Villa Door Station

User's Manual



V1.0.5

Foreword

General

This manual introduces the installation, functions and operations of the villa door station device (hereinafter referred to as "the VTO"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
Anger Danger	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.5	Modified audio.	November 2024
V1.0.4	Added structure.	May 2024
V1.0.3	Added port description.	February 2024
V1.0.2	Added structure.	February 2024
V1.0.1	Added structure.	December 2023
V1.0.0	First release.	August 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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, and comply with the guidelines when using it.

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.
- If the device is powered off for longer than a month, it should be placed in its original package and sealed. Make sure to keep it away from moisture, and store it 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

- 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.
- Keep the device away from dampness, dust, and soot.
- 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 power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- 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

Foreword	. I
Important Safeguards and Warnings	
1 Structure	1
1.1 Villa Door Station (multiple buttons)	1
1.1.1 Front Panel	1
1.1.2 Rear Panel	2
1.2 Villa Door Station (single button)	.3
1.2.1 R Series	3
1.2.2 D Series	5
1.2.3 G Series	8
1.2.4 E Series	9
1.2.5 F Series 1	2
1.3 Button Model 2	3
1.3.1 Front Panel2	3
1.3.2 Rear Panel	.4
2 Initializing the VTO2	6
2.1 Web	6
2.2 DMSS App2	:6
3 Login and Resetting Password	0
3.1 Login	0
3.2 Resetting Password	0
4 Home Page	;1
5 Setup Wizard3	2
5.1 Setting as SIP Server	2
5.2 Not Setting as SIP Server	3
6 Local Device Configuration	4
6.1 Basic Settings	4
6.1.1 Villa Door Station	4
6.1.2 Second Confirmation Station	
6.2 Access Control	9
6.2.1 Config	9
6.2.2 RS-485	
6.2.3 Configuring the Password	
6.3 Configuring Wiegand	
6.4 Layout4	
6.4.1 Layout (Multiple Buttons)4	
6.4.2 Layout (Multiple Modules) 4	-5

6.5 Adding the IPC	
6.5.1 Adding the IPC One by One	
6.5.2 Exporting the IPC Information in Batches	
6.5.3 Importing the IPC Information in Batches	48
7 System	
7.1 Video	
7.2 Audio	51
7.3 Time	52
7.4 ONVIF User	
7.5 Config	55
7.6 Maintenance	55
7.7 Updating	56
7.8 Legal Information	56
7.9 System Information	
8 Device Setting	
8.1 VTO No. Management	
8.2 VTH Management	59
8.3 VTS Management	61
9 Person Management	63
10 Network Settings	67
10.1 TCP/IP	67
10.2 Port	68
10.3 SIP Server	68
10.4 Second Confirmation Station Cascading	72
10.5 Cloud Service	73
10.6 UPnP	73
10.6.1 Enabling UPnP Services	74
10.6.2 Adding UPnP Services	74
10.7 Wi-Fi	76
10.8 Basic Services	76
11 Log Management	79
11.1 Call History	79
11.2 Alarm Logs	79
11.3 Unlock Records	80
11.4 Log	80
12 Security Management	
12.1 Security Status	82
12.2 System Service	82
12.3 Attack Defense	83
12.3.1 Firewall	83

12.3.2 Account Lockout	84
12.3.3 Anti-DoS Attack	85
12.4 CA Certificate	85
12.5 Video Encryption	
12.6 Security Warning	
13 Button Model Configuration	88
13.1 Cable Connection	88
13.2 VTH Configuration	89
Appendix 1 Security Recommendation	91

1 Structure

1.1 Villa Door Station (multiple buttons)

1.1.1 Front Panel

Figure 1-1 Front panel

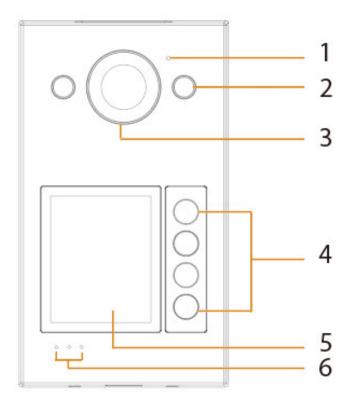


Table 1-1 Components

No.	Name	Function
1	МІС	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

1.1.2 Rear Panel

 \square

The multi-function port might differ depending on the actual models.

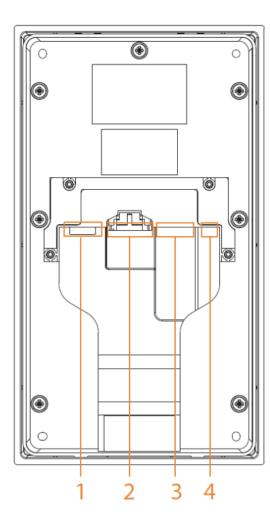


Figure 1-2 Rear panel

Multi-function port П DOOR_COM DOOR_NO DOOR_NC ALM_COM ALM_IN DC_OUT ALM_NO DC_IN DOOR_EXIT DOOR_SR RS485A RS485B DC_IN+ GND GND GND

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	Multi-function port	Alarm port, door detector port, 485 port, power port and other ports.
3	Network port	RJ-485 network port to connect to the network.
4	Reset button	Press and hold the button for several seconds to reset to factory settings.

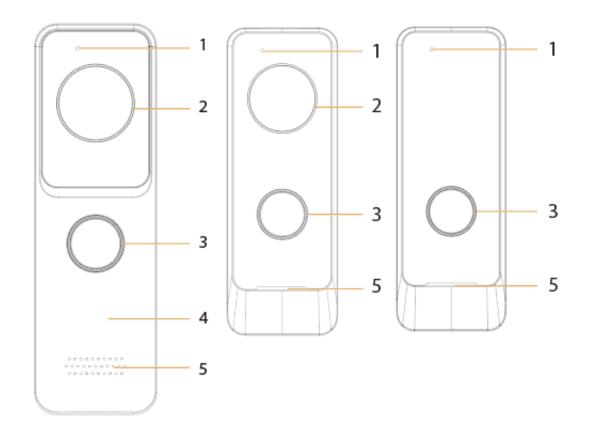
1.2 Villa Door Station (single button)

1.2.1 R Series

1.2.1.1 Front Panel

Size and appearance might differ depending on the models of product.

