Villa Door Station

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the functions and operations of the villa door station and second confirmation station (hereinafter referred to as the "VTO"), and the accessory (hereinafter referred to as the "VTM").

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Revision Content	Release Time	Revision Content
V1.0.0	First Release.	November 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user’s manual, use our CD-ROM, scan

the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it, and keep the manual safe for future reference.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Improper use of the battery might result in a fire or explosion.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.

- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.

- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Table of Contents

1 Structure

1.1 Villa Door Station (multiple buttons)

1.1.1 Front Panel

Figure 1-1 Front panel

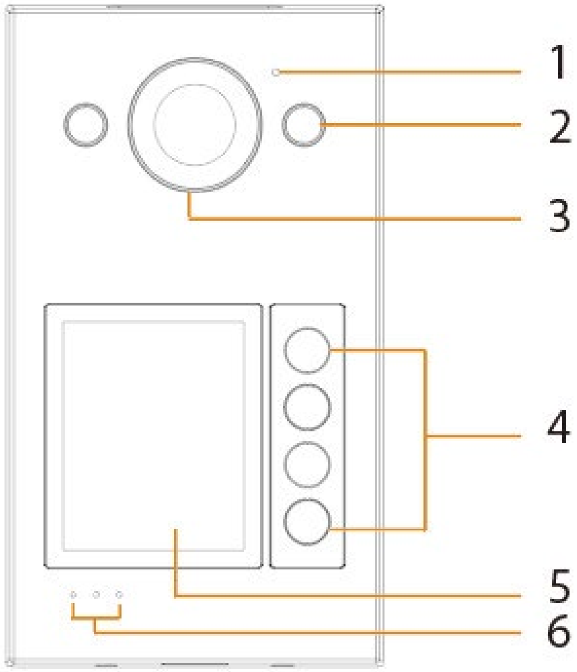


Table 1-1 Components

No.	Name	Function
1	MIC	Audio input.
2	Illuminator	Provide a constant light to focus more easily on a subject in dark surroundings.
3	Camera	Capture images or record videos for the VTO.
4	Call buttons	Call the VTH.
5	Card swiping area	Swipe the registered cards to unlock doors.
6	Indicators	From left to right: ● Ring：VTO is calling the VTH. ● Talking：VTO is on the talk with the VTH. ● Unlocking：VTO unlocking successful.

1.1.2 Rear Panel

The function ports might differ depending on the model.

Figure 1-2 Rear panel

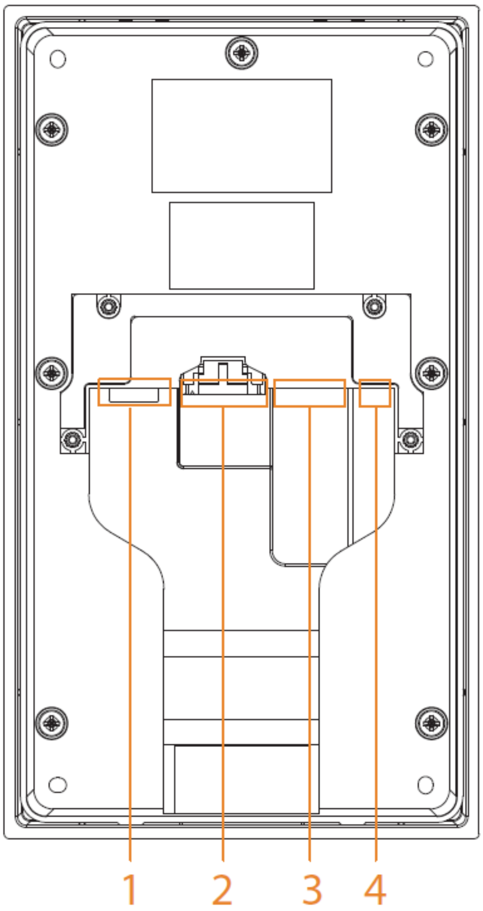


Table 1-2 Components

No.	Name	Function
1	SD card slot	Used to insert SD card so that data information such as images and videos can be stored.
2	Functional ports	Alarm port, door detector port, 485 port, power port and etc.
3	Network port	RJ-485 network port to connect to the network.
4	Reset button	Press and hold the button for several seconds to do factory reset.

1.2 Villa Door Station (single button)

1.2.1 Front Panel

There are different models with different front panel. Differences in size and appearance are found depending on your model.

Figure 1-3 Front panel

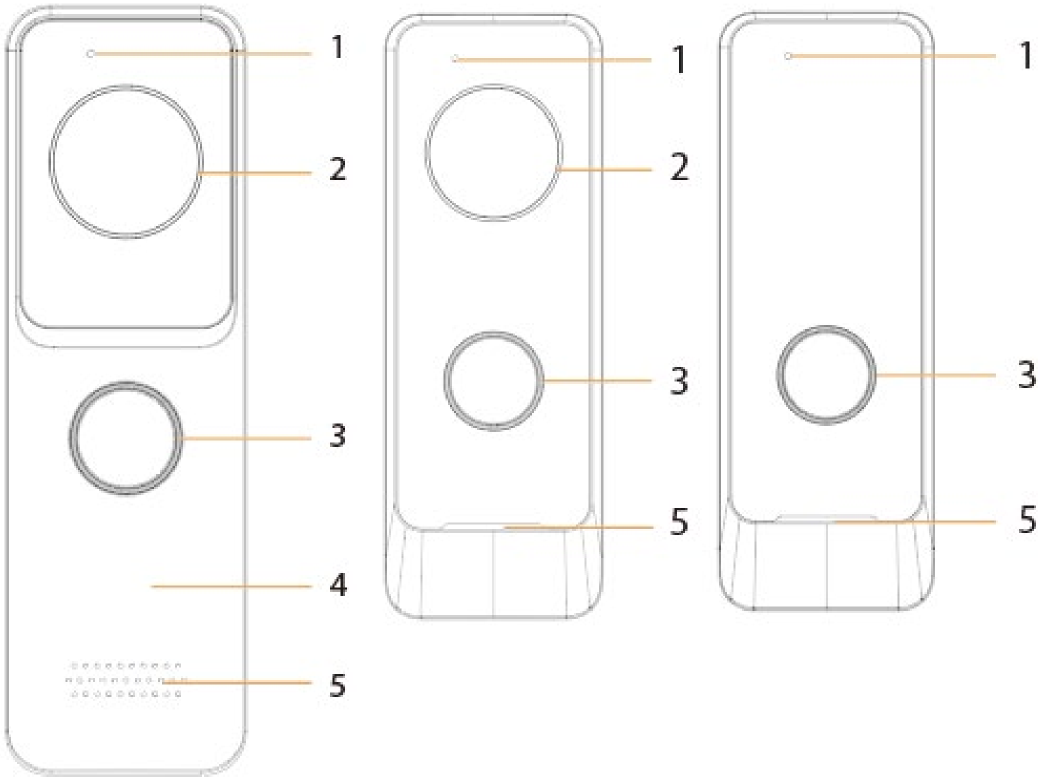


Table 1-3 Components

No.	Name	Function
1	MIC	Audio input.
2	Camera	Capture images or record videos for the VTO.
3	Call button	Call the VTH.
4	Card swiping area	Swipe the registered cards to unlock doors. 📖 The card swiping function is only supported by some models.
5	Speaker	Audio output.

1.2.2 Rear Panel

📖

The function ports might differ depending on the model. Here are two models used as examples.

Figure 1-4 Rear panel (1)

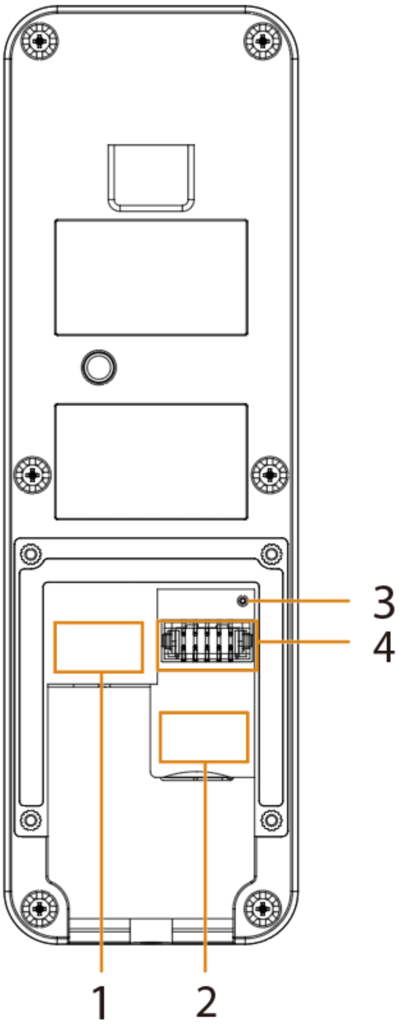


Table 1-4 Components

No.	Name	Function
1	Network port	Used to connect to the network.
2	SD card slot	Used to insert SD card so that data information such as images and videos can be stored.
3	Reset button	Press and hold the button for several seconds to do factory reset.
4	Functional port	● For some models, the functional port only has a power input port to connect to power supply. ● For some models, the functional port includes a power input port and a door detector port.

Figure 1-5 Rear panel (2)

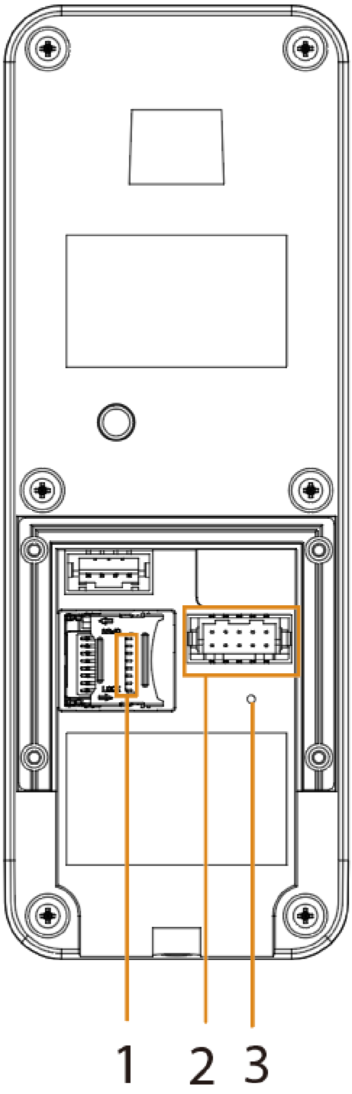


Table 1-5 Components

No.	Name	Function
1	SD card slot	Used to insert SD card so that data information such as images and videos can be stored.
2	Power port	Used to connect to the power supply.
3	Reset button	Press and hold the button for several seconds to do factory reset.

1.3 Button Model

1.3.1 Front Panel

Figure 1-6 Front panel

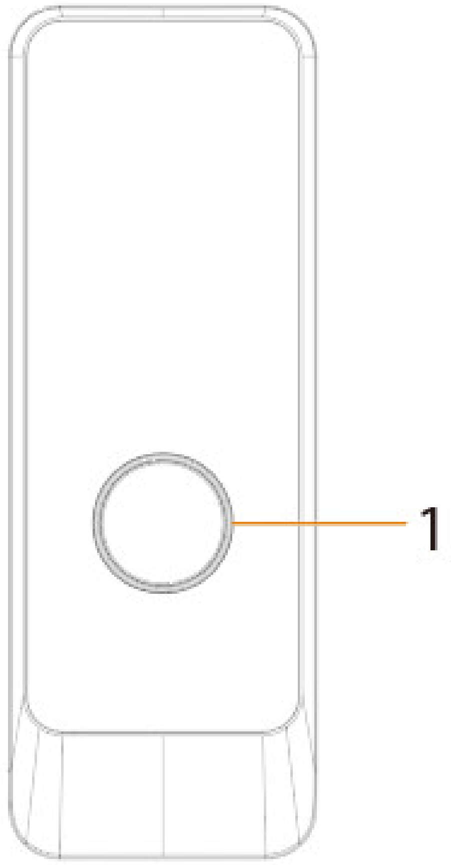


Table 1-6 Components

No.	Name	Function
1	Press button	The button model can be connected to the VTH. Press the button on the model and the VTH receives an alarm signal.

