Model F VTO
VTO6441F/VTO6421F

Quick Start Guide

V1.0.0

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

⚠ CAUTION

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 B devices, 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	November 2018

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

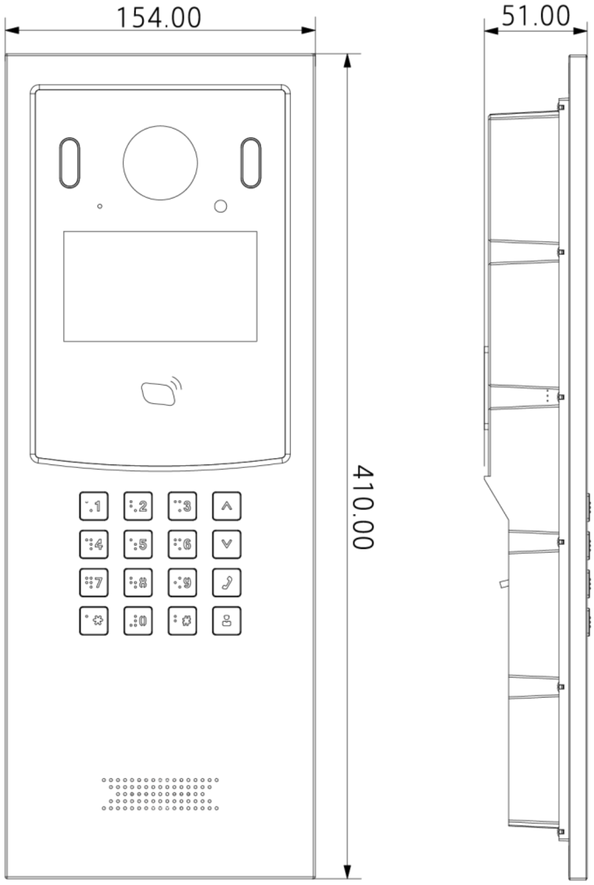
Regulatory Information II
Foreword III
Important Safeguards and Warnings V
1 Appearance 1
1.1 Dimension 1
1.2 Front Panel 2
1.3 Rear Panel 3
2 Installation 5
2.1 Installation Requirement 5
2.1.1 Notice 5
2.1.2 Guidance 5
2.2 Connecting Cable 5
2.2.1 Door Lock Port 5
2.2.2 RS-485 Port 7
2.2.3 Alarm I/O and Power Port 7
2.2.4 Wiegand Port 8
2.3 Installing VTO 9
3 Configuration 10
3.1 Configuration Process 10
3.2 Config Tool 10
3.3 Configuring VTO 10
3.3.1 Initialization 10
3.3.2 Configuring VTO Number 11
3.3.3 Configuring Network Parameters 12
3.3.4 Configuring SIP Server 13
3.3.5 Adding VTO Devices 14
3.3.6 Adding Room Number 15
3.4 Verifying Configuration 17
3.4.1 Calling VTH from VTO 17
3.4.2 Doing Monitor from VTH 17
4 Operating VTO 19
4.1 Call Function 19
4.1.1 Calling single VTH 19
4.1.2 Calling Multiple VTH Devices 19
4.1.3 Calling Management Center 19
4.2 Unlock Function 19
4.2.1 Unlock with Face Recognition 19
4.2.2 Unlock with Password 19
4.2.3 Unlock with IC Card 19
4.2.4 Unlock From VTH 20
4.2.5 Unlock From the Management Center 20

4.3 Project Mode ... 20
4.3.1 Entering Project Mode ... 20
4.3.2 Modifying IP Address ... 20
4.3.3 Adding Face Data ... 20
4.3.4 Issuing Card ... 21
Appendix 1 Cybersecurity Recommendations ... 22
Appendix 2 Packing List ... 25

1 Appearance

1.1 Dimension

Figure 1-1 Dimension (mm)



1.2 Front Panel

For the description of the front panel, see Table 1-1.

Face recognition is available on select models.

Figure 1-2 Front panel

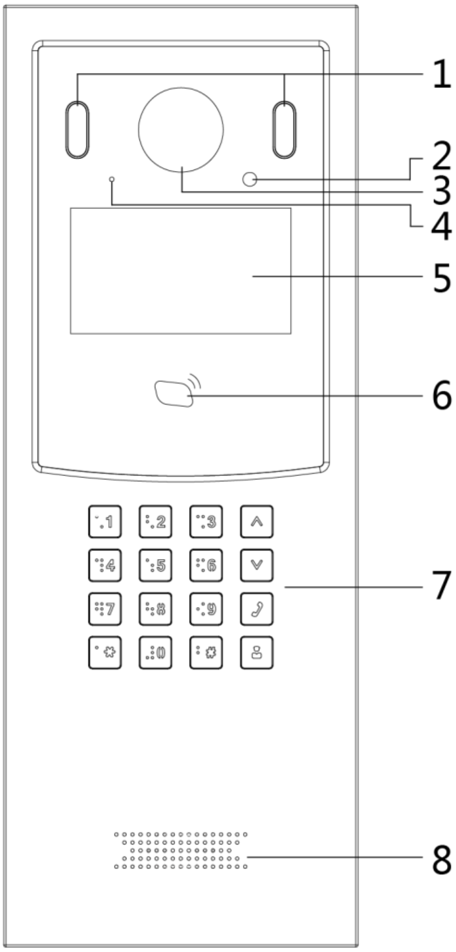


Table 1-1 Front panel description

No.	Name	Description
1	Fill light	● Provides extra light when recognizing faces. ● Provides extra light to the camera during dark condition.
2	Light sensor	Detects ambient lighting condition.
3	Camera	Monitors door area, and recognizes face information.
4	MIC	Inputs audio.
5	Screen	Displays information.
6	Access card reader	● Recognizes access card and unlock the door. ● Issues other access cards.

No.	Name	Description
7	Dialing area	Press to operate the VTO. ● Number 0–9: Press to input numbers; 2/4/6/8 can act as up/down/left/right when selecting options. ● ✱: Press to delete the previous character, resume to the previous interface, or end the current call. ● #: Press to go to the password input interface, or confirm. ● ☎: Press to call a certain room after entering the room number. ● 👤: Press to call the management center. ● ∧/∨: Press to select options.
8	Speaker	Outputs audio.

