Digital VTH (Version 4.0)

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, installation process, debugging and verification process of digital VTH 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 Front Panel

Different models of devices may have different front panel dimensions and key types, but keys or indicators with the same silkscreen or icon have the same function. Please refer to Table 1-1 for details.

Icon or Silkscreen	Name	Description
	SOS	Press this key to call the Call Center in case of emergency.
	Menu	Press this key to return to main menu.
	Call	● In case of incoming call, press this key to answer the call. ● During talk, press this key to hang up. ● During monitoring, press this key to speak to unit VTO, villa VTO and fence station. ● During speaking, press this key to exit speaking.
	Monitor	● In standby mode, press this key to monitor the main VTO. ● During monitoring, press this key to exit monitoring.
	Unlock	In case of incoming call, talk, monitoring and speaking of VTO, press this key to unlock corresponding VTO.
	Message indicator	If this indicator turns on, it represents that there are unread messages.
	Power indicator	If this indicator turns on in green, it represents normal power supply.
Network	Network indicator	● If this indicator turns on, it represents normal communication with VTO. ● If this indicator turns off, it represents abnormal communication with VTO.
DND	DND indicator	If this indicator turns on in green, it represents that DND function is enabled. Note For DND settings, please scan QR code on the front cover, and refer to the user's manual.

Table 1-1

1.2 Rear Panel Port

1.2.1 VTH5221 Series /VTH5241 Series

VTH5221 series and VTH5241 series have different port positions at the rear panel, but the same port provides the same function. Taking VTH5221 as an example, specific functions of ports are introduced, as shown in Figure 1-1.

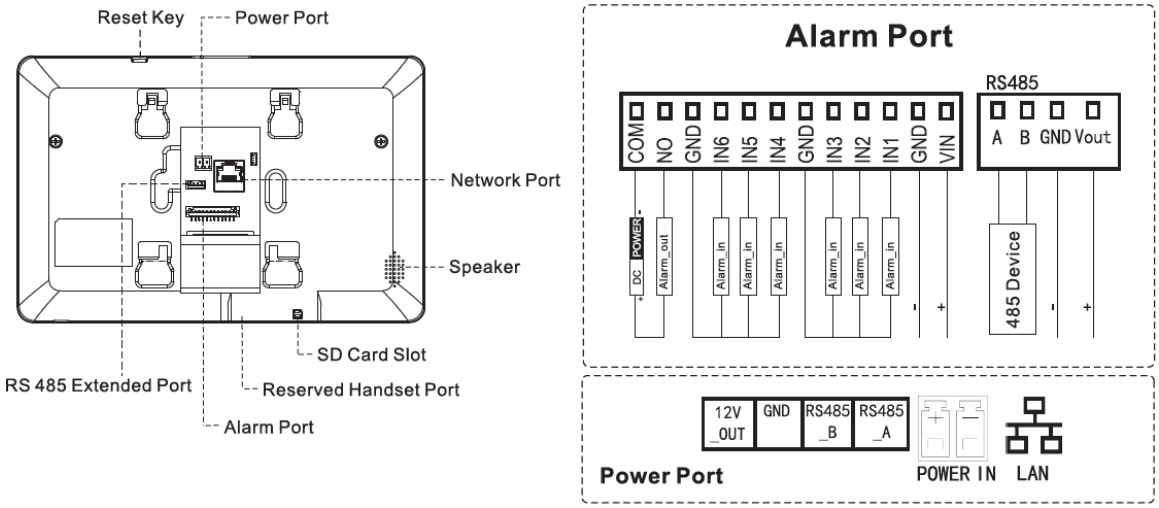

Figure 1-1

1.2.2 VTH15 Series Type A/Type B/Type CH

In VTH15 series, different types of digital VTH have different port positions, but the same port provides the same function. Taking VTH1550CH as an example, specific functions of ports are introduced, as shown in Figure 1-2.