1.3.2 Rear Panel

Figure 1-7 Rear panel

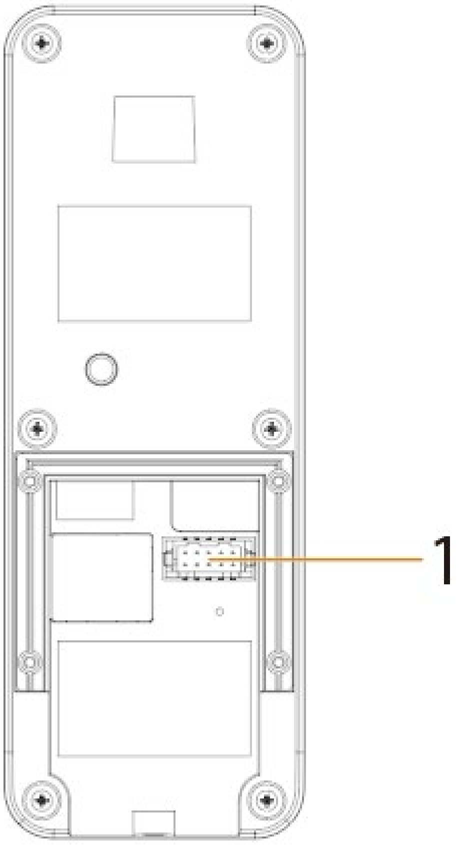


Table 1-7 Components

No.	Name	Function
1	Functional port	Used for alarm input.

2 Installation

2.1 Preparations

This chapter introduces precautions in installation. For detailed steps, see the corresponding installation guide.

- Do not expose the VTO to condensation, high temperature, direct sunlight, stain, dust, and chemically corrosive substances.
- Installation should be done by professional teams. Do not dismantle or repair the VTO by yourself in case of device failure. Contact after-sales service if you need any help.
- Prepare cross screwdrivers and gloves yourself.

2.2 Installation Guide

2.2.1 Villa Door Station (multiple buttons)

Step 1 Open the port cover of the VTO, drill screw holes on the wall according to the dimension of the mounting hole on the rear panel of the VTO, and put the expansion bolts into the holes.

Step 2 Complete the cable wiring.

Step 3 Fix the port cover to the rear panel of the VTO with four screws.

Step 4 Fix the bare VTO on the wall with four screws.

Step 5 Install the mount box on the VTO from top to the bottom, and then fix it with two screws.

Step 6 Fix the rain over on the top of the VTO with two screws.

Figure 2-1 Dimension (mm [inch])

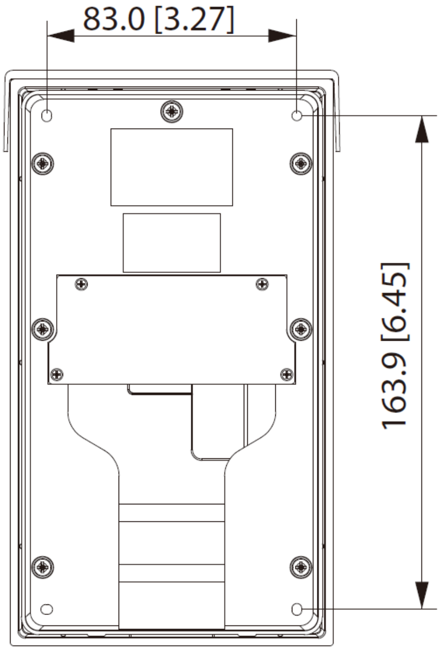
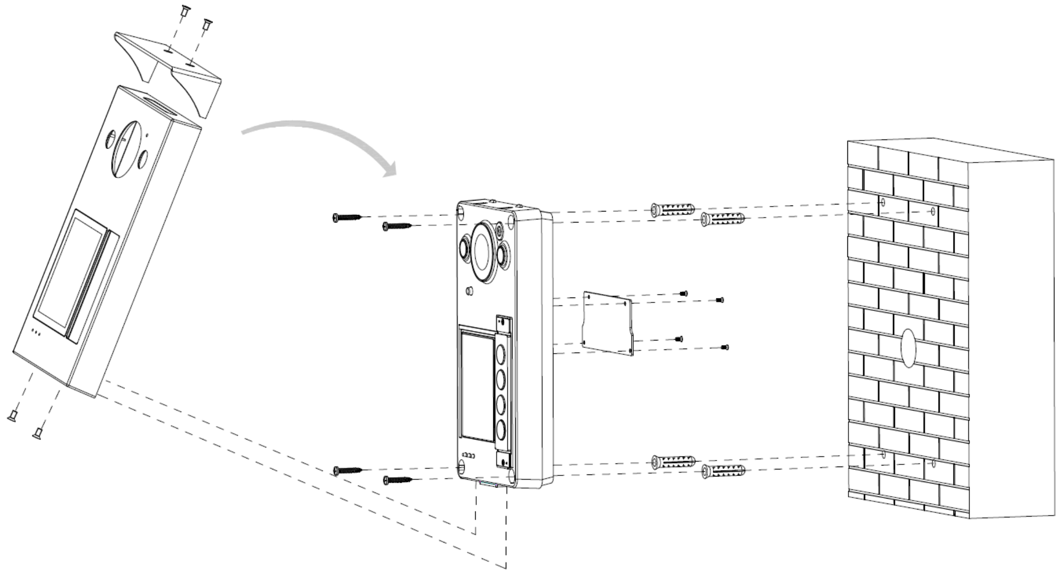


Figure 2-2 Installation



2.2.2 Villa Door Station (single button)

Here are examples of two model's installation, depending on differences in model dimensions.

Model Example 1:

Step 1 Open the port cover of the VTO, drill screw holes on the wall according to the dimension of the mounting hole on the rear panel of the VTO.

Step 2 Complete the cable wiring.

Step 3 Fix the port cover to the rear panel of the VTO with four screws.

Step 4 Fix the VTO on the wall with screws.

Figure 2-3 Dimension (mm [inch])

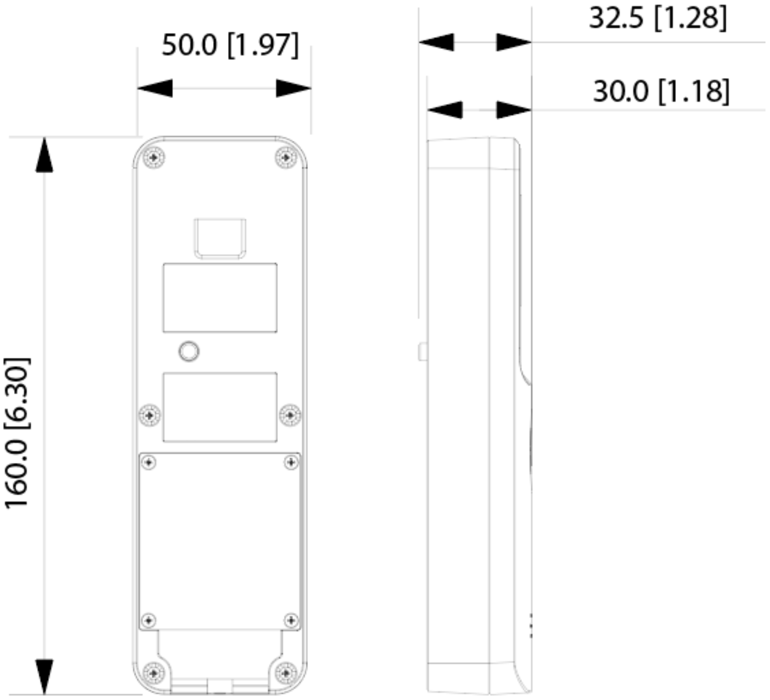
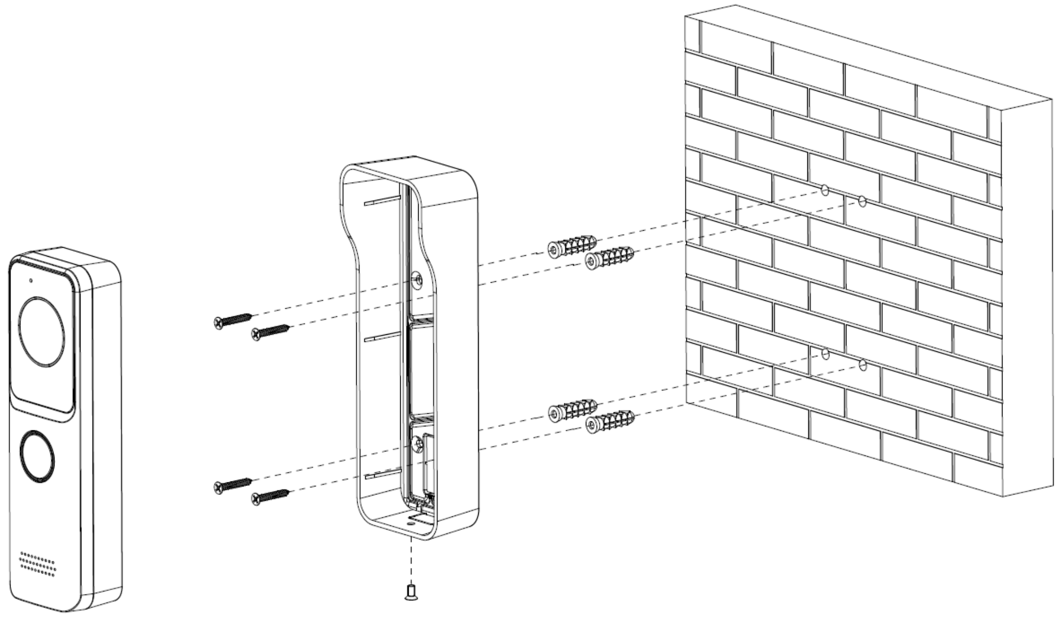


Figure 2-4 Installation



Model Example 2:

Step 1 Open the port cover of the VTO, drill screw holes on the wall according to the dimension of the mounting hole on the rear panel of the VTO.

Step 2 Complete the cable wiring.

Step 3 Fix the port cover to the rear panel of the VTO with four screws.

Step 4 Fix the VTO on the wall with screws.