1.3 Rear Panel

Figure 1-3 Rear panel

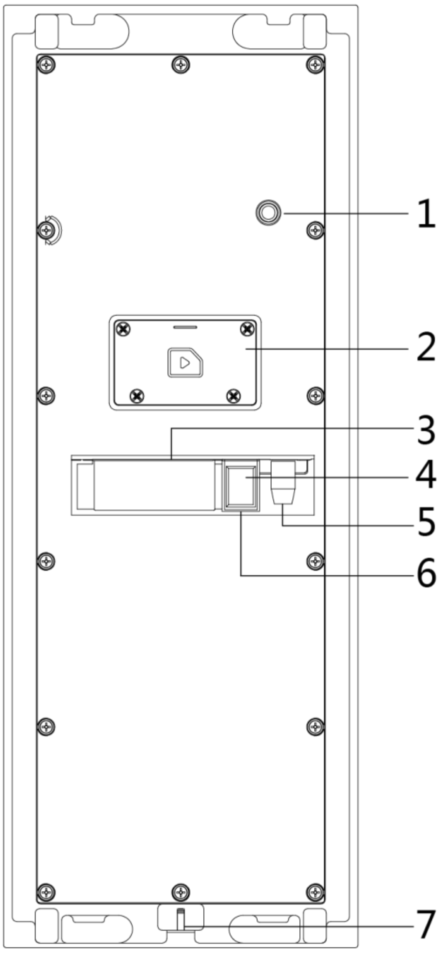


Table 1-2 Rear panel description

No.	Name	Description
1	Tamper switch	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.
2	SD card slot	Reserved for future use.
3	Cable ports	See "2.2 Connecting Cable."
4	Ethernet port	Connects to the network with Ethernet cable.
5	Power port	Inputs 12V DC power.
6	USB port	Reserved for future use.
7	Screw hole	Put in screws to fix the VTO.

2 Installation

2.1 Installation Requirement

2.1.1 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.

2.1.2 Guidance

See Figure 2-1 for the reference of the installation position, and for the VTO horizontal viewing angle, see Table 2-1.

Figure 2-1 Installation position reference

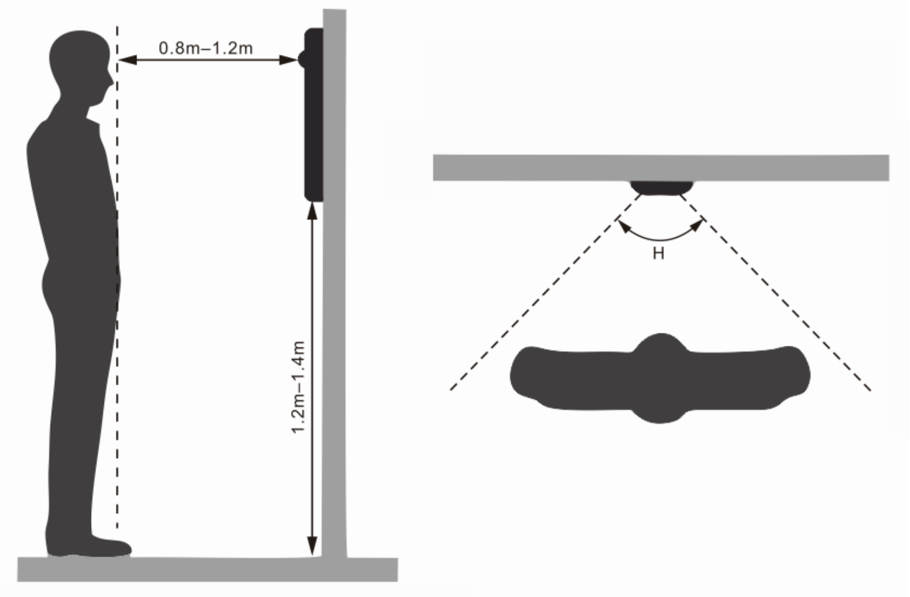


Table 2-1 Horizontal viewing angle

Model	Angle of View (H)
VTO6441F/VTO6421F	75°

2.2 Connecting Cable

2.2.1 Door Lock Port

This port can be used to connect to door locks, and the connection method varies with different locks. See Figure 2-2, Figure 2-3, and Figure 2-4.

Figure 2-2 Electronic lock connection

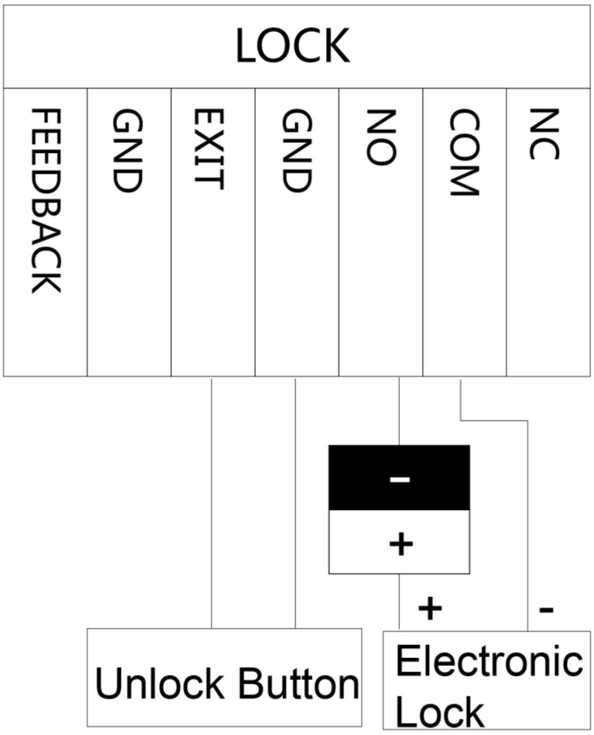


Figure 2-3 Magnetic lock connection

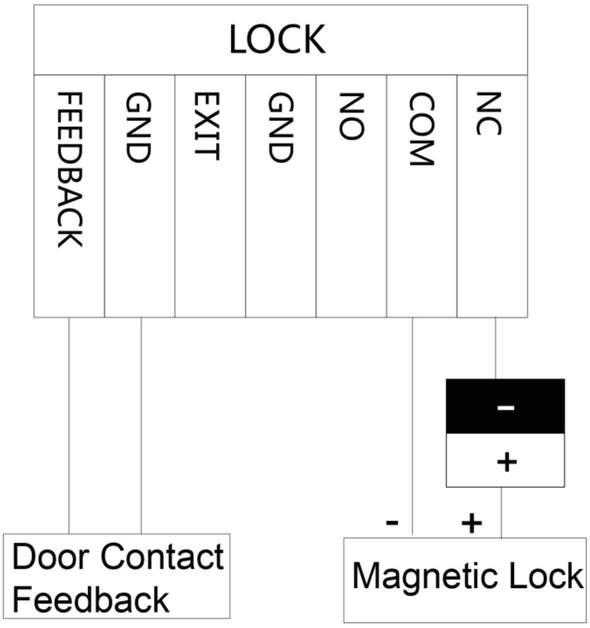
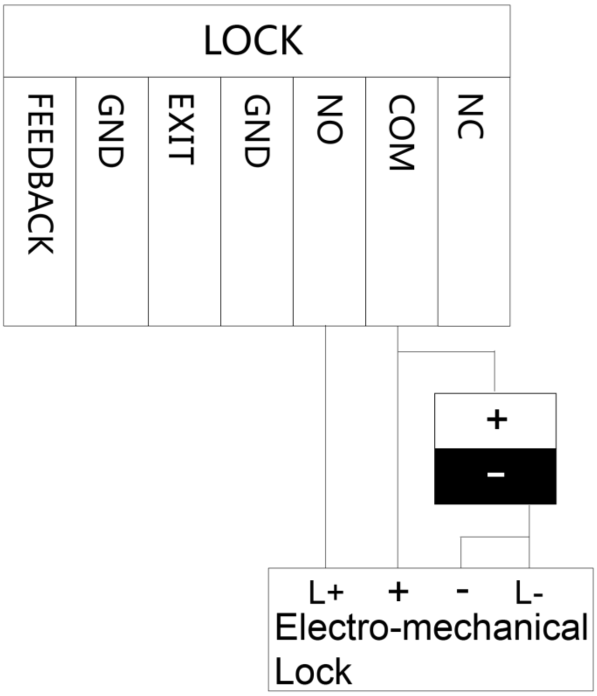


