Villa Door Station (Version 4.5)

Quick Start Guide



V1.0.0

Foreword

General

This manual introduces the structure, mounting process, and basic configuration of the villa door station (hereinafter referred to as "VTO").

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Date
V1.0.0	First release.	December 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.

- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The following description is the correct application method of the device. Please read the manual carefully before use to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirements

- Do not expose the device to direct sunlight or heat source.
- Do not install the device in a humid or dusty area.
- Install the device horizontally at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device, or put on the device anything filled with liquids.
- Install the device at a well-ventilated place and do not block its vent.
- Use the device only within rated input and output range.
- Do not dismantle the device by yourself.
- Transport, use and store the device within allowed humidity and temperature range.

Power Requirements

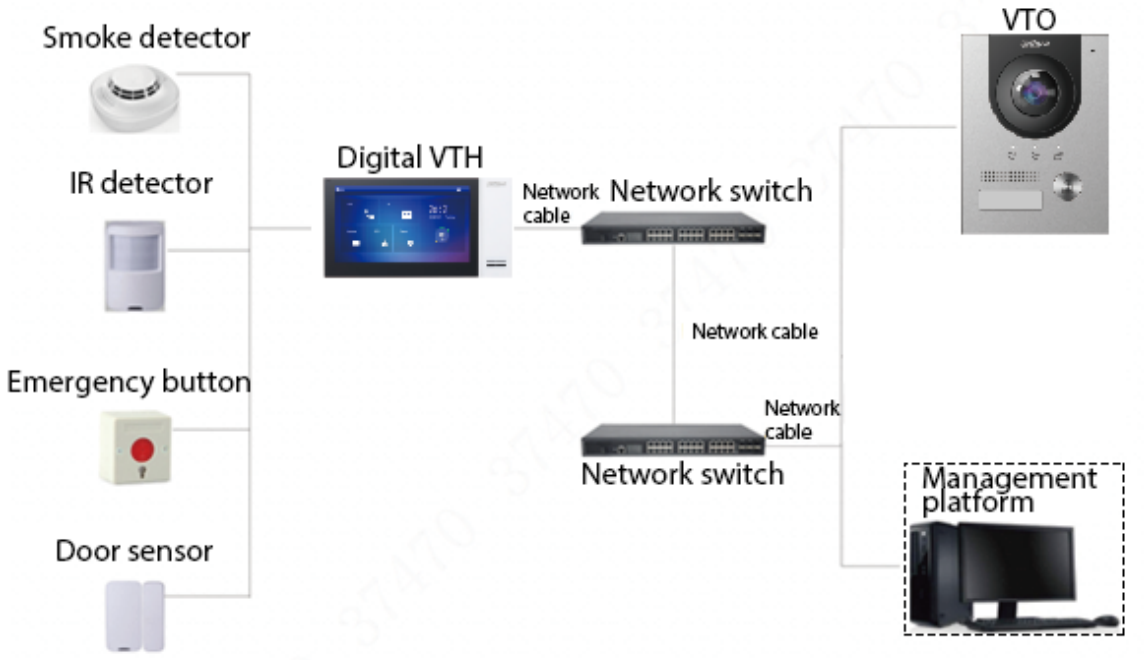
- The product must use electric wires that conform to your local requirements.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Network Diagram 1
2 Appearance 2
2.1 VTO2101E-P 2
2.1.1 Front Panel 2
2.1.2 Rear Panel 3
2.2 VTO2202F-P-S2/ VTO2202F-P/VTO2202F/VTO2201F-P 4
2.2.1 Front Panel 4
2.2.2 Rear Panel 5
2.3 VTO2111D-P-S2/VTO1101D-P 6
2.3.1 Front Panel 6
2.3.2 Rear Panel 7
2.4 VTO3211D-P-S2 8
2.4.1 Front Panel 8
2.4.2 Rear Panel 9
2.5 VTO3221E-P 10
2.5.1 Front Panel 10
2.5.2 Rear Panel 11
2.6 VTO2211G-P/VTO1201G-P 12
2.6.1 Front Panel 12
2.6.2 Rear Panel 13
3 Installation 15
4 Configuration 16
4.1 Procedure 16
4.2 Configuration Tool 16
4.3 Configuring VTO 16
4.3.1 Initialization 16
4.3.2 Configuring VTO Number 17
4.3.3 Configuring Network Parameters 18
4.3.4 Configuring SIP Server 19
4.3.5 Configuring Call Number and Group Call 20
4.3.6 Adding VTOs 20
4.3.7 Adding Room Number 21
4.4 Commissioning 23
4.4.1 VTO Calling VTH 23
4.4.2 VTH Monitoring VTO 23
5 EasyViewer Plus 25
Appendix 1 Cybersecurity Recommendations 26

1 Network Diagram

Figure 1-1 Network diagram



In certain applications such as villa, Management Center/Platform is usually unnecessary.

2 Appearance

2.1 VTO2101E-P

2.1.1 Front Panel

Figure 2-1 VTO2101E-P

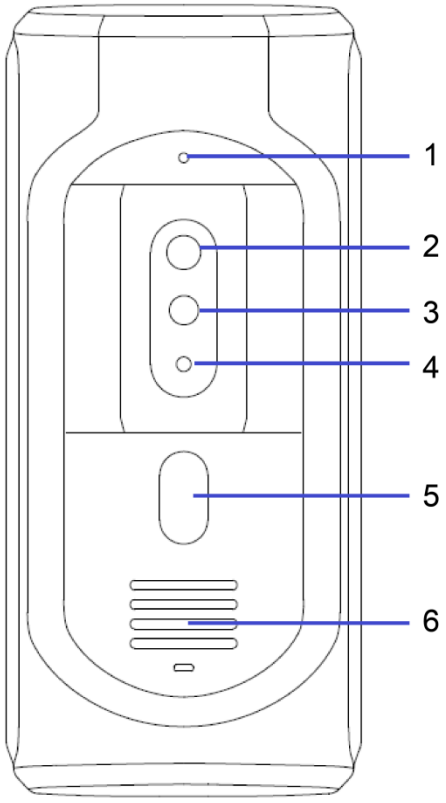


Table 2-1 Front panel description

No.	Name	Description
1	Microphone	—
2	Camera	—
3	IR illunimation light	Provides extra IR light for the camera when it is dark.
4	Light sensor	Detects ambient lighting condition.
5	Call button	Call VTHs or the management center.
6	Speaker	—

2.1.2 Rear Panel

Figure 2-2 VTO2101E-P

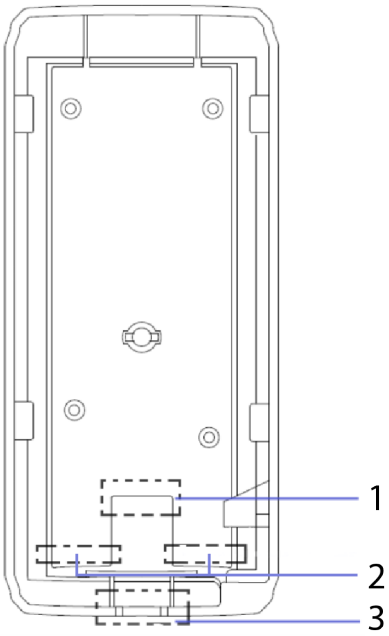


Table 2-2 Rear panel description

No.	Name	Description
1	Network port	Connects to the network cable.
2	RS-485 ports	See the figure and the table below.
3	Cable outlet	Thread the cables here.

