VTO2202F (Version 1.0)

Quick Start Guide

V1.0.0

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. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

Regulatory Information

The regulatory information herein might vary according to the model you purchased. Some information is only applicable for the country or region where the product is sold.

FCC Information

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC conditions:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC compliance:

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication.

- For class A device, these limits are designed to provide reasonable protection against harmful interference in a commercial environment. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
- For class B device, these limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna.
  - Increase the separation between the equipment and receiver.
  - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
  - Consult the dealer or an experienced radio/TV technician for help.

Foreword

General

This Guide introduces the structure, mounting process, and basic configuration of the device.

Safety Instructions

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

Signal Words	Meaning
 **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.
 **NOTE**	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Date
1	V1.0.0	First release	April, 2019

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 Guide

- The Guide is for reference only. If there is inconsistency between the Guide 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 Guide.
- The Guide 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 Guide. 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 Guide 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

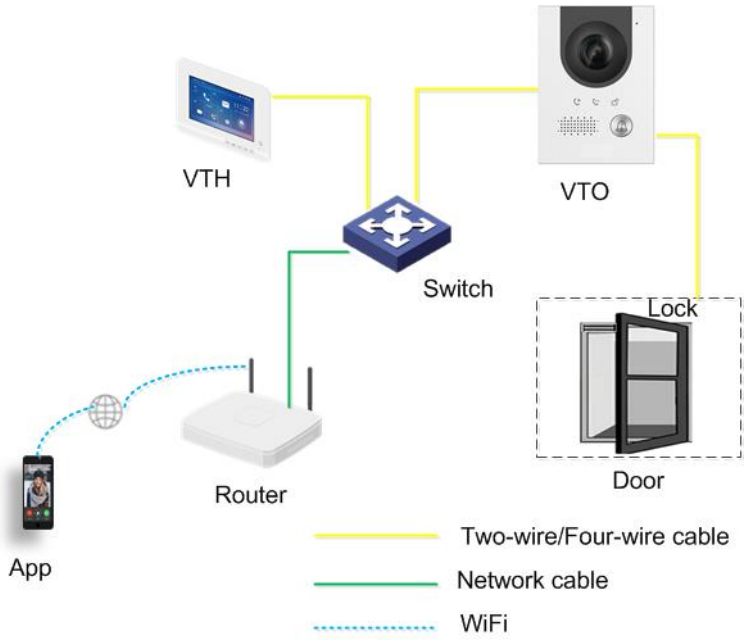
- Please don’t place and install the device in an area exposed to direct sunlight or near heat generating device.
- Please don’t install the device in a humid, dusty or fuliginous area.
- Please keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Please don’t 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 Network Diagram



2 Appearance

2.1 Front Panel

Figure 2-1 Front panel

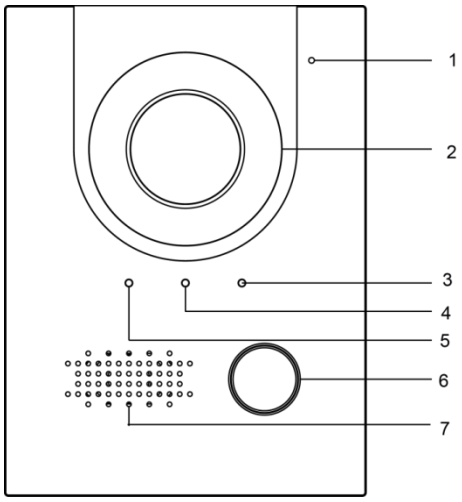


Table 2-1 Front panel description

No.	Name	Description
1	MIC	Inputs audio.
2	Camera	Monitors door area.
3	Indicator	When you are calling, this indicator will be on.
4	Indicator	During the call communication, this indicator will be on.
5	Indicator	When the door is unlocked, this indicator will be on.
6	Call button	Press to call VTH or the management center.
7	Speaker	Outputs audio.

2.2 Rear Panel

Figure 2-2 Rear panel

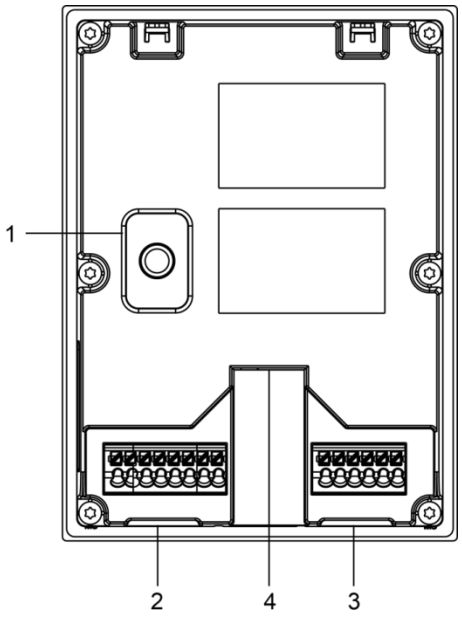


Table 2-2 Rear panel description

Name	NO	Description
Tamper switch	1	The 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 VTO whose models end with “P” support PoE.

3 Installation

3.1 Installation Requirement

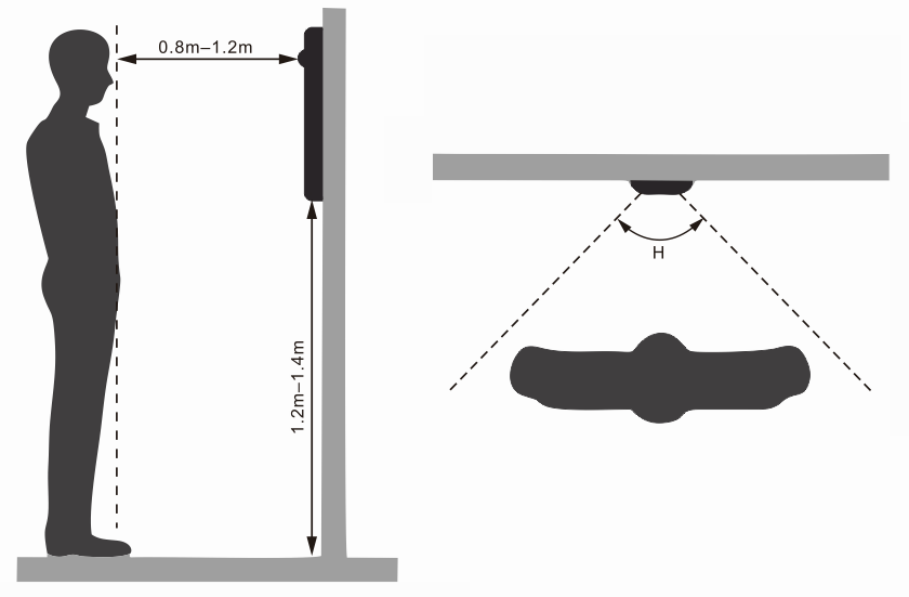
3.1.1 Notice

- Do not install the VTO to places with condensation, high temperature, grease or dust, chemical corrosion, direct sunlight, or zero shelter.
- The installation and adjustment must be finished by professional crew, and do not disassemble the VTO.