Figure 2-5 Dimension (mm [inch])

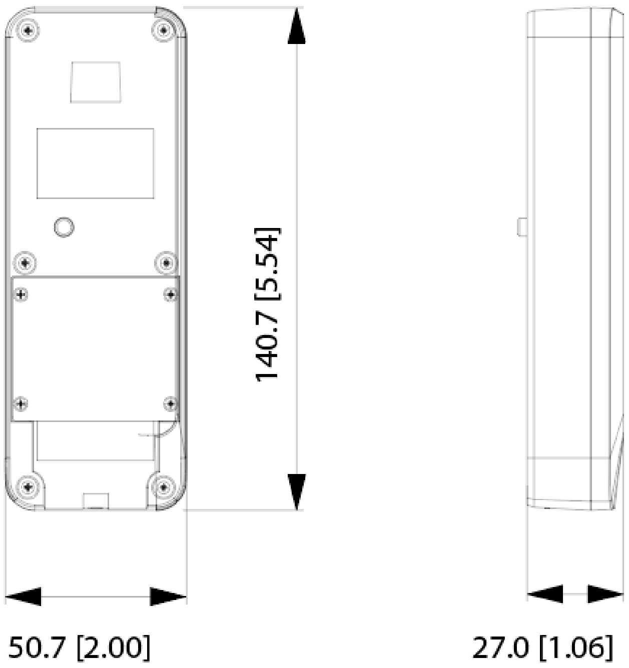
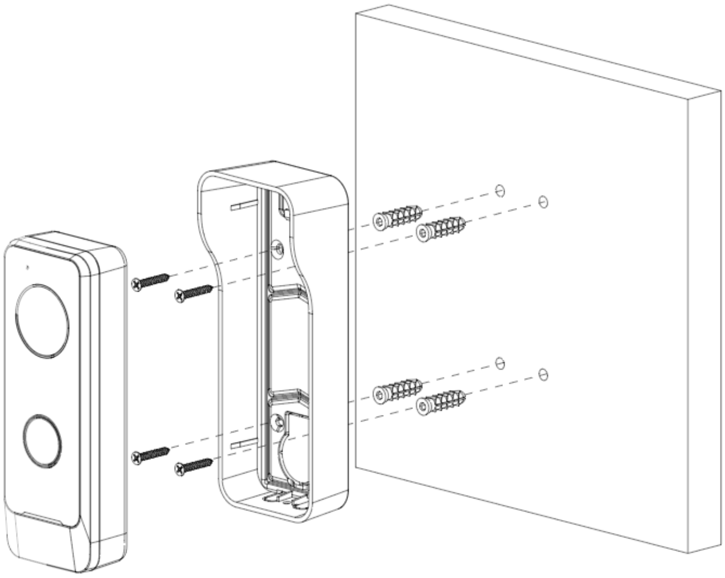


Figure 2-6 Installation



2.2.3 Button Model

Step 1 Open the port cover of the button model, drill screw holes on the wall according to the dimension of the mounting hole on the rear panel of the button model.

Step 2 Complete the cable wiring.

Step 3 Fix the port cover to the rear panel of the button model with four screws.

Step 4 Fix the button model on the wall with screws.

Figure 2-7 Dimension (mm [inch])

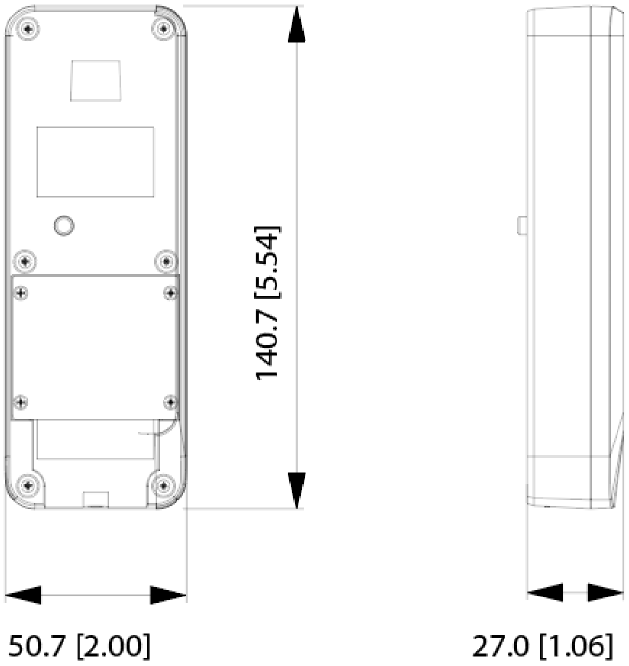
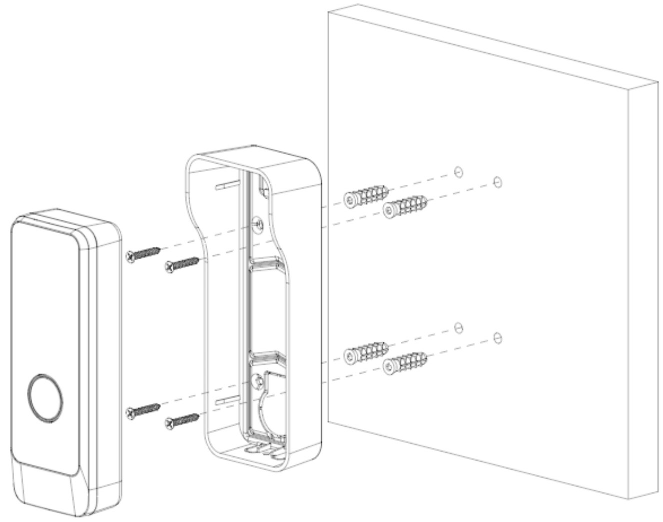


Figure 2-8 Installation



3 Web Configuration

This chapter provides a step-by-step configuration of the VTO, as well as how to register digital indoor monitors (hereinafter referred to as the "VTH") into the VTO to realize its intercom function. Follow the instructions below to get started.

📖

- The snapshots are for reference only and slight differences might be found in the actual web page of the VTO, depending on your model.
- You can download the configuration tool “VDPConfig” and use it to configure and update multiple devices. For details, see the corresponding user's manual.

3.1 Initializing VTO

For the first time login, you need to initialize the VTO.

Step 1 Power on the VTO.

Step 2 Go to the default IP address (192.168.1.108) of the VTO in the browser address bar, and then press the Enter key to go to the web page of the VTO.

📖

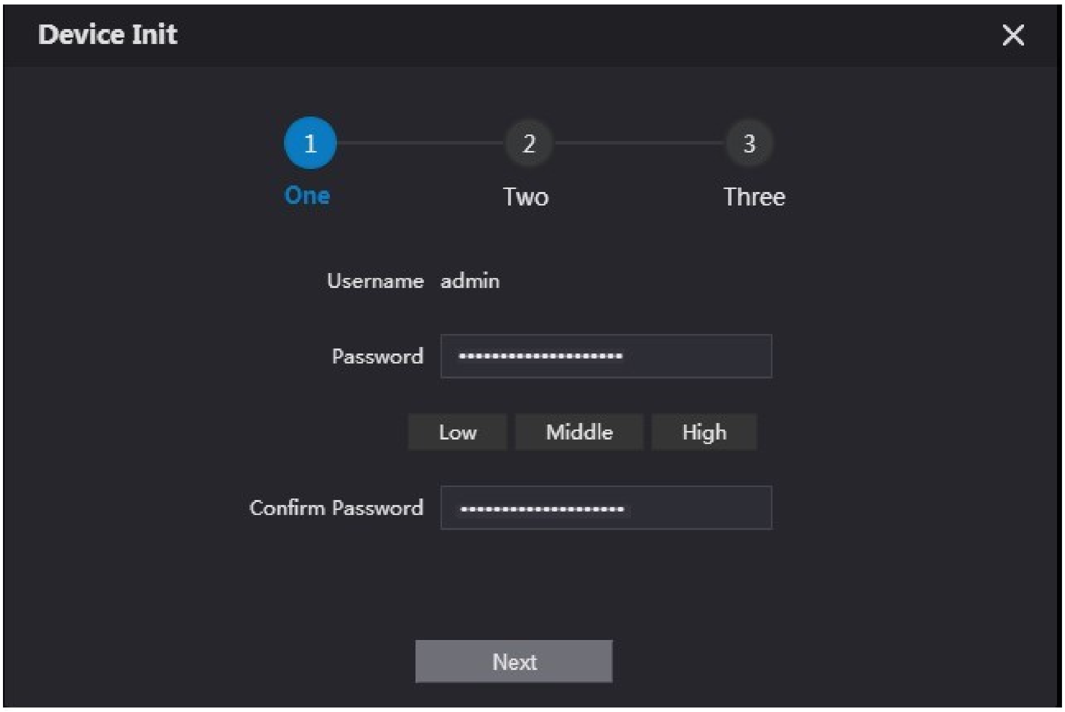
- The user name is admin by default.
- Make sure that the IP address of the PC is on the same network segment as the VTO.

Step 3 On the **Device Init** page, enter and confirm the password, and then click **Next**.

📖

The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).

Figure 3-1 Device initialization



Device Init

Username admin

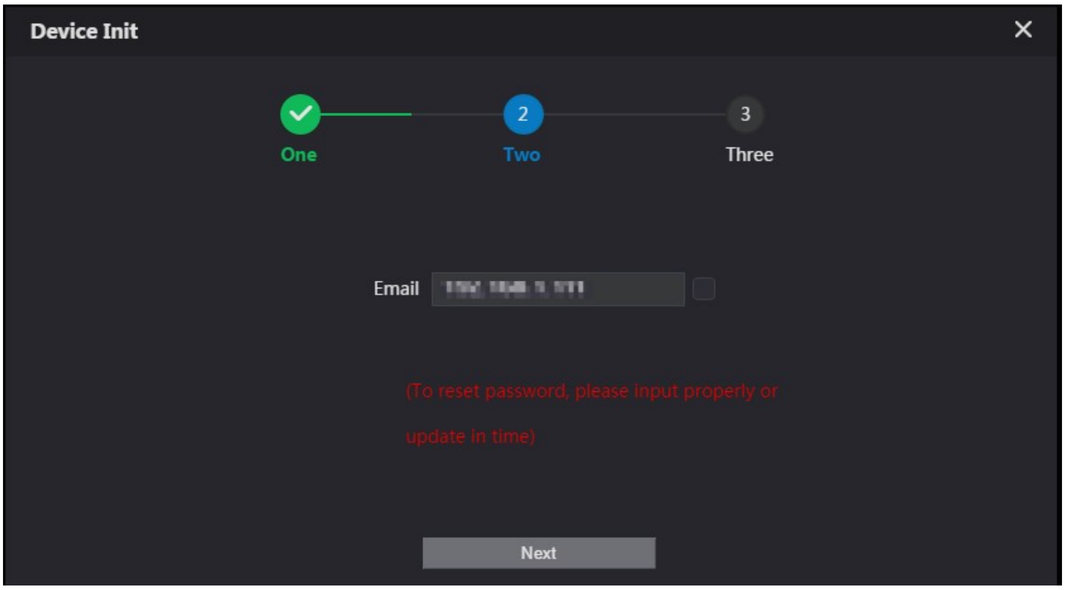
Password ••••••••••••••••••••

Confirm Password ••••••••••••••••••••

Step 4 Select the **Email** checkbox and enter email address.

This helps you to reset your password when your password is lost or forgotten.

