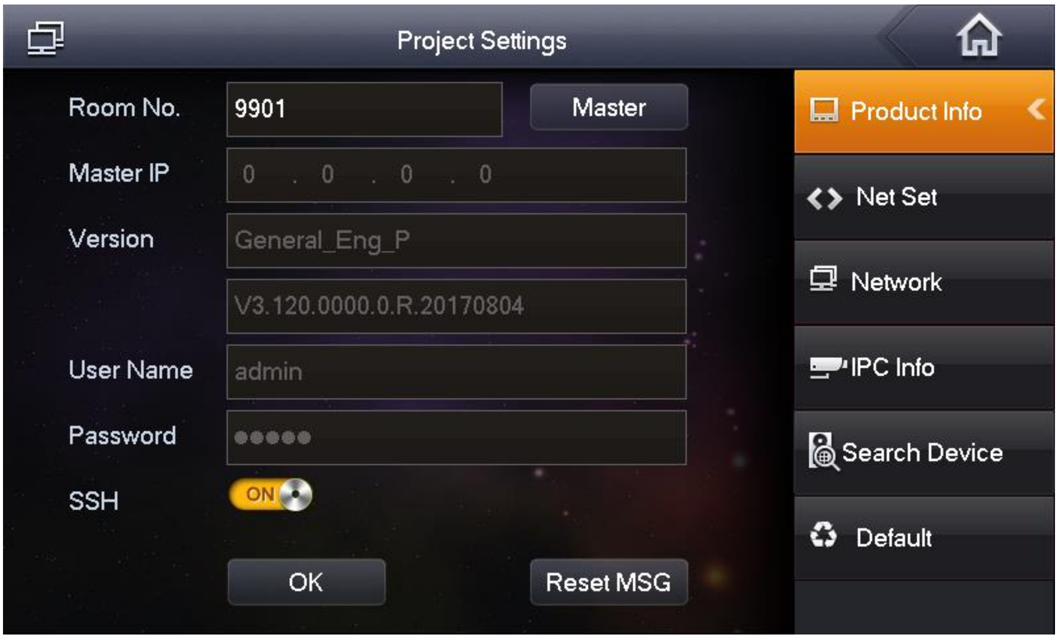
Step 1 Select “System Config>Project Settings”.

The system pops up “Password” prompt box.

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

Step 3 Click [Product Info].

The system displays “Product Info” interface, as shown in Figure 3-15.



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 3-15

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

“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.

Step 5 Click [OK] to save the settings.

3.1.2.4 Network Terminal Setting

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

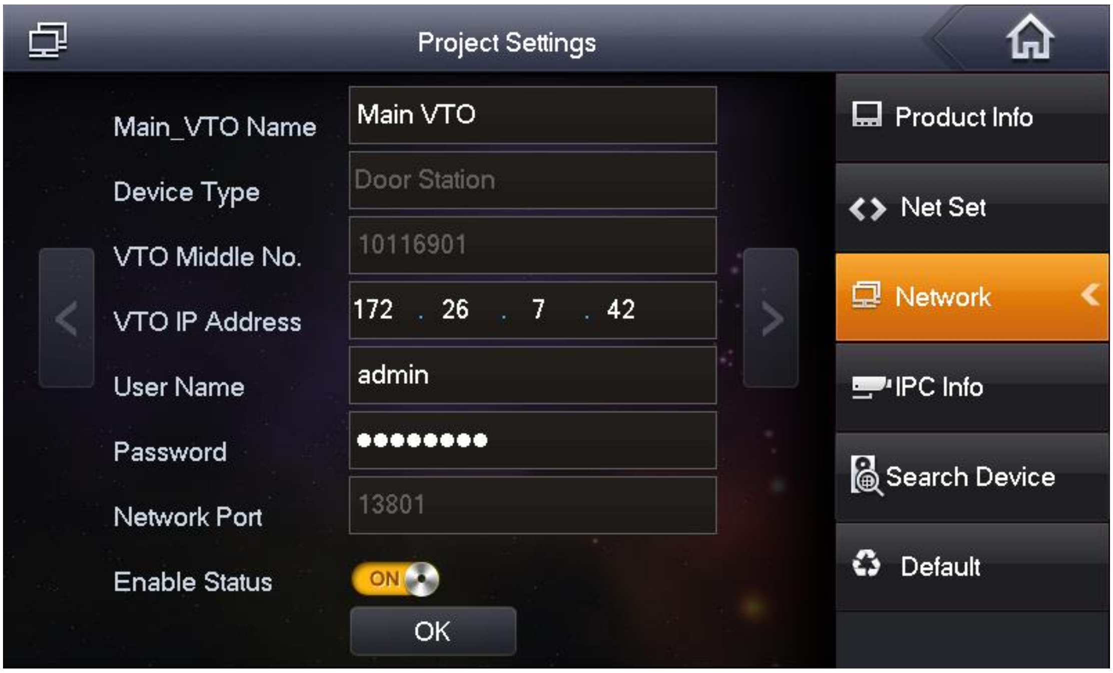
Step 1 Select “System Config>Project Settings”.