Figure 2-3 Cable connection

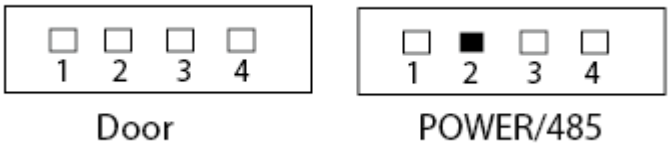


Table 2-3 Port description

DOOR		POWER/485	
No.	**Name**	**No.**	**Name**
1	NO	1	+12V
2	NC	2	GND
3	COM	3	RS-485A
4	ALARM IN or Unlock (default)	4	RS-485B

2.2 VTO2202F-P-S2/ VTO2202F-P/VTO2202F/VTO2201F-P

2.2.1 Front Panel

Figure 2-4 Front panel

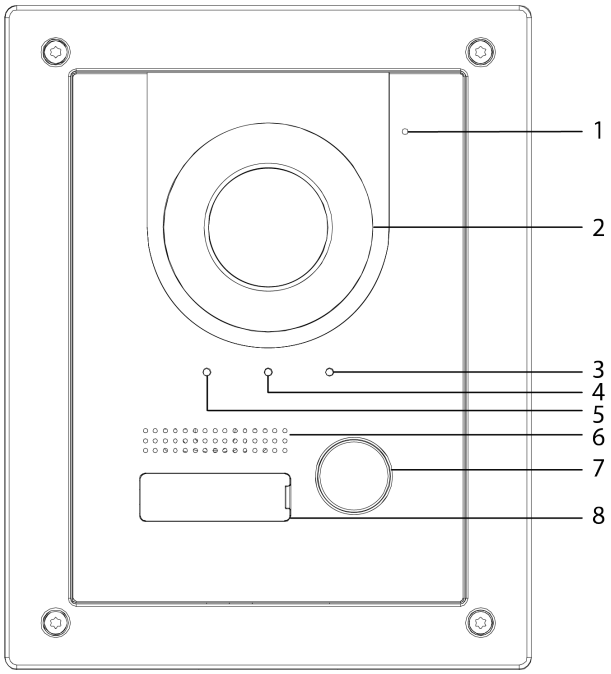


Table 2-4 Front panel description

No.	Name	Description
1	Microphone	—
2	Camera	—
3	Indicator	On: Door unlocked.
4		On: In a call.
5		On: Calling.
6	Speaker	—
7	Call button	Call other VTHs or the management center.
8	Name tag	Host name.

2.2.2 Rear Panel

Figure 2-5 Rear panel

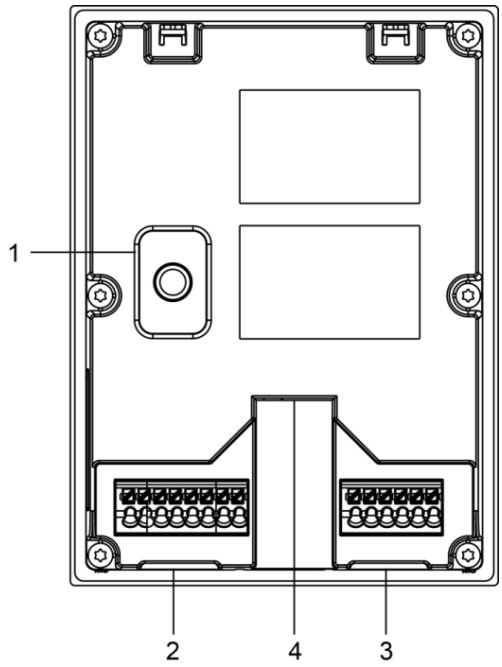


Table 2-5 Rear panel description

NO	Name	Description
1	Anti-tampering switch	When the VTO is removed from the wall forcibly, an alarm will be triggered and the alarm information will be sent to management center.
2	Port	From left to right: GND +12V_OUT RS485_B RS485_A ALARM_NO ALARM_COM VTO2202F-P-S2: 2-wire + (48V); VTO2202F-P and VTO2202F: EOC1 (+12V); VTO2201F: +24V. VTO2202F-P-S2: 2-wire - (GND); VTO2202F-P and VTO2202F: EOC2 (GND); VTO2201F: GND.
3		From left to right: DOOR_BUTTON DOOR_FB GND DOOR_NC DOOR_COM DOOR_NO
4	Ethernet port	Connects to the network with an Ethernet cable. Only models with "P" support PoE.

2.3 VTO2111D-P-S2/VTO1101D-P

2.3.1 Front Panel

Figure 2-6 Front panel

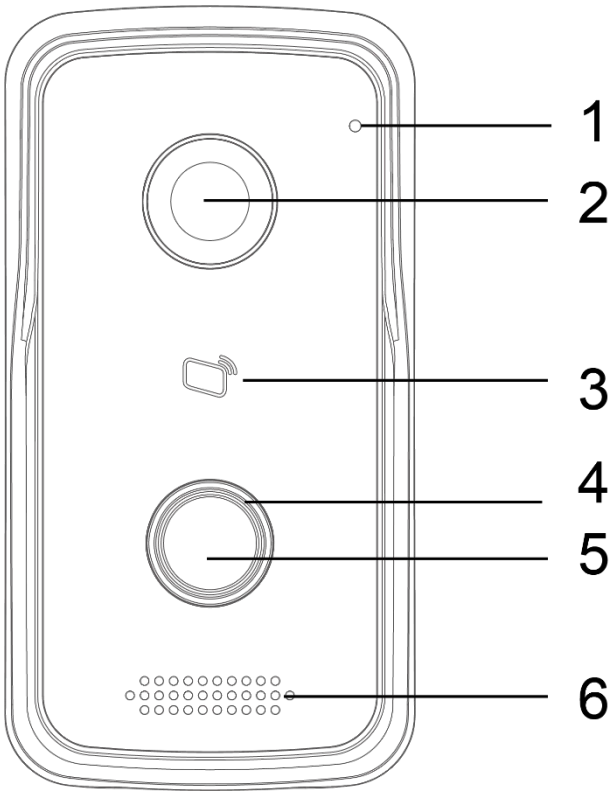


Table 2-6 Front panel description

No.	Name	Description
1	Microphone	—
2	Camera	—
3	Card reading area	Swipe to unlock or issue card.
4	Indicator	● Solid blue: Standby mode. ● Flashes blue: Calling or there is no network.
5	Call button	Call VTHs or the management center.
6	Speaker	—

2.3.2 Rear Panel

Figure 2-7 Rear panel

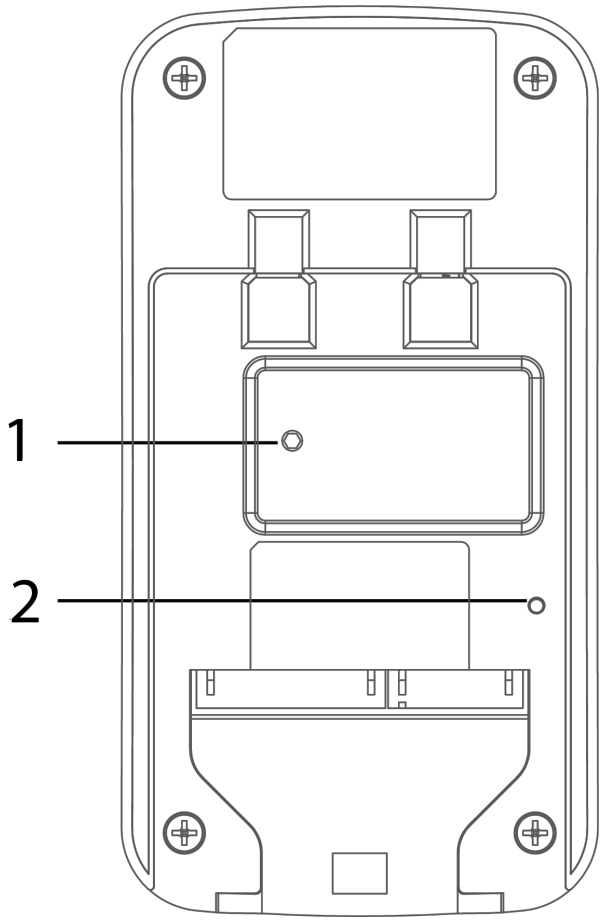


Table 2-7 Rear panel description

No.	Name	Description
1	Anti-tampering switch	When the VTO is removed from the wall forcibly, an alarm will be triggered and the alarm information will be sent to management center.
2	RESET	Press and hold it for 10 seconds to reset all settings.