Figure 1-3 Front panel





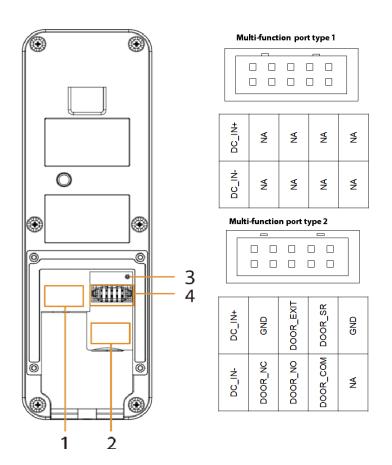
No.	Name	Function
1	MIC	Audio input.
2	Camera	Capture images or record videos for the VTO.
3	Call button	Call the VTH.
4	Card swiping area	Swipe the registered cards to unlock doors. The card swiping function is only available on select models.
5	Speaker	Audio output.

1.2.1.2 Rear Panel

\square

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







No.	Name	Function
1	Network port	Connects to the network.
2	SD card slot	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 reset to factory settings.
4	Multi-function port	 Type 1: The multi-function port only has a power input port to connect to power supply. Type2: The multi-function port includes a power input port and a door detector port.

Figure 1-5 Rear panel (2)

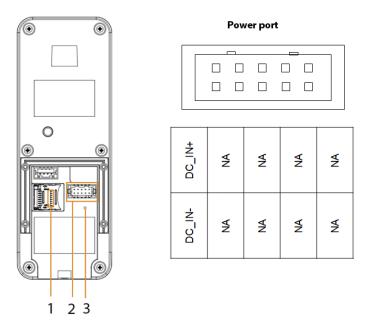


Table	1-5	Components
-------	-----	------------

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

1.2.2 D Series

1.2.2.1 Front Panel



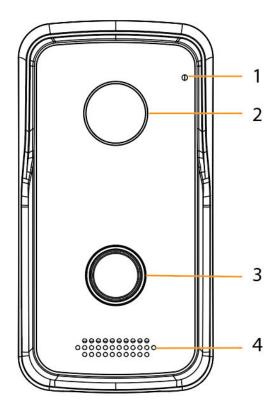


Table 1-6 Components

No.	Name	Function
1	MIC	Audio input.
2	Camera	Capture images or record videos for the VTO.
3	Call button	Call the VTH.
4	Speaker	Audio output.

1.2.2.2 Rear Panel

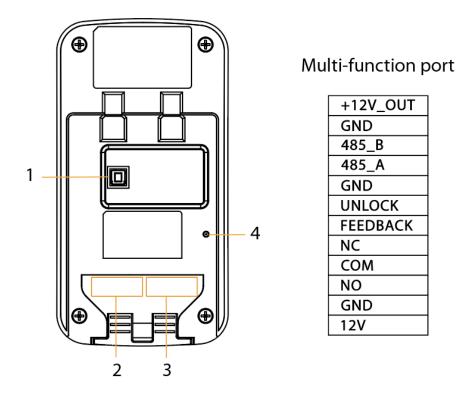


Figure 1-7 Rear panel

Table 1-7 Components

No.	Name	Function	
1	Tamper button	 After the installed device is removed from the wall or other places, the device beeps and the alarm record will be generated. Within 5 minutes after the device is powered on, if you press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information. The alarm record will be generated. 	
2	Multi-function ports	Alarm port, door detector port, 485 port, power port and more.	
3	Network port	Connects to the network.	
4	Reset button	Press and hold the button for several seconds to reset to factory settings.	

1.2.3 G Series

1.2.3.1 Front Panel

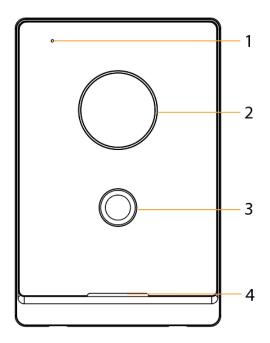


Figure 1-8 Front panel

Table 1-8 Components

No.	Name	Function
1	MIC	Audio input.
2	Camera	Capture images or record videos for the VTO.
3	Call button	 Call the VTH. The button displays different colors in different statuses. Standby: No light. Call not answered: Solid green. Call answered: Solid blue. Unlock when the device is in standby status: Red. Unlock when the call is not answered: Flashes green, yellow and then green. Unlock after the call is answered: Flashes blue, pink and then blue. Network disconnected: Green breathing light.
4	Speaker	Audio output.

1.2.3.2 Rear Panel

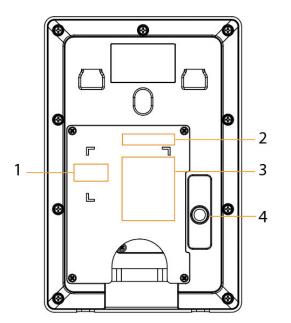


Figure 1-9 Rear panel

NA	DOOR1_PUSH
NA	GND
NA	DOOR1_FB
NA	GND
NA	DOOR1_NO
NA	DOOR1_COM
NA	DOOR1_NC
ALARM_COM	RS485A
ALARM_NO	RS485B
GND	GND
ALARM_IN	+12V_OUT
DC_IN-	DC_IN+

Multi-function port

Table 1-9 Components

No.	Name	Function
1	Network port	Connects to the network.
2	Multi-function port	Alarm port, door detector port, 485 port, power port and more.
3	SD card slot	Insert SD card so that data information such as images and videos can be stored.
4	Tamper button	 After the installed device is removed from the wall or other places, the device beeps and the alarm record will be generated. Within 5 minutes after the device is powered on, if you press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information. The alarm record will be generated.

1.2.4 E Series

1.2.4.1 Front Panel

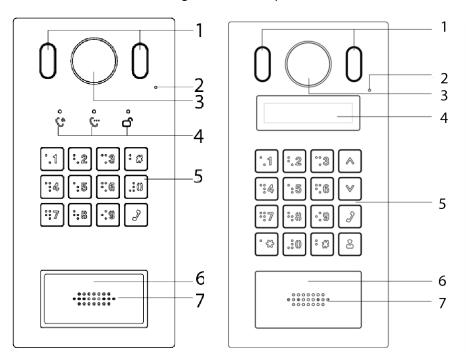


Figure 1-10 Front panel

Table 1-10 Front panel description

No.	Name	Description
1	Illuminator	Provides extra light for the camera when it is dark.
2	Microphone	Audio input.
3	Camera	Capture images or record videos for the VTO.
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	Audio output.