The system pops up “Password” prompt box.

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

Step 3 Click [Network].

The system displays “Network” interface, as shown in Figure 3-16.



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 3-16

Step 4 Add VTO or fence station.

- Add main VTO.

1. In Figure 3-16, 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 fence station.

1. Press > to switch to sub VTO setting interface.

2. Select device type to be “fence station”; enter sub VTO name (fence station name), VTO middle no. (fence station middle no.), “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 5 Click [OK] to save the settings.

3.1.3 VTH Settings (Version 4.0)

3.1.3.1 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 3-17.

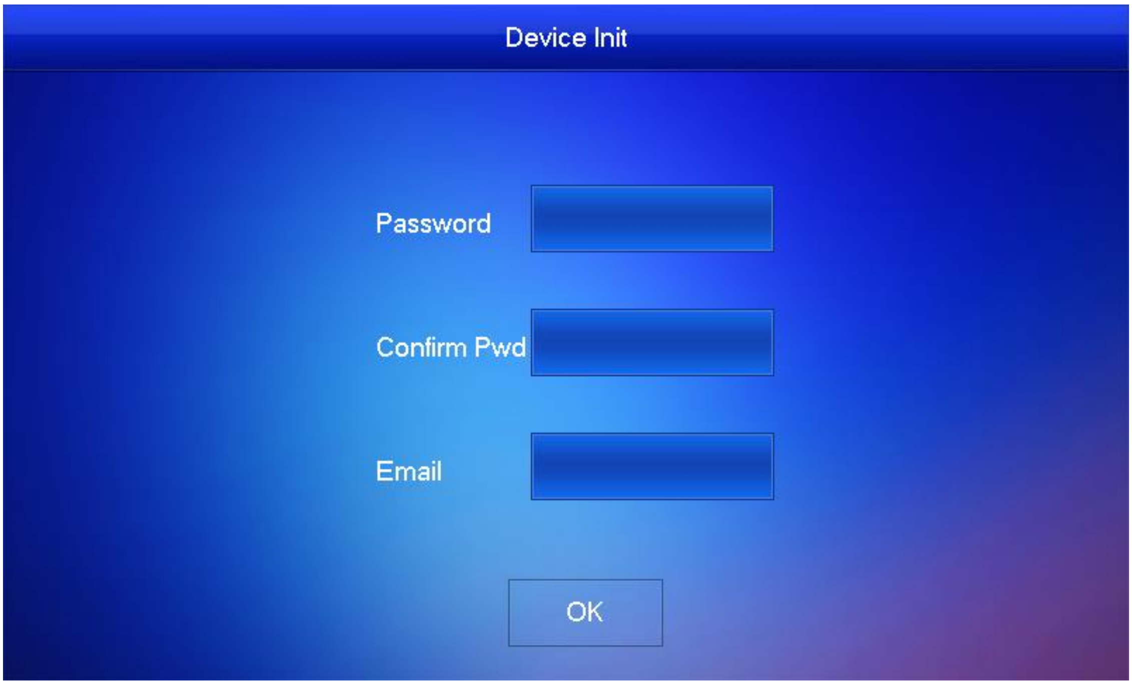


Figure 3-17

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

The system displays main interface.

3.1.3.2 Network Settings

Set VTH network info according to actual network access mode.

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.

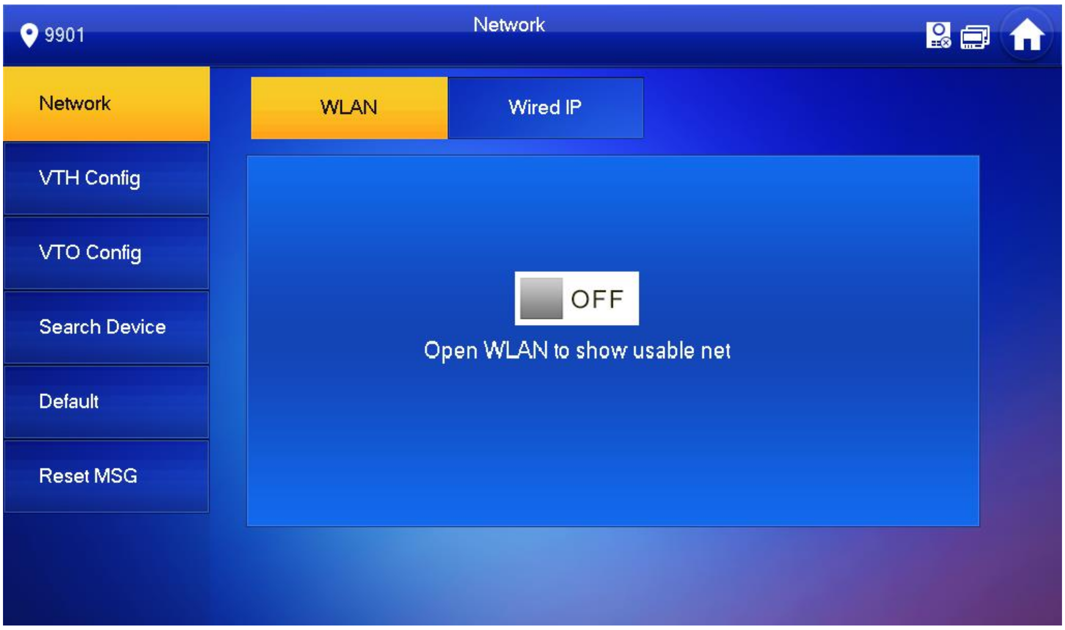
Step 2 Enter the password set during initialization, and click [OK].