Figure 2-8 Cable connection

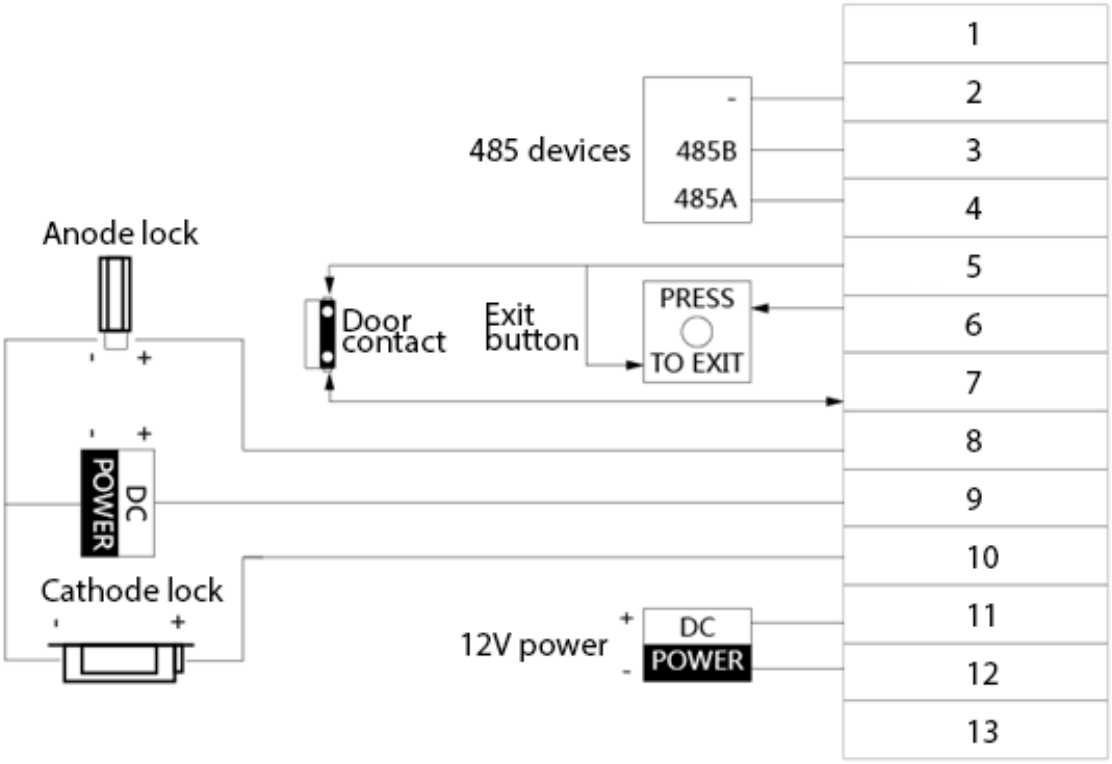


Table 2-8 Port description

No.	Description	No.	Description
1	N/A	8	NC
2	GND	9	COM
3	485_B	10	NO
4	485_A	11	GND
5	GND	12	12V
6	UNLOCK	13	NET
7	FEEDBACK	—	—

2.4 VTO3211D-P-S2

2.4.1 Front Panel

The number of buttons on the front panel varies with models. VTO3211D-P-S2 has one button, VTO3211D-P2-S2 has two buttons, and VTO3211D-P4-S2 has four buttons. Here we take VTO3211D-P4-S2 as an example.

Figure 2-9 VTO3211D-P4-S2

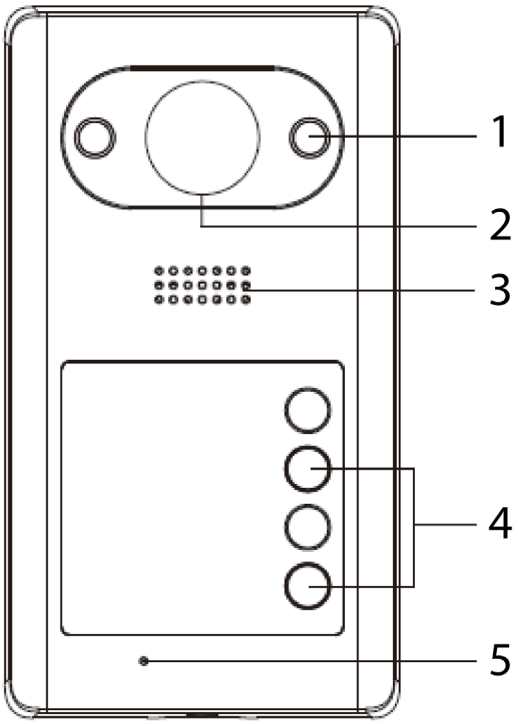


Table 2-9 Front panel description

No.	Name	Description
1	IR illuminator	Provides extra IR light for the camera when it is dark.
2	Camera	—
3	Speaker	—
4	Call button	Call VTHs or the management center.
5	Microphone	—

2.4.2 Rear Panel

Figure 2-10 VTO3211D-P4

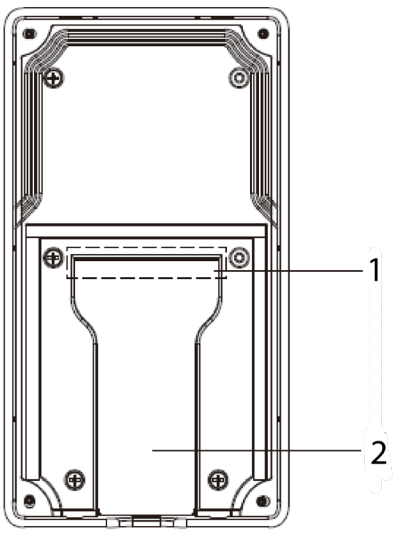


Table 2-10 Rear panel description

No.	Name	Description
1	Cable ports	See the figure and the table below.
2	Cable outlet	Thread the cables here.

Figure 2-11 Cable connection

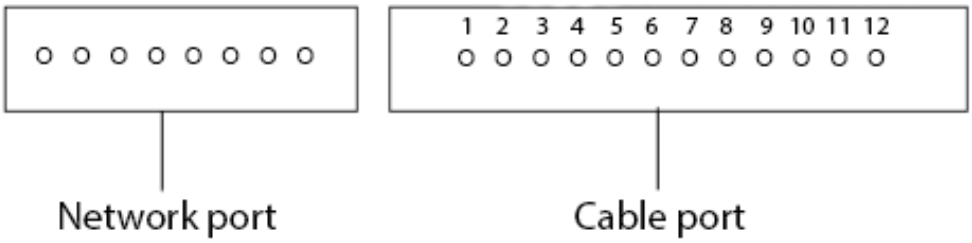


Table 2-11 Cable port description

No.	Name	No.	Name
1	ALM_COM	7	DOOR_FEED
2	ALM_NO	8	DOOR_NC
3	ALM_IN	9	DOOR_COM
4	RS485B	10	DOOR_NO
5	RS485A	11	GND
6	DOOR_OPEN	12	DC 12V

2.5 VTO3221E-P

2.5.1 Front Panel

Figure 2-12 Front panel

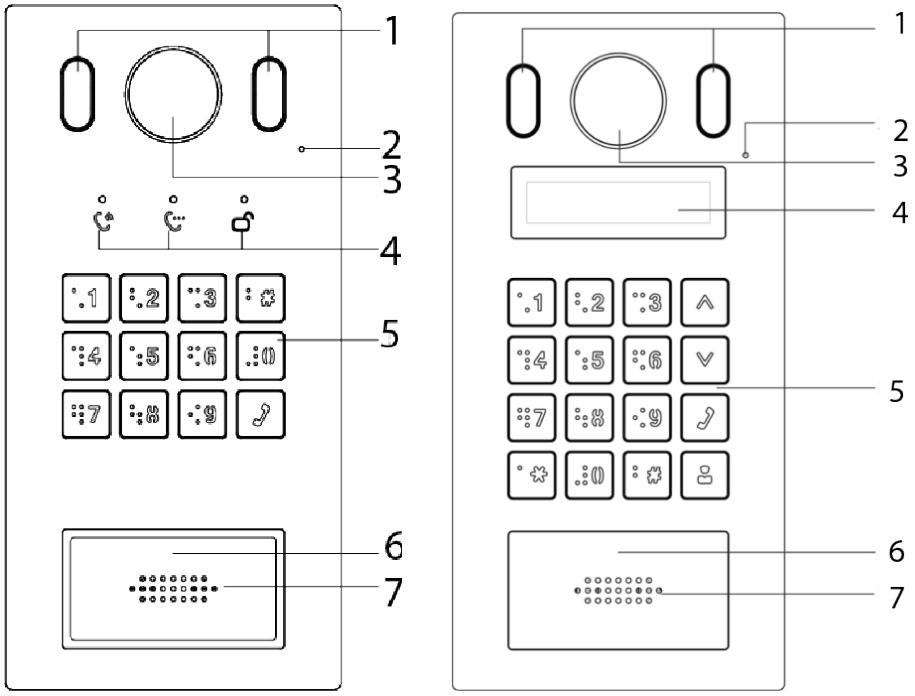


Table 2-12 Front panel description

No.	Name	Description
1	Illuminator	Provides extra light for the camera when it is dark.
2	Microphone	—
3	Camera	—
4	Indicators	Displays status on calling, talking and unlock.
5	Keypad	—
6	Card reading area	Swipe a card here to unlock the door.
7	Speaker	—