3.1.2 Guidance

See Figure 3-1 for the reference of the installation position. The VTO horizontal angle of view varies with different model, try to face the center of the VTO as much as possible.

Figure 3-1 Installation position reference



3.2 Installing Process

The VTO can be installed on the wall or in the wall.

3.2.1 Installed on the Wall

Step 1 With the help of installation diagram, hammer four expansion screws into the wall.

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

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

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

Step 5 Put the VTO into the mounting box.

Step 6 Fix the VTO to the mounting box by screwing two M3×8 screws from the bottom of the mounting box.

Figure 3-2 Installed on the wall

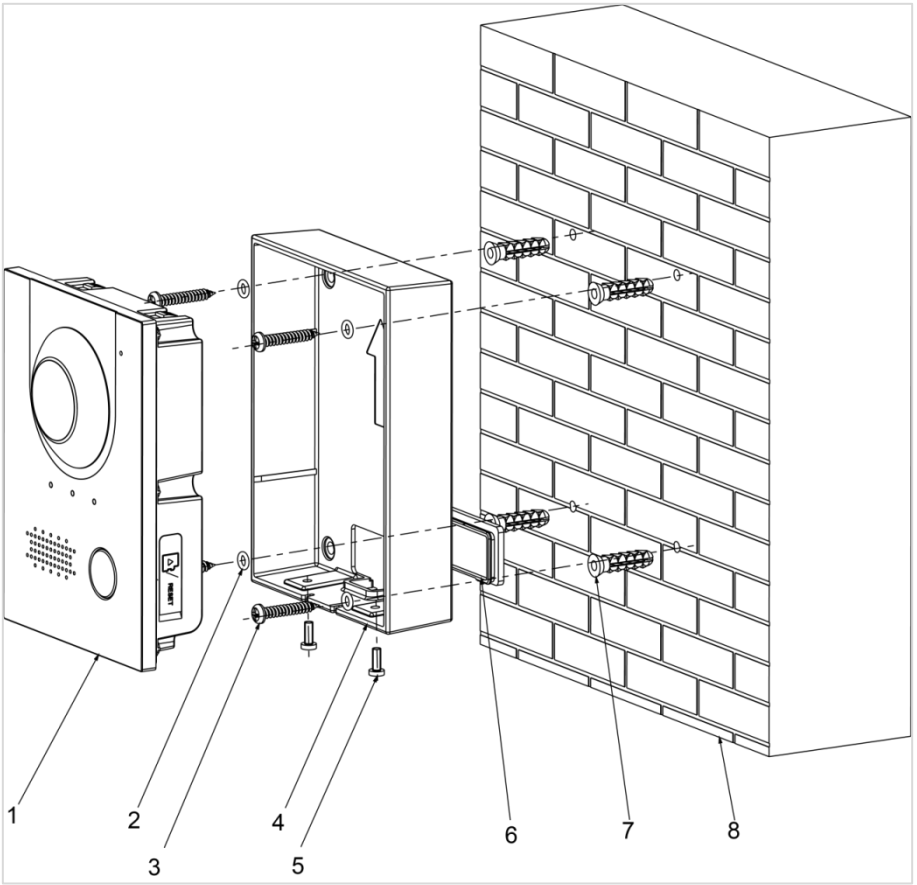


Table 3-1 Names of numbers (1)

No.	Name
1	VTO
2	Waterproof ring
3	ST4×25 self-tapping screw
4	Mounting box
5	M3×8 Screw
6	Waterproof silica gel pad
7	Expansion screw
8	Wall

3.2.2 Installed in the Wall

Step 1 Install the mounting box rear cover in the wall.

Step 2 Install VTO on the mounting box front cover.

Step 3 Fix the VTO to the mounting box front cover by screwing two M3×8 screws into the VTO from the bottom of the mounting box front cover.

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

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

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

Figure 3-3 Installed in the Wall

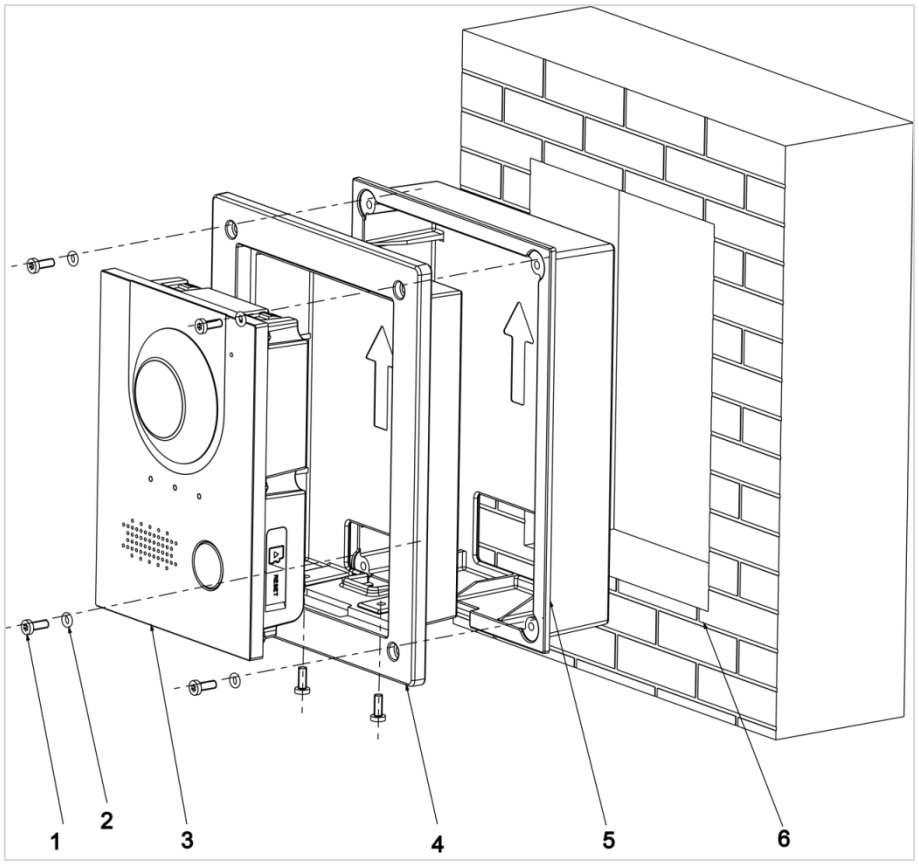


Table 3-2 Names of numbers (2)

No.	Name
1	M3×8 Screw
2	Waterproof ring
3	VTO
4	Mounting box front box
5	Mounting box rear box
6	Wall

4 Configuration

This chapter introduces how to initialize, connect, and make primary configurations to the VTO and VTH devices to realize basic functions, including device management, calling, and monitoring. For more detailed configuration, see the user's Manual.