Step 3 Click [Network].

The system displays “Network” interface, as shown in Figure 3-18 or Figure 3-19.

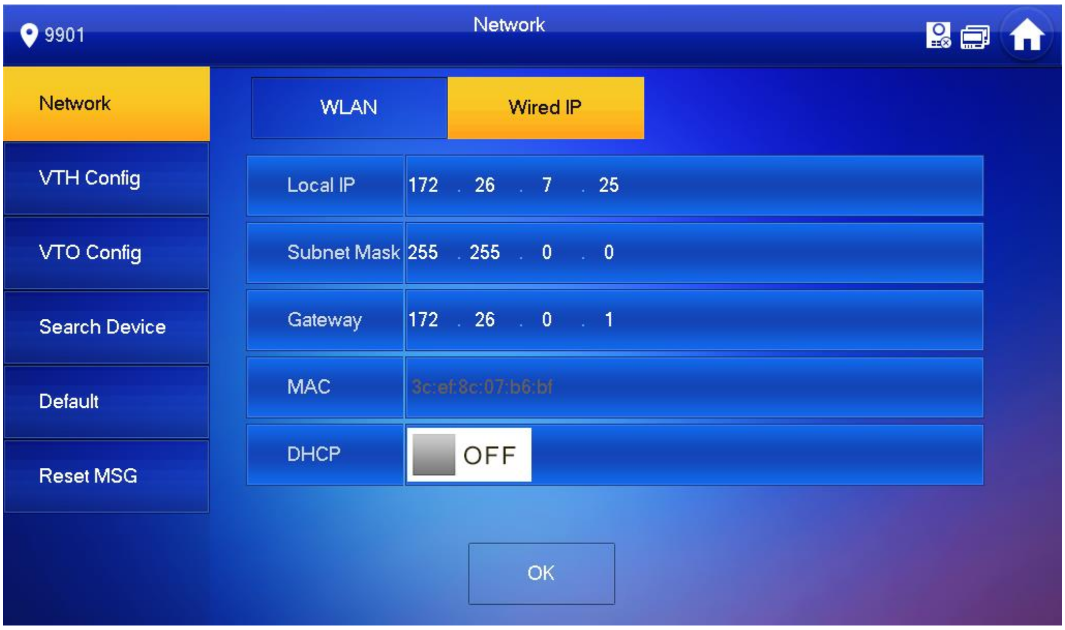
Note

Only devices with wireless function own wireless network access function.



Open WLAN to show usable net

Figure 3-18



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 3-19

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.

