IP Villa System

Quick Start Guide

V1.0.0

Foreword

General

This document mainly introduces structure, installation process, debugging, and verification process of the IP villa system.

Safety Instructions

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

Signal Words	Meaning
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release	September 2019

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 manual, CD-ROM, QR code or our official website. If there is inconsistency between paper 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 manual (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. 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

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; don’t put on the device anything filled with liquids to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- The device shall be used with screened network cables.

Power Requirement

- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- 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, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.
- Do not cut off power supply during device upgrade. Power supply can be cut off only after the device has completed upgrade and has rebooted.

Table of Contents

1 Overview

1.1 Outdoor Station (VTO) Front Panel

Figure 1-1 VTO front panel

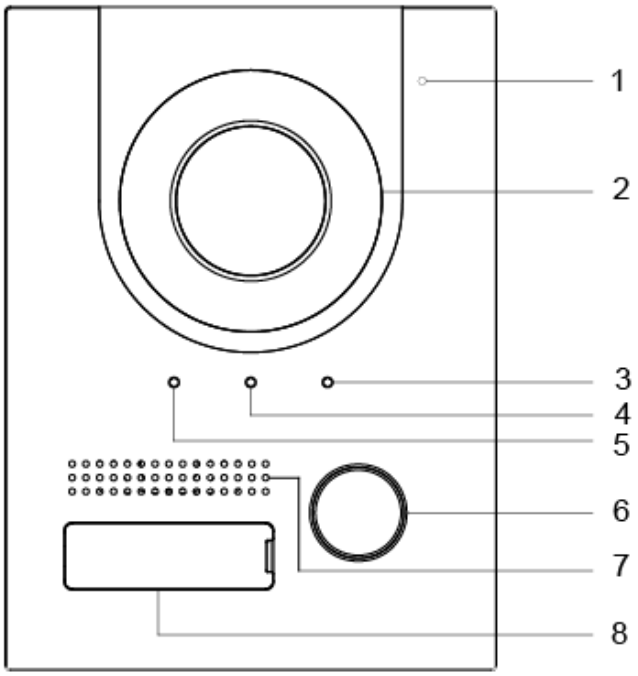


Table 1-1 Front panel description

No.	Name	Description
1	MIC	Inputs audio.
2	Camera	Monitors door area.
3	Indicator	After you have started a call, this indicator will be on.
4	Indicator	During the communication, this indicator will be on.
5	Indicator	When the door is unlocked, this indicator will be on.
6	Call button	Press to call indoor monitor (VTH) or the management center.
7	Speaker	Outputs audio.
8	Paper slot	You can put paper notes in the paper slots. Paper slot is available on select models.

1.2 Outdoor Station (VTO) Rear Panel

Figure 1-2 Outdoor station (VTO) rear panel

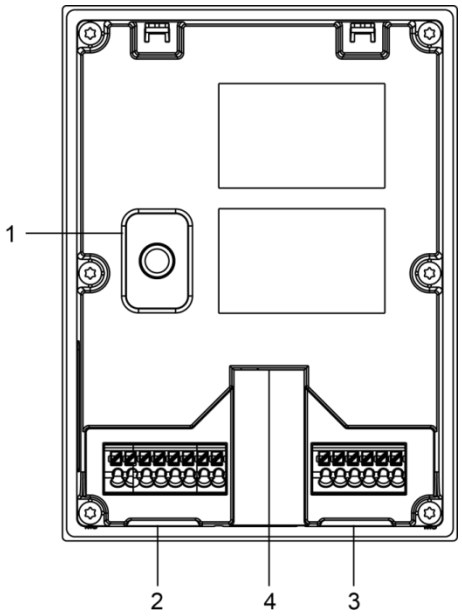


Table 1-2 Rear panel description

Name	NO	Description
Tamper switch	1	The outdoor station (VTO) would make alarm sound if it is being removed from the wall by force, and the alarm will also be sent to the management center.
Cable ports	2	GND: Ground +12V_OUT: Output 12V/100ma power RS485_B: RS-485 communication RS485_A: RS-485 communication ALARM_NO: Switch quantity output ALARM_COM: Switch quantity output EOC2: Two-wire port EOC1: Two-wire port
	3	DOOR_BUTTON: Unlock button DOOR_FEEDBACK: Door contact feedback GND: GROUND DOOR_NC: Connected to access controller to control door locks DOOR_COM: Connected to access controller to control door locks DOOR_NO: Connected to access controller to control door locks
Ethernet port	4	Connects to the network with Ethernet cable. Only outdoor station (VTO) whose models end with "P" support PoE.

1.3 Indoor Monitor (VTH) Front Panel

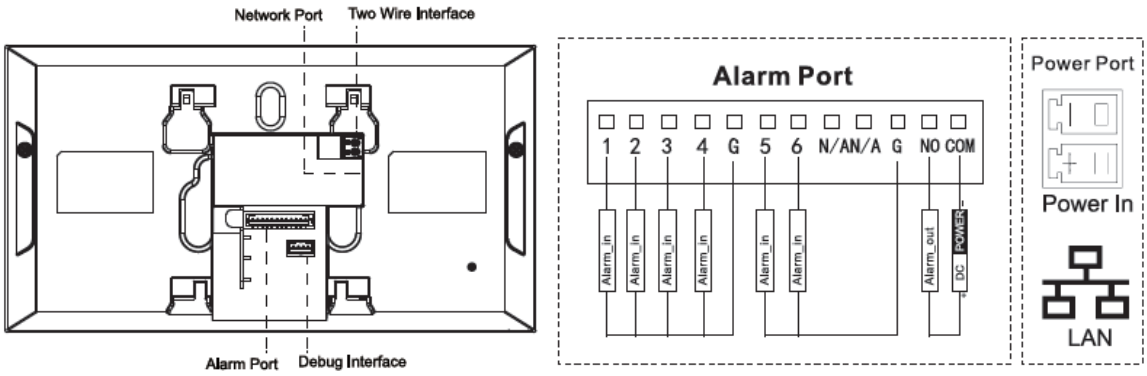
Different models of devices might have different front panel dimensions and key types, but keys or indicators with the same silkscreen or icon have the same function. See Table 1-3.