4.1 Configuration Process

Before configuration, check every device and make sure there is no short circuit or open circuit in the circuits.

Step 1 Plan IP address for every device, and also plan the unit number and room number you need.

Step 2 Configure VTO. See "4.3 Configuring VTO."

1) Initialize VTO. See "4.3.1 Initialization."
2) Configure VTO number. See "4.3.2 Configuring VTO Number."
3) Configure VTO network parameters. See "4.3.3 Configuring Network Parameters."
4) Configure SIP Server. See "4.3.4 Configuring SIP Server."
5) Configure target room number and group call. See "4.3.5 Configuring Call No. and Group Call."
6) Add VTO devices to the SIP server. See "4.3.6 Adding VTO Devices."
7) Add room number to the SIP server. See "4.3.7 Adding Room Number."

Step 3 Configure VTH. See the VTH users' manual.

Step 4 Verify Configuration. See "4.4 Verifying Configuration."

4.2 Config Tool

You can download the "ConfigTool" and perform device initialization, IP address modification and system upgrading for multiple devices at the same time. For the detailed information, see the corresponding user's manual.

4.3 Configuring VTO

Connect the VTO to your PC with network cable, and for first time login, you need to create a new password for the web interface.

4.3.1 Initialization

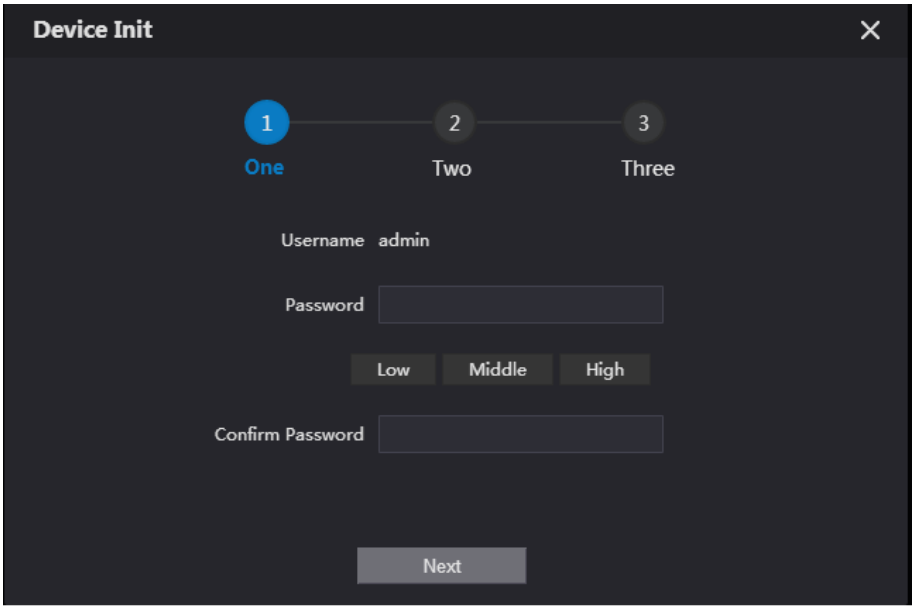
The default IP address of VTO is 192.168.1.110, and make sure the PC is in the same network segment as the VTO.

Step 1 Connect the VTO to power source, and then boot it up.

Step 2 Open the internet browser on the PC, then enter the default IP address of the VTO in the address bar, and then press Enter.

The **Device Init** interface is displayed. See Figure 4-1.

Figure 4-1 Device initialization



Step 3 Enter and confirm the password, and then click **Next**.

The Email setting interface is displayed.

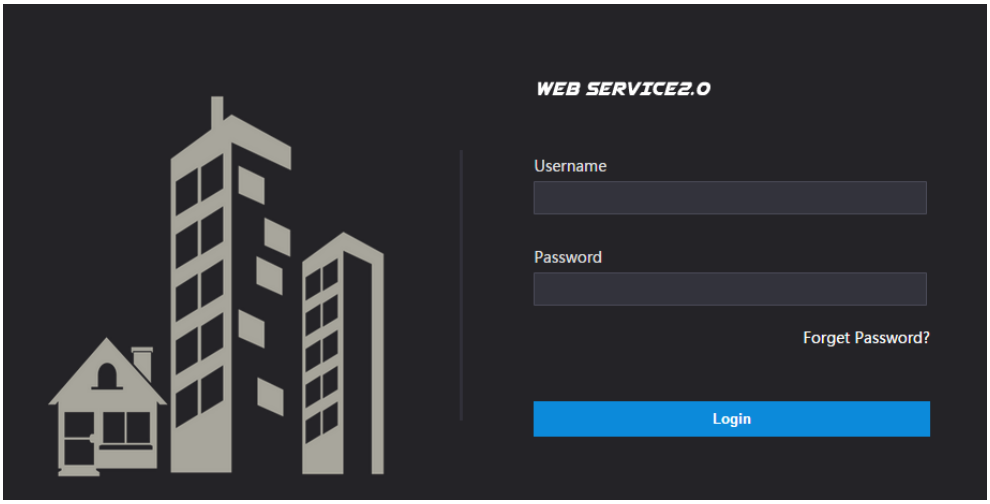
Step 4 Select the **Email** check box, and then enter your Email address. This Email address can be used to reset the password, and it is recommended to finish this setting.

Step 5 Click **Next**. The initialization succeeded.

Step 6 Click **OK**.

The login interface is displayed. See Figure 4-2.