1.2.4.2 Rear Panel



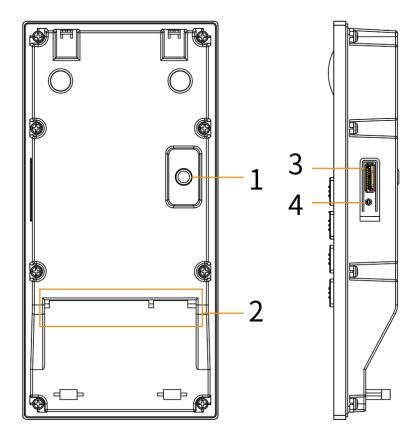
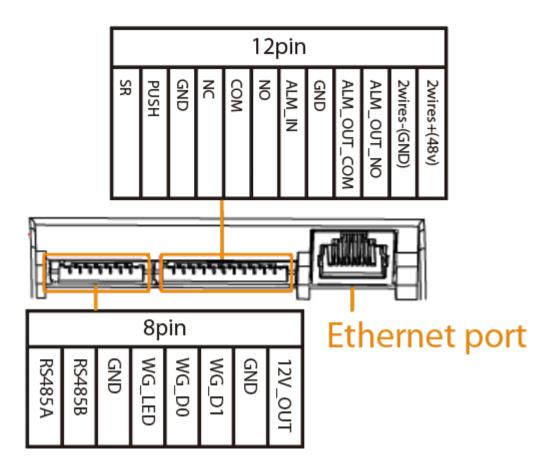


Table 1-11 Rear panel description

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	Multi-function port	For details, see Figure 1-12 .
3	SD card slot	Plug in the SD card.
4	Reset button	Press and hold it for 10 seconds to reset all settings.

Figure 1-12 Multi-function port



1.2.5 F Series

1.2.5.1 Front Panel

Figure 1-13 Front panel

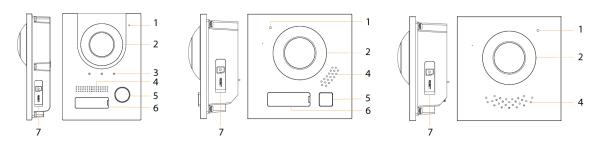


Table 1-12 Front panel description

No.	Name	Description
1	Microphone	Audio input.
2	Camera	Capture images or record videos for the VTO.

No.	Name	Description	
3	Indicators	Display status on calling, talking and unlock.	
4	Speaker	Audio output.	
5	Call button	Call the VTH and the management center.	
6	Nameplate	Displays the custom information.	
7	Card slot and reset button	 Insert SD card so that data information such as images and videos can be stored. Press and hold the button for several seconds to reset to factory settings. 	

1.2.5.2 Rear Panel

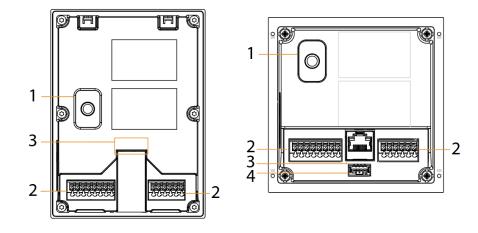


Figure 1-14 Rear panel

Table 1-13 Rear panel description

No.	Name	Function	
1	Tamper button	 After the installed device is removed from the wall or other places, the device beeps and the alarm record will be generated. Within 5 minutes after the device is powered on, if you press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information. The alarm record will be generated. 	
2	Multi-function ports	Alarm port, door detector port, 485 port, power port and more.	
3	Network port	Connect to the network.	
4	Cascade connection port	Connect to other modules.	

Figure 1-15 Multi-function ports

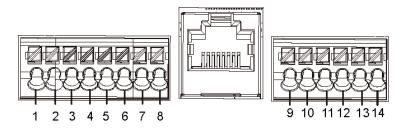


Table 1-14 Port description

No.	Description	No.	Description
1	GND	8	 2wires-(GND) for a digital 2-wire camera module GND for a full digital camera module
2	+12V_OUT	9	DOOR_BUTTON
3	RS-485_B	10	DOOR_FEEDBACK
4	RS-485_A	11	GND
5	ALARM_NO	12	DOOR_NC
6	ALARM_COM	13	DOOR_COM
7	 2wires+(48V) for a digital 2- wire camera module 12 V_IN for a full digital camera module 	14	DOOR_NO

1.2.5.3 Indicator Module



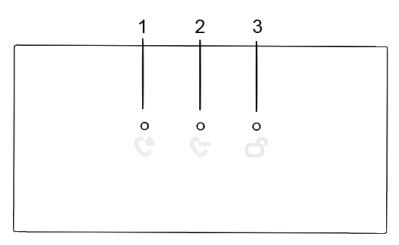


Table 1-15 Front panel description

No.	Name	Description
1	Call indicator	
2	Talk indicator	Activity status.
3	Unlock indicator	

Figure 1-17 Rear panel

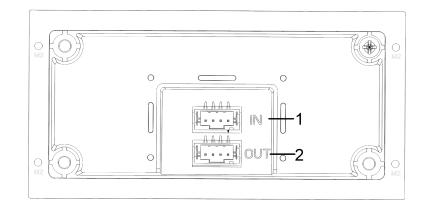


Table 1-16 Rear panel description

No.	Name	Description	
1	Cascade input	- Connect to other modules.	
2	Cascade output	Connect to other modules.	

1.2.5.4 Button Module

One-button module, two-button module, and five-button module are available with the same function. Here we take the five-button module as an example.

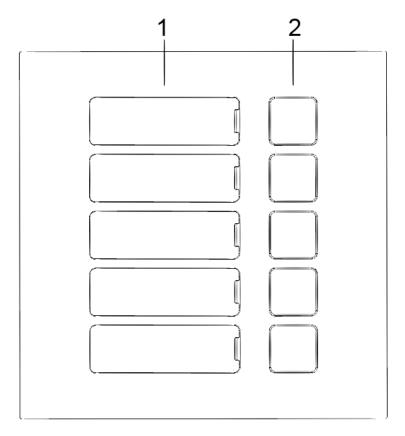


Figure 1-18 Front panel of the five-button module

Table 1-17 Front panel description

No.	Name	Description
1	User directory	Put name cards here.
2	Call buttons	Call other VTHs or the management center.