Figure 3-2 Set an email address



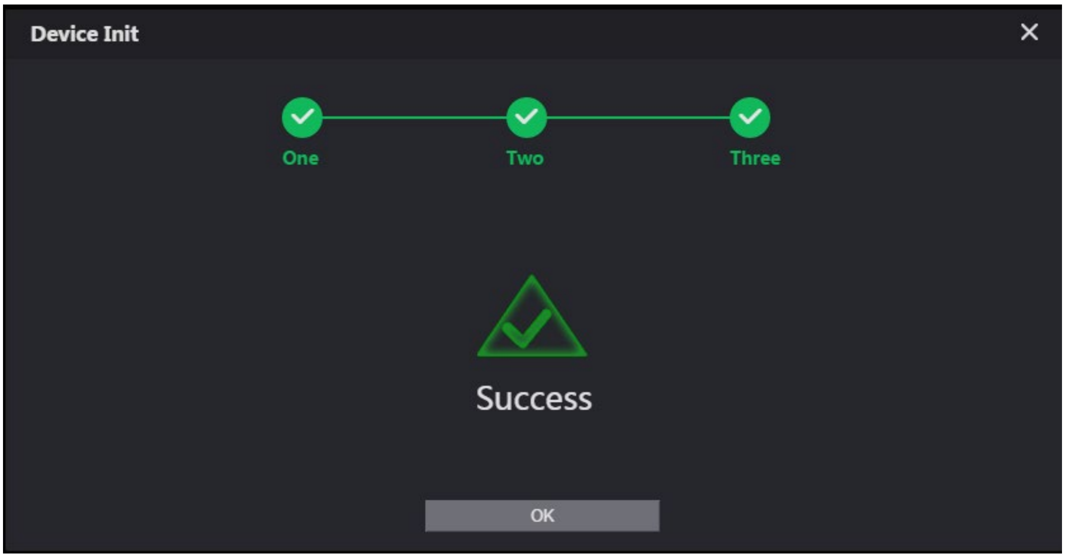
Device Init

Email [redacted] □

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

Step 5 Click **Next**.

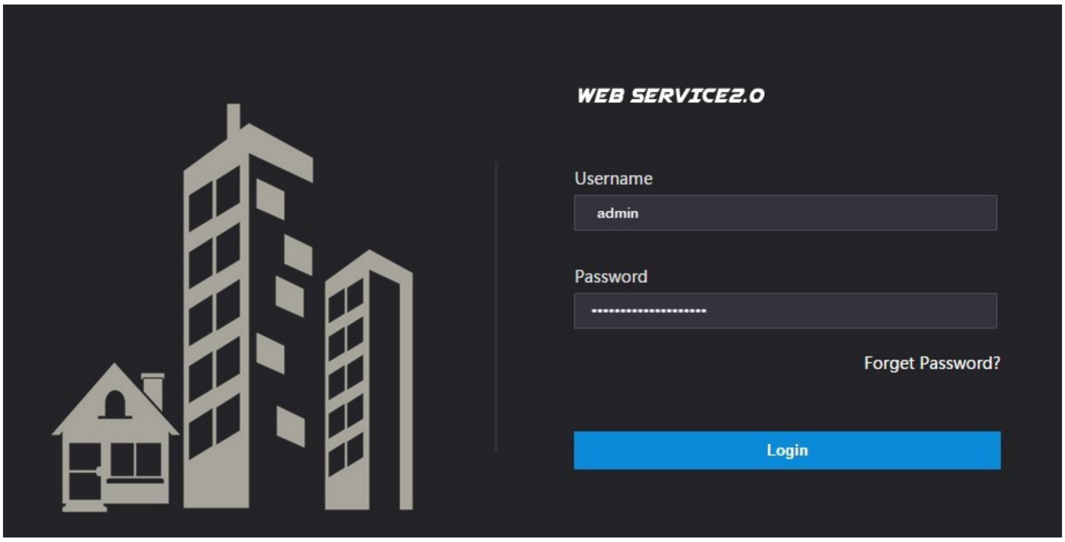
Figure 3-3 Initialization successful



Step 6 Click **OK**.

Enter username (admin by default) and the new password to log in to the web page.

Figure 3-4 Login page



3.2 Configuring Network Parameters

You need to configure the TCP/IP information to connect the VTO to the network. The descriptions below are for models with a Wireless LAN card. A Wireless LAN device is optional.

Wireless LAN

Step 1 Log into the VTO web page.

Step 2 Select **Network** > **Basic**.

Step 3 Configure the TCP/IP parameters in the **WLAN** section.

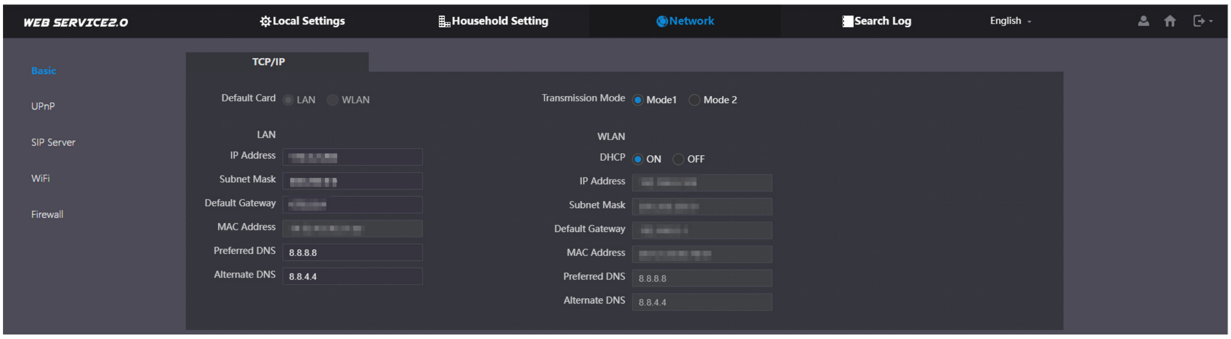
LAN

Step 1 Log into the VTO web page.

Step 2 Select **Network** > **Basic**.

Step 3 Configure the TCP/IP parameters in the **LAN** section.

Figure 3-5 Network configuration



Default Card ○ LAN ○ WLAN

Transmission Mode ● Mode1 ○ Mode 2

LAN

IP Address [redacted]

Subnet Mask [redacted]

Default Gateway [redacted]

MAC Address [redacted]

Preferred DNS 8.8.8.8

Alternate DNS 8.8.4.4

WLAN

DHCP ● ON ○ OFF

IP Address [redacted]

Subnet Mask [redacted]

Default Gateway [redacted]

MAC Address [redacted]

Preferred DNS 8.8.8.8

Alternate DNS 8.8.4.4

Table 3-1 Parameter description

Parameter	Description
IP Address	Your planned IP address for the VTO.
Preferred DNS	The default is 8.8.8.8.
Alternate DNS	The default is 8.8.4.4.
Transmission Mode	● Mode 1: Multicast streaming (UDP). ● Mode 2: RTSP streaming (TCP). ● It is transmission Mode 1 by default.
DHCP	Enable the function to get the allocated IP address for the VTO.

3.3 Configuring SIP Servers

When connected to the same SIP server, VTOs and VTHs can call each other. You can use a VTO or

a platform as the SIP server. We recommend you use a VTO as the SIP server in the villa scenario.

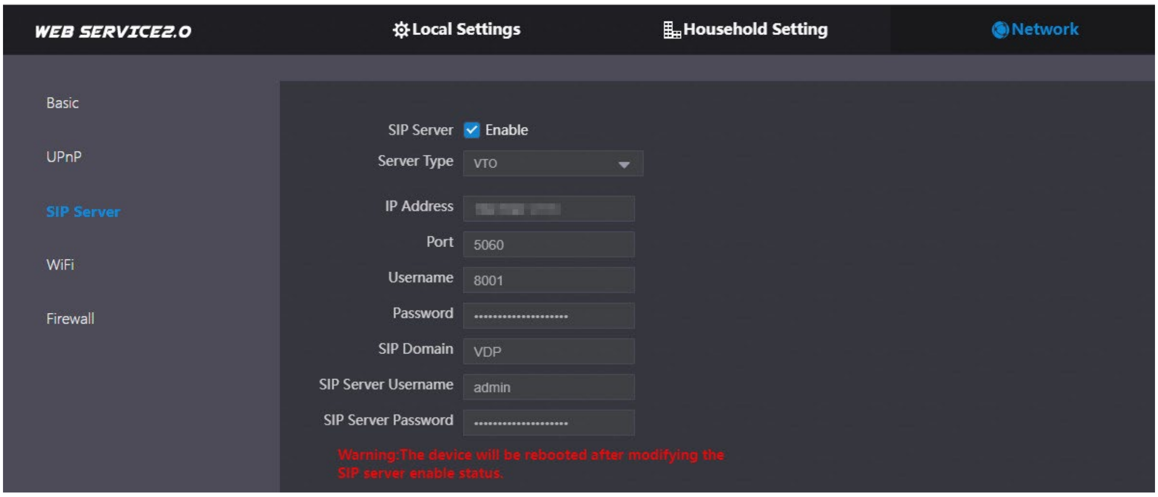
Step 1 Log in to the VTO web page.

Step 2 Select **Network** > **SIP Server**.

Step 3 Configure the parameters.

1) If the current VTO you have logged in works as the SIP server, **enable SIP Server**, and then keep other parameters by default.

Figure 3-2 Current VTO as the SIP server

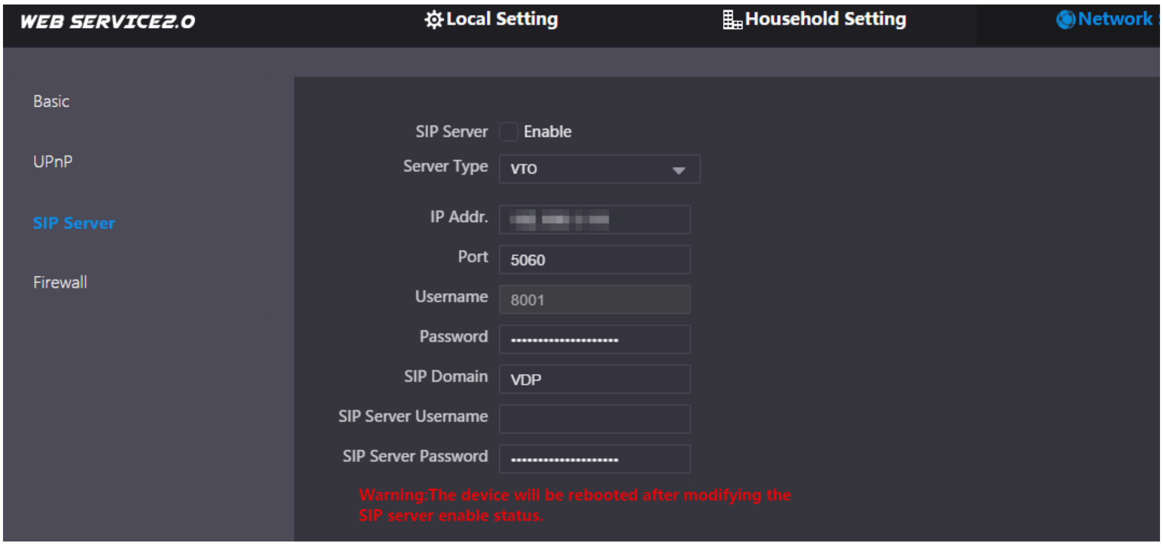


SIP Server ☑ Enable
Server Type VTO
IP Address [redacted]
Port 5060
Username 8001
Password ••••••••••••••••••••
SIP Domain VDP
SIP Server Username admin
SIP Server Password ••••••••••••••••••••
Warning:The device will be rebooted after modifying the SIP server enable status.

2) If other VTOs work as the SIP server, set **Server Type** as **VTO**, and then configure the parameters.

Do not enable **SIP Server**, otherwise the connection fails.

Figure 3-3 Other VTOs as the SIP server



SIP Server □ Enable
Server Type VTO
IP Addr. [redacted]
Port 5060
Username 8001
Password ••••••••••••••••••••
SIP Domain VDP
SIP Server Username
SIP Server Password ••••••••••••••••••••
Warning:The device will be rebooted after modifying the SIP server enable status.