Table 1-3 Front panel button

Icon or Silkscreen	Name	Description
	SOS	Tap this key to call the call center in case of emergency.
	Menu	Tap this key to return to main menu.
	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 outdoor station (VTO), villa outdoor station (VTO) and fence station. ● During speaking, press this key to exit speaking.
	Monitor	● In standby mode, press this key to monitor the main outdoor station (VTO). ● During monitoring, press this key to exit monitoring.
	Unlock	When there is an incoming call from an outdoor station (VTO), or during the call between an outdoor station (VTO) and an indoor monitor (VTH), or when you are watching real-time videos by an outdoor station (VTO), press this key, and then you can unlock the door beside the outdoor station (VTO).
	Message indicator	The indicator is on when there are unread messages.
	Power indicator	The indicator is green when power supply is normal.
Network	Network indicator	● The indicator is on when communication with outdoor station (VTO) is normal. ● The indicator is off when communication with outdoor station (VTO) is abnormal.
DND	DND indicator	The indicator is green when DND function is enabled. For DND settings, scan QR code on the front cover, and refer to the user's manual.

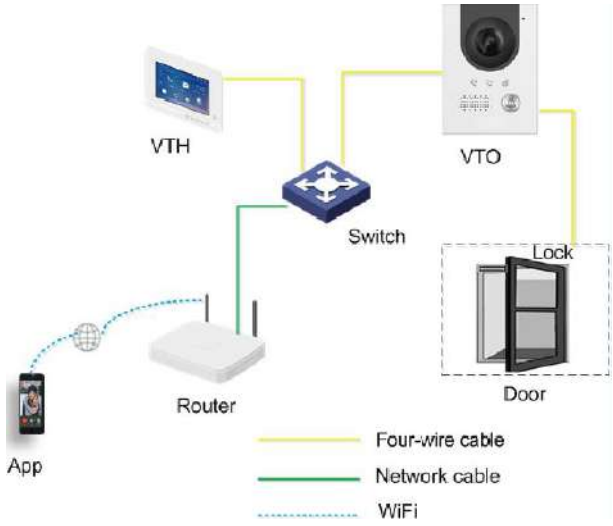
1.4 Indoor Monitor (VTH) Rear Panel

Figure 1-3 Indoor monitor (VTH) rear panel



1.5 Network Diagram

Figure 1-4 Network diagram



2 Installation and Configuration

- Do not install the device in environment with condensation, high temperature, stained, dusty, chemically corrosive and direct sunshine.
- In case of abnormality after power on, pull out network cable and cut off power supply at once. Power on again after troubleshooting.
- Installation and commission shall be done by professionals. Do not dismantle or repair arbitrarily in case of device failure. 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 Outdoor Station (VTO) Installation

2.1.1 Surface Mount

Figure 2-1 Surface mount

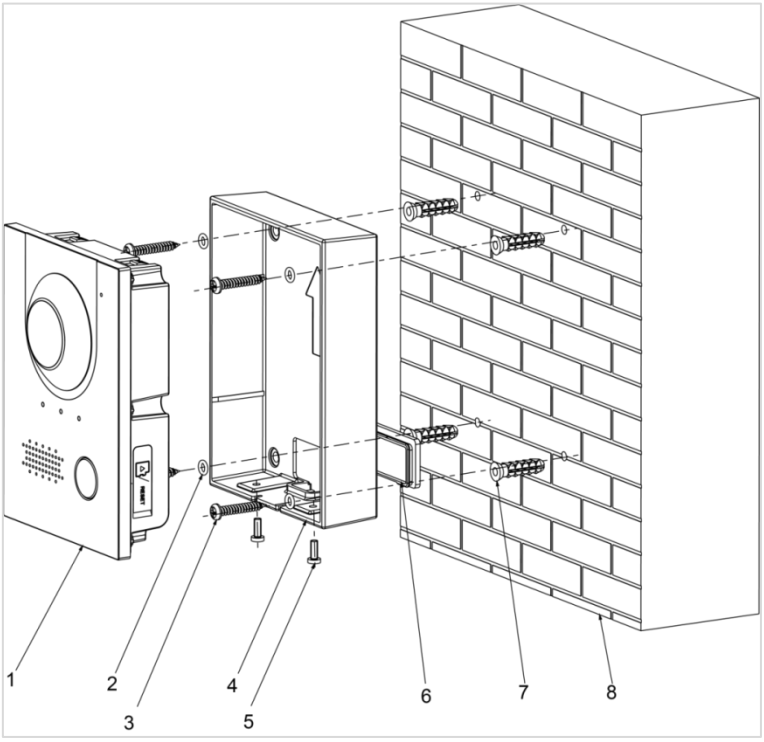


Table 2-1 Names of numbers (1)

No.	Name
1	Outdoor station (VTO)
2	Waterproof ring
3	ST4×25 self-tapping screw
4	Surface mount box

No.	Name
5	M3×8 Screws
6	Waterproof silica gel pad
7	Expansion screw
8	Wall

Step 1 Hammer four expansion screws into the wall.

Step 2 Install the waterproof silica gel pad on the surface mount box from the back of the surface mount box.

Step 3 Put four waterproof rings on four ST4×25 self-tapping screws.

Step 4 Install the mounting box on the wall by screwing the four ST4×25 self-tapping screws into the expansion screws.

Step 5 Put the outdoor station (VTO) into the surface mount box.

Step 6 Fix the outdoor station (VTO) to the surface mount box by screwing two M3×8 screws from the bottom of the surface mount.