2.5.2 Rear Panel

Figure 2-13 VTO3221E-P

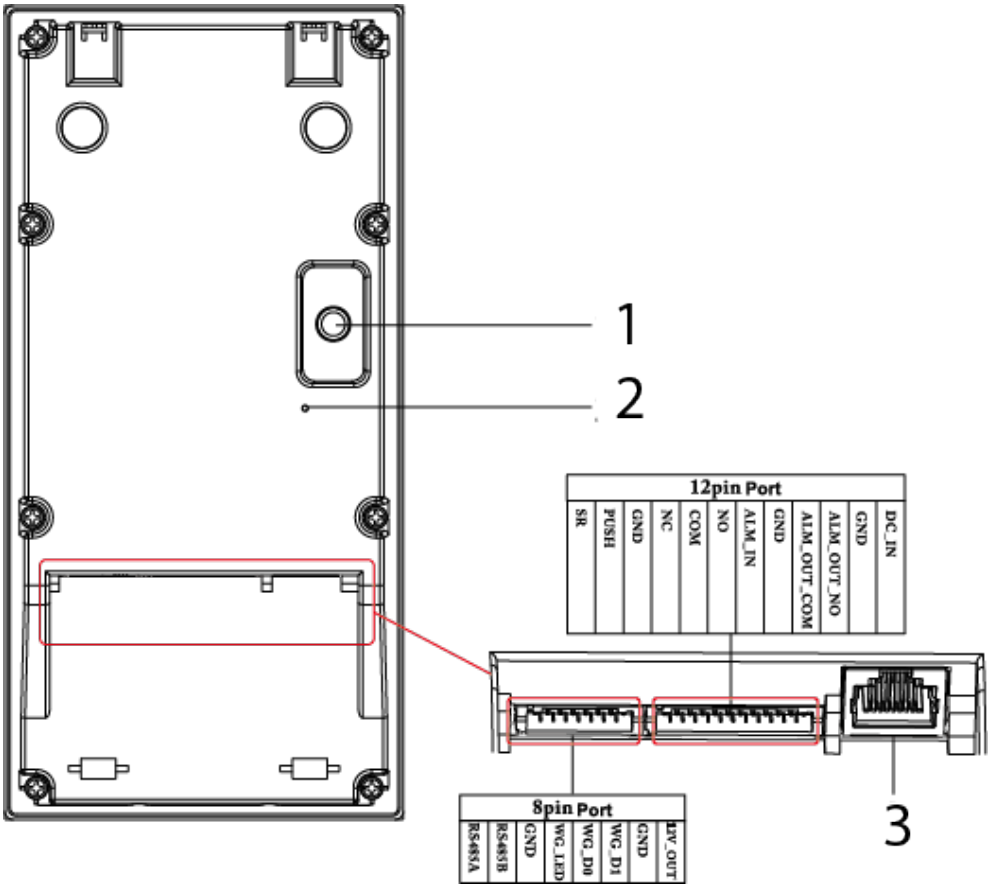


Table 2-13 Rear panel description

No.	Name	Description
1	Anti-tampering switch	When the VTO is removed from the wall forcibly, an alarm will be triggered and the alarm information will be sent to management center.
2	Reset button	Press and hold it for 10 s to reset all settings.
3	Ethernet port	Connects to the Ethernet cable.

2.6 VTO2211G-P/VTO1201G-P

2.6.1 Front Panel

Figure 2-14 Front panel of VTO2211G/VTO1201G

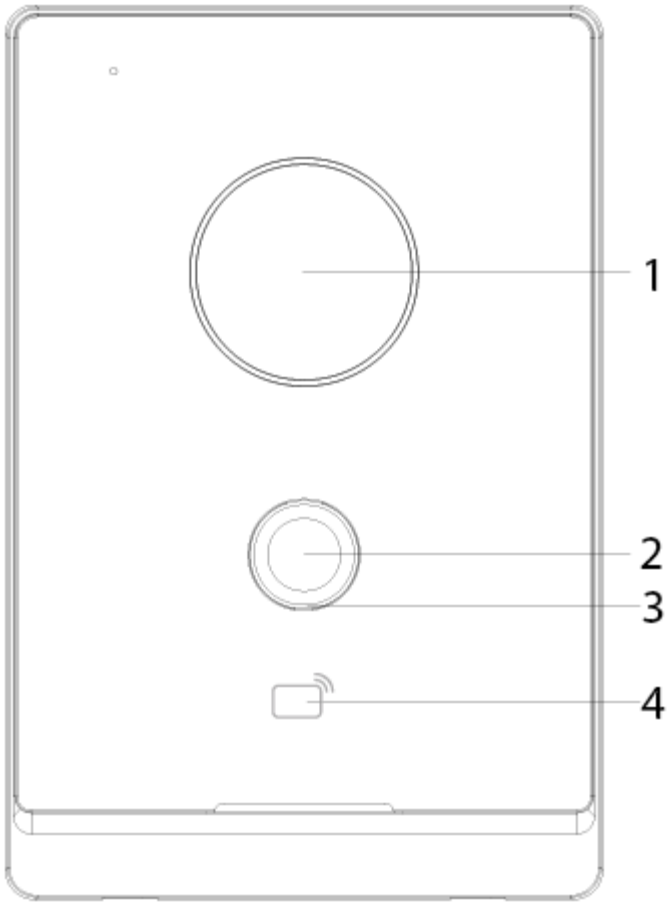


Table 2-14 Front panel description

No.	Name	Description
1	Camera	—
2	Call button	Call VTHs or the management center.
3	Indicator	● Off: The device is in standby mode. ● Solid green: Making a call. ● Solid blue: In a call. ● Yellow-green: Door unlocked by VTH while the VTO is making a call. ● Red-blue: Door unlocked by VTH when the VTO is in a call. ● Blue breathing: Network disconnected.
4	Card reading area	Swipe a card here to unlock the door (only for VTO2211G-P).

2.6.2 Rear Panel

Figure 2-15 Rear panel of VTO2211G-P/VTO1201G-P

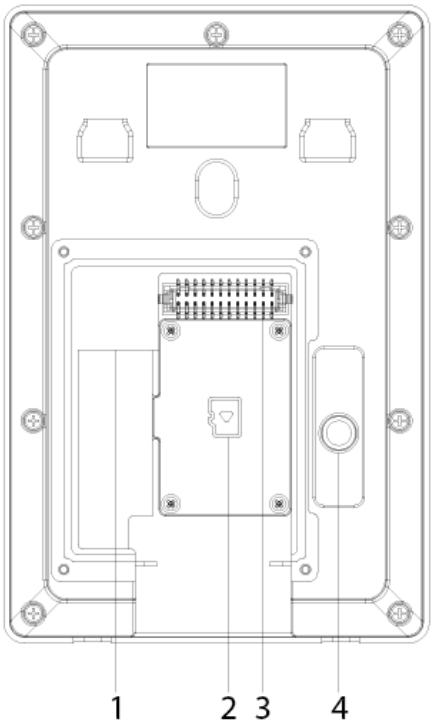
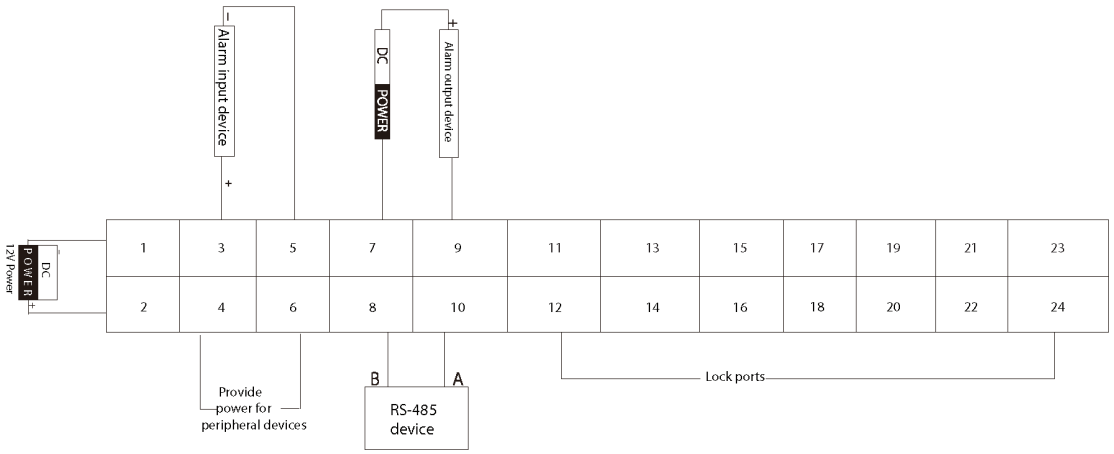


Table 2-15 Rear panel description

No.	Description	No.	Description
1	Network port	3	Ports
2	SD card cover	4	Anti-tampering switch

Figure 2-16 VTO2211G-P cable connection



Ports 12, 14, 16, 18, 20, 22 and 24 are used to connect to locks.