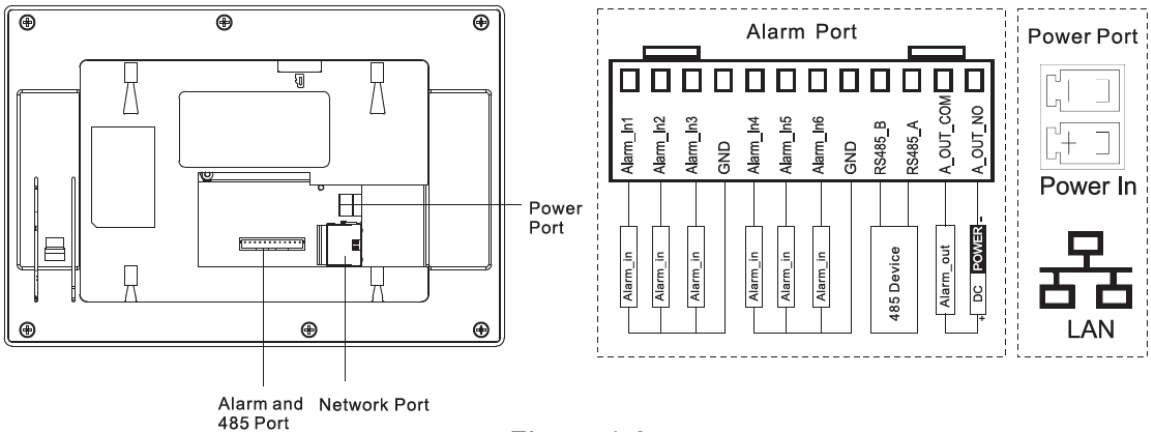

Figure 1-2

In VTH type A/type B series, different types of digital VTH have different port positions, but the same port provides the same function. Taking VTH1560B as an example, specific functions of ports are introduced, as shown in Figure 1-3.

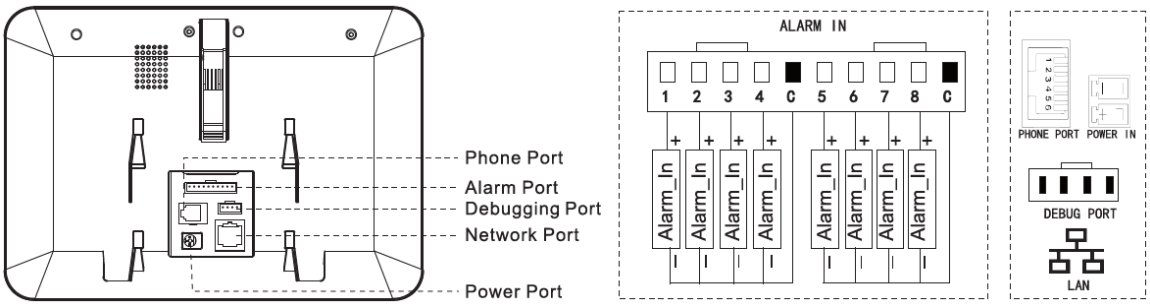

Figure 1-3

1.2.3 VTH5222CH/VTH1550CHW-2

Except different numbers of 2-wire port, VTH5222CH and VTH5222CHW-2 are the same in other aspects. VTH5222CH has 1 group of 2-wire port, while VTH1550CHW-2 has 3 groups of 2-wire port. VTH5222CH is shown in Figure 1-4.

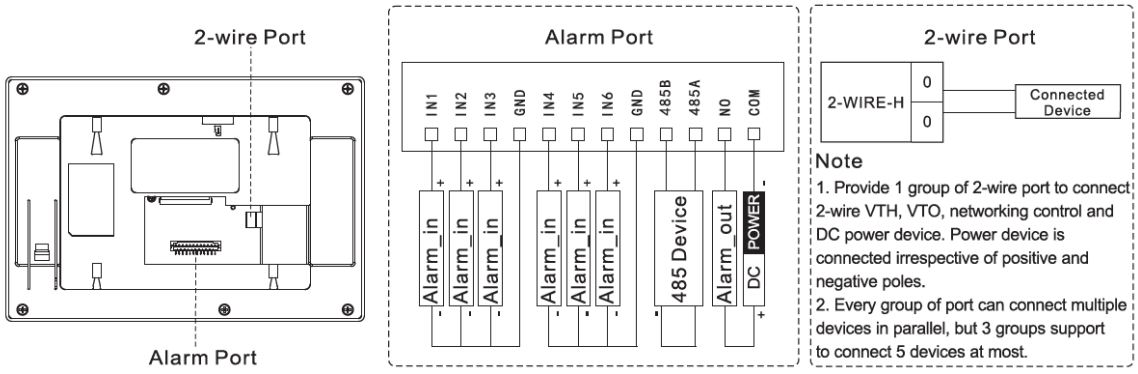

Figure 1-4

1.2.4 VTH1660CH

Its ports are described in Figure 1-5.

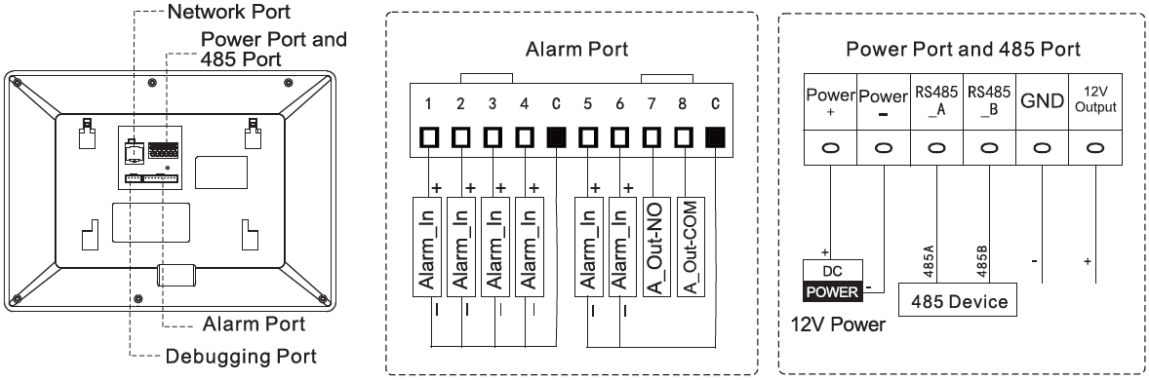

Figure 1-5

1.2.5 VTH2221A

Its ports are described in Figure 1-6.