2.1.2 Flush Mount

Figure 2-2 Flush mount

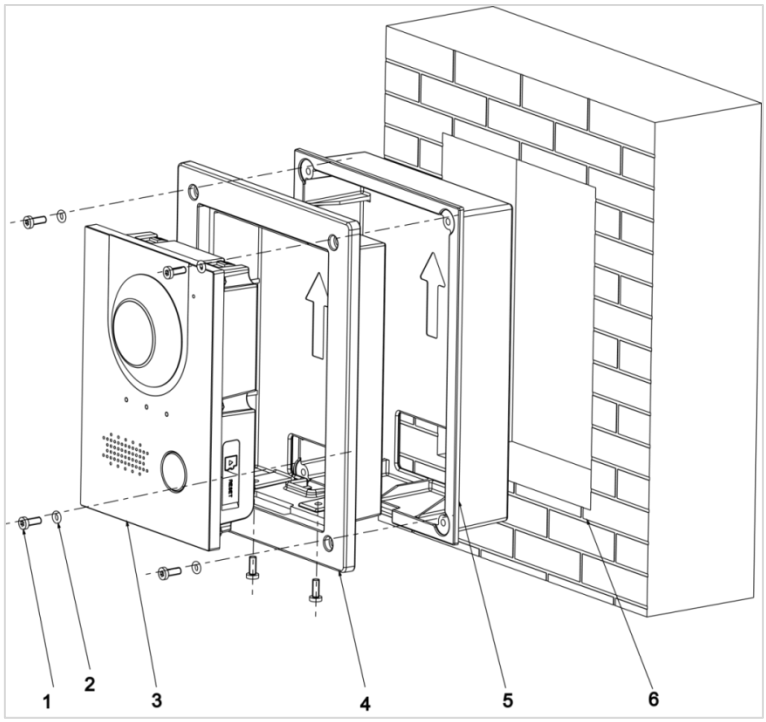


Table 2-2 Names of numbers (2)

No.	Name
1	M3×8 Screw
2	Waterproof ring
3	VTO
4	Front box of flush mount box
5	Rear box of flush mount box
6	Wall

Step 1 Install the rear box in the wall.

Step 2 Install outdoor station (VTO) on the front box.

Step 3 Fix the outdoor station (VTO) to the front box by screwing two M3×8 screws into the outdoor station (VTO) from the bottom of the front box.

Step 4 Put the front box (with VTO) into the rear box.

Step 5 Put waterproof rings to the M3×8 screws.

Step 6 Screw four M3×8 screws (with waterproof ring) into the front box.

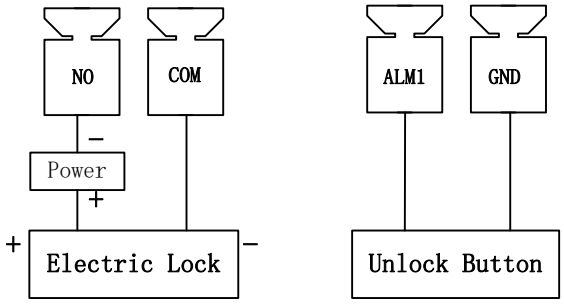
2.2 Electric Lock and Magnetic Door Lock

2.2.1 Electric Door Lock

When connect the outdoor station (VTO) to the electric door lock, connect the positive end of the electric door lock to the NO of the outdoor station (VTO), connect the negative end of the electric door lock to the public end.

When connect the outdoor station (VTO) to the on-off button, connect one end of the on-off button to one end of the on-off button of the outdoor station (VTO), and then connect the other end of the on-off button to the GND of outdoor station (VTO). See Figure 2-3.

Figure 2-3 Electric door lock connection

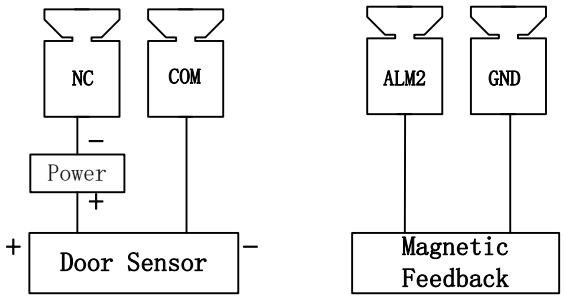


2.2.2 Magnetic Door Lock

When connect the outdoor station (VTO) to the magnetic door lock, connect the positive end of the magnetic door lock to the NC of the outdoor station (VTO), connect the negative end of the magnetic door lock to the public end.

When connect the outdoor station (VTO) to the magnetic door lock feedback, connect one end of the feedback to one end of the feedback of the outdoor station (VTO), and then connect the other end of the feedback to the GND of outdoor station (VTO). See Figure 2-4.

Figure 2-4 Magnetic door lock connection



2.3 Indoor Monitor (VTH) Installation

2.3.1 Installing with 86 Box

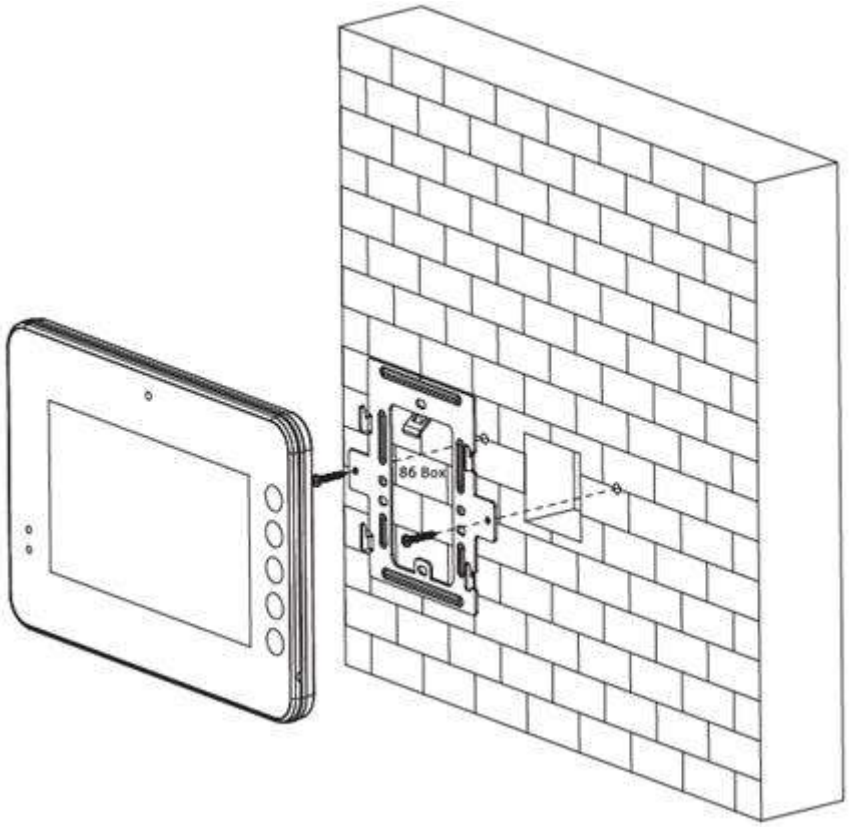
Install the device with 86 box, which is suitable for all types of devices. Take "VTH1560B/BW" for example.