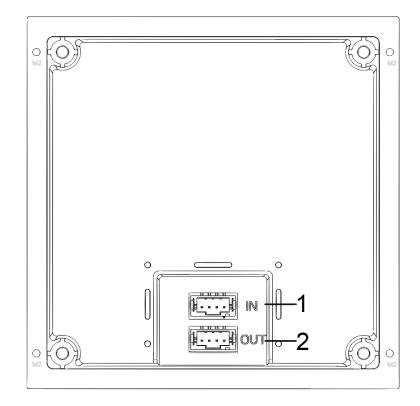


Figure 1-19 Rear panel of the five-button module

Table 1-18 Rear panel description

No.	Name	Description
1	Cascade input	Connect to other modules.
2	Cascade output	connect to other modules.

1.2.5.5 Keyboard Module (with Braille)

The rear panel of keyboard module is the same as the button module.

Figure 1-20 Keyboard module

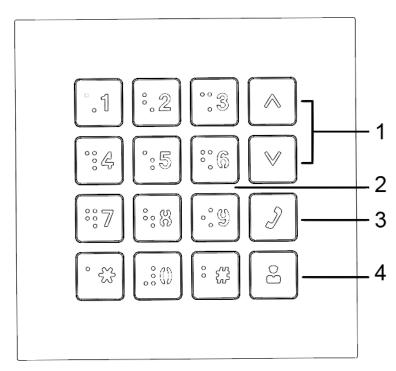


Table 1-19 Keyboard module description

No.	Name	Description
1	Selection	Tap the button to select the contact.
2	Numbers	Enter password or VTH numbers.
3	Call	Call according to the numbers.
4	Call management center	Call the management center.

1.2.5.6 Card Module

There are 2 types of the card module. Select from the ID card module and IC card module as needed.

The rear panel of card module is the same as the button module.

Figure 1-21 Card module



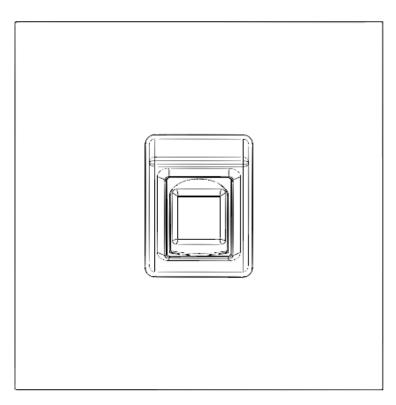
1.2.5.7 Fingerprint Module

Collects and verifies fingerprints.

 \square

- The rear panels of fingerprint module and button module have different port positions, but port functions are the same.
- When there is a fingerprint module accessed and you want to add a new fingerprint module, clear the fingerprint information on the original fingerprint module.

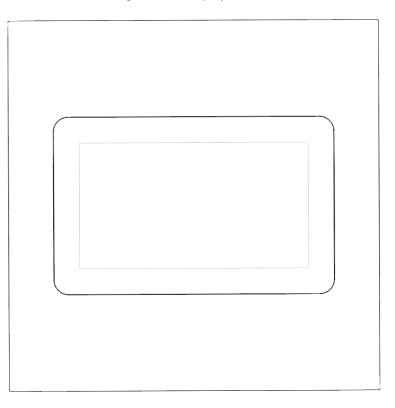
Figure 1-22 Fingerprint module



1.2.5.8 Display Module

Displays user information.

Rear panels of display module and button module have different port positions, but port functions are the same.

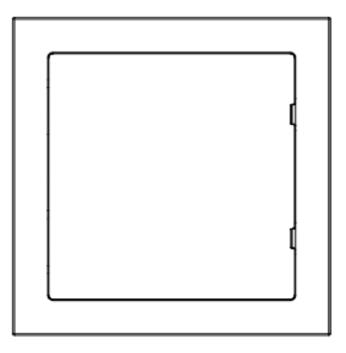




1.2.5.9 Information Module

Displays room number and guest message.

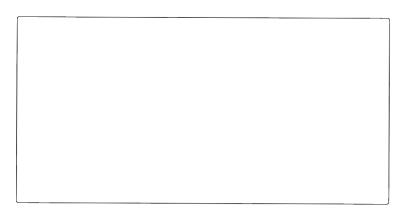
Figure 1-24 Information module



1.2.5.10 Blank Module

For a better appearance, use the blank module if there is an extra space while putting up modules together.

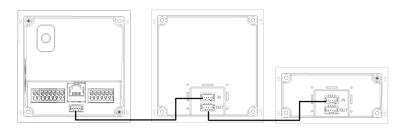
Figure 1-25 Blank module



1.2.5.11 Cascade Connection

Cascade connection is needed for all the modules to work together.

Figure 1-26 Cascade connection example



1.3 Button Model

1.3.1 Front Panel

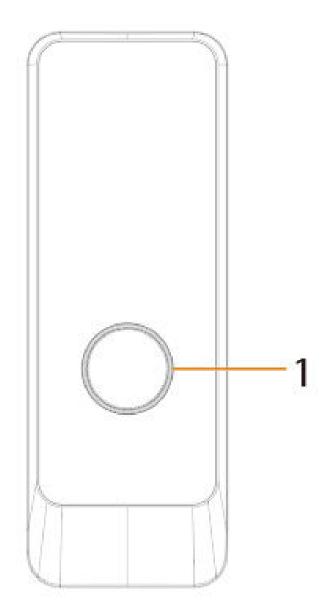


Figure 1-27 Front panel

Table 1-20 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

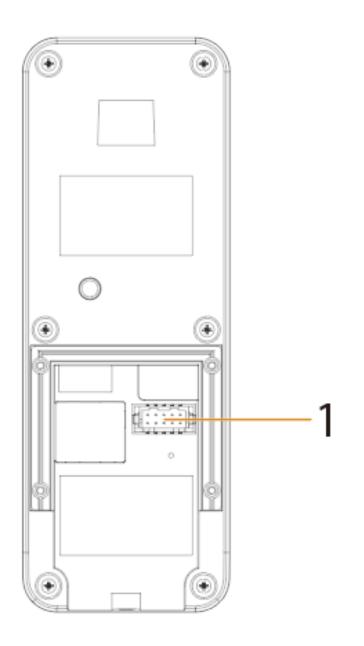


Figure 1-28 Rear panel

Table 1-21 Components

No.	Name	Function
1	Multi-function port	Used for alarm input.