Table 3-2 Parameter description

Parameter	Description
IP Address	The one that you planned for the VTO.
Port	5060 by default when a VTO works as SIP server.
SIP Domain	● When the VTO you logged in works as the SIP server, leave the SIP domain value by default. ● When another VTO works as the SIP server, you can leave the SIP domain by default or keep it null.
Username/Password	Used to log in to the web page of the VTO.

Parameter	Description
SIP Server Username/ Password	Used to log in to the SIP server.

3.4 Configuring VTO Numbers

Numbers can be used to distinguish each VTO. In the villa scenario, we recommend you configure the VTO numbers based on your needs.

Background Information

- The VTO number can contain up to 5 numbers, and it must not be the same as other room number you have already configured.
- If a VTO serves as the SIP server, its room number is 8001 by default. You cannot change it.

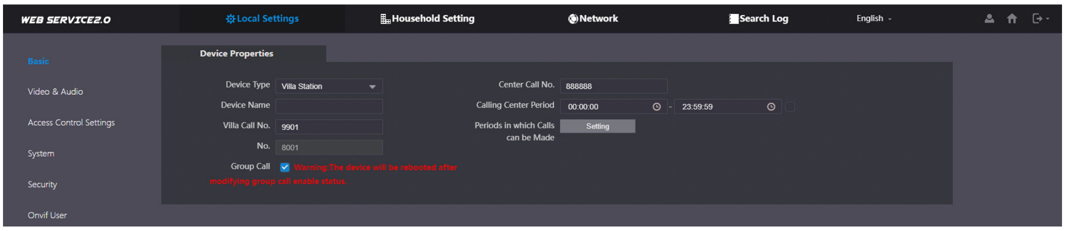
Procedure

Step 1 Log in to the VTO web page.

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

Step 3 Enter the room number you planned for the VTO in **No.**, and then click **Confirm**.

Figure 3-7 Configuring VTO Numbers



Device Type: Villa Station
Device Name:
Villa Call No.: 9901
No.: 8001
Group Call: ☑ Warning:The device will be rebooted after modifying group call enable status.
Center Call No.: 888888
Calling Center Period: 00:00:00 - 23:59:59
Periods in which Calls can be Made: Setting

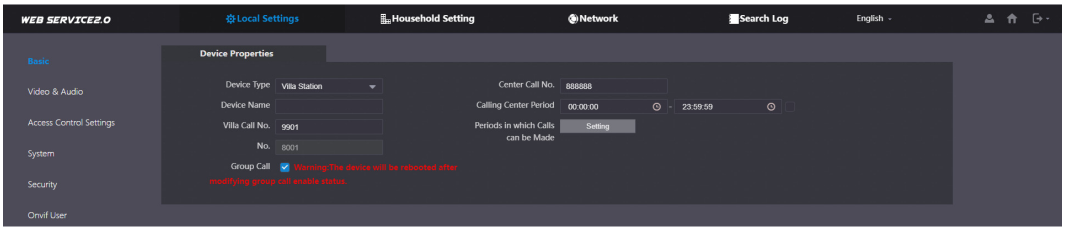
3.5 Configuring Call Numbers and Group Call

Configure basic properties for the VTO, including group call functions, center call number and villa call numbers.

Step 1 Log in to the VTO web page.

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

Figure 3-8 Device properties



Device Type: Villa Station
Device Name:
Villa Call No.: 9901
No.: 8001
Group Call: ☑ Warning:The device will be rebooted after modifying group call enable status.
Center Call No.: 888888
Calling Center Period: 00:00:00 - 23:59:59
Periods in which Calls can be Made: Setting

Step 3 Configure the parameters.

Table 3-3 Parameter description

Parameter	Description
Device Type	Villa Station.
Device Name	The name you planned for your VTO. You could keep it null.
Villa Call No.	Used to call VTHs. It should contain no more than 9 numbers.
Center Call No.	Used to call the center station. It is 888888 by default.
No.	VTO number. 📖 8001 by default when the VTO is selected to work as the SIP server.
Group Call	Enable it for group call.

Step 4 Click **Save**.

3.6 Adding VTOs

You can add other VTOs to the SIP server (in the Villa scenario a VTO serves as the SIP server), and all the VTOs connected to the same SIP server can make video call to each other.

Prerequisites

Before you start, make sure that you have already select a VTO to work as the SIP server (VTO number 8001).

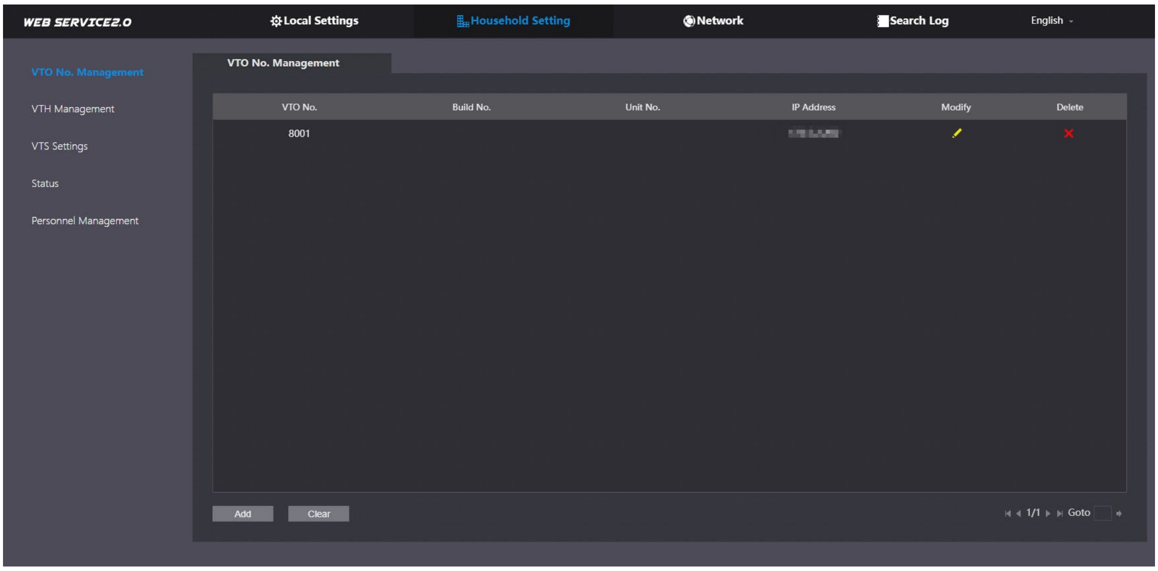
Procedure

Step 1 Log in to the web page of the VTO that works as the SIP server.

Step 2 Select **Household Setting** > **VTO No. Management**.

Step 3 Select **Add**.

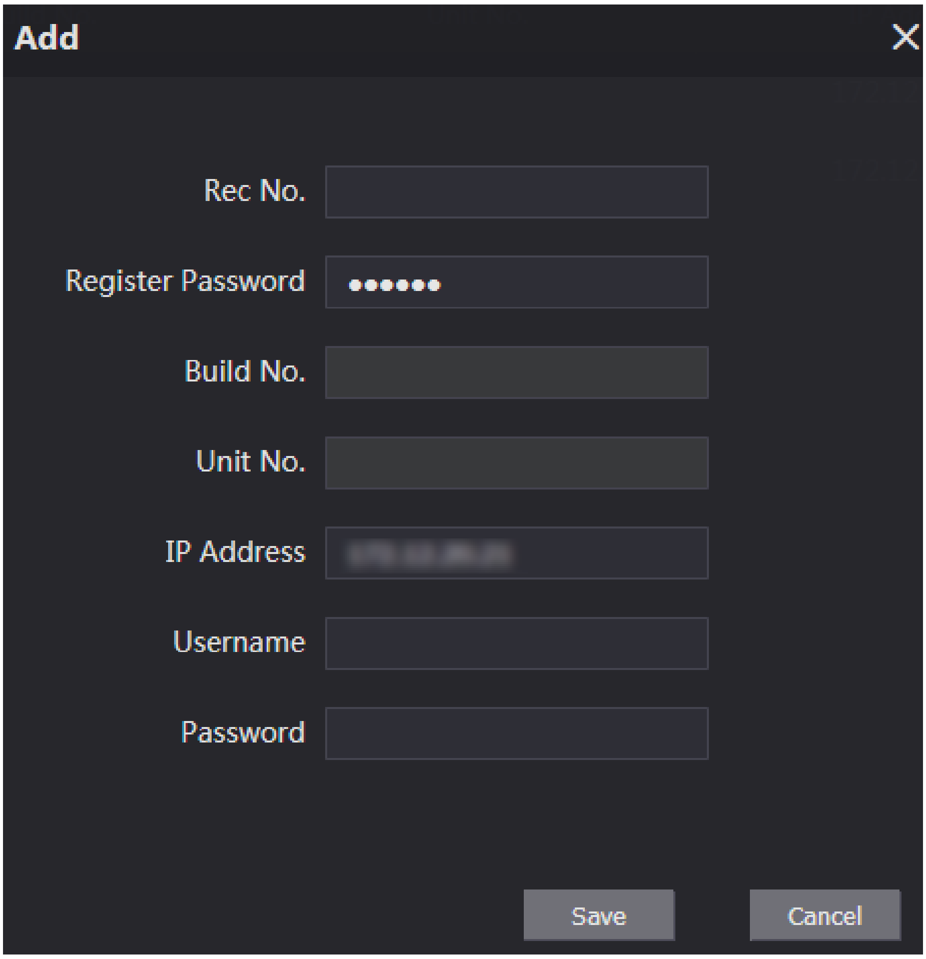
Figure 3-9 VTO No. Management



VTO No.	Build No.	Unit No.	IP Address	Modify	Delete
8001			[redacted]	✎	✕

Step 4 Configure the parameters.

Figure 3-10 Add VTOs



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

Table 3-4 Parameters

Parameter	Description
Rec No.	VTO room number.

Parameter	Description
Register Password	Keep it by default.
Build No.	Keep them null when the VTO serves as the SIP server. The two parameters are only applicable when the platform works as the SIP server.
Unit No.	
IP Address	VTO IP address.
Username	The username and password used to log in to the web page of the VTO.
Password	

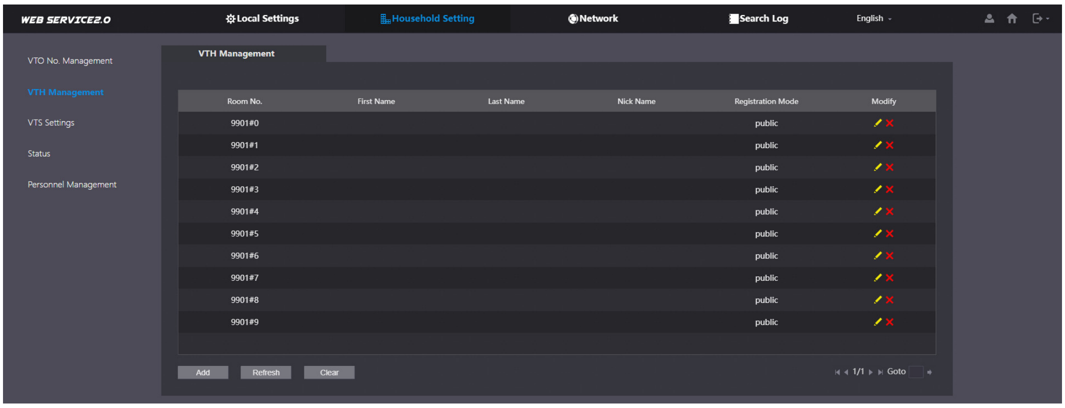
3.7 Adding VTH Room Number

When VTO serves as the SIP server, you can add VTH into the main VTO to achieve intercom functions.