Figure 4-2 Login interface



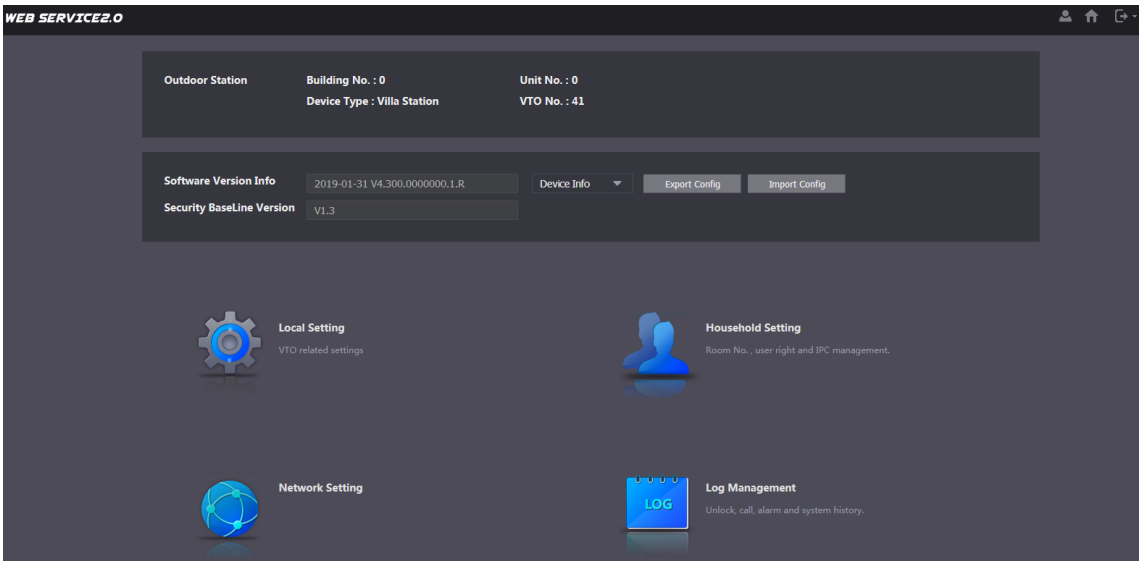
4.3.2 Configuring VTO Number

The VTO number can be used to differentiate each VTO, and it is normally configured according to unit or building number.

- You can change the number of a VTO when it is not working as SIP server.
- The VTO number can contain 5 numbers at most, and it cannot be the same as any room number.

Step 1 Log in the web interface of the VTO, and then the main interface is displayed. See Figure 4-3.

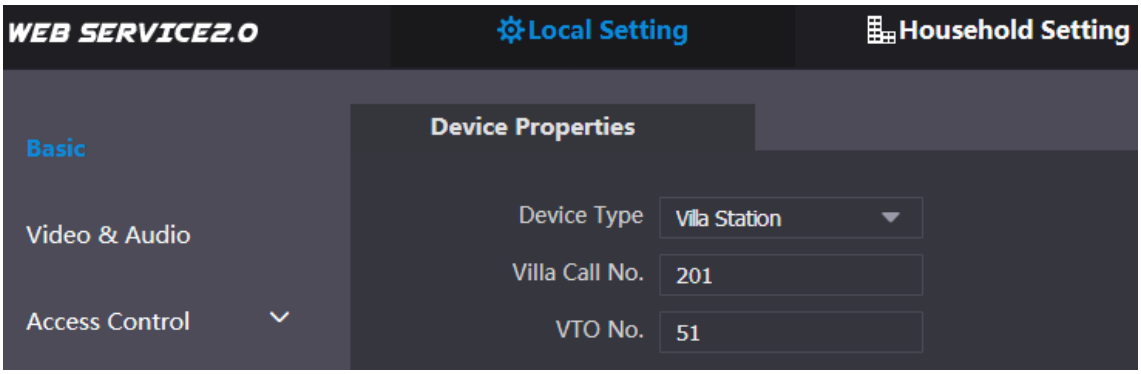
Figure 4-3 Main interface



Step 2 Select Local Setting > Basic.

The device properties are displayed. See Figure 4-4.

Figure 4-4 Device properties



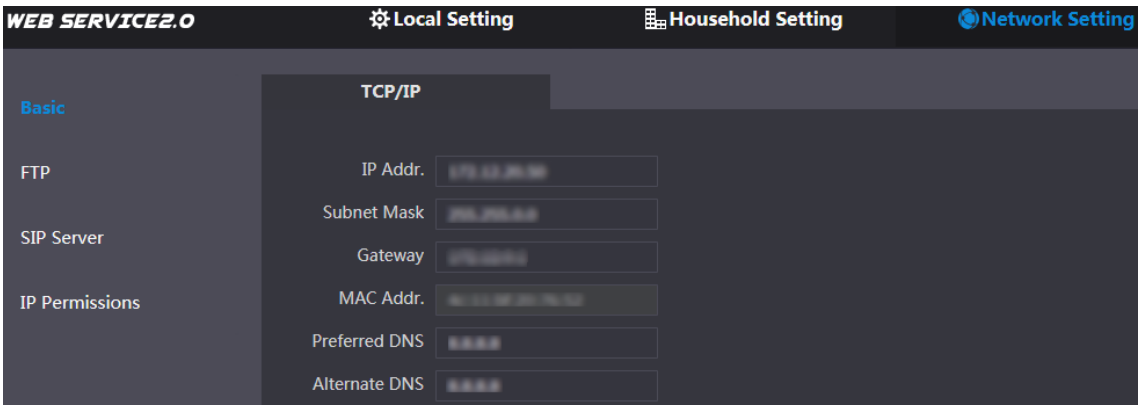
Step 3 In the **VTO No.** input box, enter the VTO number you planned for this VTO, and then click **Confirm** to save.

4.3.3 Configuring Network Parameters

Step 1 Select Network Setting > Basic.

The **TCP/IP** information is displayed. See Figure 4-5.

Figure 4-5 TCP/IP information



Step 2 Enter the network parameters you planed, and then click **Save**.

The VTO will reboot, and you need to modify the IP address of your PC to the same network segment as the VTO to log in again.

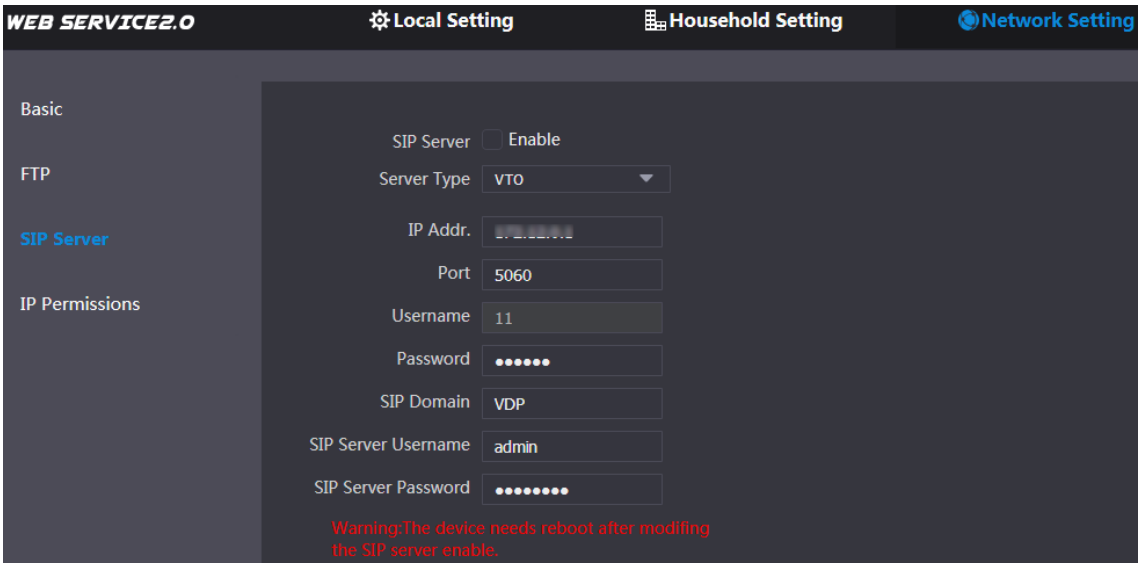
4.3.4 Configuring SIP Server

The SIP server is required in the network to transmit intercom protocol, and then all the VTO and VTH devices connected to the same SIP server can make video call between each other. You can use VTO device or other servers as SIP server.