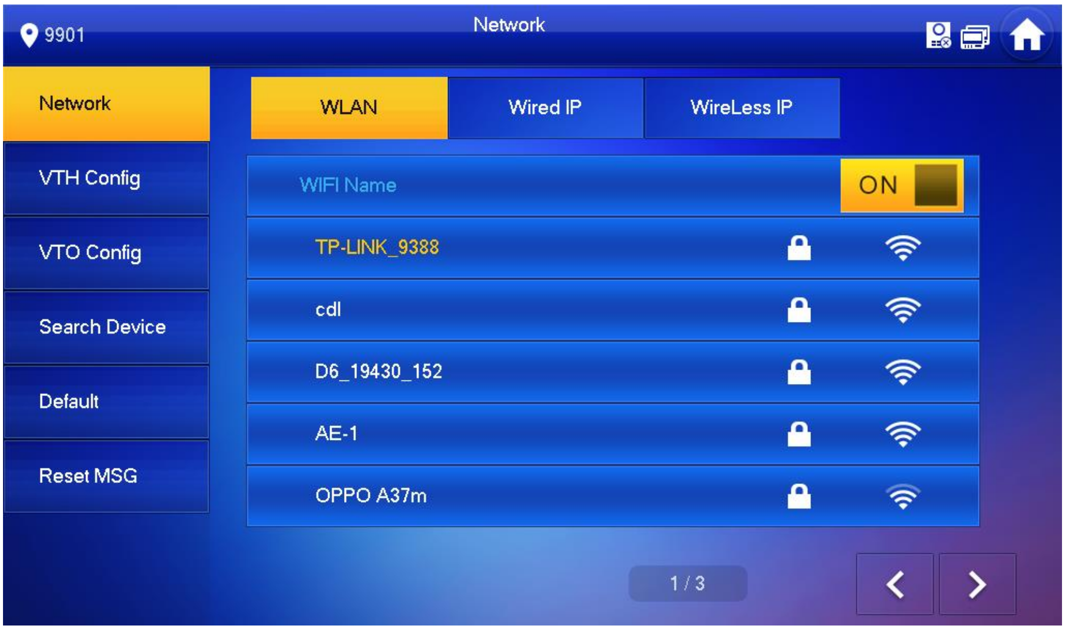
Note

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 3-20.



WIFI Name ON

TP-LINK_9388
cdl
D6_19430_152
AE-1
OPPO A37m

Figure 3-20

2. Connect WIFI.

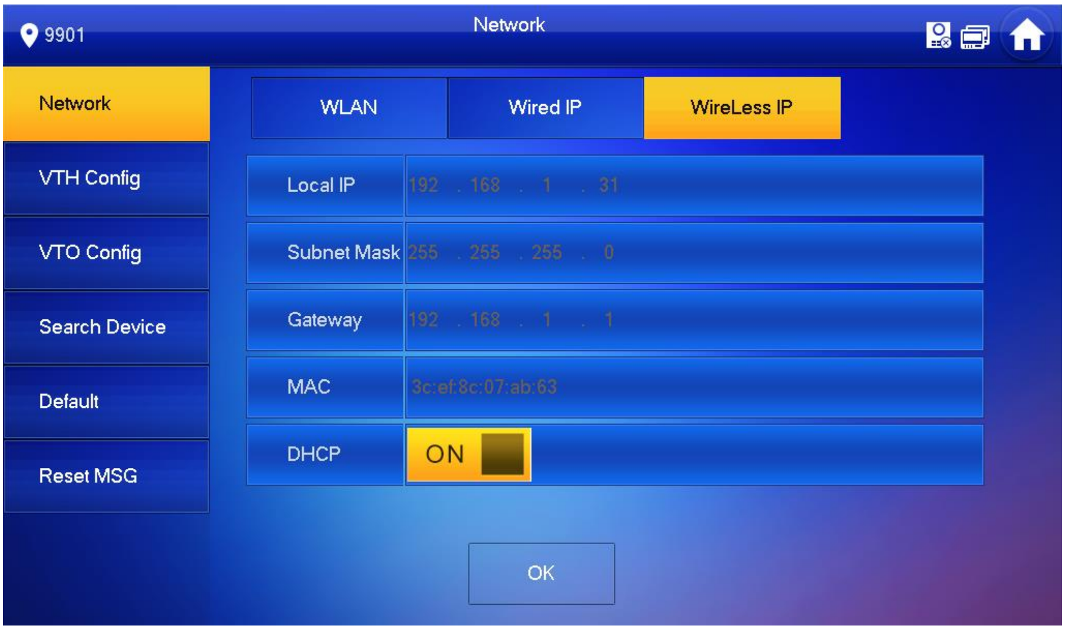
   The system has 2 access ways as follows.

◇ 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 3-21.

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 3-21

3.1.3.3 VTH Config

Set VTH "Room No.", "Type" and "Master IP" info.