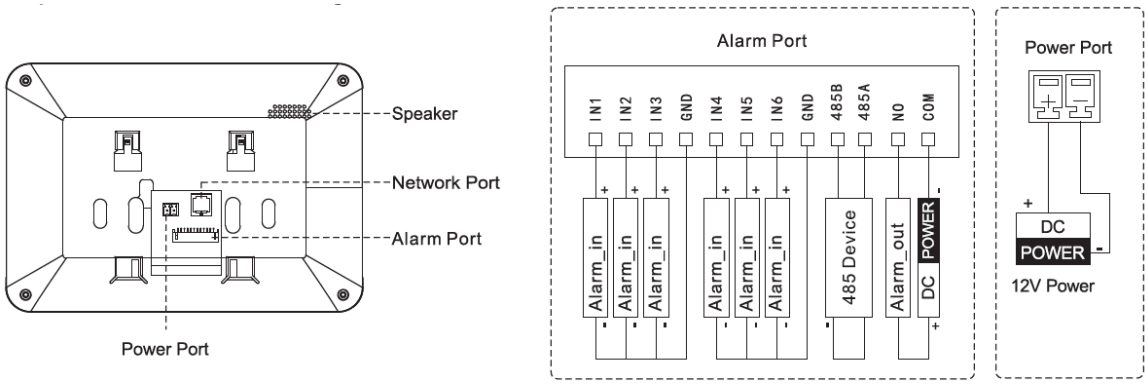

Figure 1-6

2 Installation and Debugging

2.1 Installation

Caution

- Don’t install VTH in bad environment, such as condensation, high temperature, stained, dusty, chemically corrosive and direct sunshine environment.
- In case of abnormality after power on, please pull out network cable and cut off power supply at once. Power on after troubleshooting.
- Engineering installation and debugging shall be done by professional teams. Please don’t dismantle or repair arbitrarily in case of device failure. Please contact after-sales department.
- It is suggested that installation height of device central point shall be 1.4cm～1.6cm above the ground.

2.1.1 Surface Installation

Directly install the device with a bracket onto a wall, which is suitable for all types of devices. Take “VTH1550CH” for example.

Step 1 Drill holes in the wall according to hole positions of the bracket.

Step 2 Fix installation bracket directly onto the wall with screws.

Step 3 Put the device into installation bracket from top down.

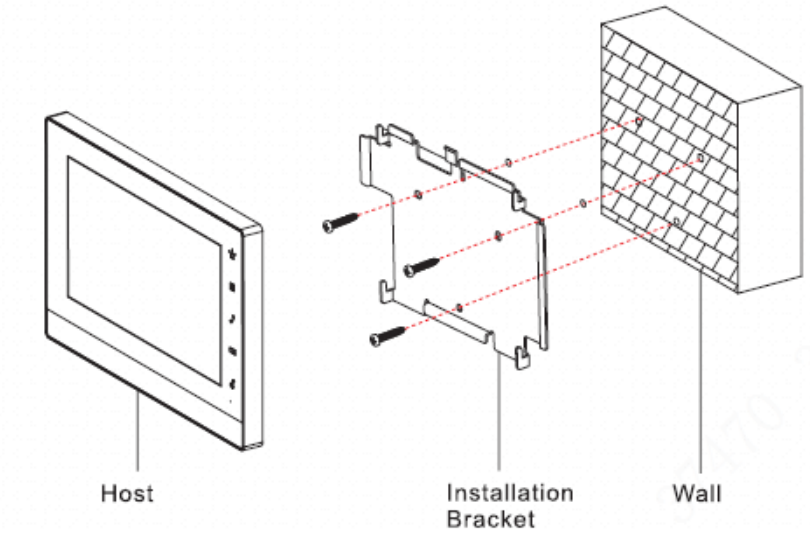

Figure 2-1

2.1.2 Installation with 86 Box

Install the device with 86 box, which is suitable for all types of devices. Take “VTH1560B/BW” for example.

Step 1 Embed 86 box into a wall at a proper height.

Step 2 Fix installation bracket onto 86 box with screws.

Step 3 Put the device into installation bracket from top down.