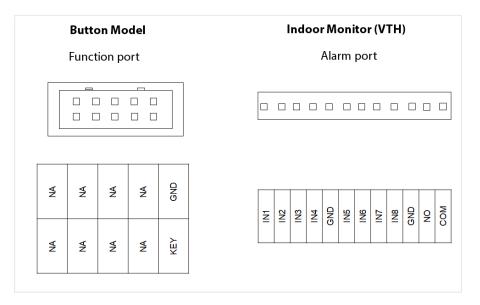


Figure 1-29 Cable connection

Connect the KEY port of the button model to any one of the alarm input ports of the indoor monitor (VTH) with a cable thread. After that, tap **Setting** > **Alarm** > **Wired Zone** on the VTH and set the **Type** of the alarm input port you chose to connect to the KEY port as **Doorbell**.

2 Initializing the VTO

2.1 Web

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

Procedure

- <u>Step 1</u> Power on the VTO.
- <u>Step 2</u> Go to the default IP address (192.168.1.108) of the VTO.

Make sure that the IP address of your PC is on the same network segment as the VTO.

- <u>Step 3</u> On the **Device Init** page, enter and confirm the password, and then click **Next**.
 - \square

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 ' ";:&).

- <u>Step 4</u> Select the **Email** checkbox and enter an email address for resetting password.
- Step 5 Click Next.
- <u>Step 6</u> Click **OK** to go to the login page.
- <u>Step 7</u> Enter the username (admin by default) and password to log in to the webpage.

2.2 DMSS App

If your model only supports Wi-Fi connection to the network, you can only initialize the VTO on the DMSS app. For detailed operation of the app, refer to its user's manual.

Prerequisites

You have downloaded the DMSS in the App Store (iOS) or Google Play (Android), and have created an account and logged in to the app.

Procedure

<u>Step 1</u> Power on the VTO.

<u>Step 2</u> Enable hotspot on the VTO through pressing and holding the call button on the VTO until you heard the voice prompt.

 \square

The hotspot function is to enable you connect the VTO to the network through **AP** configuration on the app.

- <u>Step 3</u> Add the VTO to the DMSS app.
 - 1. On the **Home** screen, tap (+), and then select **SN/Scan**.
 - 2. Add a VTO.
 - 3. You can add through scanning the QR code at the rear panel of the VTO.
 - 4. The SN number of the VTO appears automatically, and then tap Next.
 - 5. Select device type as **VTO**, and then the device information appears.
 - 6. Tap View Reasons.

Figure 2-1 Add VTO to DMSS

88 Home	Add Device	< Add Device <		Add Device	9		<	Add Device	Save
SN/Scan			3.			XVR	Add Mode		P2P
P/Domain			amera				SN: Device Name:	1940	0545-38798
Online Search		Device SN				ime i	Username:		admin
Channell Channell				n Station Alarm			Password: Wrong username or pa to add.	ssword will result in failure	© View Reasons
			ner IPC	n Station Alarm P	Panel				
Offline	Automatically scan the device QR code placed in the frame.					noke ector			
with the second s		Acce	cessory						
Device under the account						e ren			
Home Message Me	Manually Enter SN				1	0			

- 7. Configure network by switch networking to **AP Configuration**, and then tap **Next**.
- 8. Connect your phone to the hotspot you just enabled on the VTO.
 - \square
 - The hotspot name is the SN number of your VTO.
 - The current page will move on to the next step automatically after connection.

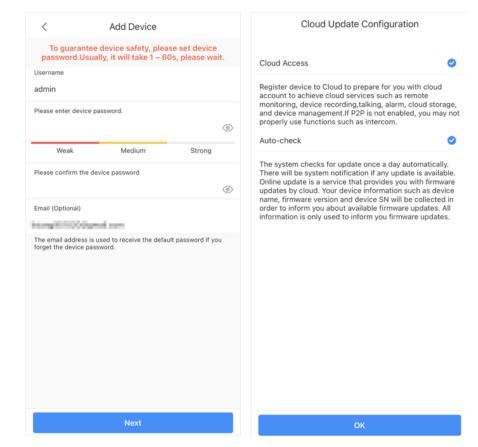
Figure 2-2 AP configuration

<	Add Device		<	Add Dev	ice	
			-			
				WLAN		
				WLAN		
				6J06	e ĉ	
	-			home-3	A 🗢	
	e sure device is connected to ble device hotspot.	power.		home-4	A 🖘	
				ease go to Wi-Fi settin phone, connect hol 0(, and page.	tspot named	
				phone, connect hol 0(, and	tspot named	
Tap the u	pper right corner to change ne	tworking.	IL9	phone, connect hol 0(, and	tspot named then return to ti	nis

- <u>Step 4</u> Complete initialization based on instructions on the app.
 - 1. Enter the password you planned for the VTO, and confirm it, and then tap Next.
 - 2. Select Cloud Access and Auto-check, and then tap OK.

The initialization process is completed.

Figure 2-3 Initialization



<u>Step 5</u> Connect the VTO to the network through Wi-Fi.

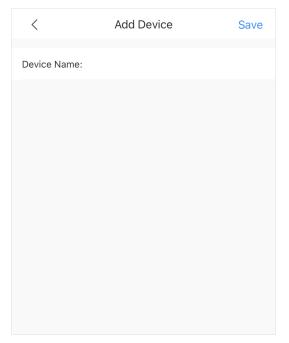
- 1. Select an available Wi-Fi.
- 2. Enter the password and tap **Next**. Wait for the VTO to connect to the router.

Figure 2-4 Wi-Fi connection

< Add Device	···· < Add Device	<	Add Device		< Add Device -
()	Please connect to a Wi-Fi hotspot near you has a strong signal.	u or to one that Refresh			
WLAN	14,400 http://doi.org	ė 🗢	(P)		
home-1 🎄 🗢	Index, NY, MARK	🖒 🗢 Wi-Fi Netv	vork		Ŷ
home-2 â 🕈	19-086,033A	6 🔹 CLoses	es.30		
home-4 a e	ALC: 198	🖒 🗢 Wi-Fi Pass	word		
Searching available Wi-Fi nearby	100527-00305	ė 🕈		۲	
	Name (1997)	ė 🜩	Dual band router fails to support 5	SG WI-FL 🕜	58
	13.amm.0	ė 🕈			s
	1880	ė 🜩			Connecting to the router
	10.2003.019200	ė 🕈			
	Sector, 401041	Ċ 🕈			
	Offer				
			Next		Cancel Config

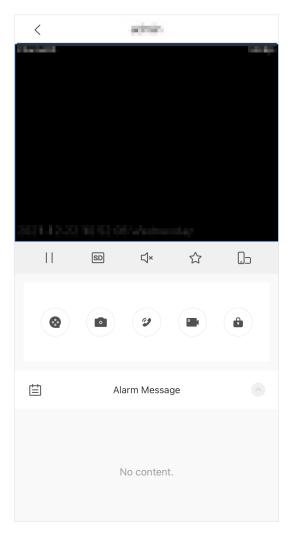
<u>Step 6</u> Configure device name, and then tap **Save**.