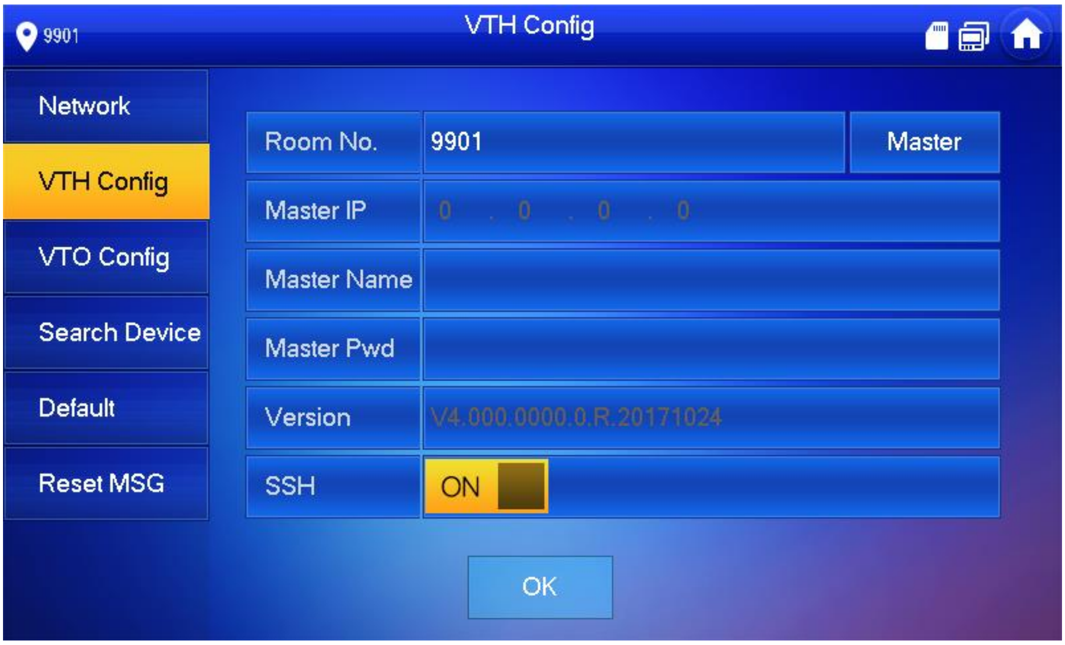
Step 1 Press [Setting] for more than 6 seconds.

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 3-22.



Room No. 9901

Master IP 0 . 0 . 0 . 0

Master Name

Master Pwd

Version V4.000.0000.0.R.20171024

SSH ON

Figure 3-22

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 user name and password of master VTH. Default user name is admin, and the password is the one set during device initialization.

Step 5 Press [OK] to save settings.

3.1.3.4 VTO Config

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

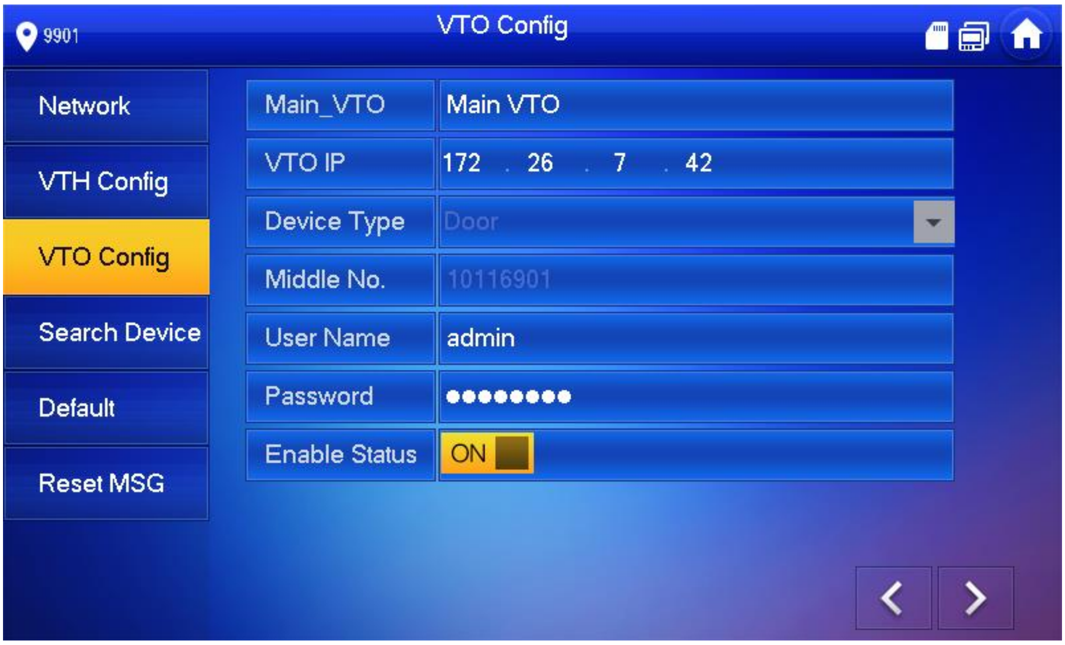
Step 1 Press [Setting] for more than 6 seconds.

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 3-23.



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

Figure 3-23

Step 4 Add VTO or fence station.

- Add main VTO.

1. In Figure 3-23, 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 fence station.

1. Press > to switch to sub VTO setting interface.
2. Select device type to be “Fence Station”, enter sub VTO name (fence station name), VTO middle no. (fence station middle no.), “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.

3.2 Debugging Verification

3.2.1 Verification with Version 3.1 VTH

3.2.1.1 VTO Calls VTH

Press call key at VTO or dial VTH room no. (9901) to call VTH. VTH pops up monitoring image and operating keys, as shown in Figure 3-24. It represents successful debugging.