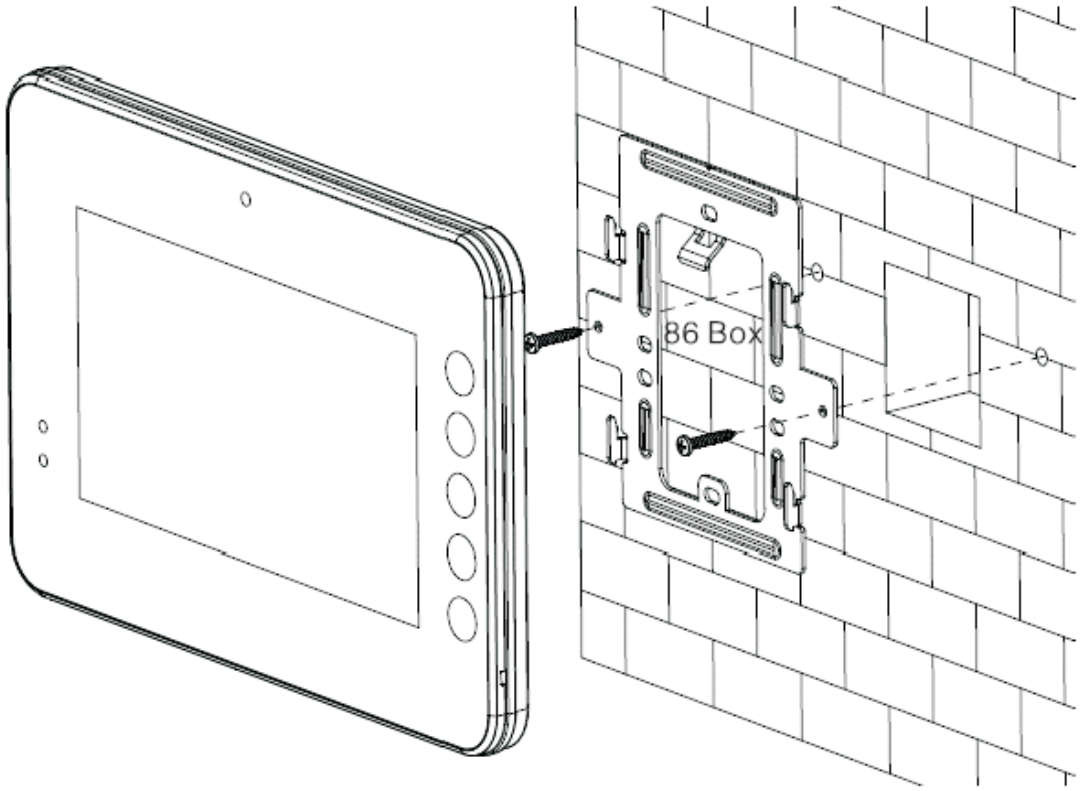

Figure 2-2

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.

- 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. of every VTO and VTH have been planned.
- For specific operations, please scan QR code on the front cover.

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.

2.2.1 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 2-3.

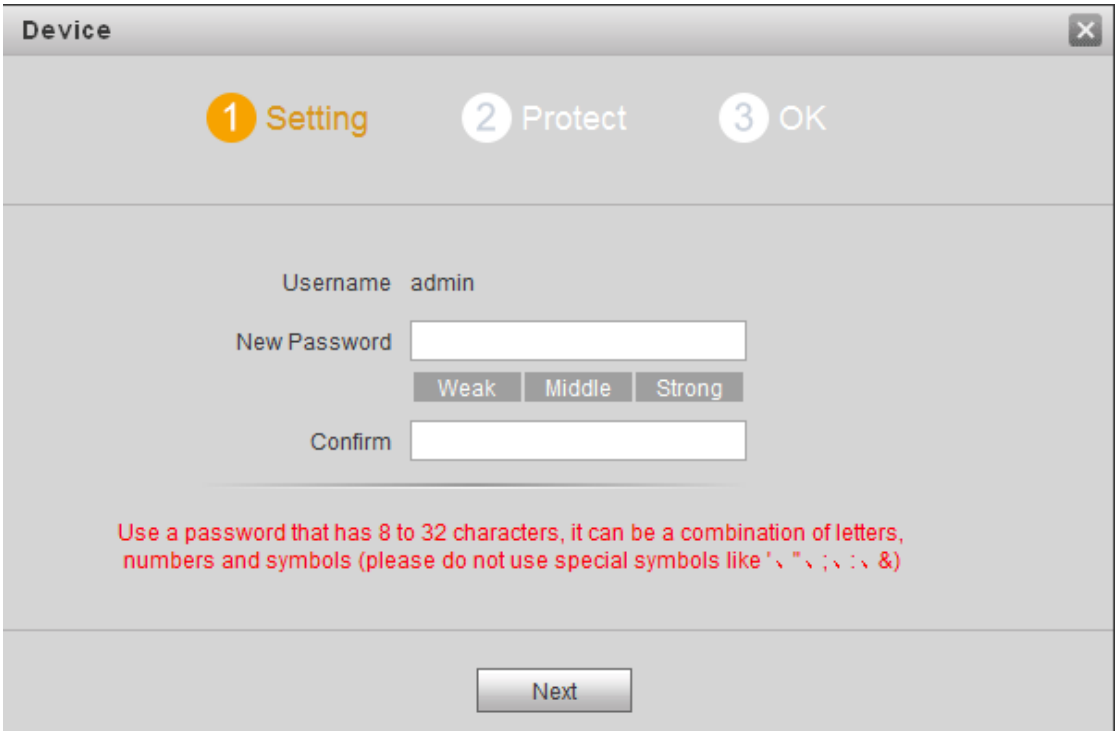

Figure 2-3

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 2-4.