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

Step 2 Fix installation bracket on the 86 box with screws.

Step 3 Hang the indoor monitor (VTH) on the installation bracket.

Figure 2-5 Installing with 86 box



2.3.2 Installing with Desktop Bracket

Install the device with bracket on the desktop, which only applies to handset indoor monitor (VTH). Take “VTH5221E-H” for example.

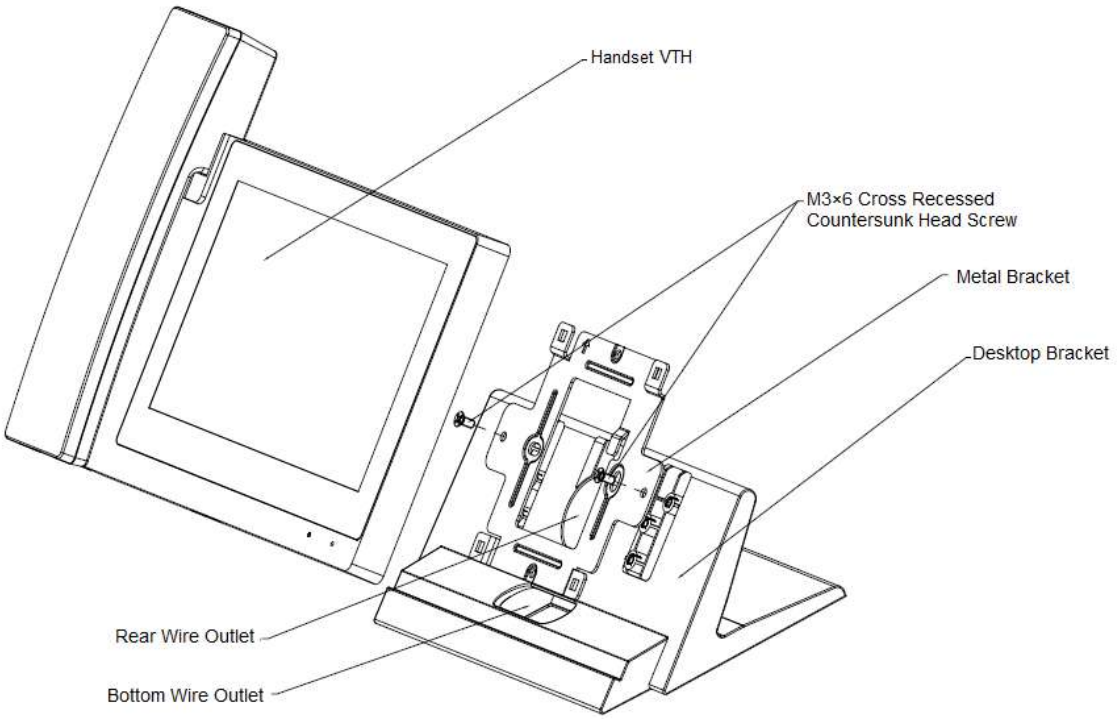
Step 1 With two M3×6 cross recessed countersunk head screws, tighten the metal bracket on the top two nuts of desktop bracket.

Step 2 Connect cables.

Step 3 Thread the cable through the rear cable outlet or bottom cable outlet.

Step 4 Hang the indoor monitor (VTH) on the metal bracket.

Figure 2-6 Installing with desktop bracket



2.4 Configuration

- Before configuration, check whether the following work has been completed or not.
- Check whether there is short circuit or open circuit. Power on the device only after the circuit is normal.
- IP addresses and No. of every outdoor station (VTO) and indoor monitor (VTH) have been planned.
- Scan QR code on the cover for details.

Set outdoor station (VTO) info and indoor monitor (VTH) info at web interface of every outdoor station (VTO), set indoor monitor (VTH) info, network info and outdoor station (VTO) info on every indoor monitor (VTH) so that video and voice communication can be realized.

2.4.1 Indoor Monitor (VTH) Settings

2.4.1.1 Initialization

When the indoor monitor (VTH) is used for the first time, you need to select a language that you prefer, initialize the indoor monitor (VTH) to get a password to enter project setting interface and an email to retrieve your password.

Step 1 Power on the device.

Welcome is displayed, and then the **Device Init** interface is displayed. See Figure 2-7.