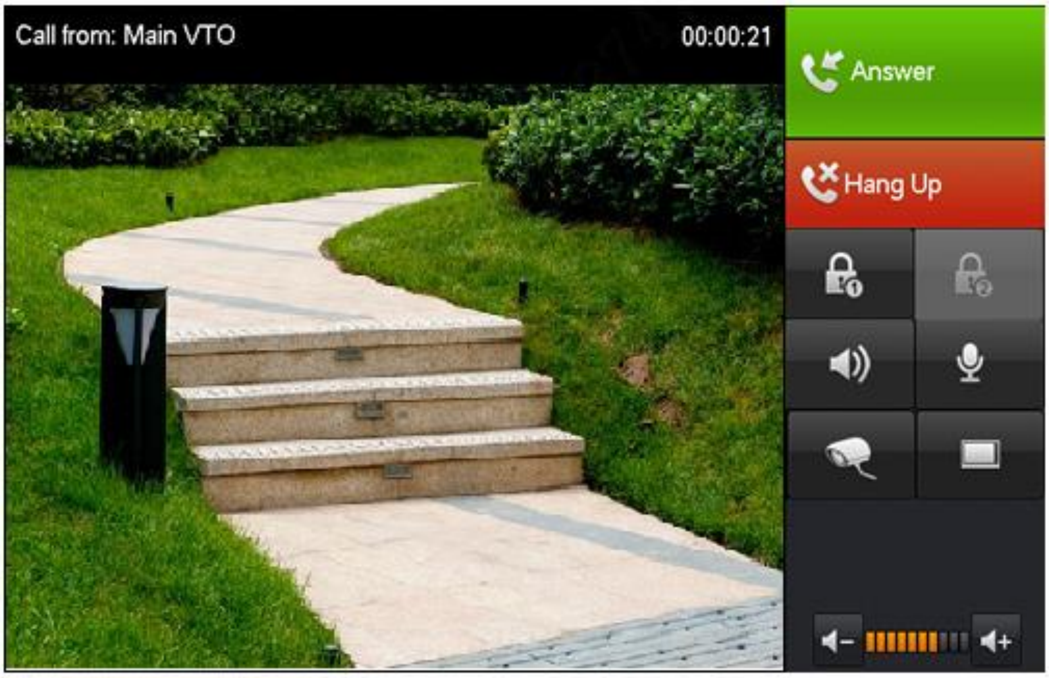


Figure 3-24

3.2.1.2 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 3-25. Select the VTO to enter monitoring image, as shown in Figure 3-26.