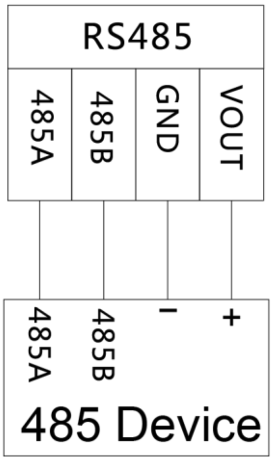
Figure 2-4 Electro-mechanical lock connection



2.2.2 RS-485 Port

This port can be used to connect to RS-485 devices. See Figure 2-5.

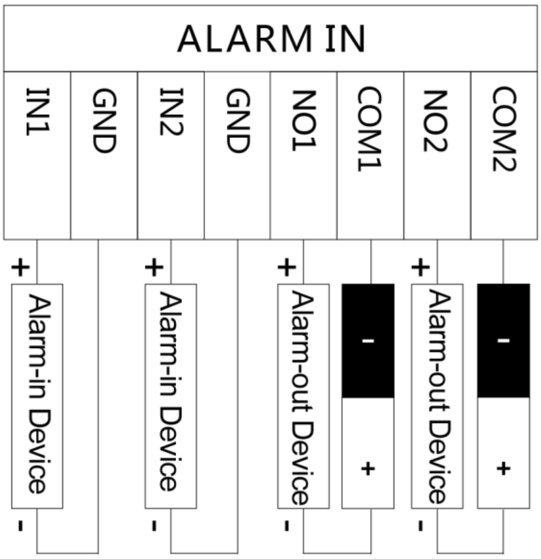
Figure 2-5 RS-485 port



2.2.3 Alarm I/O and Power Port

This port can be used to connect to 2 alarm-in devices and 2 alarm-out devices. See Figure 2-6.

Figure 2-6 Alarm I/O and power Port



2.2.4 Wiegand Port

The Wiegand port can be used to connect to the Wiegand card reader or access control device. See Figure 2-7.

Figure 2-7 Connect to Wiegand card reader

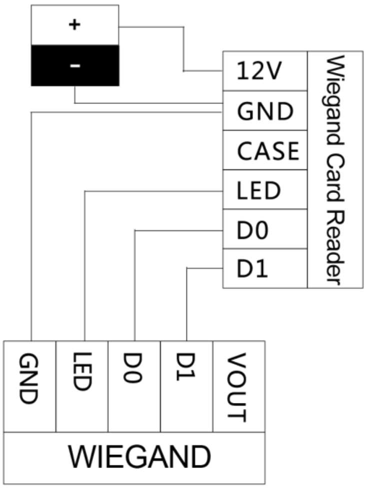
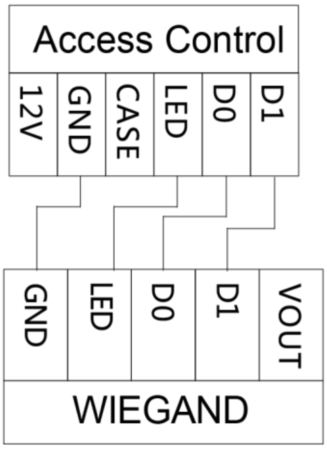


Figure 2-8 Connect to access control



2.3 Installing VTO

Figure 2-9 VTO installation

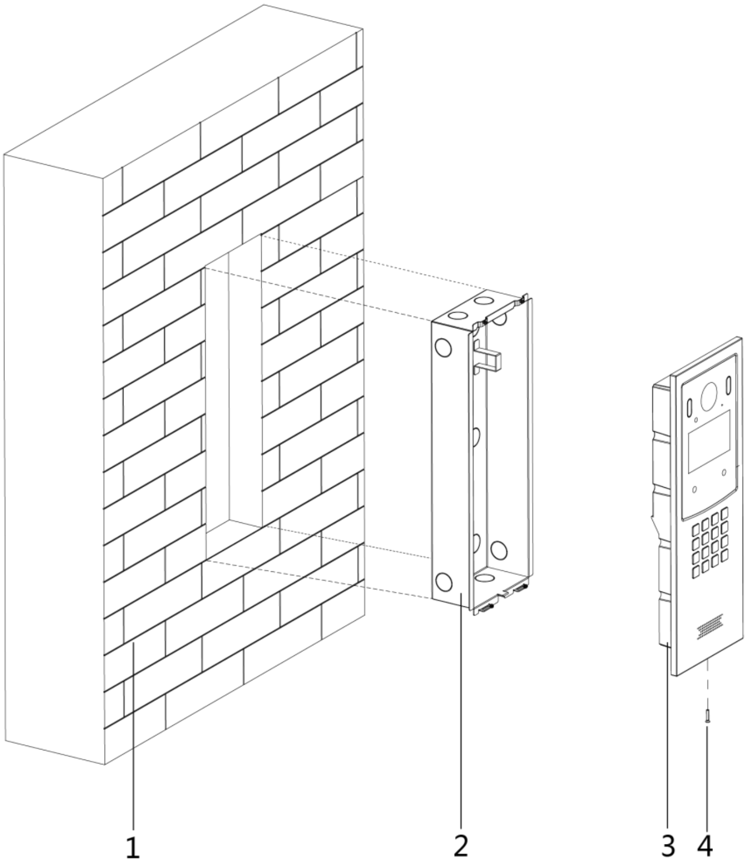


Table 2-2 Item list

No.	Item	No.	Item
1	Wall	2	Mounting box
3	VTO	4	Screw

Step 1 Cut an opening with the size of the mounting box in the wall.