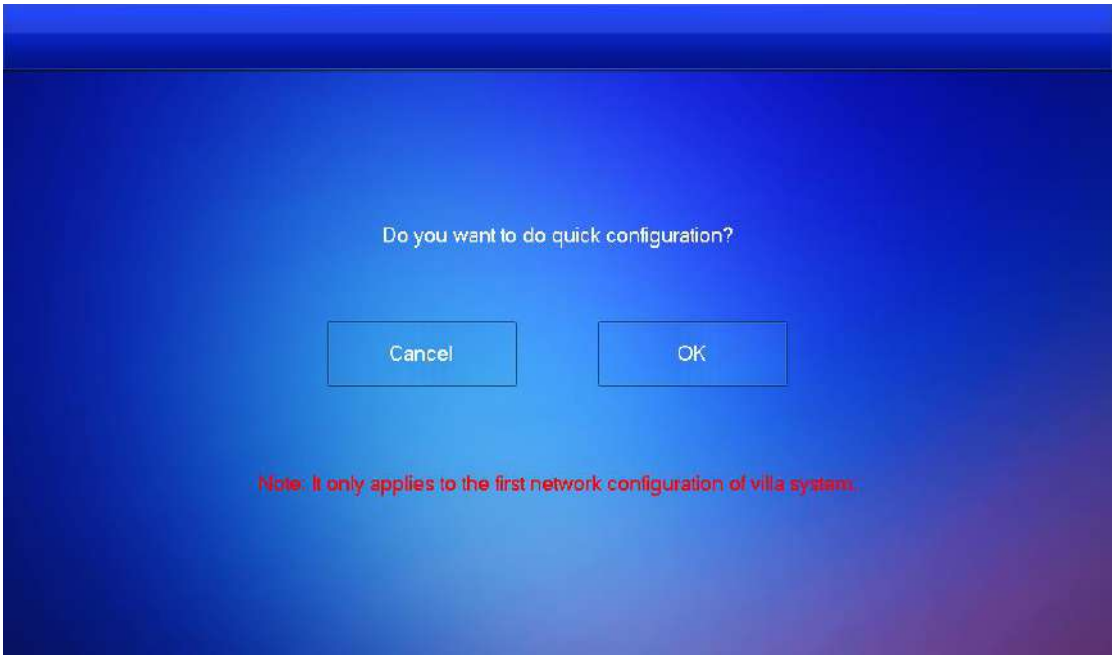
Figure 2-7 Device initialization

Step 2 Enter password, confirm Pwd, and email, and then press **OK**.
The indoor monitor (VTH) is initialized.

2.4.1.2 Quick Configuration

After the indoor monitor (VTH) is initialized, the message **Do you want to do quick configuration?** appears. See Figure 2-8.

Figure 2-8 Select quick configuration or not



Step 1 Tap **OK**.
All video intercoms and voice intercoms in the network will be displayed automatically. See Figure 2-9.

Tap **Cancel**, you need to configure parameters for the indoor monitor (VTH) according to your needs.

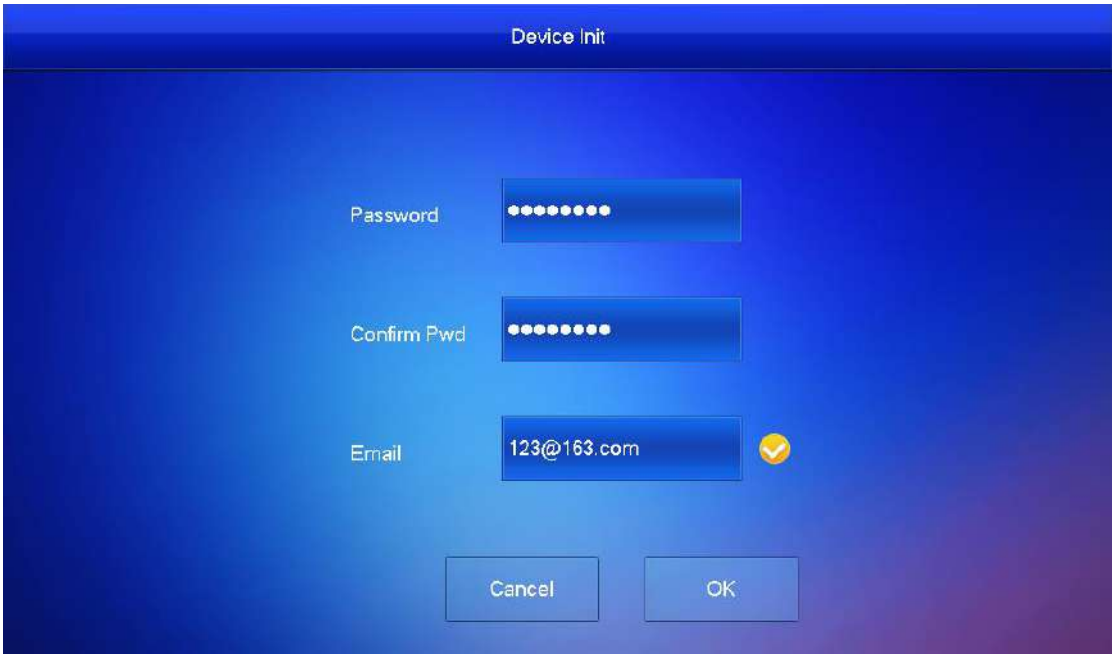
Figure 2-9 All intercoms displayed

Step 2 Select an uninitialized device.

The **Device Init** interface is displayed. See Figure 2-10.

- Initialization of all intercoms must be done on the indoor monitor (VTH); otherwise the quick configuration might fail.
- If no device is uninitialized, tap **Next** to go to the configuration interface. See Figure 2-11.

Figure 2-10 Device Init



Step 3 Enter password, confirm password, and email for the device you are to initialize.

Step 4 Tap **OK**.

The intercom list interface is displayed again. See Figure 2-11.

After intercoms need initialization have been initialized, click **Next** on Figure 2-9, the configuration interface will be displayed. See Figure 2-11.

Figure 2-11 Configuration interface

Step 5 Tap **Edit** behind each device to do configurations.

- Configure main VTH and Sub-VTH. There must be only one main VTH and one or more sub VTHs.

If there are no sub VTHs, then you do not need to do sub VTH configurations.

1) Select an indoor monitor (VTH).
   The **VTH Config** interface is displayed. See Figure 2-12.

Figure 2-12 Indoor Monitor (VTH) config

2) Select **Main** or **Sub**.
3) Enter local IP, Network, and gateway.
4) Tap **OK**.

The VTH configuration is completed.

- Configure Main outdoor stations (VTO) and sub outdoor stations (VTO). There must be only one main outdoor stations (VTO) and one or more sub outdoor stations (VTO).