Table 2-16 Port description

No.	Name	No.	Name
1	DC_IN-	13	Not available
2	DC_IN+	14	DOOR1_COM

No.	Name	No.	Name
3	ALARM_IN	15	Not available
4	+12V_OUT	16	DOOR1_NO
5	GND	17	Not available
6	GND	18	GND
7	ALARM_NO	19	Not available
8	RS485B	20	DOOR1_FB
9	ALARM_COM	21	Not available
10	RS485A	22	GND
11	Not available	23	Not available
12	DOOR1_NC	24	DOOR1_PUSH

Figure 2-17 VTO1201G-P cable connection

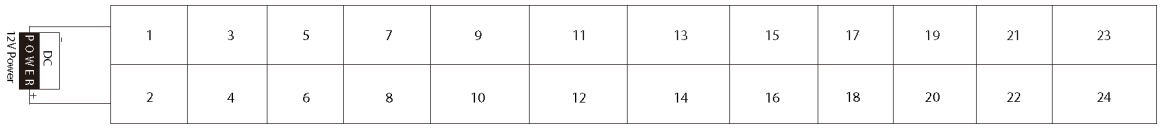
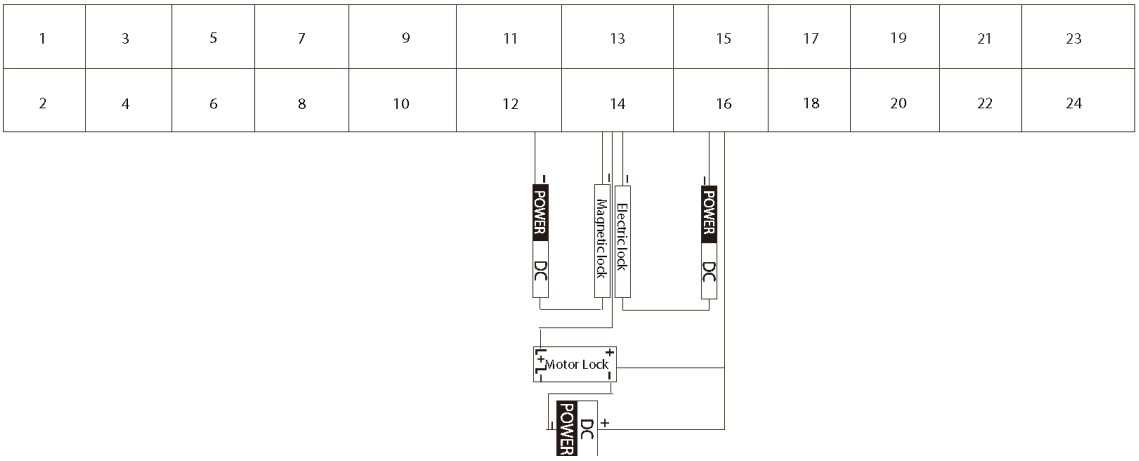


Table 2-17 Port description

No.	Name
1	DC_IN-
2	DC_IN+
3-24	Reserved function

Figure 2-18 Lock cable connection

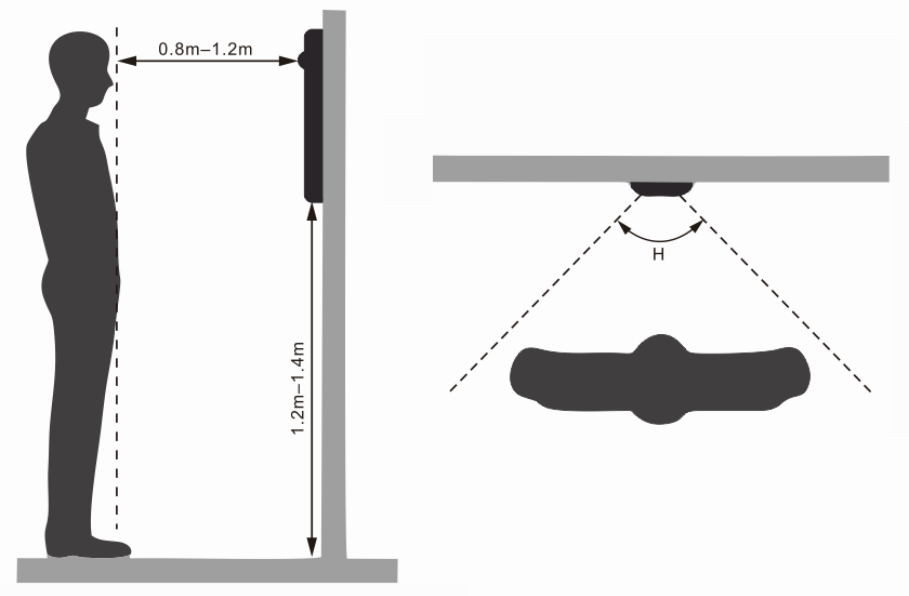


You can connect a magnetic lock or electric lock as needed. See the above figure for the port connection rules.

3 Installation

- Installation and configuration must be done by professional teams. Contact technical support if you need to repair the device.
- See the figure below for the installation position. The horizontal view angle of the device varies with models, and the human face should aim at the center of the device.

Figure 3-1 Installation position



4 Configuration

This chapter introduces basic configurations to the VTO and VTH devices. See the user's manual for details.

Interfaces might vary with software version. The actual interface shall prevail.

4.1 Procedure

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

Step 1 Plan IP and number (works as a phone number) for each device.

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

Step 3 Configure the VTH. See the VTH user's manual.

Step 4 Check if all settings are correct. See "4.4 Commissioning".

4.2 Configuration Tool

You can download the configuration tool "VDPConfig" and use it to configure and update multiple devices. For more details, see the corresponding user's manual.

4.3 Configuring VTO

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

4.3.1 Initialization

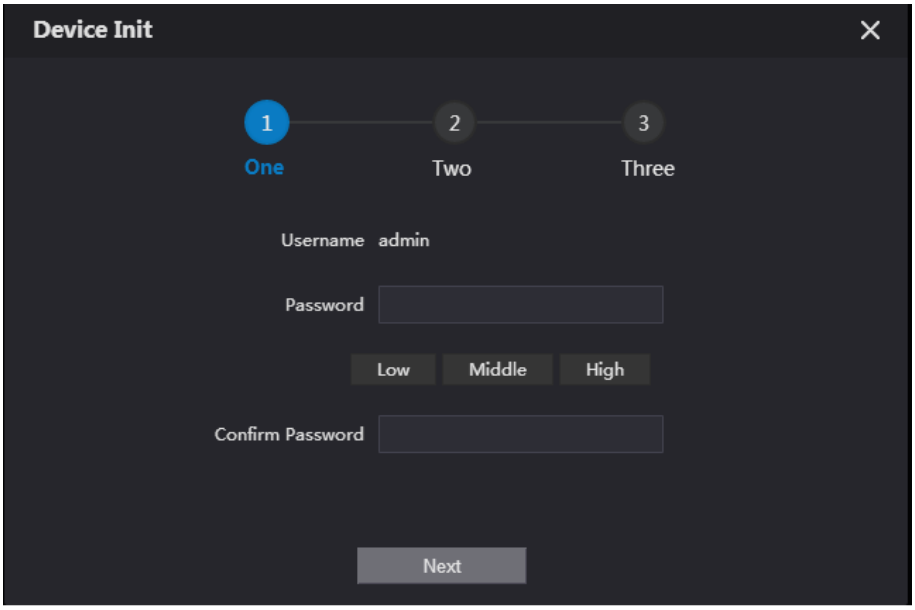
Make sure that the PC is in the same network segment.

Step 1 Power on the VTO.

Step 2 Go to the IP address of the VTO in the browser.

For first-time login, enter the default IP (192.168.1.108). If you have multiple VTOs, we recommend changing the default IP address (**Network > Basic**) to avoid conflict.