Step 2 Pull the reserved cables through the cable hole in the mounting box.

Step 3 Fix the mounting box in the wall with cement or screws.

Step 4 Connect the cables to the ports on the VTO rear panel. See "2.2 Connecting Cable."

Step 5 Fix the VTO in the mounting box with the screws.

Step 6 Put sealant between the VTO, mounting box, and the wall.

3 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.

3.1 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 "3.3 Configuring VTO."

1) Initialize VTO. See "3.3.1 Initialization."
2) Configure VTO number. See "3.3.2 Configuring VTO Number."
3) Configure VTO network parameters. See "3.3.3 Configuring Network Parameters."
4) Configure SIP Server. See "3.3.4 Configuring SIP Server."
5) Add VTO devices to the SIP server. See "3.3.5 Adding VTO Devices."
6) Add room number to the SIP server. See "3.3.6 Adding Room Number."

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

Step 4 Verify Configuration. See "3.4 Verifying Configuration."

3.2 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.

3.3 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.

3.3.1 Initialization

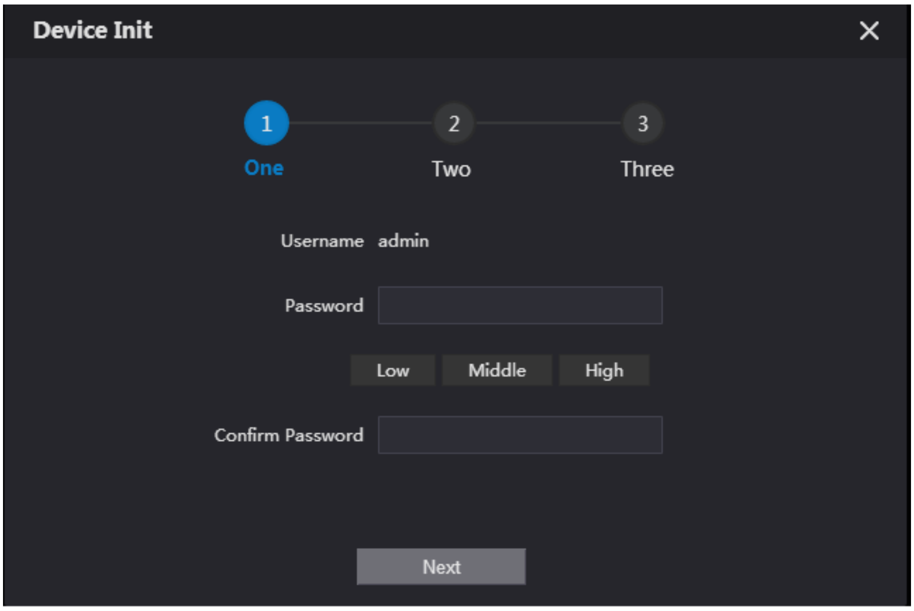
The default IP address of VTO is 192.168.1.110, and make sure the PC is in the same network segment as the VTO.

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 3-1.

Figure 3-1 Device initialization



Username admin

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

The Email setting interface is displayed.

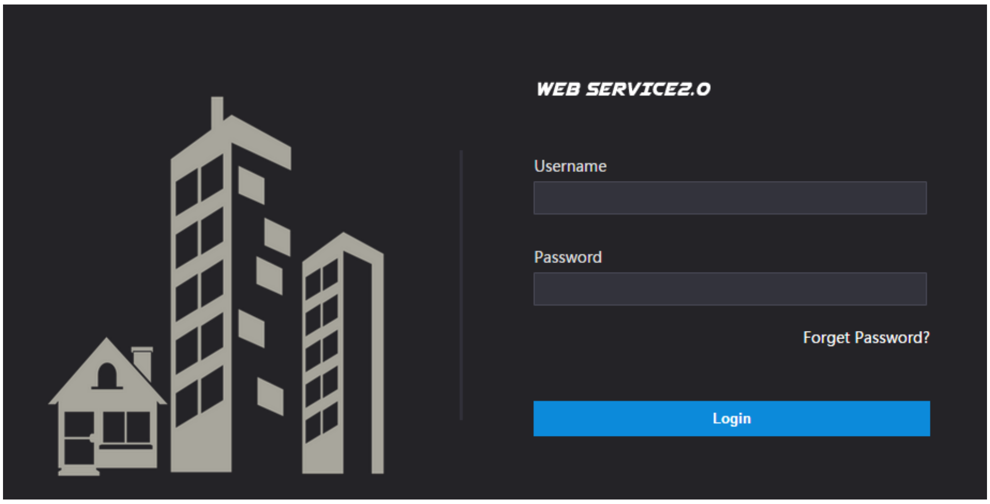
Step 4 Select the **Email** check box, and then enter your Email address. This Email address can be used to reset the password, and it is recommended to finish this setting.

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

Step 6 Click **OK**.

The login interface is displayed. See Figure 3-2.

Figure 3-2 Login interface



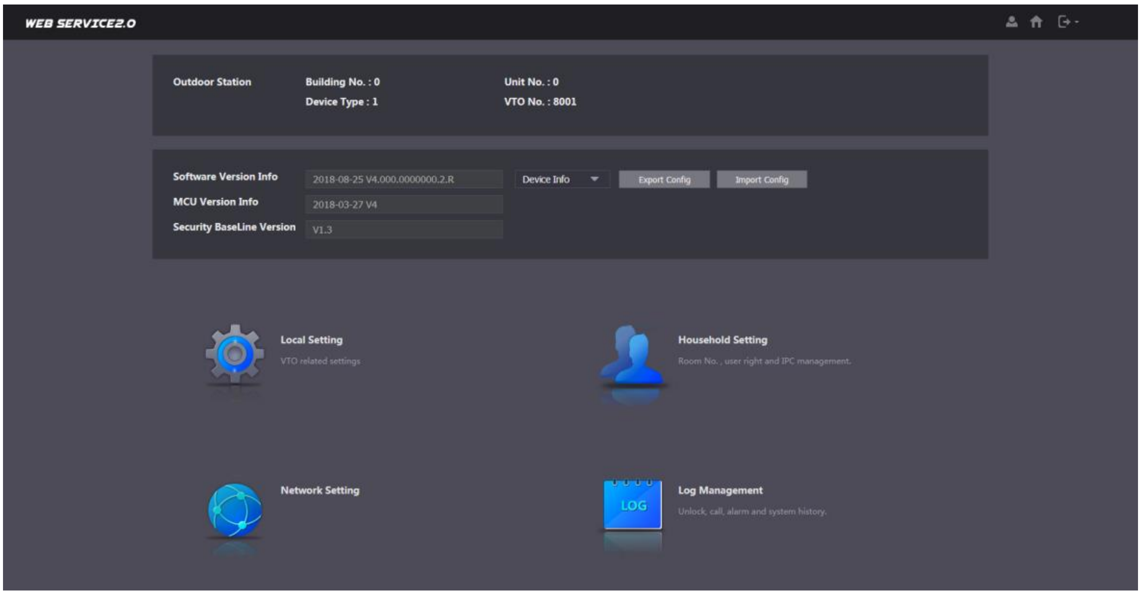
3.3.2 Configuring VTO Number

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 3-3.