Step 1 Log in to the VTO web page.

Step 2 Select **Household Setting** > **VTH Management**.

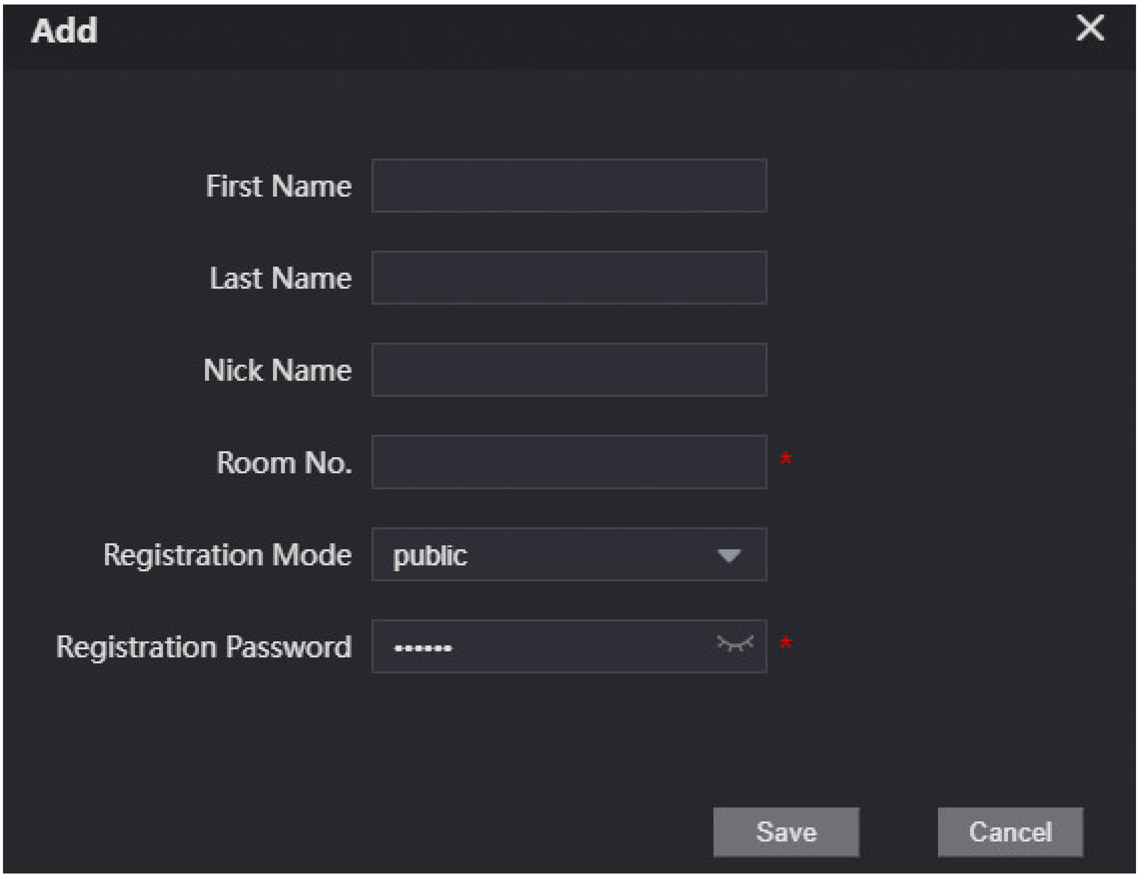
Figure 3-11 VTH Management



Room No.	First Name	Last Name	Nick Name	Registration Mode	Modify
9901#0				public	✎ ✕
9901#1				public	✎ ✕
9901#2				public	✎ ✕
9901#3				public	✎ ✕
9901#4				public	✎ ✕
9901#5				public	✎ ✕
9901#6				public	✎ ✕
9901#7				public	✎ ✕
9901#8				public	✎ ✕
9901#9				public	✎ ✕

Step 3 Select **Add** to register new VTH onto the main VTO.

Figure 3-12 Add VTH



Add

First Name

Last Name

Nick Name

Room No. *

Registration Mode: public

Registration Password: •••••• *

Step 4 Configure the parameters.

Table 3-5 Description

Parameters	Description
First Name	Information used to differentiate each room. You can also keep them null.
Last Name	
Nick Name	
Room No.	The room number can contain 6 digits of numbers of letters or their combination at most, and it cannot be the same as any VTO number. When there are multiple VTHs, the room number for the master VTH should end with #0 and the room numbers for extension VTHs with #1, #2…
Registration Mode	Select **Public**.
Registration Password	Leave it as default.

Step 5 Click **Save**.

Related Operations

Click ✎ to modify room information, and ✕ to delete the room.

3.8 Binding VTH Room Numbers (For Certain Models Only)

This section only applies to the VTO model that with multiple buttons.

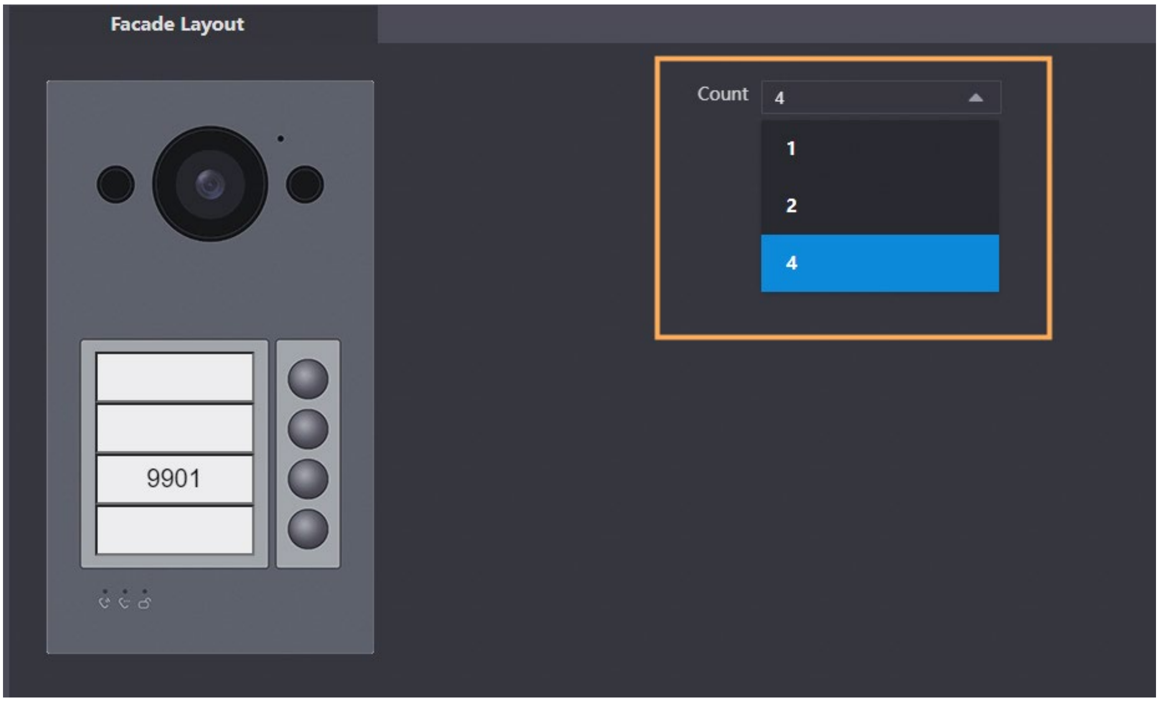
Step 1 Log in to the VTO web page.

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

Step 3 In the **Façade Layout** section, select **Count** types.

Count 1: Can only bind one room number.
Count 2: Can bind two room numbers.
Count 4: Can bind four room numbers.

Figure 3-4 Count



Facade Layout

Count 4

Step 4 Click on the white module, and select the room number from the **Room List** you want to bind.

Figure 3-5 White module

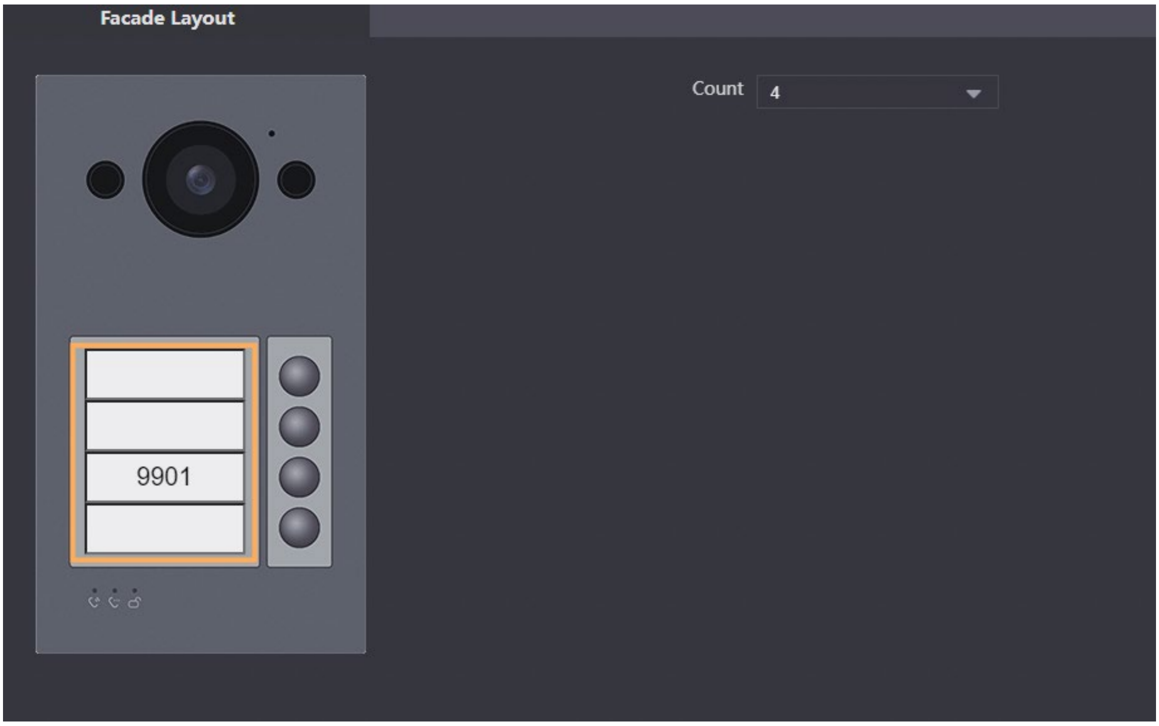
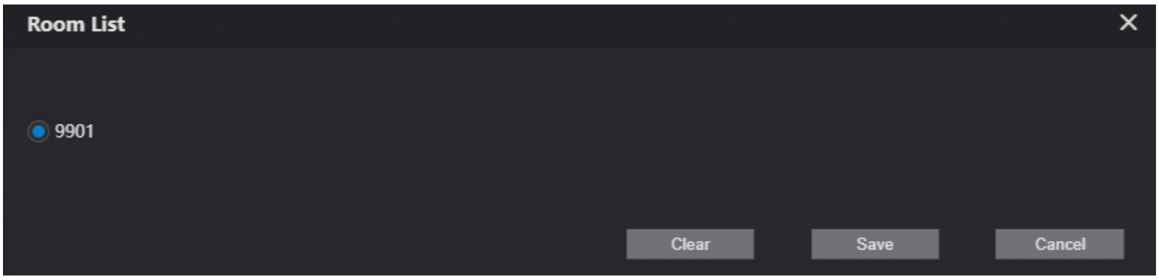