Step 1 Select Network Setting > SIP Server.

The **SIP Server** interface is displayed. See Figure 4-6.

Figure 4-6 SIP server



Step 2 Select the server type you need.

- If the VTO you are visiting works as SIP server

  Select the **Enable** check box at **SIP Server**, and then click **Save**.

  The VTO will reboot, and after rebooting, you can then add VTO and VTH devices to this VTO. See "4.3.6 Adding VTO Devices and 4.3.7 Adding Room Number."

If the VTO you are visiting does not work as SIP server, do not select the **Enable** check box at **SIP Server**, otherwise the connection will fail.

- If other VTO works as SIP server

  Select **VTO** in the **Server Type** list, and then configure the parameters. See Table 4-1.

Table 4-1 SIP server configuration

Parameter	Description
IP Addr.	The IP address of the VTO which works as SIP server.
Port	5060
Username	Keep the default value.
Password	
SIP Domain	VDP
SIP Server Username	The user name and password for the web interface of the SIP server.
SIP Server Password	

- If other servers work as SIP server
  Select the server type you need in the **Server Type** list, and then see the corresponding manual for the detailed configuration.

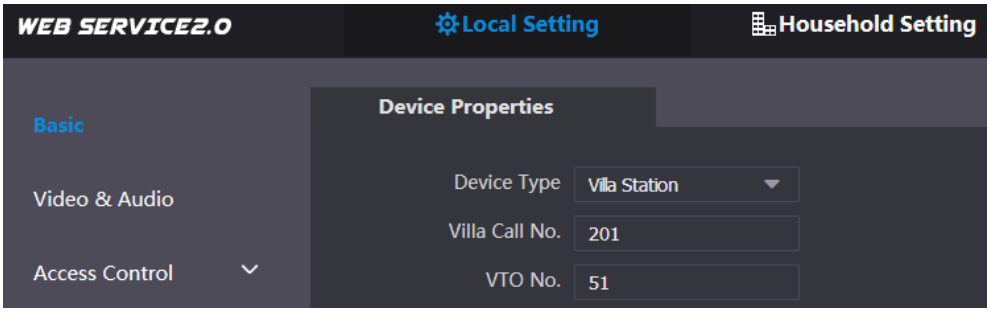
4.3.5 Configuring Call No. and Group Call

You need to configure call No. on every VTO, and then all the VTO will call the defined room when you press the call button. On the SIP server, you can enable group call function, and when calling a master VTH, the extension VTH devices receive the call as well.

Enabling or disabling group call function will erase all the added VTH, so you need to perform this operation before adding VTO and VTH.

Step 1 Select Local Setting > Basic.
The device properties are displayed. See Figure 4-7.

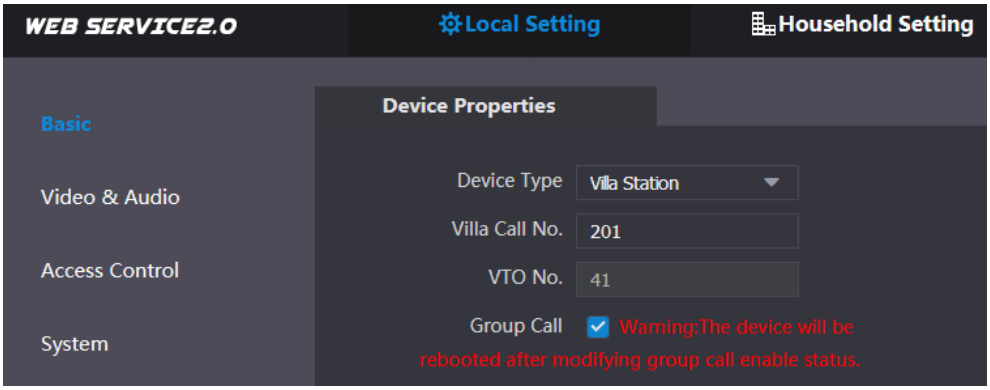
Figure 4-7 Device properties



Step 2 In the **Villa Call No.** input box, enter the room number you need to call, and then click **Confirm** to save. Repeat this operation on every villa VTO web interface.

Step 3 Log in the web interface of the SIP server, and then select **Local Setting > Basic**.
The device properties are displayed. See Figure 4-8.

Figure 4-8 SIP server device properties



Step 4 Select the **Group Call** check box, and then click **Confirm**.
The VTO will reboot, and when calling a master VTH, the extension VTH devices receive the call as well.

4.3.6 Adding VTO Devices

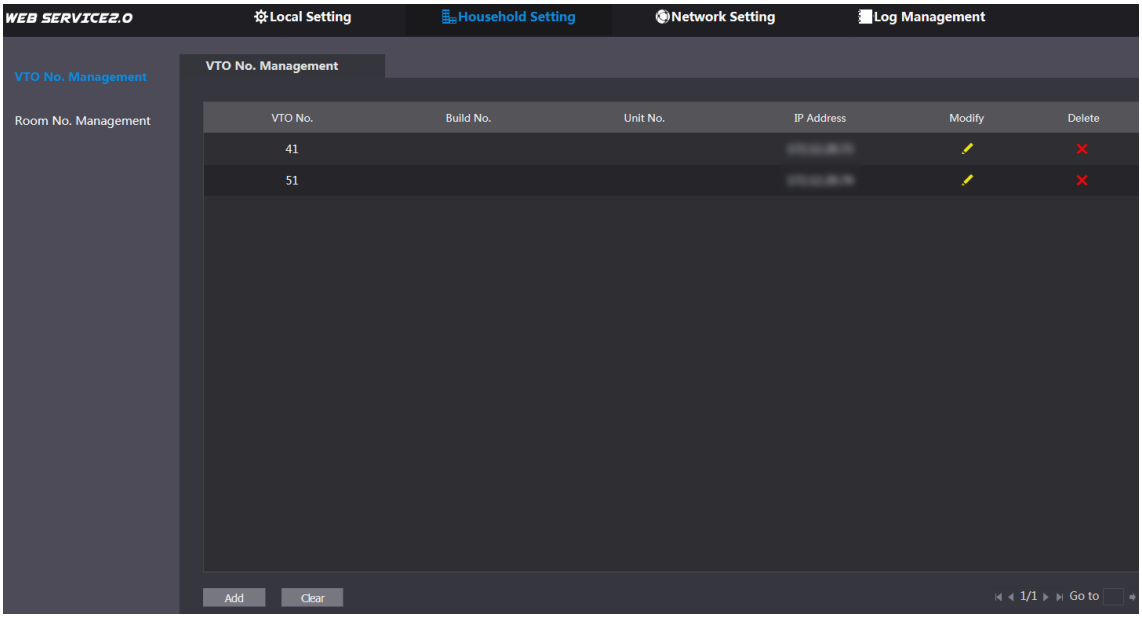
You can add VTO devices to the SIP server, and all the VTO devices connected to the same SIP server can make video call between each other. This section applies to the condition in

which a VTO device works as SIP server, and if you are using other servers as SIP server, see the corresponding manual for the detailed configuration.