Figure 3-3 Main interface



Outdoor Station

Building No. : 0

Device Type : 1

Unit No. : 0

VTO No. : 8001

Software Version Info: 2018-08-25 V4.000.0000000.2.R

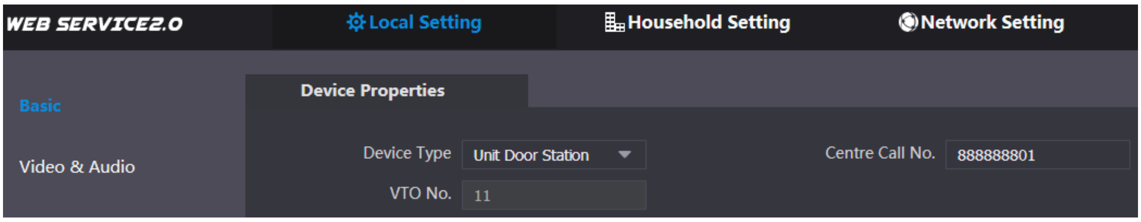
MCU Version Info: 2018-03-27 V4

Security BaseLine Version: V1.3

Step 2 Select **Local Setting > Basic**.

The device properties are displayed. See Figure 3-4.

Figure 3-4 Device properties



Device Type: Unit Door Station

VTO No.: 11

Centre Call No.: 888888801

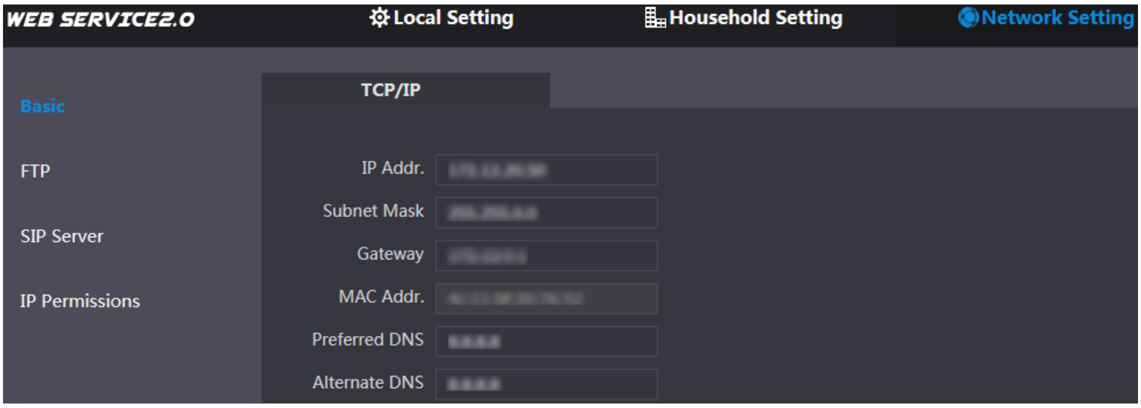
Step 3 In the **VTO No.** input box, enter the VTO number you planned for this VTO, and then click **Confirm** to save.

3.3.3 Configuring Network Parameters

Step 1 Select **Network Setting > Basic**.

The TCP/IP information is displayed. See Figure 3-5.

Figure 3-5 TCP/IP information



IP Addr.: [redacted]

Subnet Mask: [redacted]

Gateway: [redacted]

MAC Addr.: [redacted]

Preferred DNS: [redacted]

Alternate DNS: [redacted]

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.

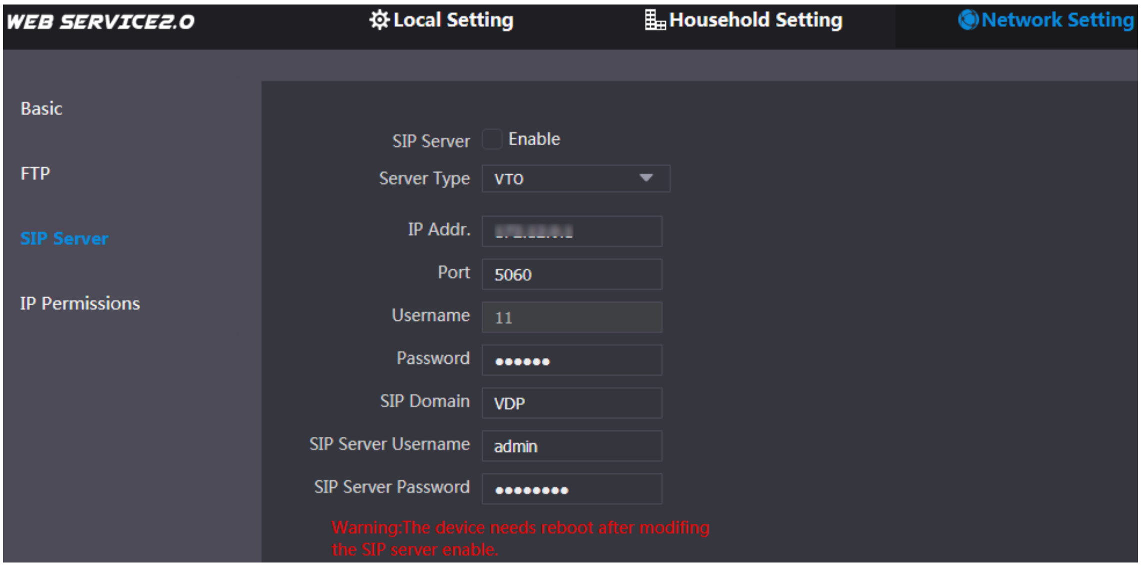
3.3.4 Configuring SIP Server

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 3-6.

Figure 3-6 SIP server



SIP Server ☐ Enable

Server Type VTO

IP Addr. [redacted]

Port 5060

Username 11

Password ••••••

SIP Domain VDP

SIP Server Username admin

SIP Server Password ••••••••

Warning:The device needs reboot after modifing the SIP server enable.

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 the details in "3.3.5 Adding VTO Devices" and "3.3.6 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 3-1.

Table 3-1 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.