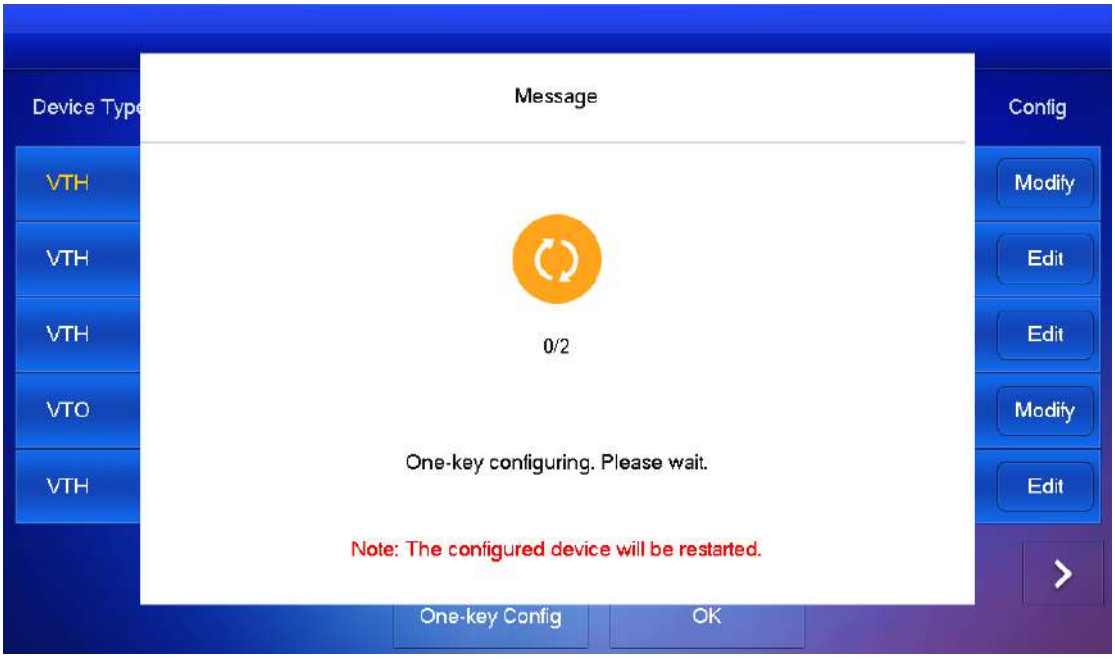
  If there are no sub outdoor stations (VTO), then you do not need to do sub outdoor stations (VTO) configurations.

1) Select an outdoor station (VTO).
   The **VTO Config** interface is displayed. See Figure 2-13.

Figure 2-13 VTO config

2) Select **Main** or **Sub**.
   Enter local IP, Network, gateway; select video standard, date format, time format; set date and time.
3) Tap **OK**.
   The **Configuration** interface is displayed. See Figure 2-14.

Figure 2-14 Making the configuration effective



4) Click **One-key Config**.
The VTO configuration is completed.

2.4.2 Outdoor Stations (VTO) Settings

Indoor stations (VTH) and outdoor stations (VTO) are always used together so you need to configure outdoor stations (VTO) parameters in advance to ensure the communication between indoor stations (VTH) and outdoor stations (VTO). For configuration of outdoor station (VTO) and indoor station (VTH), see their quick start guide.

2.5 Function Verification

2.5.1 Calling Indoor Monitors (VTH) from Outdoor Stations (VTO)

Dial indoor monitor (VTH) room No. (such as 101) at outdoor station (VTO) to call indoor monitor (VTH). The monitoring image and operating icons are displayed, see Figure 2-15. It represents successful debugging.

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

Figure 2-15 Calling VTHs from VTOs

2.5.2 Watching Monitoring Videos at Indoor Monitors (VTH)

You can watch monitor places where outdoor station (VTO), fence station or IPC are installed. Here outdoor station (VTO) will be taken as an example.

Step 1 Select **Monitor > Door**.

The **Door** interface is displayed. See Figure 2-16.

Step 2 Select an outdoor station (VTO) to watch monitoring videos. See Figure 2-17.

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

Figure 2-16 Door

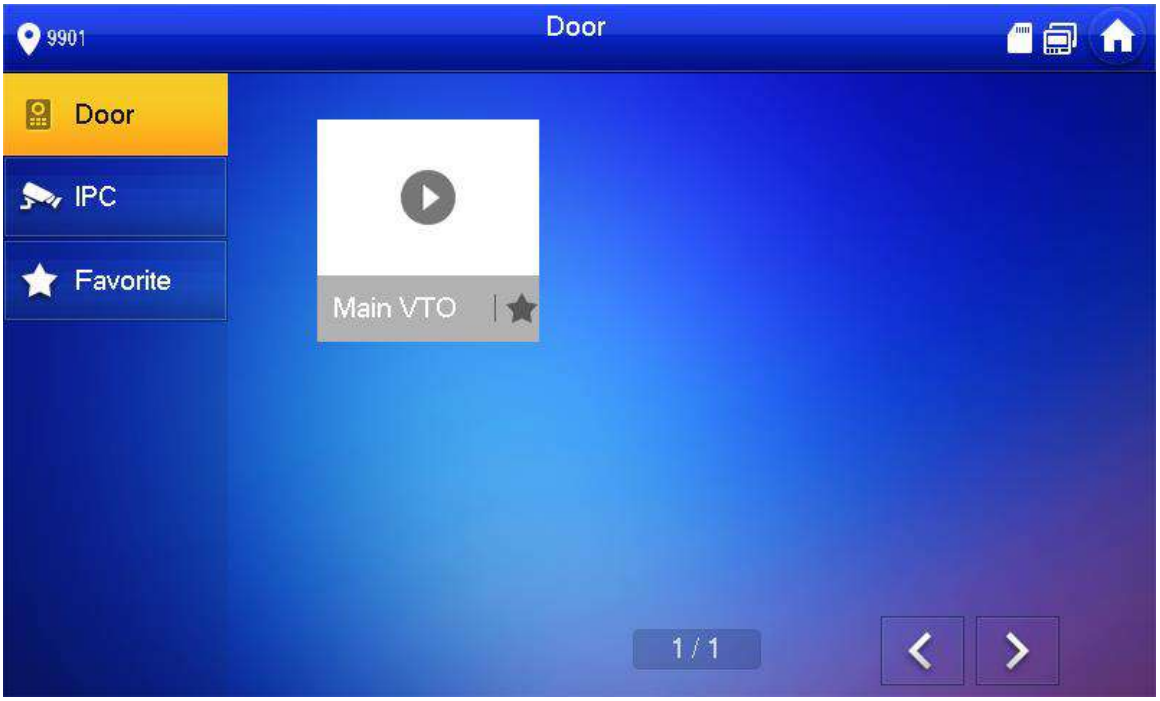
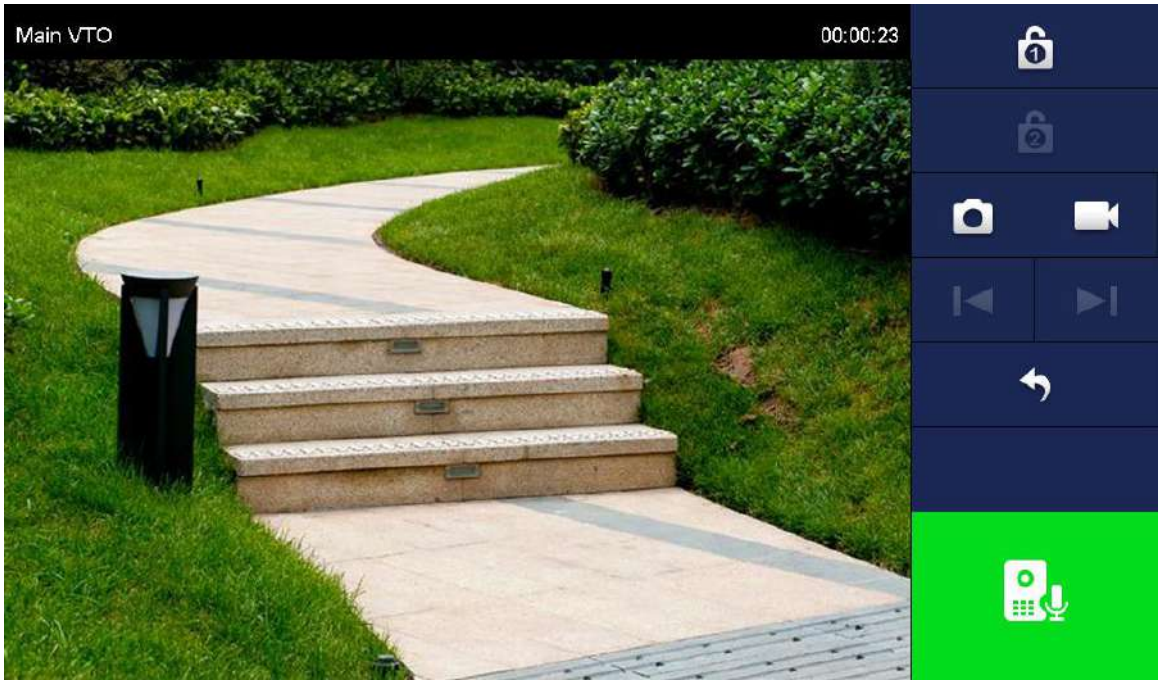