Figure 2-5 Configure device name



<u>Step 7</u> View monitoring video from the camera on the VTO.

Figure 2-6 Monitor



3 Login and Resetting Password

3.1 Login

Before login, make sure that the computer is on the same network segment as the VTO.

Procedure

<u>Step 1</u> Go to the IP address of the VTO in the browser.

 \square

For first-time login, enter the default IP (192.168.1.108). If you have multiple VTOs, we recommend that you change the default IP address to avoid conflict.

<u>Step 2</u> Enter **admin** as the username, and enter the password you set during initialization, and then click **Login**.

A Username	
Password	
	Forgot password?

Figure 3-1 Login

3.2 Resetting Password

Procedure

- <u>Step 1</u> On the login page, click **Forgot Password?** , and then click **Next**.
- <u>Step 2</u> Scan the QR code, and then you will get a string of numbers and letters.
- <u>Step 3</u> Send the string to the email account displayed on the page, and then the security code will be sent to the email address configured during initialization.

<u>Step 4</u> Enter the security code in the input box, and then click **Next**.

- If you did not set an email address during initialization, contact your supplier or customer service for help.
- The security code will be valid only for 24 hours upon receipt.
- If you enter the wrong security code for 5 consecutive times, your account will be locked for 5 minutes.

<u>Step 5</u> Enter and confirm the new password, and then click **OK**.

4 Home Page

	1		2	3
I WEB SERVICE			Setup Wizard	冬 admin 🗑 器 Product Material 🔀
			-= ©	
	Local Device Config	Device Setting	Person Management	4
		ر ک و		
	Network Settings	Log	System	

Table 4-1 Home page introduction

No.	Function	Description
1	Home button	Go back to the home page.
2	Setup Wizard	Configure the VTO SIP server.
3	Navigation bar	 Change language of the webpage of the VTO. A admine: Change password, log out of the current device, restart the system, and restore the device to factory settings. View and configure the security settings. Wroduct Material: Scan the QR code to get the product material. View the webpage in full screen mode.
4	VTO function	Different function areas of the VTO.

5 Setup Wizard

Through the setup wizard, you can finish the process of adding VTO/VTH and specific any VTO as the SIP server. You can also cancel its status of working as a SIP server.

5.1 Setting as SIP Server

Set the VTO as the SIP server.

Prerequisites

You have added VTOs on the webpage. If not, you can add them in **Set as SIP Server** page or in the **Device Setting** section.

Procedure

<u>Step 1</u> Log in to the webpage of the VTO.

<u>Step 2</u> Select **Setup Wizard** > **Set as SIP Server**, and then click **Next**.

Figure 5-1 Set as SIP server

1 Step 1		2) Step 2
	Set as SIP Server	
	Do not Set as SIP Server	
	Exit Next	

<u>Step 3</u> Select the VTO to be set as the SIP server, and then click **OK**.

You can also click **Add** to add VTOs if you have not had one to work as the SIP server.

Figure 5-2 Select the SIP server

	Step 1			2 Step 2
Add Delete Clear Refresh				Please enter Q
Device Type	T SIP No.	IP Address	Online Status	Operation
VTO	8001	127.0.0.1	Online	∠ ⊡
VTH VTH	9901#0		• Offline	∠ ⊡
VTH	9901#1		• Offline	∠ ⊡
VTH	9901#2		• Offline	∠ ⊡
VTH	9901#3		Offline	∠ ⊡
VTH	9901#4		Offline	∠ ⊡
VTH	9901#5		Offline	∠ ⊡
VTH	9901#6		Offline	<u>∠</u> ⊡
VTH	9901#7		Offline	<u>/</u> ū
UTH UTH	9901#8		Offline	∠ ⊡
11 records		Exit Back	ок	< 1 2 > 10 / page < Go to Page

5.2 Not Setting as SIP Server

If you want to change the SIP server, you need to remove the current one from the list. Procedure

- <u>Step 1</u> Log in to the webpage of the VTO.
- <u>Step 2</u> Select **Setup Wizard** > **Do not Set as SIP Server**, and then click **Next**.

Figure 5-3 Do not set as SIP server

1 Step 1		(2) Step 2
	Set as SIP Server	
	Do not Set as SIP Server	
	Exit Next	

<u>Step 3</u> Configure the information of the VTO that you do not want to set as SIP server, and then click **OK**.

Figure 5-4 Configure information

Step 1		2 Step
	* VTO ID	8002
	Server Type	Device V
	IP Address	172
	Port	5060
	Username	
	Password	•••••
	SIP Domain	VDP
	SIP Server Username	admin
	SIP Server Password	
		Exit Back OK

6 Local Device Configuration

This chapter introduces the detailed configuration of the VTO.

 \square

Slight differences might be found in different models.

6.1 Basic Settings

Configure basic settings of the device.

6.1.1 Villa Door Station

- $\underline{Step 1} \qquad Select \ \textbf{Local Device Config} > \textbf{Basic Settings}.$
- <u>Step 2</u> Configure the parameters.

Local Device Config	
Device Type	Villa Station \vee
Device Name	
Villa Room No.	9901
VTO ID	8001
Group Call	
Management Center	888888
Management Center Call Peri	00:00:00 🕓 - 23:59:59 🕓
Call Period	Setting
Functions	
Storage Method	SD Card \lor
SD Card Usage	OM/OM
	Format SD Card If the SD card cannot be recognized, you can format it.
Auto Capture while Unlocking	
Auto Capture during Call	
Upload Messages and Videos	
Auto Record while Calling	
Please regularly perform	backups to avoid data loss.
Apply Refresh Defa	ult

Figure 6-1 Basic settings (villa station)

Device Type	Small Apartment 🗸
Device Name	
VTO ID	8001
Group Call	
Management Center	888888

Figure 6-2 Basic settings (small apartment)

Table 6-1 Basic parameter description

Parameter	Description
Device Type	Select from Villa Station and Small Apartment .
	The small apartment is available on select models.
Device Name	When other devices are monitoring this VTO, the device name will appear on the monitoring image.
Villa Room No.	VTH room number. Used to call VTHs.
	Used to differentiate each VTO, and we recommend you set it according to unit or building number, and then you can add VTOs to the SIP server by using their numbers.
VTO ID	
	The number cannot be changed when the VTO serves as the SIP server.
Management Center	888888 by default.
Management Center Call Period	Configure the time period in which the VTO can call the management center, and then enable the function.
Group Call	Enable it on the VTO that works as the SIP server, and when a main VTH receives a call, all extension VTHs will also receive the call.
Call Period	The time period in which the VTO's calling to other devices is not limited. Click Setting to configure the call period in a day/week.
Storage Method	SD card by default.