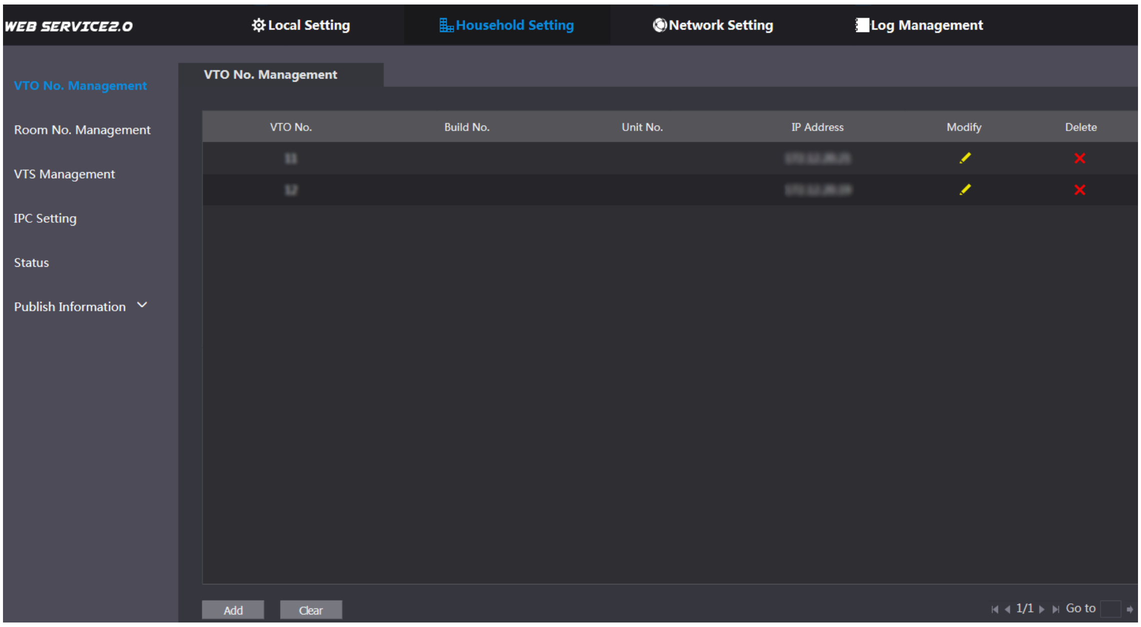
3.3.5 Adding VTO Devices

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 3-7.

Figure 3-7 VTO No. management

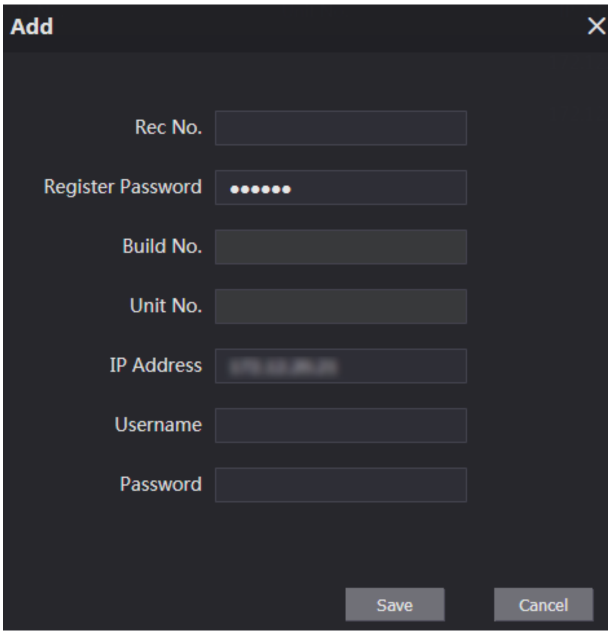


VTO No.	Build No.	Unit No.	IP Address	Modify	Delete
[redacted]			[redacted]	✎	✕
[redacted]			[redacted]	✎	✕

Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 3-8.

Figure 3-8 Add VTO



Rec No.
Register Password ●●●●●●
Build No.
Unit No.
IP Address [redacted]
Username
Password

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

Table 3-2 Add VTO configuration

Parameter	Description
Rec No.	The VTO number you configured for the target VTO. See the details in "3.3.2 Configuring VTO Number."
Register Password	Keep default value.
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**.

3.3.6 Adding Room Number

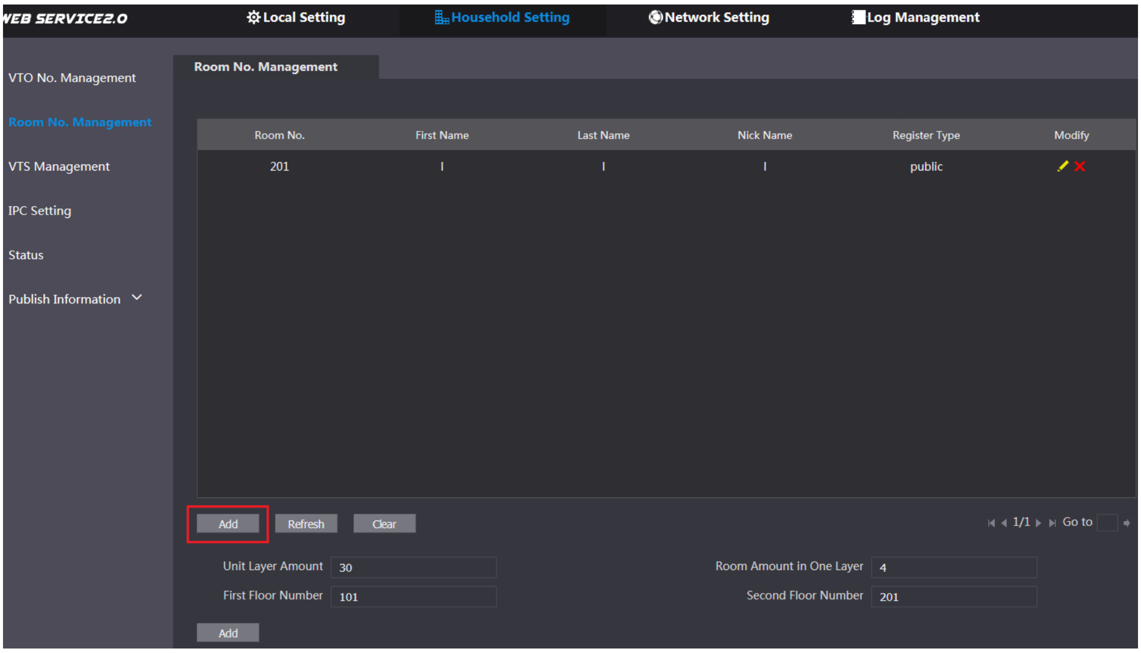
You can add the planned room number to the SIP server, and then configure the room number on VTH devices to connect them to the network. This section applies to the condition in which a VTO device works as SIP server, and if you use other servers as SIP server, see the corresponding manual for the detailed 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 3-9.