Figure 4-1 Device initialization

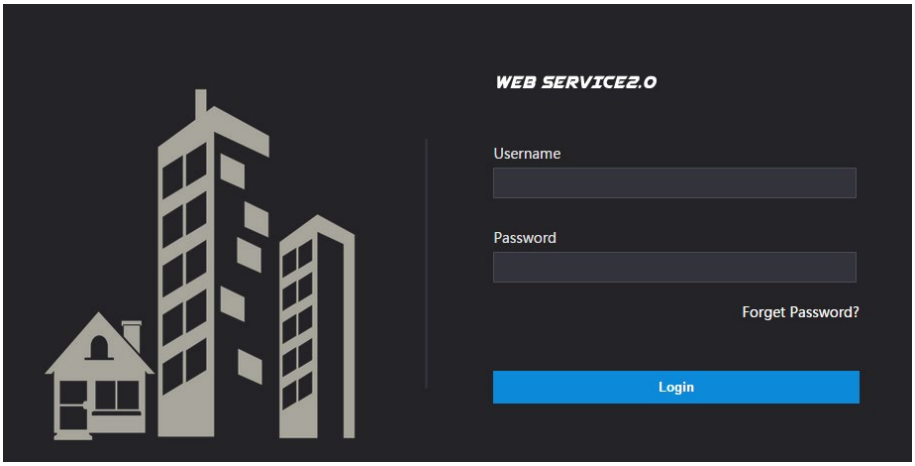


Step 3 Enter and confirm your new password, and then click **Next**.

Step 4 Select **Email** and enter email address for resetting password.

Step 5 Click **Next**, and then click **OK** to go to the login interface.

Figure 4-2 Login interface



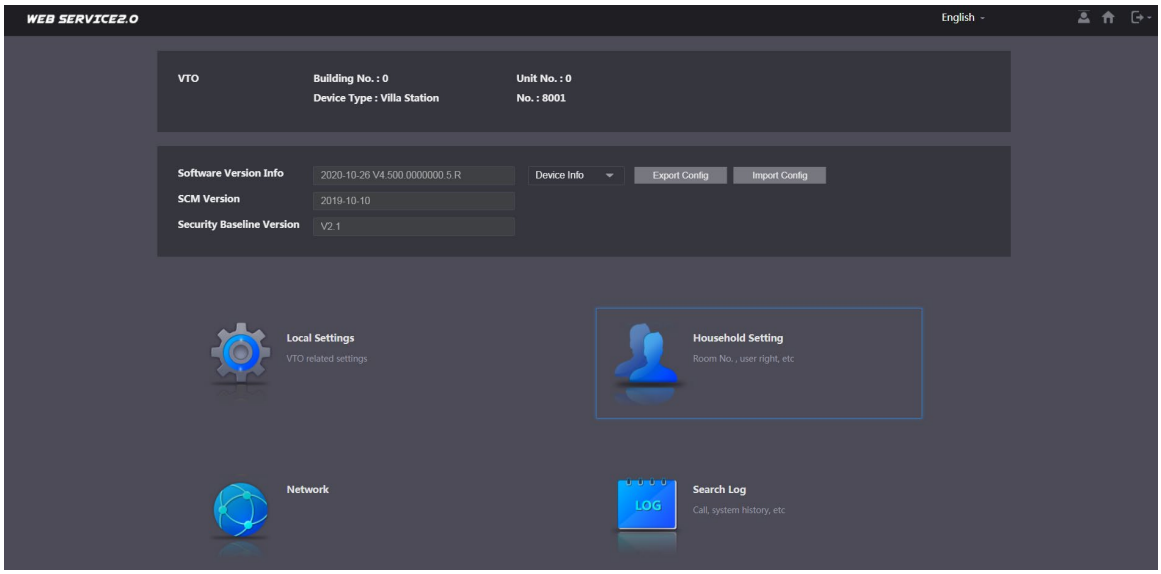
4.3.2 Configuring VTO Number

Numbers can be used to distinguish each VTO, and we recommend setting it according to unit or building number.

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

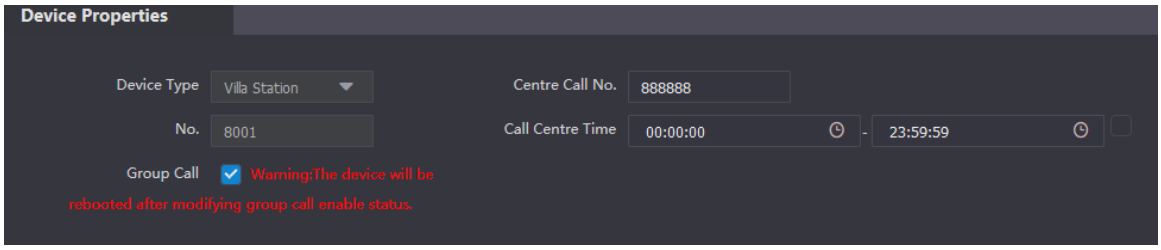
Step 1 Log in to the VTO web interface.

Figure 4-3 Main interface



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

Figure 4-4 Device properties

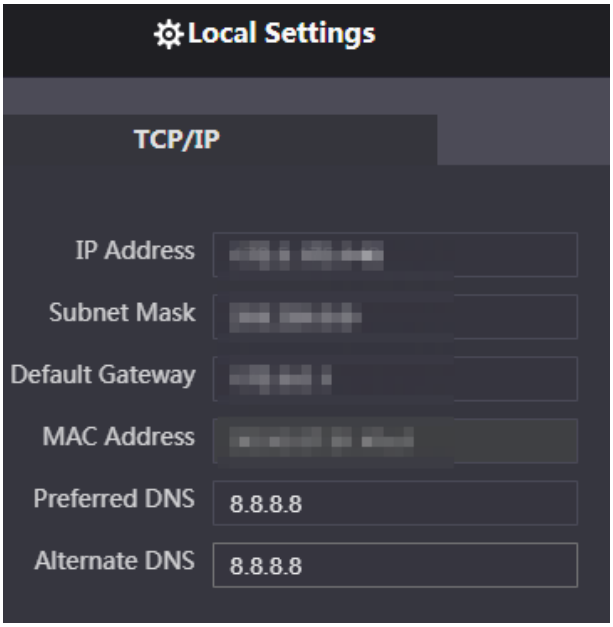


Step 3 Enter the number in **No.**, and then click **Confirm**.

4.3.3 Configuring Network Parameters

Step 1 Select **Network > Basic**.

Figure 4-5 TCP/IP information



Step 2 Enter each parameter, and then click **Save**.

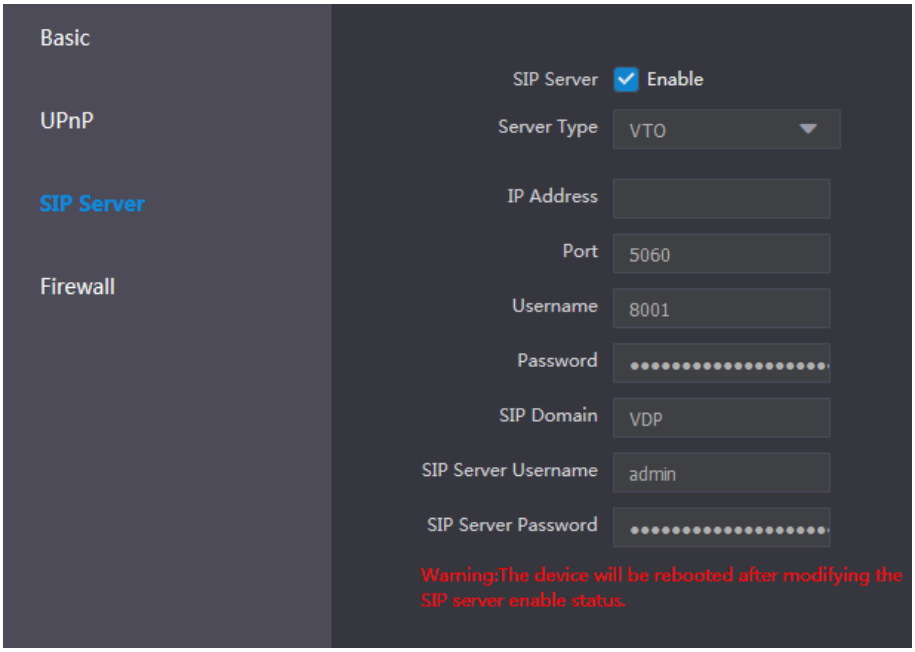
The VTO will automatically restart. You need to add the IP address of your PC to the same network segment as the VTO to log in again.

4.3.4 Configuring SIP Server

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

Step 1 Select **Network > SIP Server**.

Figure 4-6 SIP server



Step 2 Select the server type as needed.

- If the current VTO works as the SIP server, enable **SIP Server**, and then click **Save**.
  The VTO will automatically restart, and then you can add other VTOs and VTHs to this VTO. See "4.3.6 Adding VTOs and 4.3.7 Adding Room Number".

  If the current VTO does not work as the SIP server, do not enable **SIP Server**. Otherwise the connection with this VTO will fail.
- If other VTOs work as the SIP server, set **Server Type** as VTO, and then configure the parameters.