Figure 2-17 Monitoring video



3 Connecting Mobile Phone App

You can download the mobile phone app, and then add your villa outdoor monitor (VTO) to the app. When someone is calling you from the villa outdoor monitor (VTO), there will be push message on your phone, and you can talk to the visitor or unlock the door remotely on your phone.

Step 1 Scan the following QR code to download and install the app.

Figure 3-1 QR code

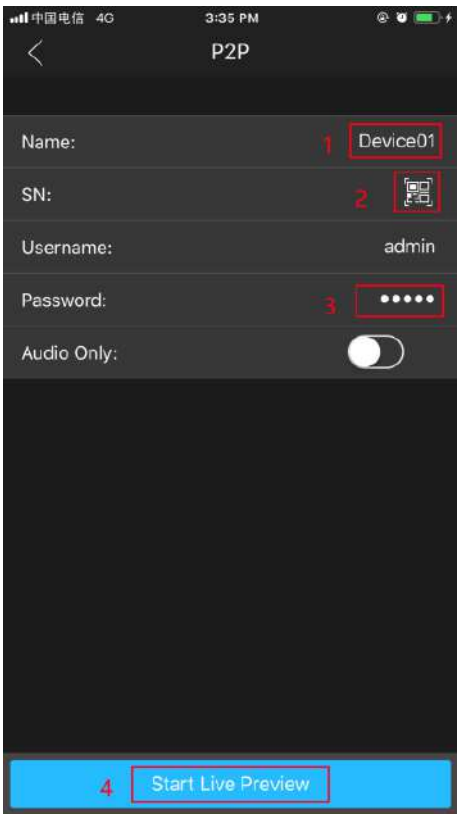
Step 2 Run the app, and then select **DOOR** on the home page. See Figure 3-2.

Figure 3-2 Home page

Step 3 Tap the "+" sign to add device, and the tap **Add Device > P2P**.

The **P2P** interface is displayed. See Figure 3-3.

Figure 3-3 P2P

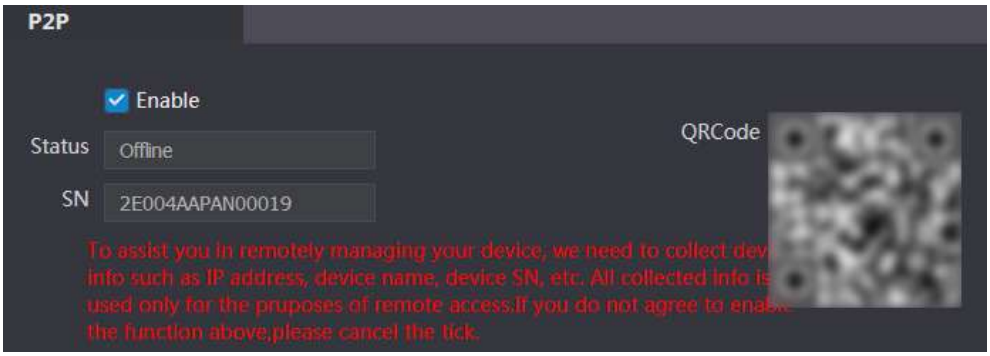


Step 4 Name your target outdoor monitor (VTO), and then tap the sign.
The mobile phone starts to scan.

Step 5 Log in to the web interface of the outdoor monitor (VTO) you need to add, and then select **Network**.
The **P2P** interface is displayed. See Figure 3-4.