Figure 3-9 Room No. Management



Room No.	First Name	Last Name	Nick Name	Register Type	Modify
201	|	|	|	public	✎ ✕

Unit Layer Amount 30

Room Amount in One Layer 4

First Floor Number 101

Second Floor Number 201

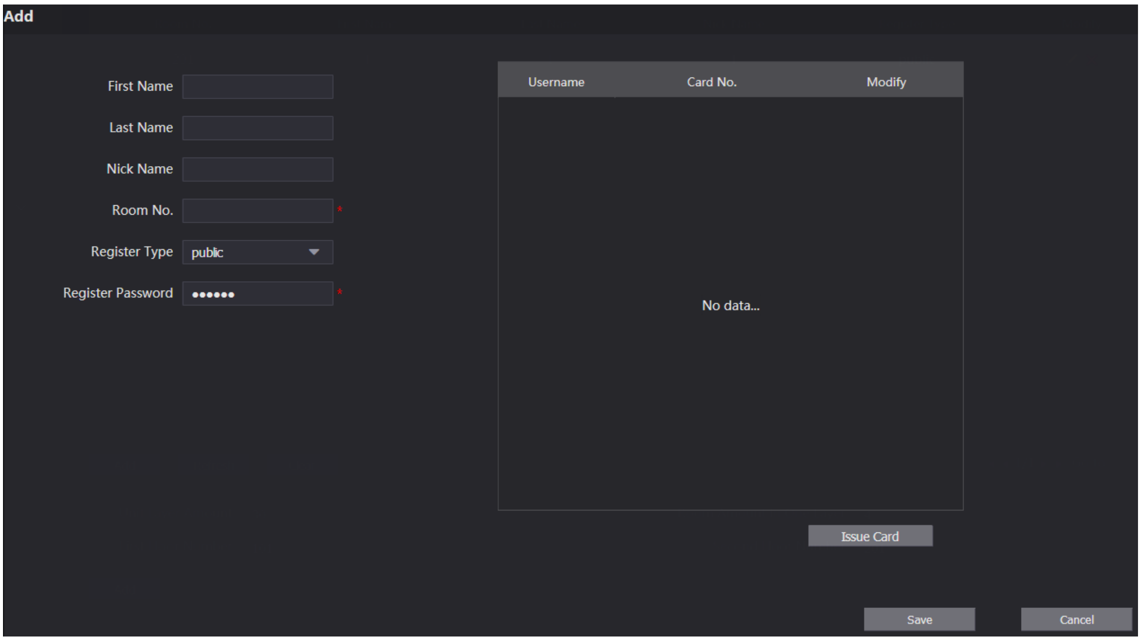
Step 2 You can add single room number or do it in batch.

- Adding single room number

1) Click the **Add** at the mid lower position. See Figure 3-9.

The **Add** interface is displayed. See Figure 3-10.

Figure 3-10 Add single room number



Register Type: public

Register Password: ••••••

2) Configure room information. See Table 3-3.

Table 3-3 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 10 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.

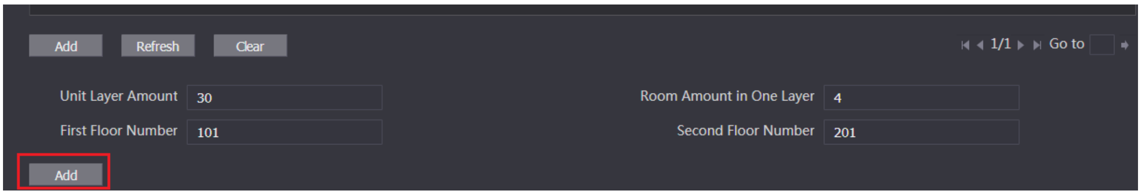
3) Click **Save**.

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

- Adding room number in batch

1) Configure the **Unit Layer Amount**, **Room Amount in One Layer**, **First Floor Number**, and **Second Floor Number** according to the actual condition.
2) Click the **Add** at the bottom position. See Figure 3-11

Figure 3-11 Add in batch



Unit Layer Amount: 30

Room Amount in One Layer: 4

First Floor Number: 101

Second Floor Number: 201

All the added room numbers are displayed. Click **Refresh** to view the latest status, and click **Clear** to delete all the room numbers.

3.4 Verifying Configuration

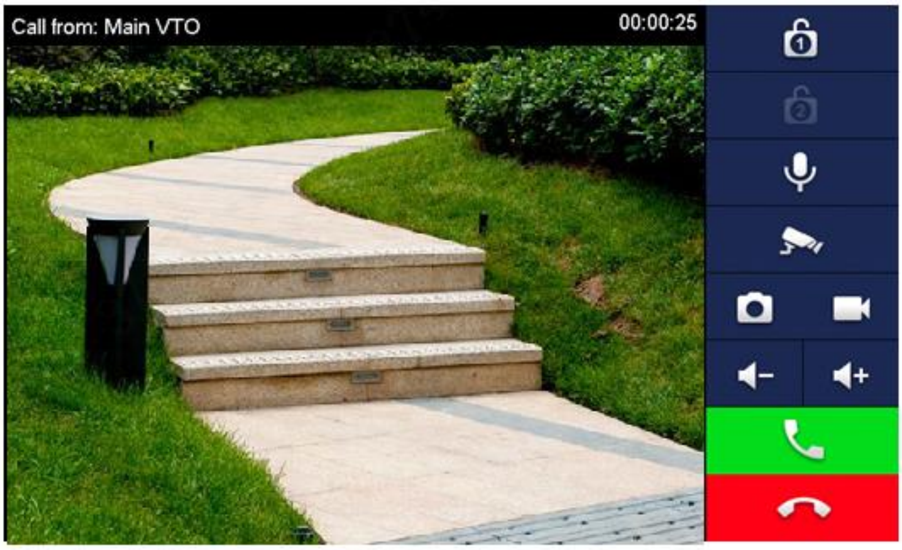
3.4.1 Calling VTH from VTO

Step 1 Dial room number on the VTO.

Step 2 Press ☎.

The VTO is calling the VTH. See Figure 3-12.