Table 4-1 SIP server configuration

Parameter	Description
IP Addr.	The IP address of the VTO that works as the SIP server.
Port	● 5060 by default when VTO work as SIP server. ● 5080 by default when the platform works as SIP server.
Username	Keep the default value.
Password	
SIP Domain	VDP.
SIP Server Username	SIP server web interface login username and password.
SIP Server Password	

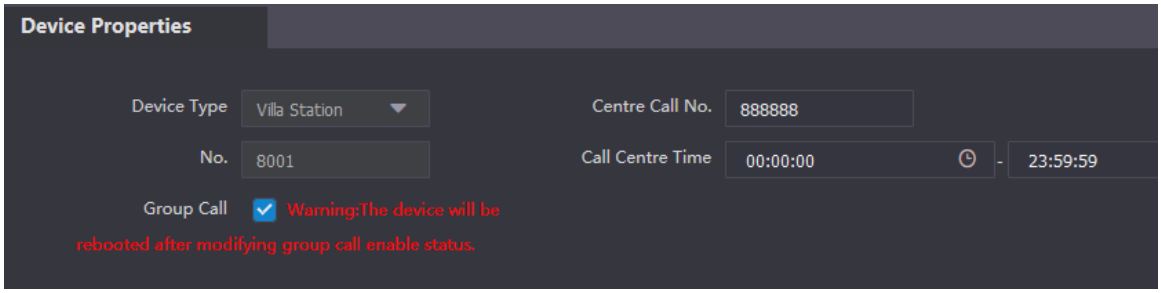
- If other servers work as the SIP server, set **Server Type** as needed, and then see the corresponding manual for details.

4.3.5 Configuring Call Number and Group Call

To dial and call a VTO, you need to configure the call number on each VTO that works as the phone number.

Step 1 Select **Local Settings > Basic**.

Figure 4-7 Device properties



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

On the SIP server, you can enable group call function. When calling a main VTH, all extension VTH will also receive the call.

The VTO will restart after enabling or disabling the group call function.

Step 3 Log in to the SIP server web interface, and then select **Local Settings > Basic**.

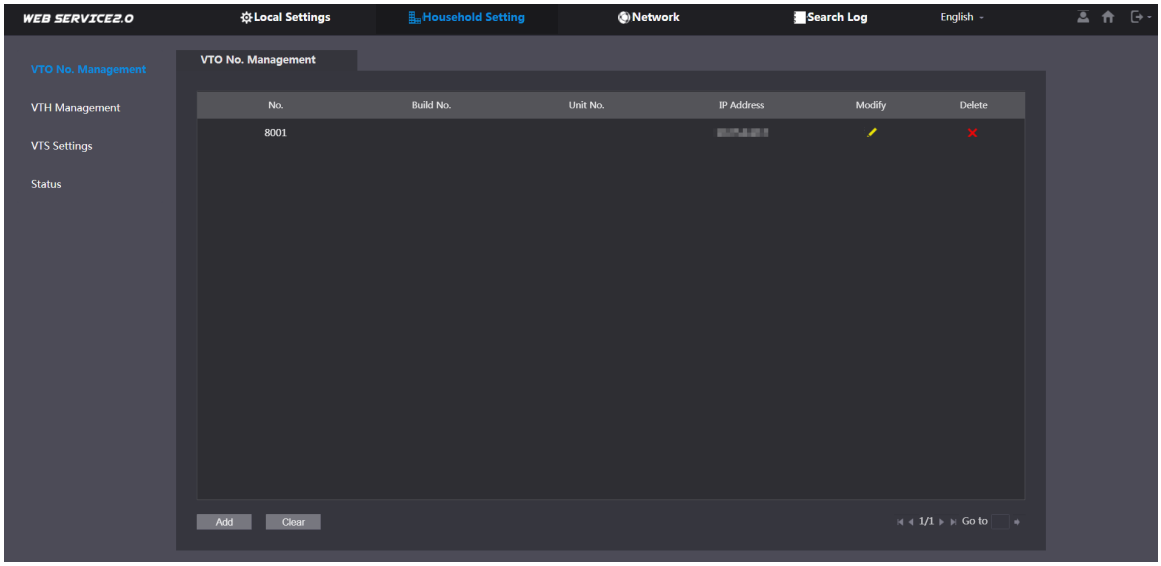
Step 4 Enable **Group Call**, click **Confirm**, and then the VTO will restart.

4.3.6 Adding VTOs

You can add VTOs to the SIP server, and all the VTOs connected to the same SIP server can make video call to each other. This section is applicable when a VTO works as the SIP server, and if you are using other servers as the SIP server, see the corresponding manual for the detailed configuration.

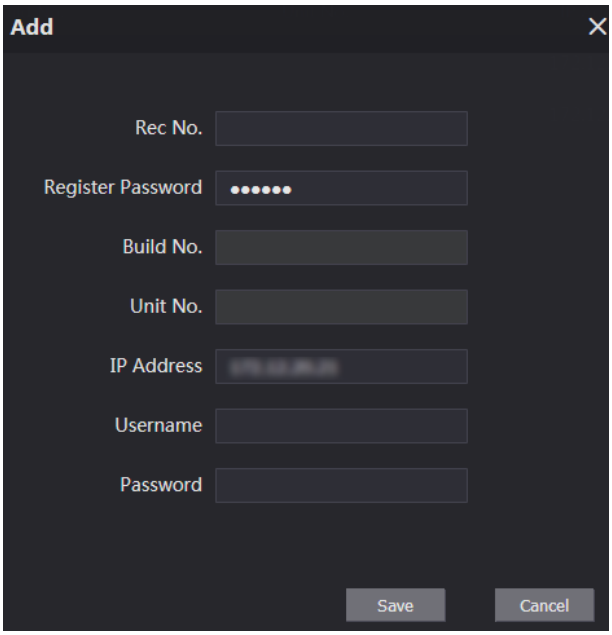
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > VTO No. Management**.

Figure 4-8 VTO No. management



Step 2 Click **Add**.

Figure 4-9 Add VTO



Step 3 Configure the parameters.

The SIP server must be added.

Table 4-2 Add door stations (VTO)

Parameter	Description
Rec No.	VTO number. See "4.3.2 Configuring VTO Number".
Register Password	Keep the default value.
Build No.	Available only when other servers work as the SIP server.
Unit No.	
IP Address	VTO IP address.
Username	VTO web interface login username and password.
Password	

Step 4 Click **Save**.

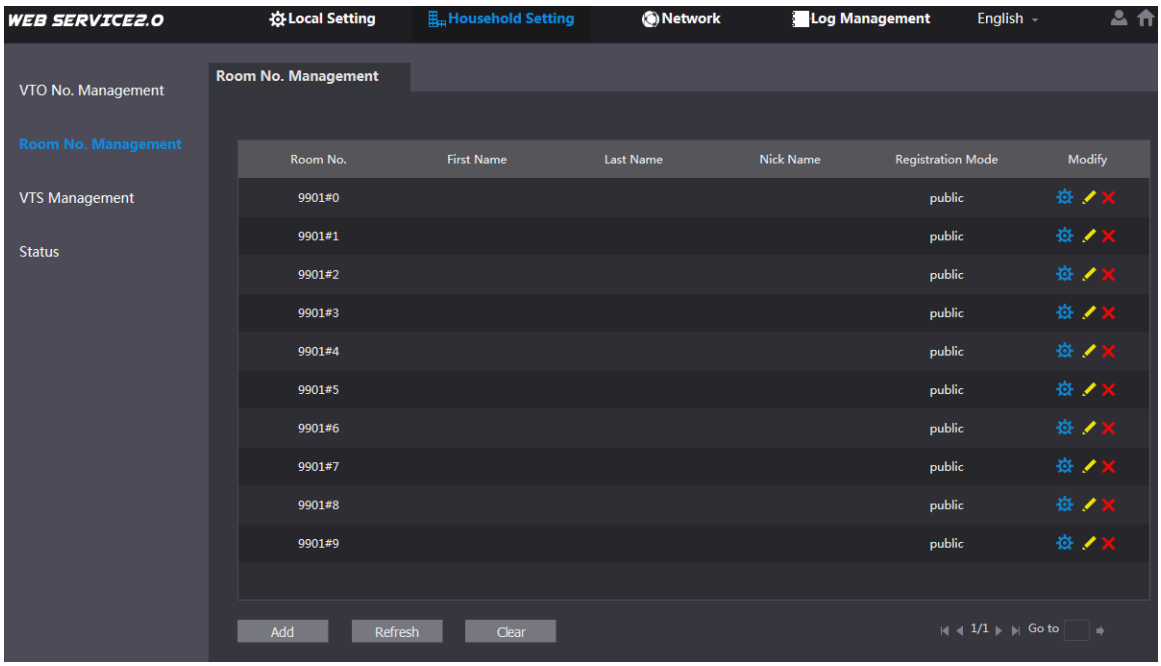
4.3.7 Adding Room Number

You can add room numbers to the SIP server, and then configure the room number on VTHs to connect them to the network. This section is applicable when a VTO works as the SIP server, and if you use other servers as the 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.