Step 1 Log in the web interface of the SIP server, and then select **Household Setting > VTO No. Management**.

The **VTO No. Management** interface is displayed. See Figure 4-9.

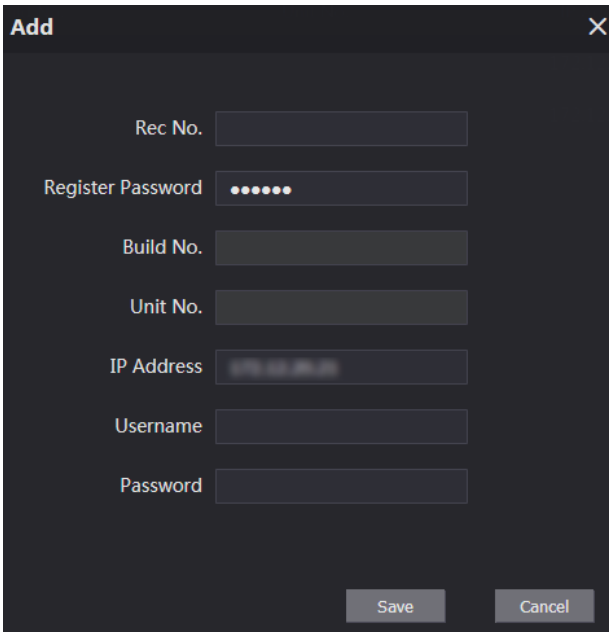
Figure 4-9 VTO No. management



Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 4-10.

Figure 4-10 Add VTO



Step 3 Configure the parameters, and be sure to add the SIP server itself too. See Table 4-2.

Table 4-2 Add VTO configuration

Parameter	Description
Rec No.	The VTO number you configured for the target VTO. See the details in "4.3.2 Configuring VTO Number."
Register Password	Keep default value.

Parameter	Description
Build No.	Available only when other servers work as SIP server.
Unit No.	
IP Address	The IP address of the target VTO.
Username	The user name and password for the web interface of the target VTO.
Password	

Step 4 Click **Save**.

4.3.7 Adding Room Number

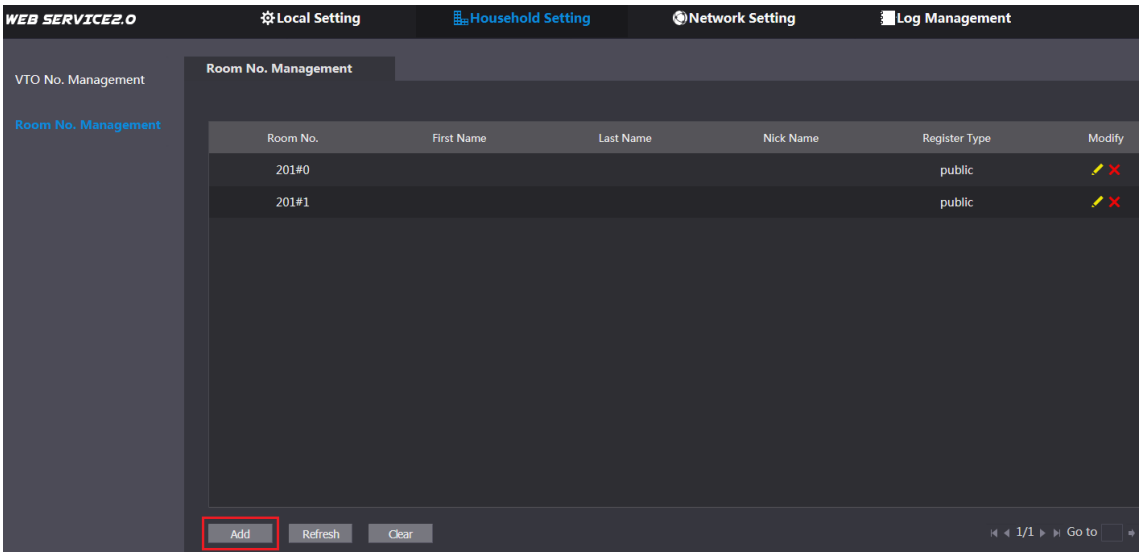
You can add the planned room number to the SIP server, and then configure the room number on VTH devices to connect them to the network. This section applies to the condition in which a VTO device works as SIP server, and if you use other servers as SIP server, see the corresponding manual for the detailed configuration.

The room number can contain 6 digits of numbers or letters or their combination at most, and it cannot be the same as any VTO number.

Step 1 Log in the web interface of the SIP server, and then select **Household Setting > Room No. Management**.

The **Room No. Management** interface is displayed. See Figure 4-11.

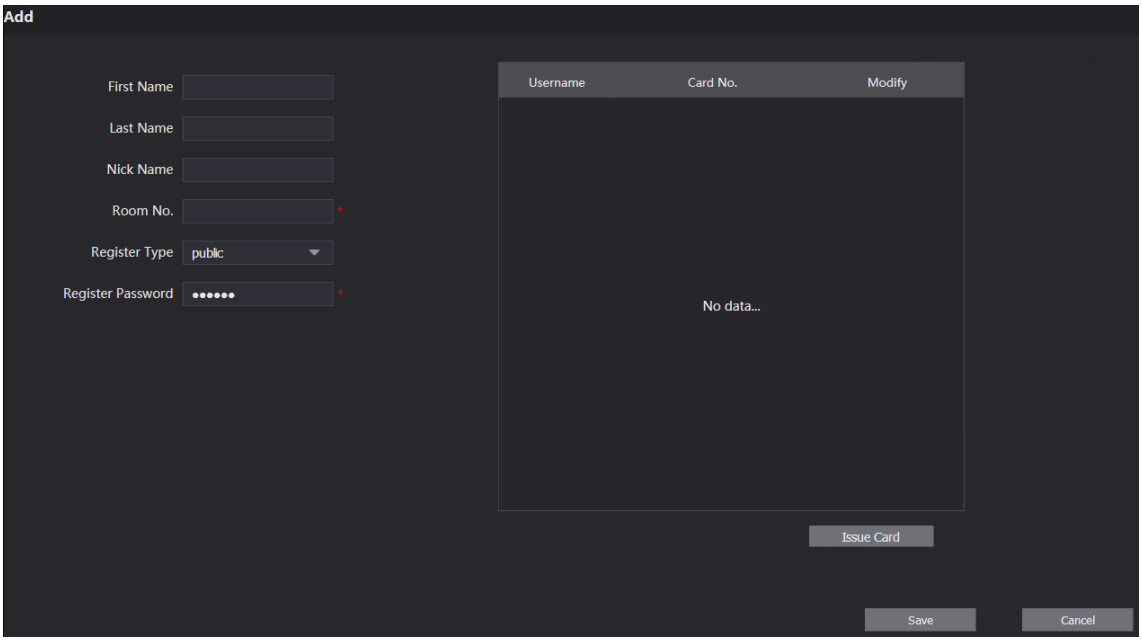
Figure 4-11 Room No. Management



Step 2 Click the **Add**. See Figure 4-11.