Figure 3-12 Call screen

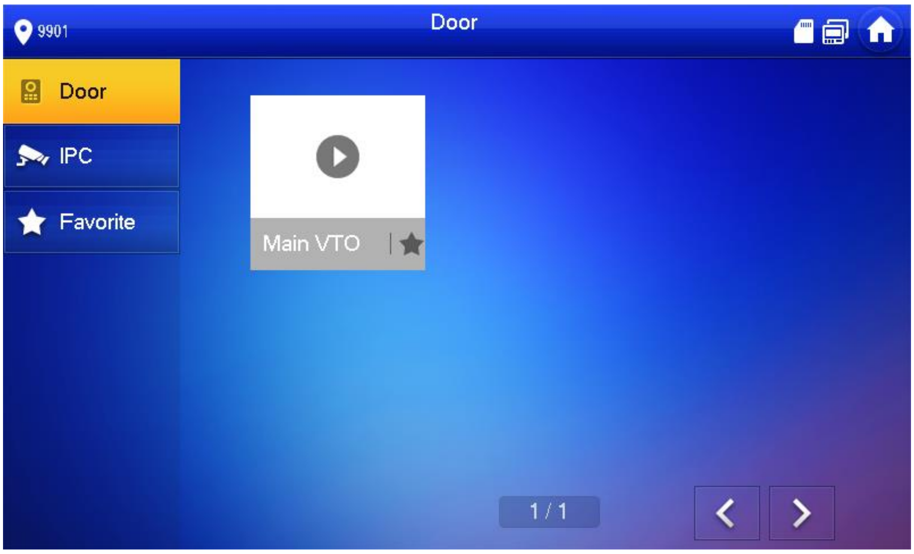


Step 3 Tap ☎ on the VTH to answer the call.

3.4.2 Doing Monitor from VTH

Step 1 In the main interface of the VTH, select **Monitor > Door**.
The **Door** interface is displayed. See Figure 3-13.

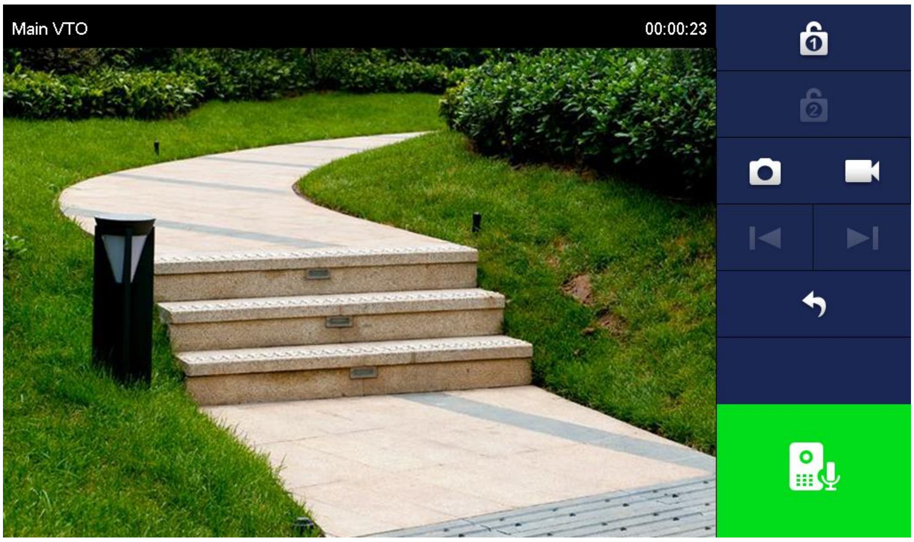
Figure 3-13 Door



Step 2 Select the VTO you need to do monitor.

The monitor screen is displayed. See Figure 3-14.

Figure 3-14 Monitor screen



4 Operating VTO

4.1 Call Function

4.1.1 Calling single VTH

See "3.4.1 Calling VTH from VTO."

4.1.2 Calling Multiple VTH Devices

If the VTO you are visiting works as SIP server, and there are multiple VTH devices being used, when you call the master VTH, all the extension VTH devices would also receive the call.

Before calling, be sure to:

- Enable **Group Call** in **Local Setting > Basic**. See the VTO user's manual.
- Add master VTH and the extension VTH. See "3.3.6 Adding Room Number."

4.1.3 Calling Management Center

Press 👤 on the VTO.

4.2 Unlock Function

4.2.1 Unlock with Face Recognition

📖

Face recognition is available on select models.

When the VTO is on sleeping mode, and when people are approaching, the screen lights up, and then starts face recognition automatically.

4.2.2 Unlock with Password

Step 1 Press 🔑 on the VTO.

Step 2 Input unlock password.

Step 3 Press 🔑 again.

4.2.3 Unlock with IC Card

Swipe the authorized access card at the access card area of the VTO to open the door.

4.2.4 Unlock From VTH

You can tap the unlock button on VTH to unlock the door when VTO and VTH are having phone call or you are doing monitor.

4.2.5 Unlock From the Management Center

You can unlock the door from the management center when VTO is calling the management center, VTO and the management center are having phone call, or you are doing monitor from the management center.

4.3 Project Mode

The project mode is only for professional or admin people, and you can make advanced configurations to the VTO under this mode, including issuing access card, modifying device IP address, and adding room number.

4.3.1 Entering Project Mode

On the main interface, enter "⚙ +project password+ ⚙ " to enter project mode.

The default project password is 888888, and you can modify it on the VTO or in the VTO web interface.

In the project mode, you can press ∧ or ∨ to select menu items; press ⚙ as return; press ⚙ as confirm.

4.3.2 Modifying IP Address

Step 1 In the project mode, select **IP Settings**.

Step 2 Press numeric keys of 2, 8, 4, and 6 as directional keys to select the item you need to modify, and then press ⚙ to start input. After inputting, press ⚙ to confirm.

Step 3 After the modification is finished, press ⚙ to exit.

4.3.3 Adding Face Data

Face recognition is available on select models.

Step 1 In the project mode, select **User Registration**.

The **Input room number** interface is displayed.

Step 1 Enter the room number for the newly added face, and then press ⚙.

You can add 50 faces at most under one room number.

Step 2 Select Face Registration.

The VTO starts recognizing and adding face data. Press to restart.

Step 3 After the registration is finished, press to confirm, and then press to exit.

4.3.4 Issuing Card

Step 1 In the project mode, select **User Registration**.

The **Input room number** interface is displayed.

Step 2 Enter the number of the room to which you need to issue access card, and then press .

Step 3 You can issue access card with master card or card issuing password.

- Issue card with master card

  Select **Issue Card > Master card**, and then swipe the master card.

You can issue master card on the SIP server. See the detailed configuration in the corresponding manual.

- Issue card with password

  Select **Issue Card > Password**, then enter the card issuing password, and then press # to confirm.

The default card issuing password is 002236, and you can modify it in the web interface. See the VTO users' manual.

Step 4 Swipe the card(s) that need to be authorized.

Step 5 After the registration is finished, press to confirm, and then press again to exit.

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.

Appendix 2 Packing List

Packing List

Open the package and check whether all the components are included.

Name	Quantity	Info
VTO	1	
Power adapter	1	
Quick Start Guide	1	
Screw package	1	