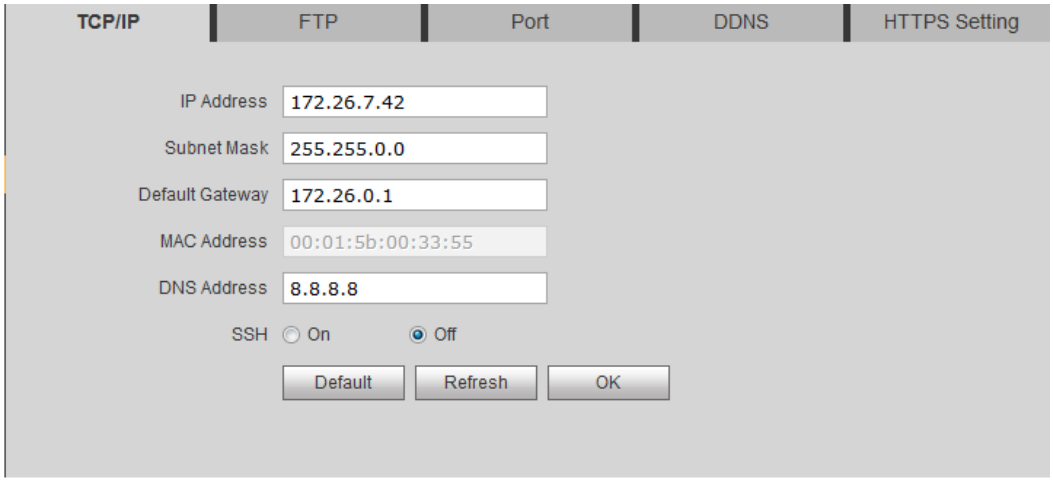

Figure 2-4

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 2-5.

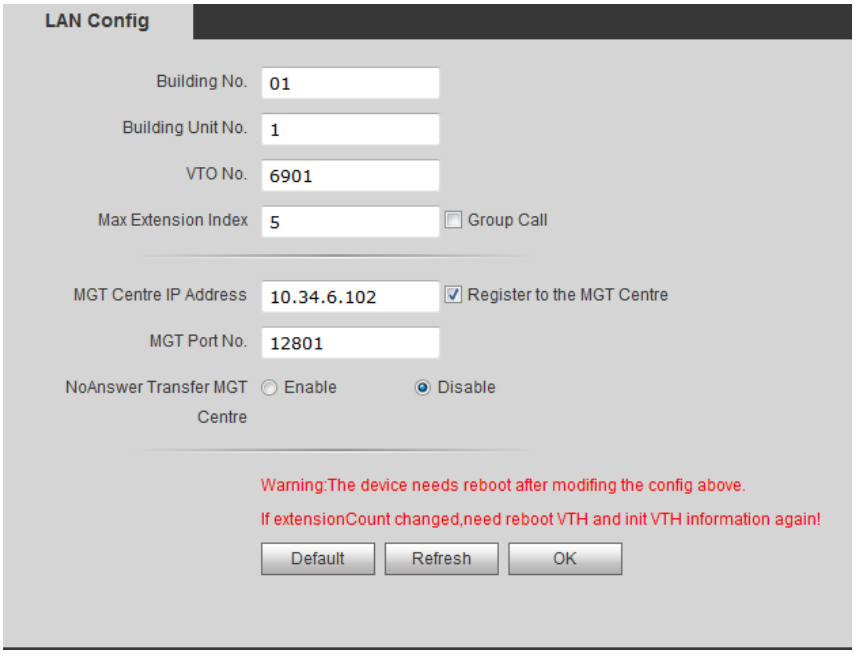

Figure 2-5

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 2-6.

Note

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

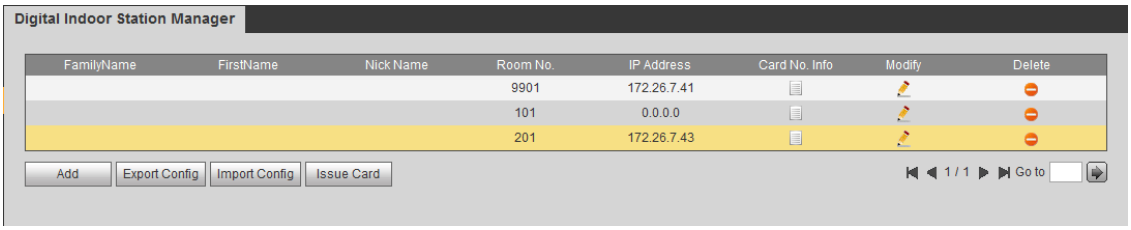

Figure 2-6

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”.