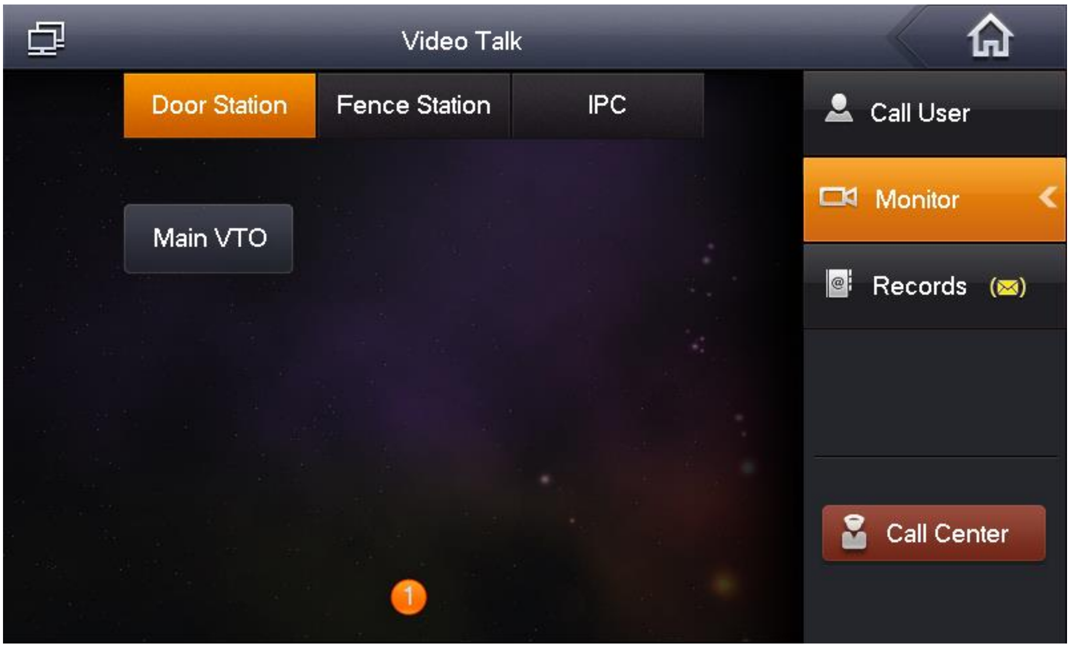


Figure 3-25

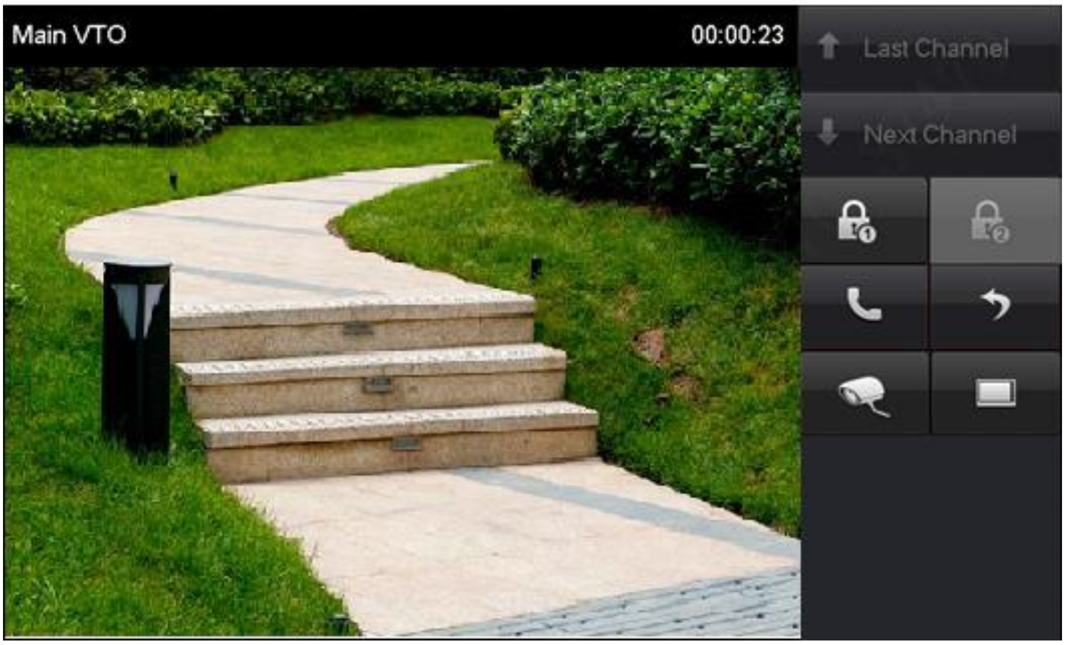


Figure 3-26

3.2.2 Verification with Version 4.0 VTH

3.2.2.1 VTO Calls VTH

Press call key at VTO or dial VTH room no. (9901) to call VTH. VTH pops up monitoring image and operating keys, as shown in Figure 3-27. 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.

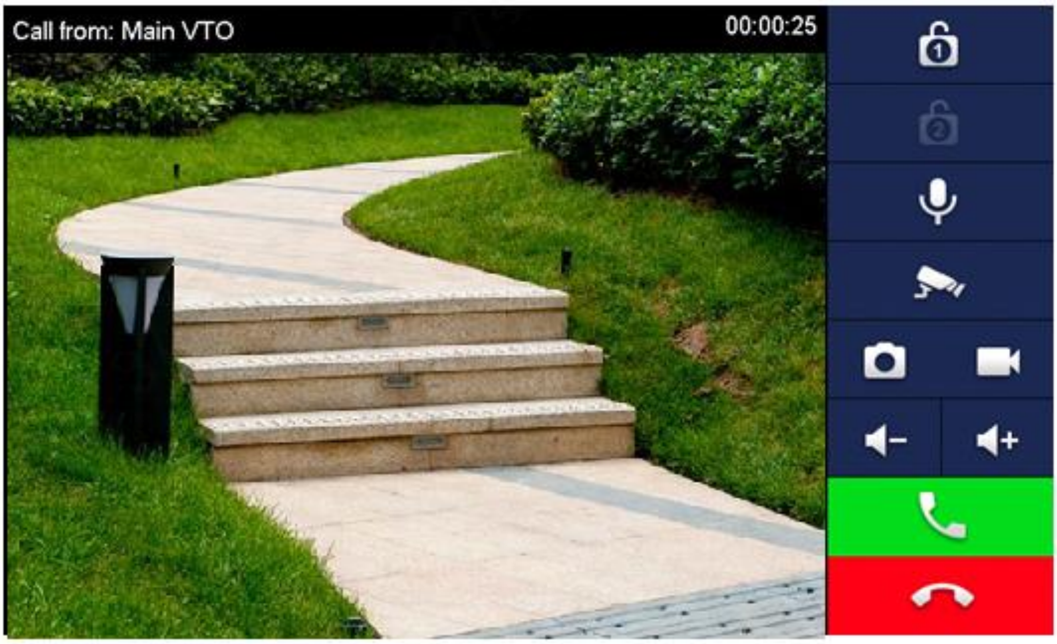


Figure 3-27

3.2.2.2 VTH Monitors VTO

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

Select “Monitor > Door”, as shown in Figure 3-28. Select the VTO to enter monitoring image, as shown in Figure 3-29.