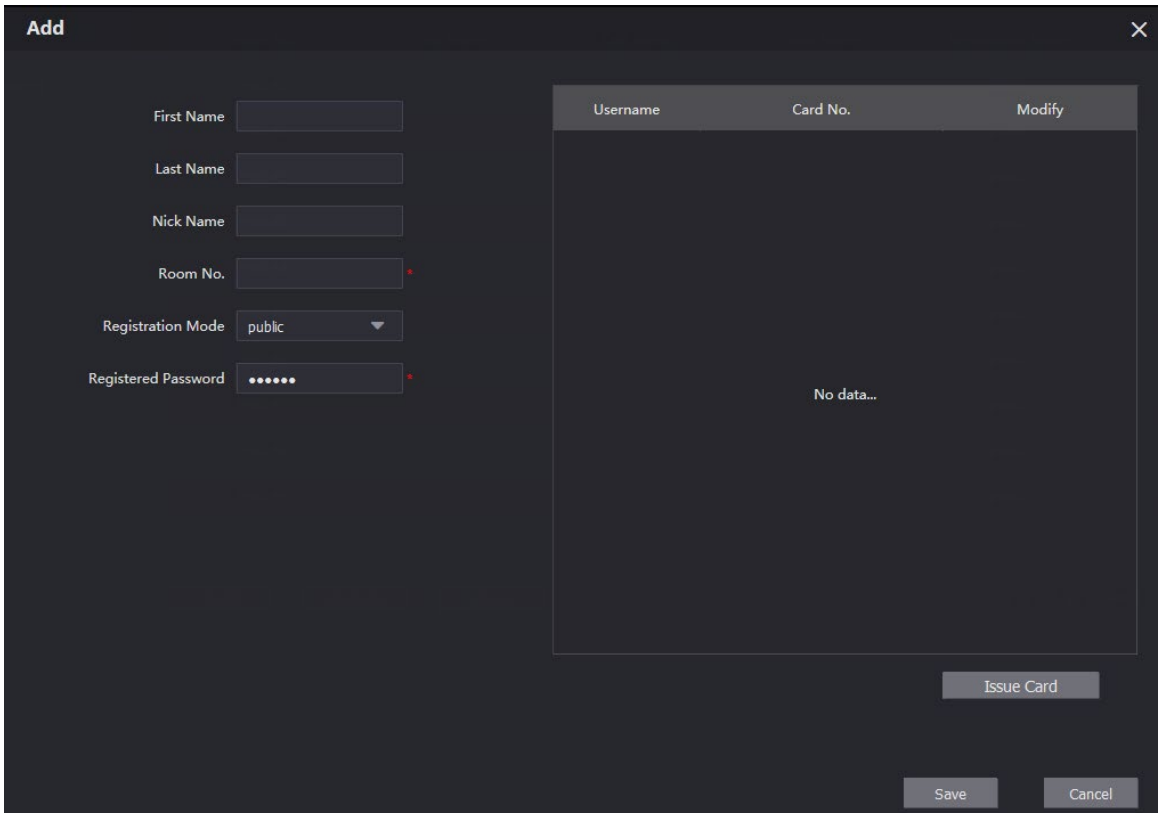
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > Room No. Management**.

Figure 4-10 Room number management



Step 2 Click **Add**.

Figure 4-11 Add a single room number



Step 3 Configure room information.

Table 4-3 Room information

Parameter	Description
First Name	Information used to differentiate each room.
Last Name	
Nick Name	
Room No.	Room number.

Parameter	Description
	 • When there are multiple VTHs, the room number for the main VTH should end with #0, and the room numbers for extension VTHs with #1, #2… • You can configure up to 9 extension VTHs for one main VTH.
Registration Mode	Select **public**.
Registered Password	Keep the default value.

Step 4 Click **Save**.

Click  to modify room information, and click  to delete the room.

4.4 Commissioning

4.4.1 VTO Calling VTH

Step 1 Dial a room number on the VTO.

Step 2 Tap  on the VTH to answer the call.

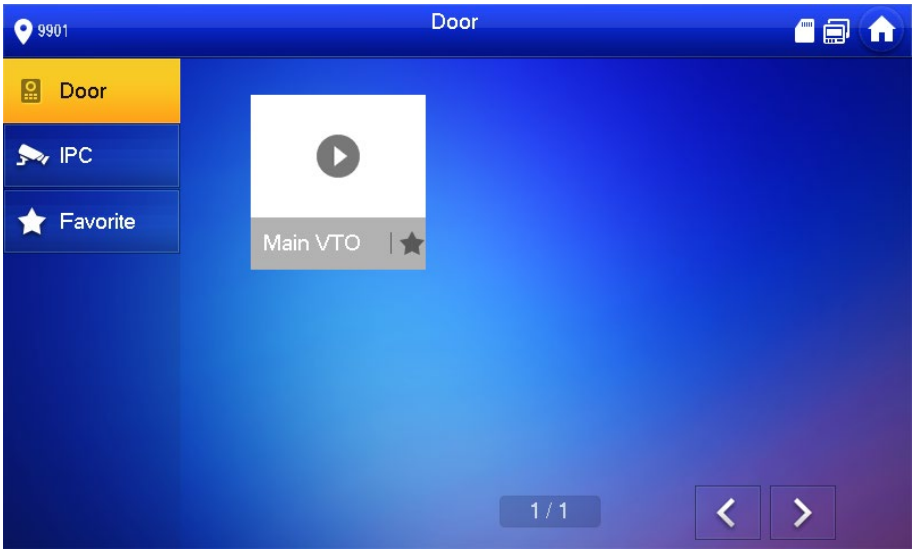
Figure 4-12 Call screen



4.4.2 VTH Monitoring VTO

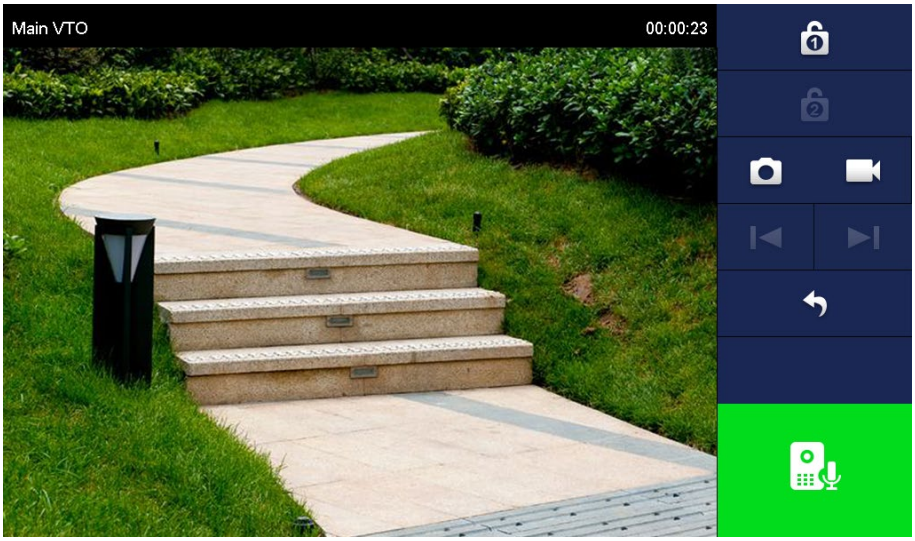
Step 1 On the main interface of the VTH, select **Monitor > Door**.

Figure 4-13 Door



Step 2 Select a VTO.

Figure 4-14 Monitoring video



5 EasyViewer Plus

The EasyViewer Plus (hereinafter referred to as the "app") allows you to manage devices, play back videos, unlock doors, and more.

Before adding the VTO to the app, you need to connect the VTO to the router through Wi-Fi, or connect the VTO to the router by using a switch, and then manually change the IP address of the VTO to the same network as the router if DHCP is not supported.

Download the app in the app store on your smartphone. On the app, select **Setting > Help and Feedback** to view instructions on each function.

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 device 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 device (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 device 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 device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device, 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 device 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 device, 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 device 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.