The **Add** interface is displayed. See Figure 4-12.

Figure 4-12 Add single room number



Step 3 Configure room information. See Table 4-3.

Table 4-3 Room information

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	
Nick Name	
Room No.	The room number you planned. ● If you use multiple VTH devices, the room number of the master VTH should be "room number#0", and the room number of the extension VTH should be "room number#1", "room number#2", and so on. ● You can have 9 extension VTH devices at most for one master VTH.
Register Type	Select **public**, and **local** is reserved for future use.
Register Password	Keep the default value.

Step 4 Click **Save**.

The added room number is displayed. Click to modify room information, and click to delete a room.

4.4 Verifying Configuration

4.4.1 Calling VTH from VTO

Press the call button on the VTO.

The VTO is calling the defined VTH. See Figure 4-13.

Figure 4-13 Call screen

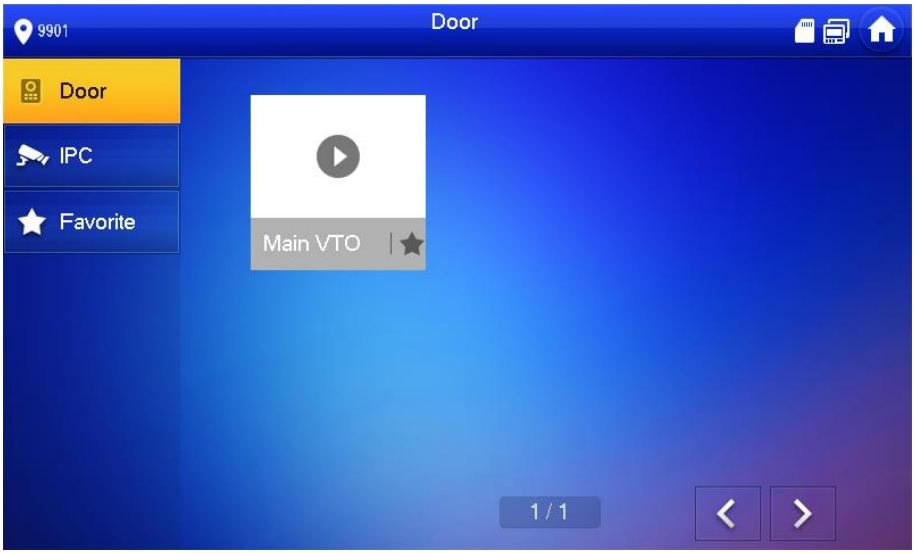
Tap  on the VTH to answer the call.

4.4.2 Doing Monitor from VTH

Step 1 In the main interface of the VTH, select **Monitor > Door**.

The **Door** interface is displayed. See Figure 4-14.

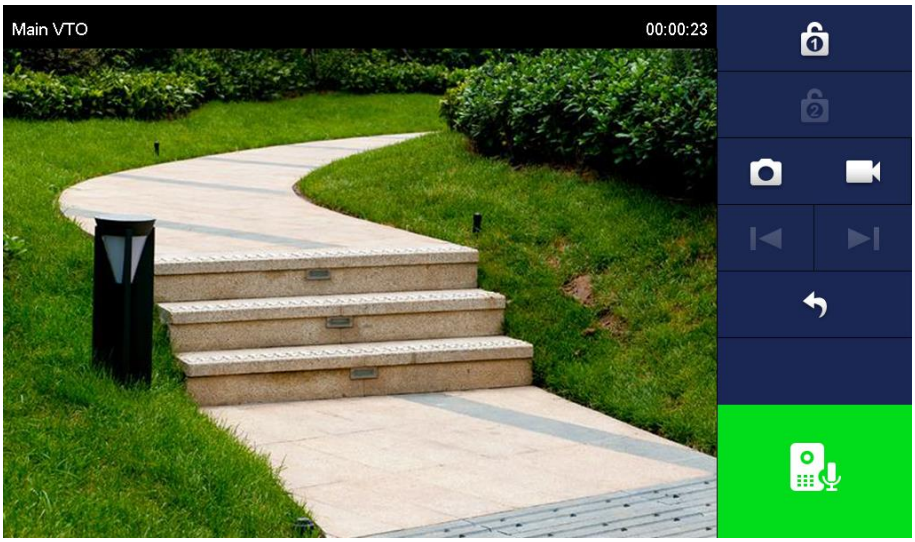
Figure 4-14 Door



Step 2 Select the VTO you need to do monitor.

The monitor screen is displayed. See Figure 4-15.

Figure 4-15 Monitor screen



5 Connecting Mobile Phone App

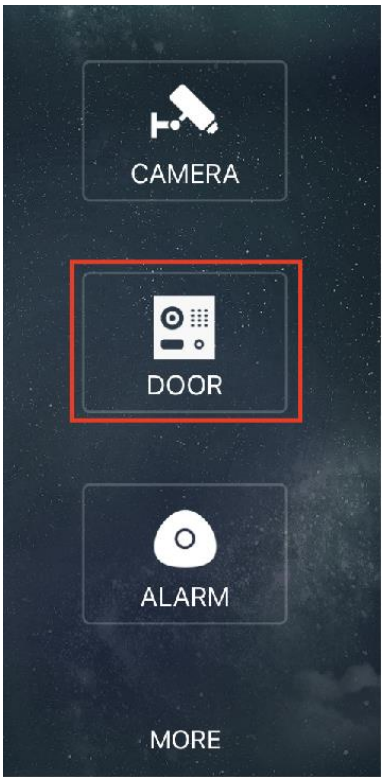
You can download the mobile phone app, and then add your villa VTO to the app. When someone is calling you from the villa VTO, there will be push message on your phone, and you can talk to the visitor or unlock the door remotely on your phone.

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

Figure 5-1 QR code

Step 2 Run the app, and then select **DOOR** on the home page. See Figure 5-2.