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.

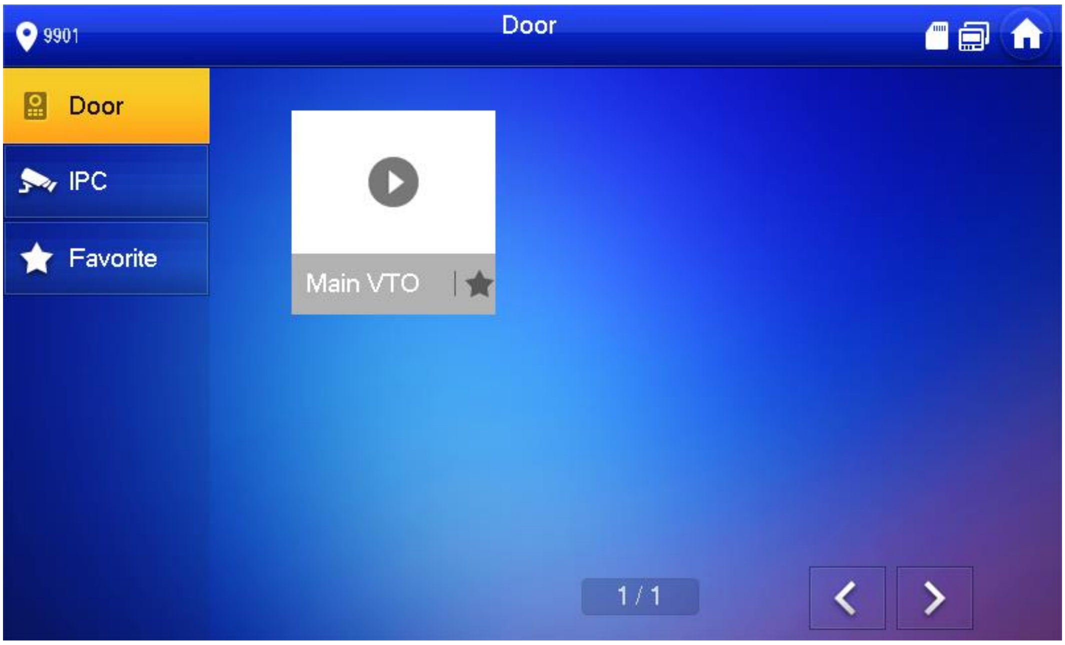


Figure 3-28

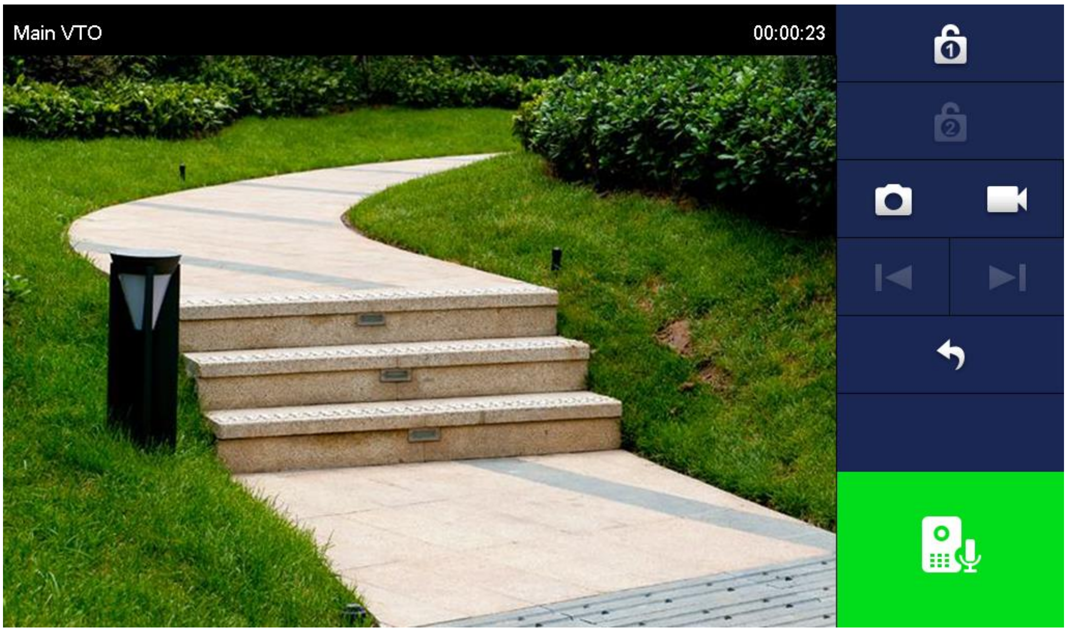


Figure 3-29