Parameter	Description
SD Card Usage	Displays the total and used capacity of the SD card. You can click Format SD Card to delete all the data in the SD card.
Auto Capture while Unlocking	Take a snapshot and save it in the SD card of the VTO when the VTO is unlocking.
Auto Capture during Call	Take a snapshot and save it in the SD card of the VTO when the VTO is calling.
Upload Messages and Videos	 When enabled: If an SD card is inserted in both the VTH and VTO, the video message will be saved both in the SD cards of the VTH and the VTO. If an SD card is only inserted in the VTH or the VTO, the video message will be saved only in the SD card of the VTH or the VTO. If no SD card is inserted in the VTH or VTO, no video message will be saved.
Auto Record while Calling	Take recording when the VTO is in a call, and save the recording in the SD card of the VTO.

Step 3 Click Apply.

6.1.2 Second Confirmation Station

\square

The configuration of second confirmation station is available on select models.

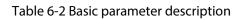
Procedure

<u>Step 1</u>	Select Local Device Config > Basic Settings.

<u>Step 2</u> Configure the parameters.

Device Type	Second Confirmation Station \lor
Device Name	
Villa Room No.	9901
VTO ID	8002
Management Center	888888
Management Center Call Peri	00:00:00 🕚 - 23:59:59 🕓 🗌
Call Period	Setting
Management Center Call Peri Call Period	

Figure 6-3 Basic settings (Second confirmation station)



Parameter	Description
Device Type	Select Second Confirmation Station.
Device Name	When other devices are monitoring this VTO, the device name will appear on the monitoring image.
Villa Room No.	VTH room number. Used to call VTHs.
VTO ID	Used to differentiate each VTO, and we recommend you set it according to unit or building number, and then you can add VTOs to the SIP server by using their numbers.
	The number cannot be changed when the VTO serves as the SIP server.
Management Center	888888 by default.
Management Center Call Period	Configure the time if you only want to receive calls from VTH during a specific period, and then enable the function.
Call Period	Click Setting to configure the call period in a day/week.

Step 3 Click Apply.

6.2 Access Control

\square

Different model series have varied access control functions. Here is the example for configuring the model Q series.

6.2.1 Config

Procedure

<u>Step 1</u> Select Local Device Config > Access Control > Config.

<u>Step 2</u> Configure the parameters.

Interval between Consecutive	15	s (1-20)	
Door Unlocked Duration	2	s (1-20)	
Check Door Detector Signal			
Door Detector Alarm Thresh	30	s (1-9999)	
Door Detector Status	● NC ○ NO		
Report Status of Door Detector			
Unlock Code	123		
Lock	Door 1 Local Lock O Door 2	Lock	
IC Card			
IC Card Encryption & Verifica			
Apply Refresh Default			

Figure 6-4 Access control

Table 6-3 Access control parameter description

Parameter	Description
Interval between Consecutive Unlocks	The door can only be unlocked again after the interval.
Door Unlocked Duration	The time during which the lock stays unlocked.
Check Door Detector Signal Before Locking	Enable the function based on your needs.
Door Detector Alarm Threshold	The threshold time when the door detector alarm is triggered.

Parameter	Description
Door Detector Status	 NC : Normally closed. NO : Normally open.
Report Status of Door Detector	Synchronize door sensor status to indoor monitors (VTHs).
Unlock Code	You can connect a third-party phone, such as a SIP phone, to the VTO, and use the code to open the door remotely.
Lock	 Door 1 Local Lock: Local lock. Door 2 Lock: RS-485 lock. Select the lock type to unlock the lock you select.
IC Card	Enable the function so that users can swipe cards to unlock door.
IC Card Encryption & Verification	Enable the function so that the IC card encryption and verification take effect.

Step 3 Click **Apply**.

6.2.2 RS-485

Procedure

- <u>Step 1</u> Select Local Device Config > Access Control > RS-485.
- <u>Step 2</u> Configure the parameters of the lock connected through the RS-485 port.

Figure 6-5 RS-485

RS-485		
Port Type	Lock \lor	
Interval between C	15	s (1-20)
Unlock Duration	2	s (1-20)
Unlock Code	456	
Lock	Ooor 1 Local Lock O Door 2	Lock
Apply Refresh	Default	

Table 6-4 RS-485 description

Parameter	Description
Port Type	Lock by default.

Parameter	Description
Interval between Consecutive Unlocks	The door can only be unlocked again after the interval.
Unlock Duration	The time during which the lock stays unlocked.
Unlock Code	You can connect a third-party phone, such as a SIP phone, to the VTO, and use the command to open the door remotely. The default command is 456.
	Select the Lock type to unlock the lock you select.
Lock	 Door 1 Local Lock: Local lock. Door 2 Lock: 485 lock.

Step 3 Click **Apply**.

6.2.3 Configuring the Password

Configure the door opening password.

Procedure

<u>Step 1</u> Log in to the webpage.

<u>Step 2</u> Select Local Device Config > Access Control > Password Settings.

Figure 6-6 Password settings

Add Export Import Clear	Refresh		
No.	Username	Password	Operation
1	nvu19	*****	∠ ⊡
2	z4qef	*****	_ ₫
3	6d39f	•••••	⊿□



Figure 6-7 Add the password

Add			Х
* Username	2		
* Password	•••••	Ø	
		OK	Cancel

<u>Step 4</u> Configure the username and the password, and then click **OK**.

Related Operations

- Edit: Click 🖉 to edit the password.
- Delete: Click to delete the password.
- Clear: Click **Clear** to delete all the passwords.
- Refresh: Click **Refresh** to refresh the page.
- Click **Export** or **Import** to export or import the password.

6.3 Configuring Wiegand

Supports access Wiegand devices. Configure the mode and the transmission mode according to your actual devices.

Procedure

<u>Step 1</u> Log in to the webpage.

<u>Step 2</u> Select Local Device Config > Wiegand Settings.

<u>Step 3</u> Configure the Wiegand parameters.