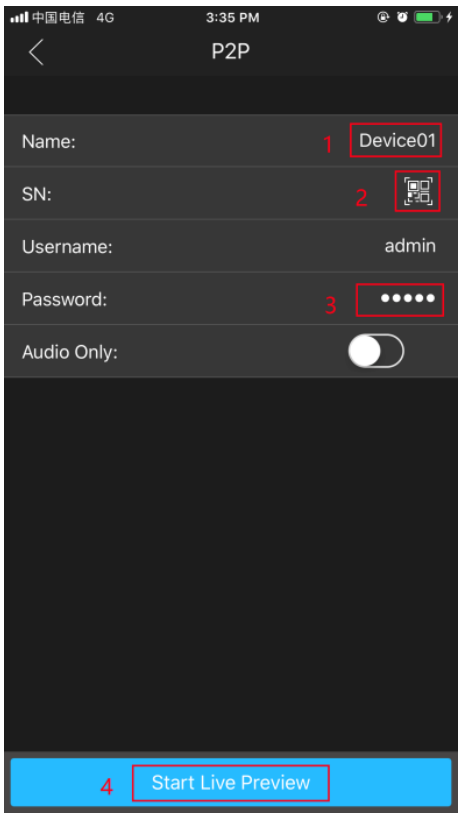
Figure 5-2 Home page



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

The **P2P** interface is displayed. See Figure 5-3.

Figure 5-3 P2P

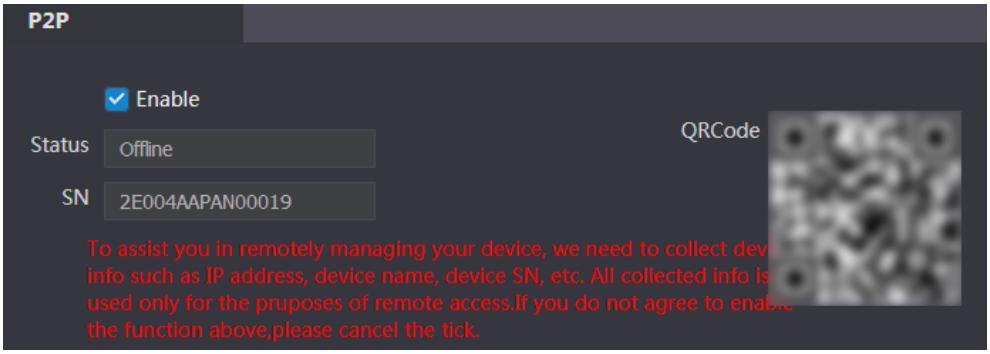


Step 4 Give a name to your target VTO, and then tap the  sign.
The mobile phone starts to scan.

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

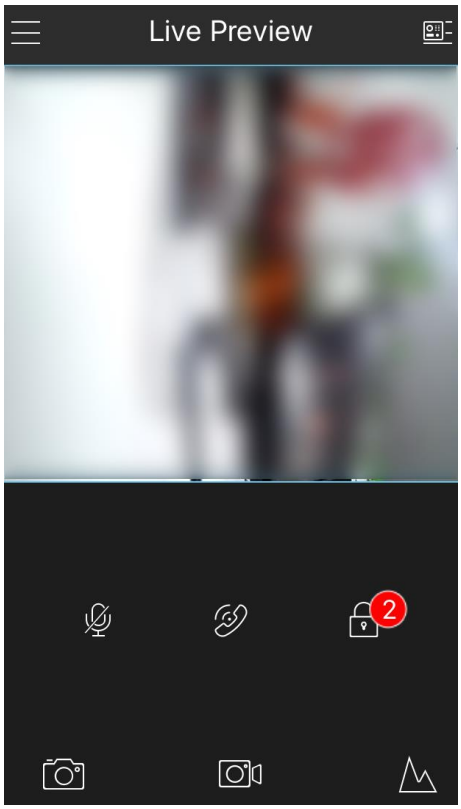
For VTO3211D, select **Household Setting > Room No. Management** to get the QR code.

Figure 5-4 P2P



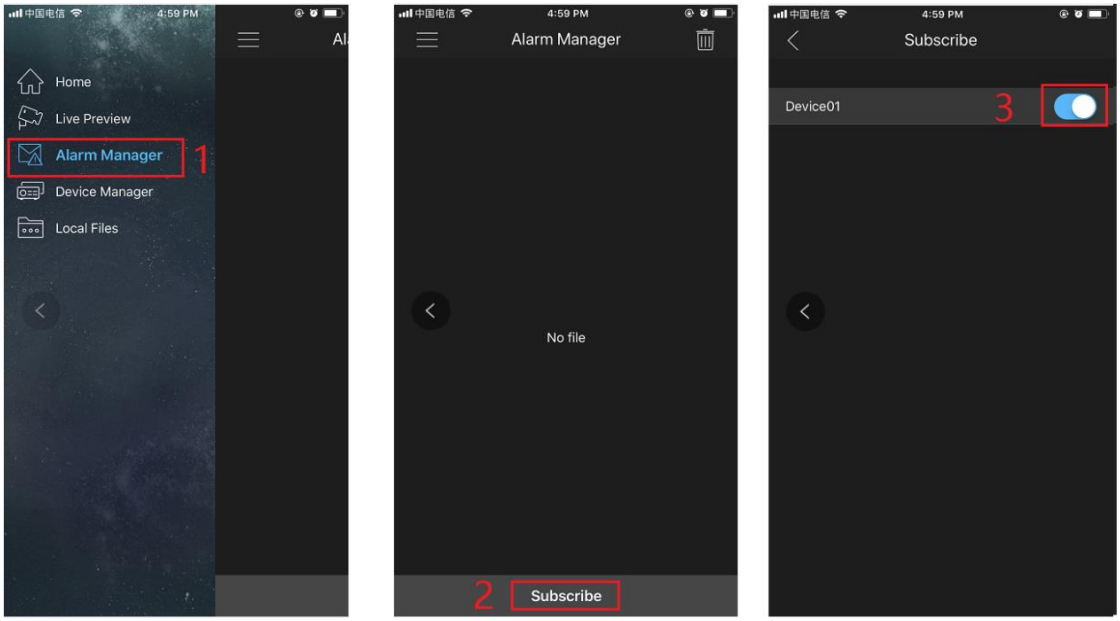
Step 6 Scan the QR code with your phone, then enter the user name and password of its web interface, and then tap **Start Live Preview**.
The live video is displayed. And you can also start audio intercom or unlock the door. See Figure 5-5.

Figure 5-5 Live



Step 7 Tap **Alarm Manager > Subscribe**, and then subscribe the VTO you need. See Figure 5-6.

Figure 5-6 Subscribe



When someone is calling you from the subscribed villa VTO, there will be push message on your phone. See Figure 5-7.

Figure 5-7 Push