2.2.2 VTH Settings

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 2-7.

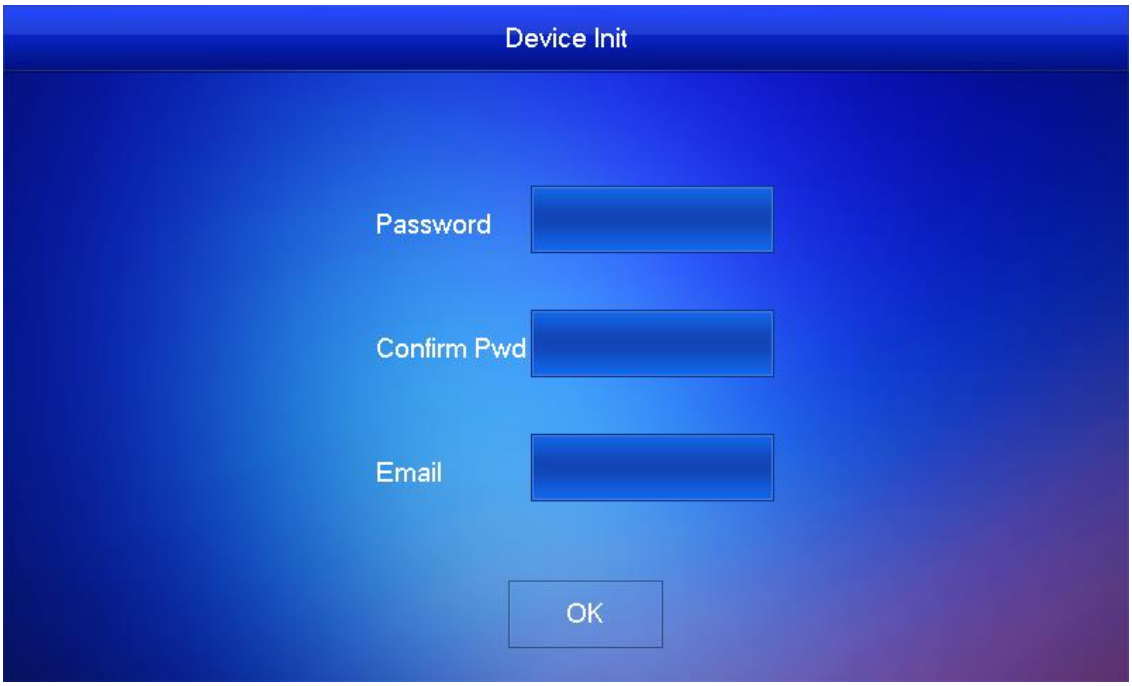

Figure 2-7

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 2-8 or Figure 2-9. 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.

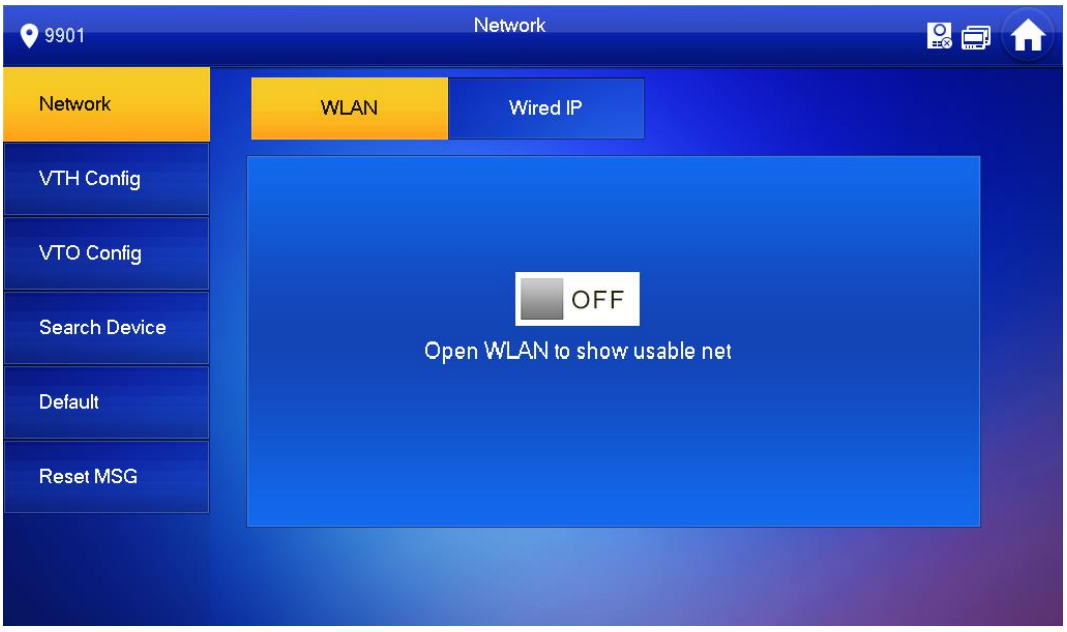

Figure 2-8

Figure 2-9

- 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 2-10.