Figure 3-6 Room list



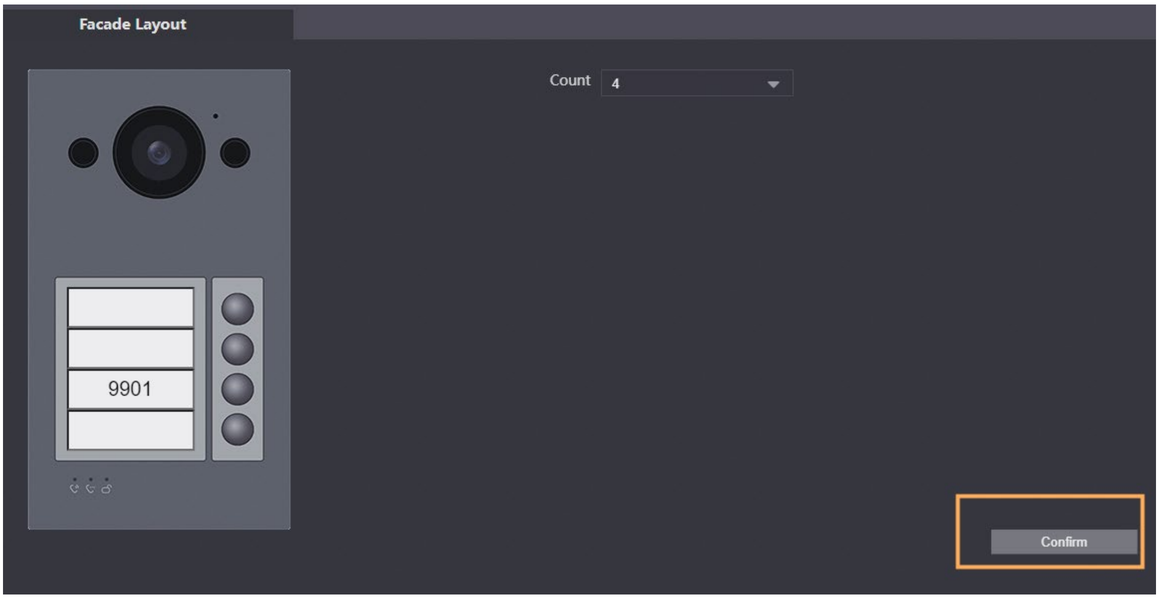
Room List

● 9901

Step 5 Click **Save** to save the selected room number.

Step 6 Click **Confirm** to save all the settings.

Figure 3-7 Confirm



3.9 Issuing Cards

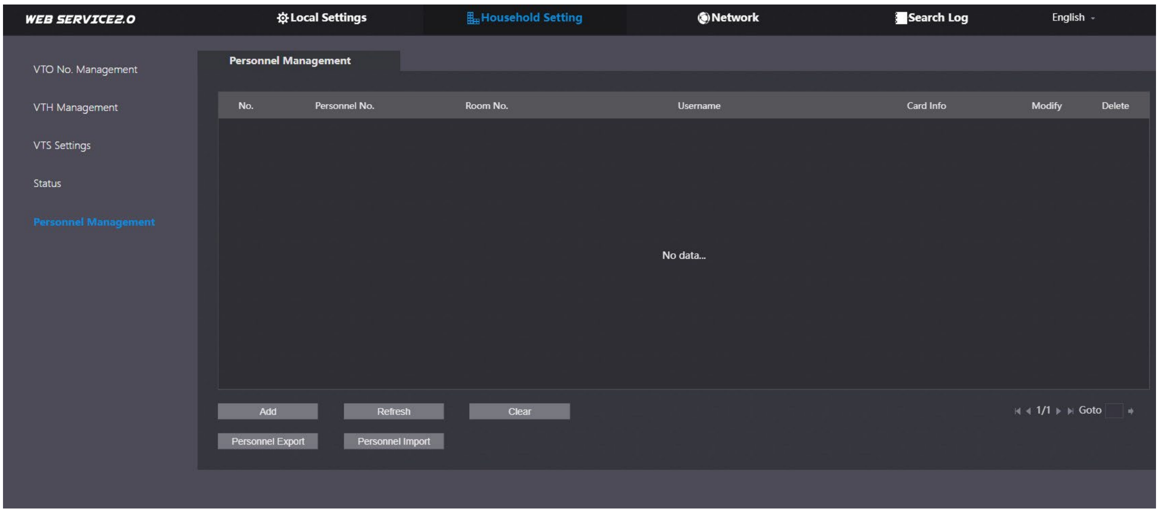
Issue an access card to unlock the door of a room.

To use this function, the VTO must have a card reader.

Step 1 Log in to the VTO web page.

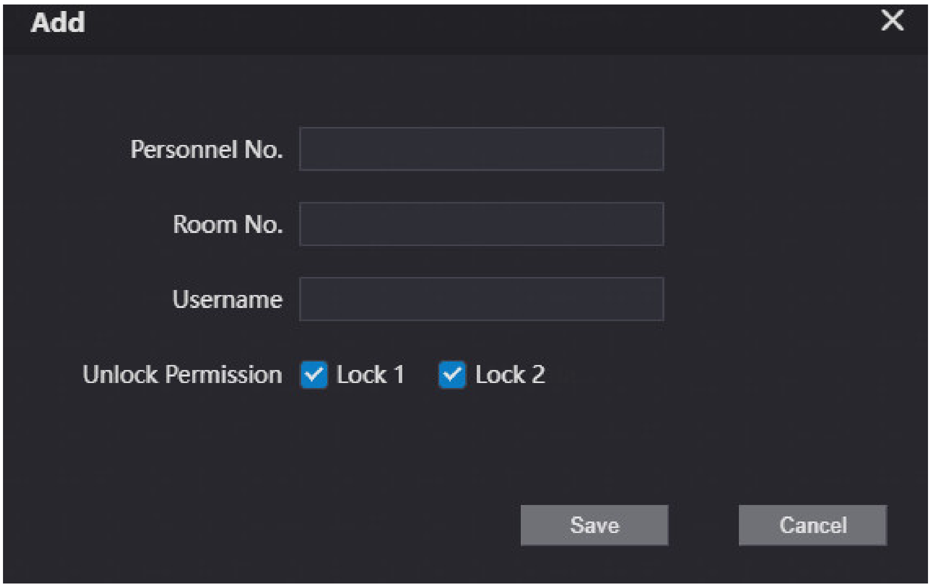
Step 2 Select **Household Setting** > **Personnel Management**.

Figure 3-8 Figure 3-13 Personnel management



Step 3 Click **Add**.

Figure 3-9 Add Personnel Information



Personnel No.

Room No.

Username

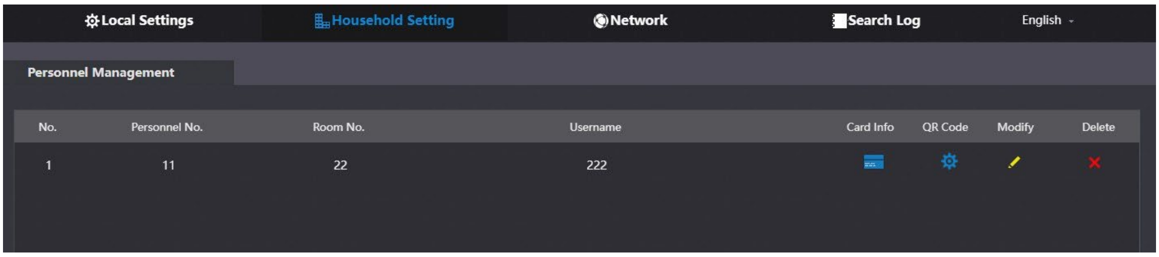
Unlock Permission ☑ Lock 1 ☑ Lock 2

Step 4 Enter the parameters, and then click **Save**.

The personnel information displays on the web page.

For some VTO models, the QR code is embedded in the **Personnel Management** page. Yet for some models, you need to go to **Network** > **Basic** > **Cloud Service** to check the QR code.

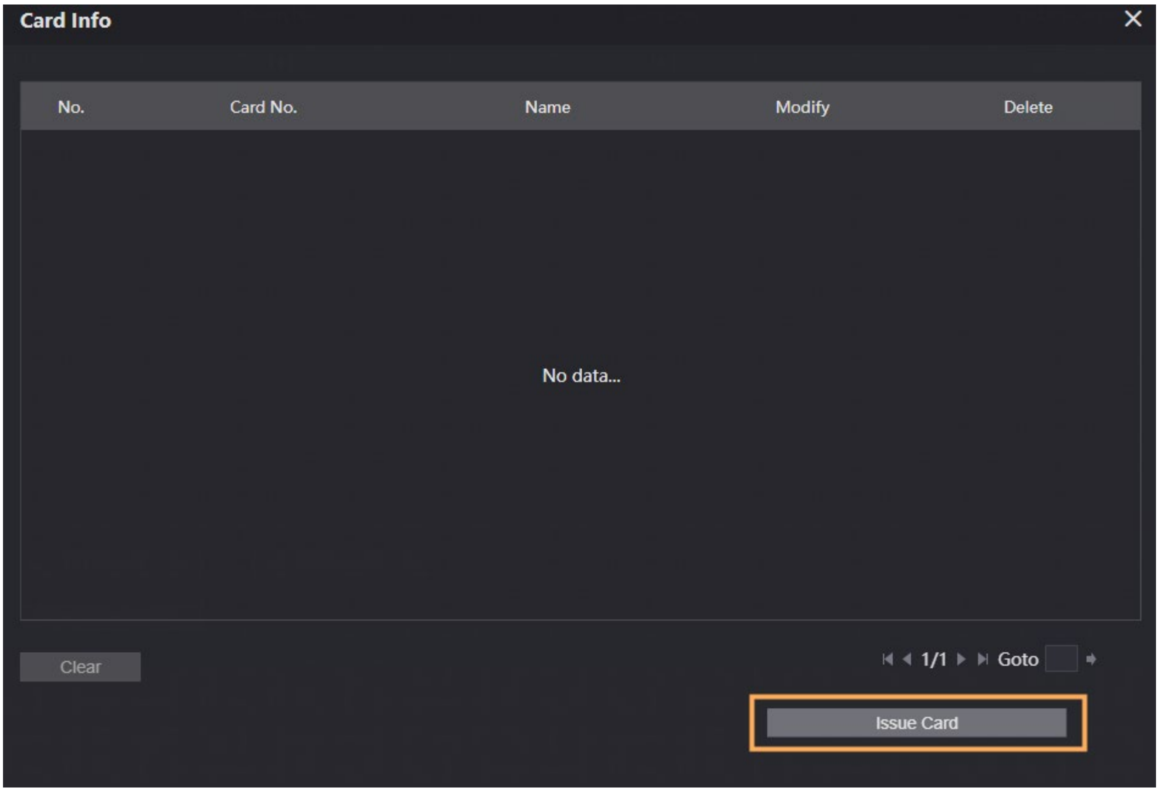
Figure 3-10 Figure 3-14 Operation succeed



No.	Personnel No.	Room No.	Username	Card Info	QR Code	Modify	Delete
1	11	22	222	▬	⚙	✎	✕

Step 5 Select 💳 to go to the card issuing window.