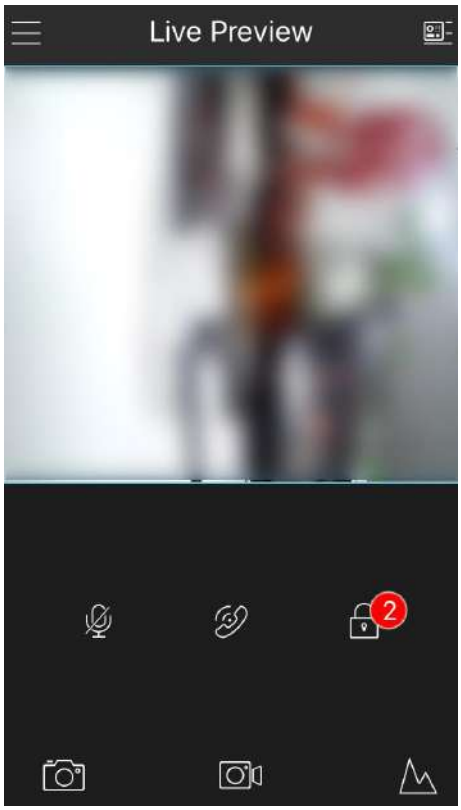
For VTO3211D, select **Household Setting > Room No. Management** to get the QR code.

Figure 3-4 P2P



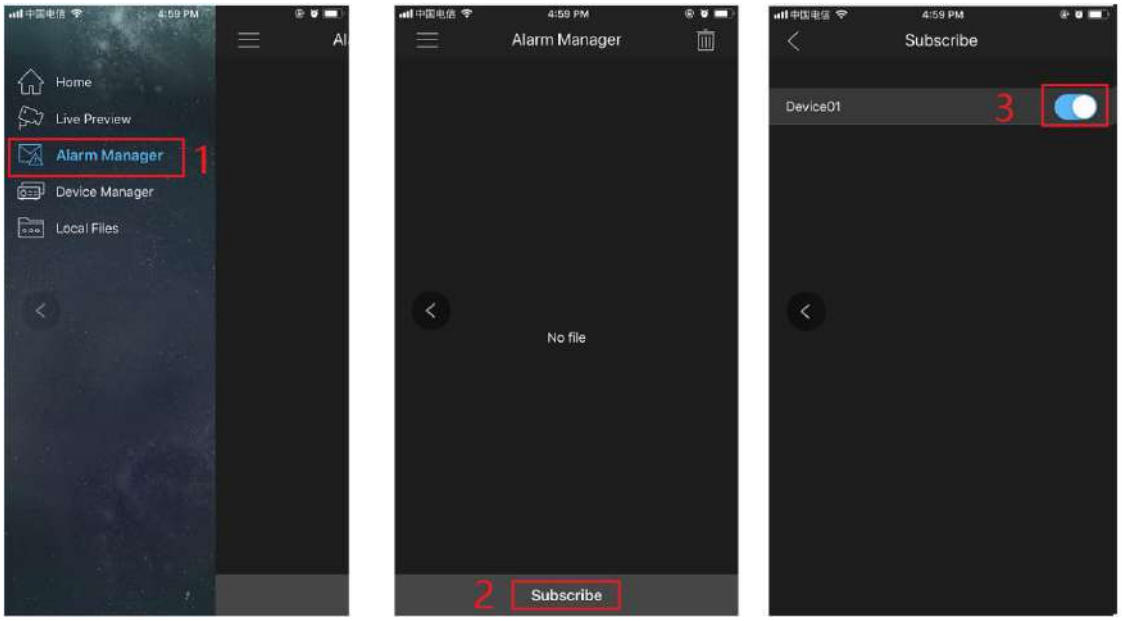
Step 6 Scan the QR code with your phone, then enter the user name and password of its web interface, and then tap **Start Live Preview**.
The live video is displayed. And you can also start audio intercom or unlock the door. See Figure 3-5.

Figure 3-5 Live



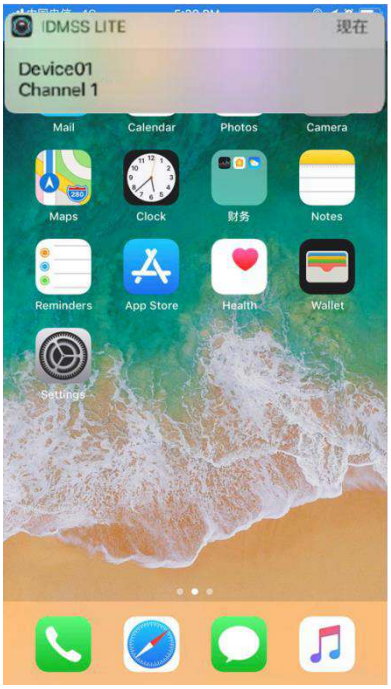
Step 7 Tap **Alarm Manager > Subscribe**, and then subscribe the outdoor monitor (VTO) you need. See Figure 3-6.

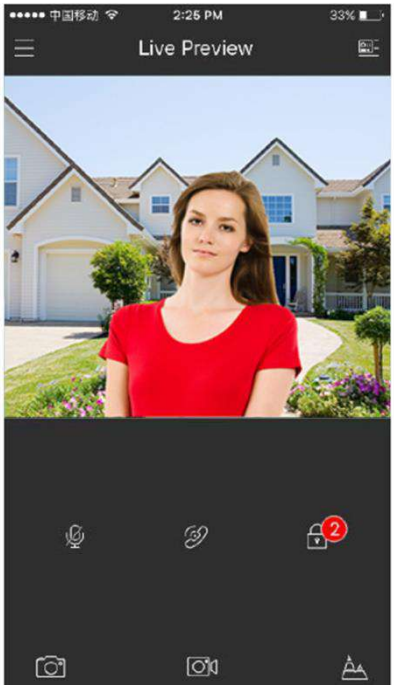
Figure 3-6 Subscribe



When someone is calling you from the subscribed villa outdoor monitor (VTO), there will be push message on your phone. See Figure 3-7.

Figure 3-7 Push





Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit web service through a secure communication channel.

7. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. **Disable Unnecessary Services and Choose Secure Modes**

    If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

    If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

    - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
    - SMTP: Choose TLS to access mailbox server.
    - FTP: Choose SFTP, and set up strong passwords.
    - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

11. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. **Network Log**

    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.