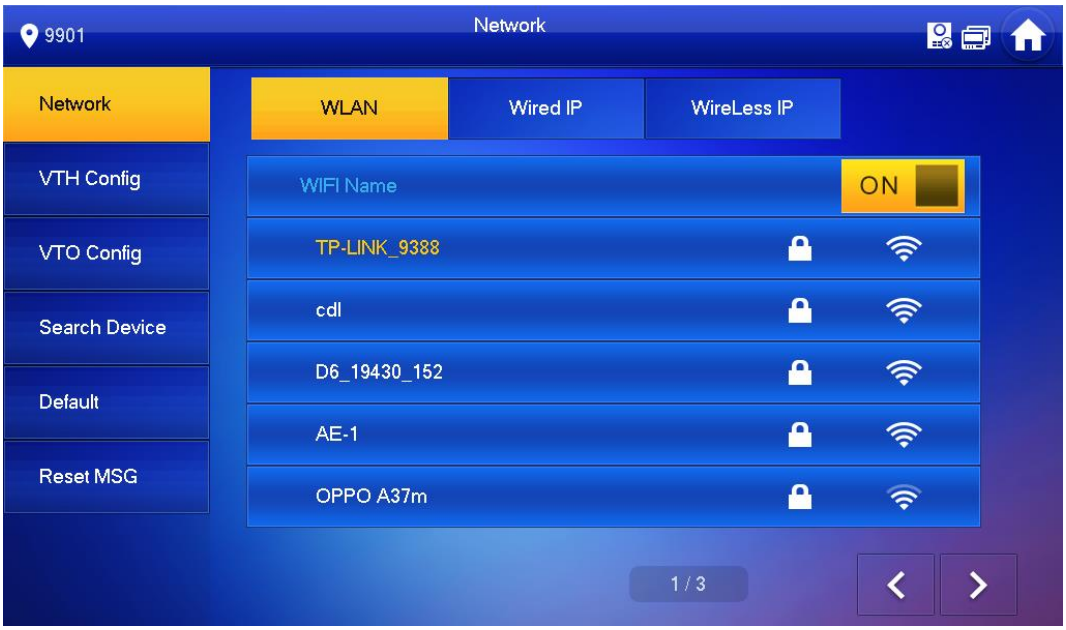

Figure 2-10

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 2-11.

   Note

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

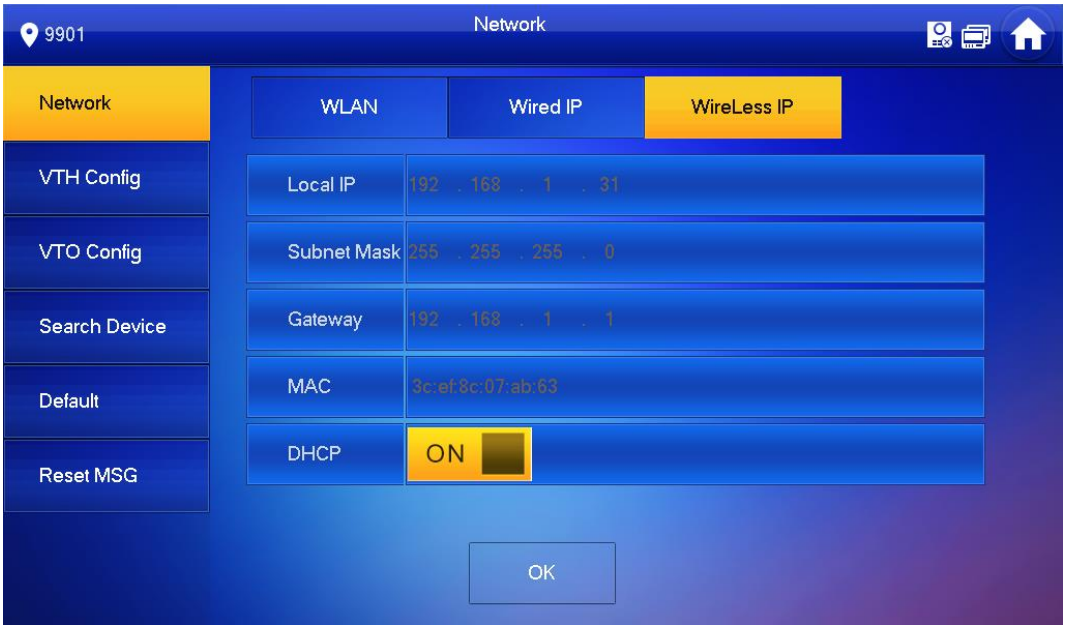

Figure 2-11

Step 6 Click [VTH Config].

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

Figure 2-12

- 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 2-13.

Figure 2-13

- Add main VTO.

1. In Figure 2-13, enter main VTO name, VTO IP, “User Name” and “Password”.
2. Switch the “Enable Status” to be ON.

Note

- “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, 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 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

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. Switch the “Enable Status” to be ON.