Figure 3-11 Figure 3-15 Card issuing window



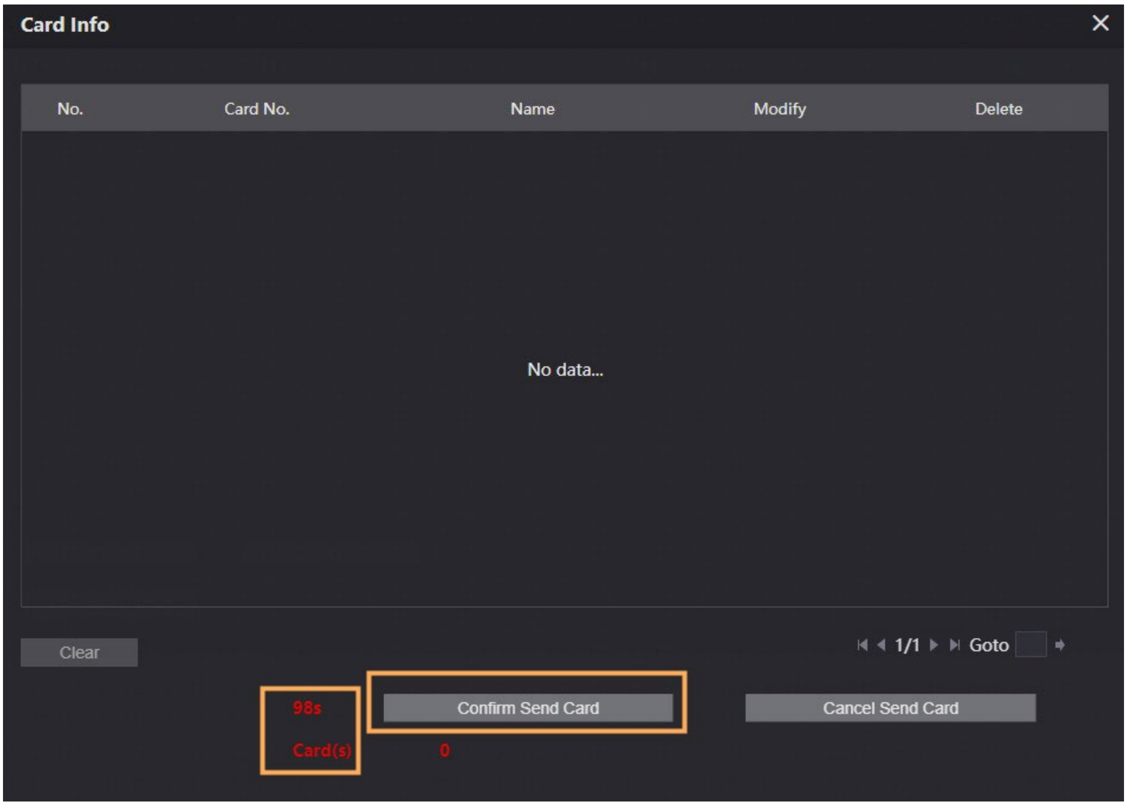
No.	Card No.	Name	Modify	Delete

No data...

Step 6 Click **Issue Card** to issue cards.

The web page displays the countdown prompt (120 s). Once the countdown starts, you need to swipe the card on the card reader of the VTO within this time period. After the swiping, the card number will be automatically recognized by the VTO.

Figure 3-12 Figure 3-16 Countdown in process



No.	Card No.	Name	Modify	Delete

No data...

Step 7 Click **Confirm Send Card** after swiping to complete the issuing process.

Other Operations

- Click 🟩 to set it to loss, and then the icon changes to 🟥. The lost card cannot be used to open the door.
- Click ✎ or ✕ to modify the username or delete the card.

4 Commissioning

After the basic configuration is complete, check whether the intercom communication works.

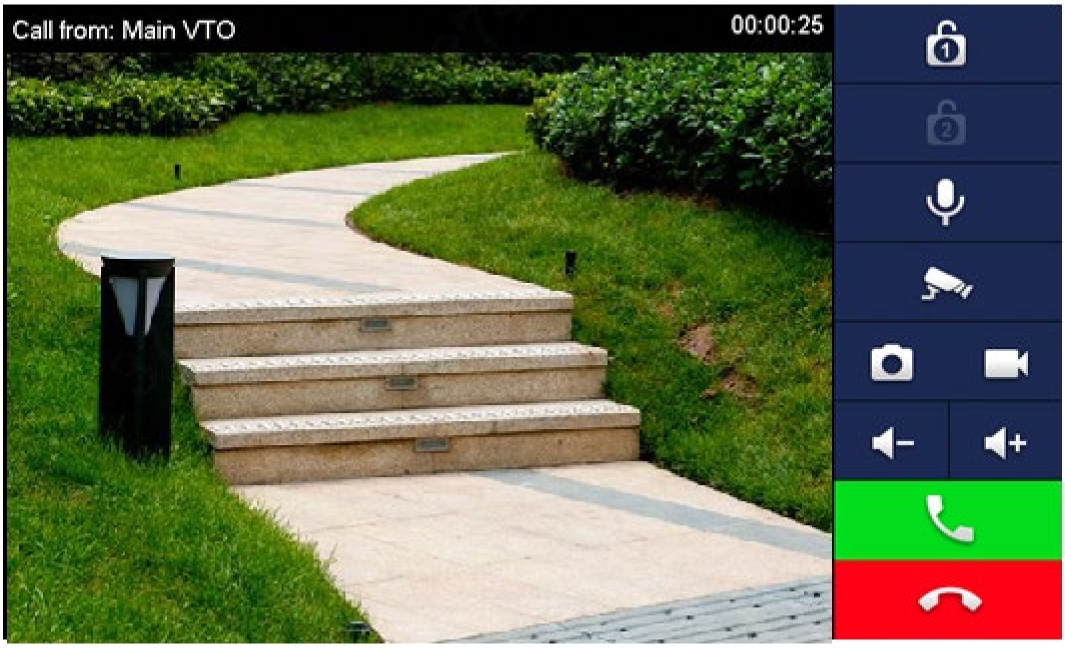
4.1 VTO Calling VTH

Once the VTO and VTH are connected, the duel communication function is enabled.

Step 1 Dial a room number (for example, 9901) on the VTO.

Step 2 Tap ☎ to answer the call on the VTH.

Figure 4-1 Call Screen



4.2 VTH Monitoring VTO

A VTH can monitor the VTO.

Step 1 On the home screen of the VTH, select **Monitor** > **Door**.

Step 2 Set the VTO to go to the monitoring screen.

Step 3 Tap the icon to view the video.

Figure 4-2 Door

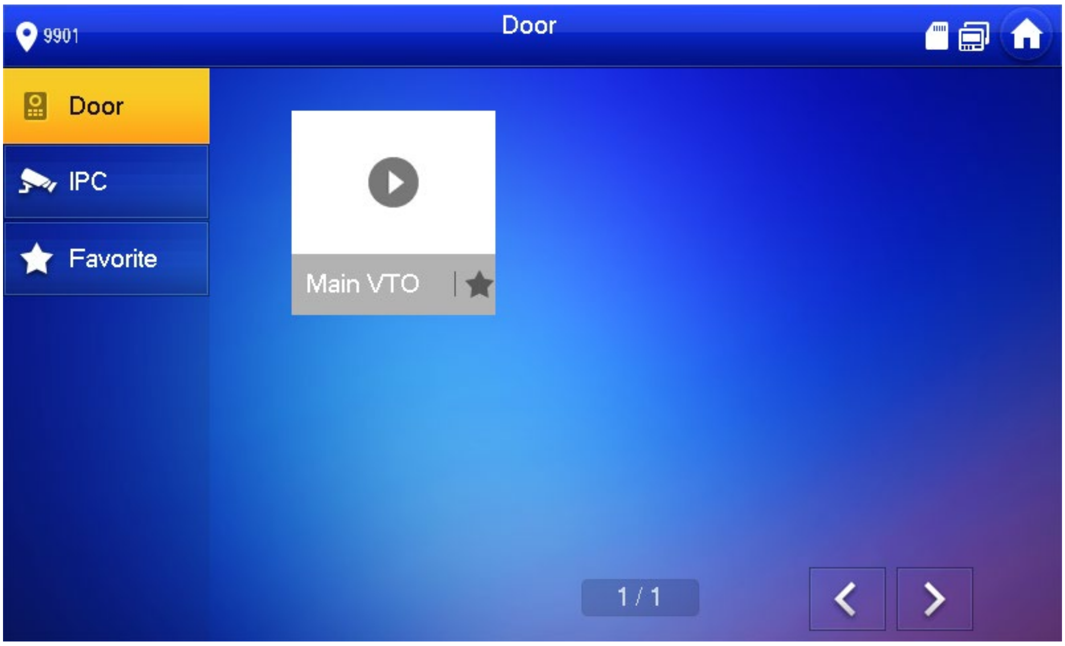
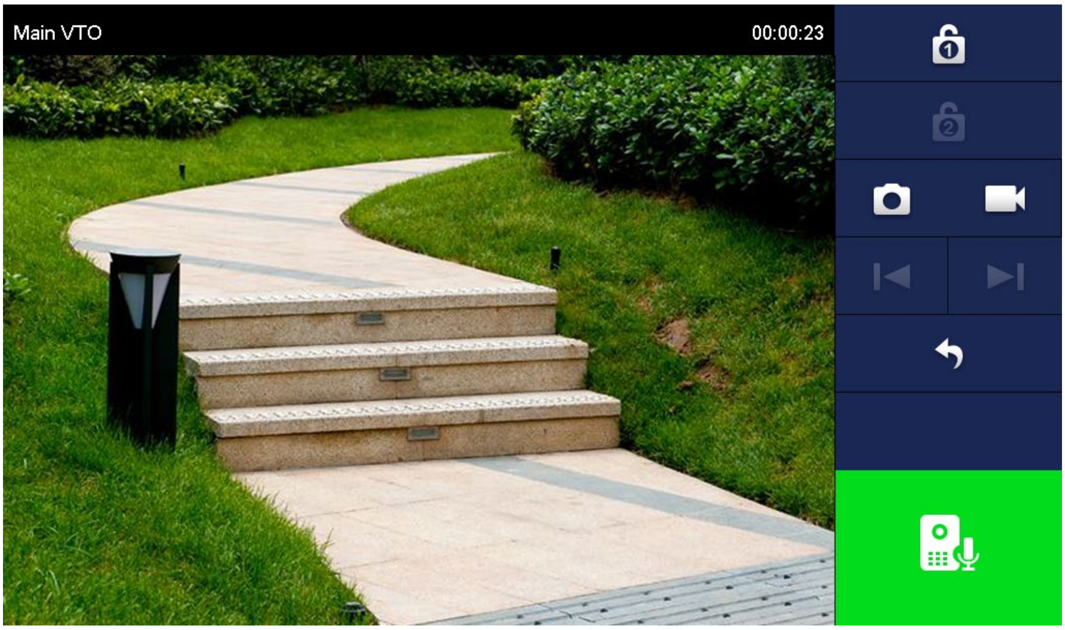


Figure 4-3 Monitoring



Appendix 1 Cybersecurity Recommendations

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 device 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. **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.

8. **Assign Accounts and Privileges Reasonably**

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

9. **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.

10. **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.

11. **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.

12. **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.

13. **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.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.