2.3 Debugging Verification

2.3.1 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 2-14. 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 2-14

2.3.2 VTH Monitors VTO

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

Select “Monitor > Door”, as shown in Figure 2-15. Select the VTO to enter monitoring image, as shown in Figure 2-16.

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.

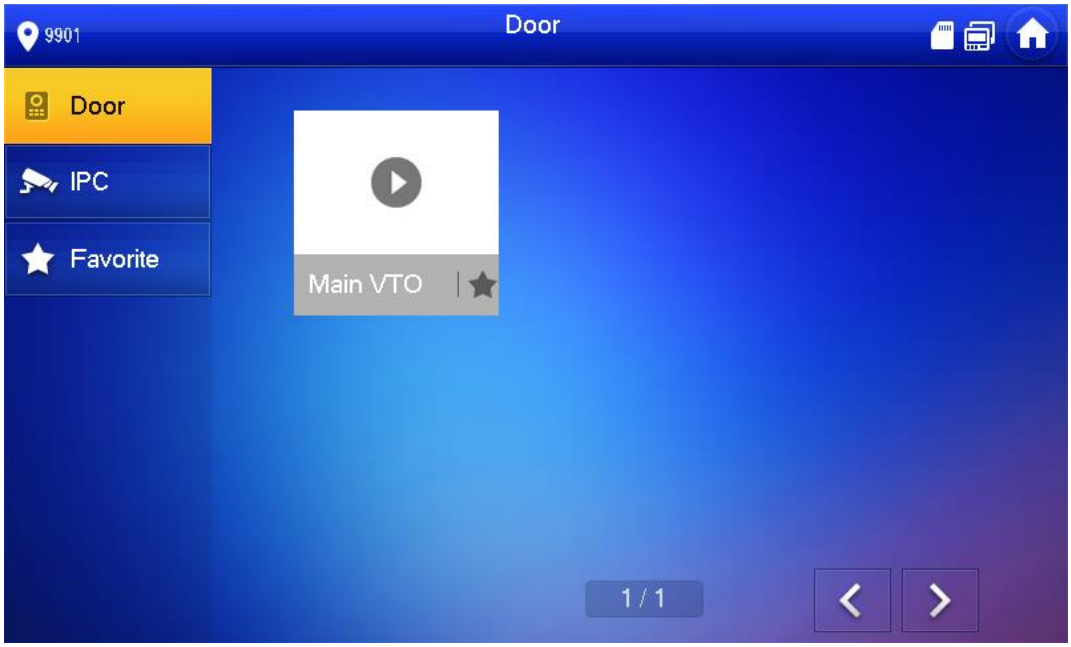

Figure 2-15

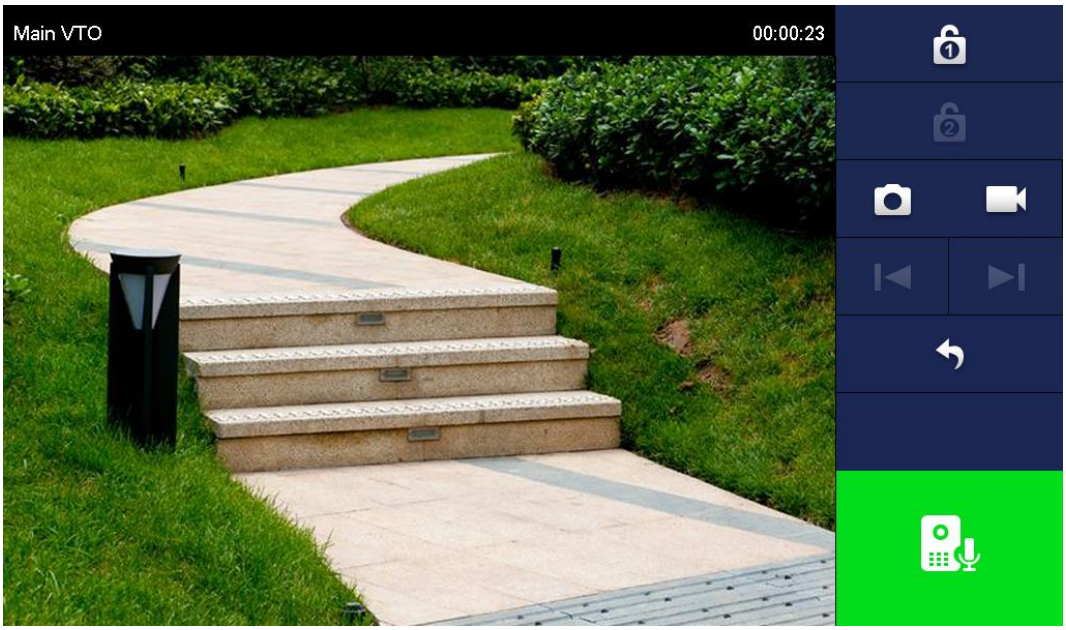

Figure 2-16