Figure 6-8 Wiegand input

Wiegand Set	ttings	● Wiegand Input 🔵 Wiegand Output	
Apply	Refresh	Default	

Figure 6-9 Wiegand output

Wiegand Settings	O Wiegand Input 💿 Wiegand	Output	
Transmission Mode	Wiegand 34 V		
Pulse Width (µs)	200	(20-200)	
Pulse Interval (µs)	1000	(200-5000)	
The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.			
Apply Refresh Default			

Parameter		Description		
Wiegand Settings		 Select Wiegand Input when other recognition devices are connected. Select Wiegand Output when the VTO works as the recognition device. You can connect the access controller or other devices to the VTO. 		
		Select a Wiegand format to read card numbers or ID numbers.		
Wiegand Output	Wiegand Output Type	 Wiegand26 : Reads three bytes or six digits. Wiegand34 : Reads four bytes or eight digits. Wiegand66 : Reads eight bytes or sixteen digits. 		
	Pulse Width	Enter the pulse width and pulse interval of		
	Pulse Interval	Wiegand output.		

Table 6-5 Description of Wiegand parameters

Step 4 Click **Apply**.

6.4 Layout

6.4.1 Layout (Multiple Buttons)

This function is only available for select models with multiple buttons (1 button, 2 buttons and 4 buttons). Here is an example of configuration for the VTO that has one button installed on its device.

Procedure

- <u>Step 1</u> Log in to the webpage of the VTO.
- <u>Step 2</u> Select Local Device Config > Layout.
- <u>Step 3</u> Click the nameplates next to where you have installed the button(s), and then select the room number(s) from the **Module** you want to bind. For example, 9901, 9902, 9903 and 9904.

 \square

- You need to first configure the room number. Otherwise, you have no room number to select from in the module list. VTH room numbers is configured in **Device Setting**. For details, see "8.2 VTH Management".
- You need to configure the room number based on your installation position of buttons. For example, if you have only installed one button next to the first nameplate, then you need to click the module of first nameplate to configure the room number on the webpage. If you have installed one button next to the fourth nameplate, then you need to click the module of fourth nameplate to configure the room number on the webpage. Keep the above configuration rule when you install 2 buttons or 4 buttons on the VTO and configure the corresponding room numbers on the webpage.

Figure 6-10 Fourth button installation

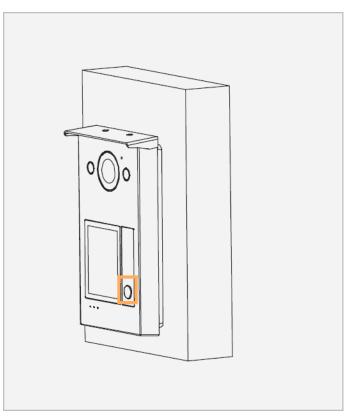


Figure 6-11 Configure the fourth nameplate (1)

· ·	Module	Clear
	9901	9902
	9903	9904
Apply Refresh		

<u>Step 4</u> Click **Apply** to save the selected room number.

· ·	Module	Clear
	9901	9902
	9903	9904
9904 S C S Refresh		

Figure 6-12 Configure the fourth nameplate (2)

<u>Step 5</u> If you want to bind room numbers when you install 2 buttons or 4 buttons for the VTO, repeat Step 3 to Step 4 until you have configured all of the room numbers.

6.4.2 Layout (Multiple Modules)

This function is only available for select models with multiple modules..

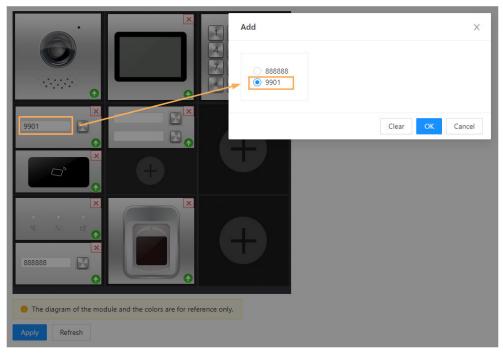
Procedure

- <u>Step 1</u> Log in to the webpage of the VTO.
- <u>Step 2</u> Select Local Device Config > Layout.
- <u>Step 3</u> Click the nameplates on the corresponding module, and then select the room number you want to bind.

\square

You need to first configure the room number. Otherwise, you have no room number to select from in the module list. VTH room numbers is configured in **Device Setting**. For details, see "8.2 VTH Management".

Figure 6-13 Configure the nameplate



<u>Step 4</u> Click **OK** to save the selected room number.

<u>Step 5</u> If you want to bind room numbers when you install other modules with nameplates for the VTO, repeat Step 3 to Step 4 until you have configured all of the room numbers.

Related Operations

Click to view the current version of the module or upload the update file to update the module.

6.5 Adding the IPC

If the current VTO works as the SIP server, you can add the IPC devices on the webpage of the VTO. The VTHs with the same online SIP server gets the IPC information.

- Supports adding the device with up to 32 channels.
- Supports directly adding IPC devices. You can get the IPC channel by adding NVR/XVR/HCVR.

6.5.1 Adding the IPC One by One

Add the information of the video monitoring device one by one.

- <u>Step 1</u> Log in to the webpage.
- <u>Step 2</u> Select Local Device Config > IPC Info.

Figure 6-14 IPC information

Refresh Import Export Default							
No. Name	IP Address	Protocol Type	Stream Type	Port	Channel No.	Device Type	Operation
1	1000	Local	Sub Stream	554	0	IPC	_ ₫
2		Local	Sub Stream	554	0	IPC	⊿₫
3		Local	Sub Stream	554	0	IPC	⊿₫
4		Local	Sub Stream	554	0	IPC	_ ₫
5	100	Local	Sub Stream	554	0	IPC	_ ₫
6		Local	Sub Stream	554	0	IPC	_ ₫
7		Local	Sub Stream	554	0	IPC	_ ₫
8		Local	Sub Stream	554	0	IPC	_ ₫

<u>Step 3</u> Click \checkmark to configure the parameters.

Figure 6-15 Configure the parameters

Edit		Х
Name		
IP Address	0.0.0.0	
Protocol Type	Local \lor	
Stream Type	Sub Stream \lor	
Device Type	IPC V	
Channel No.	0	
Encryption		
Username	admin	
* Password		
Port	554	
		OK Cancel

Parameter	Description
IPC Name	Enter the name of the IPC/VNR/XVR/HCVR device.
IP Address	Enter the IP address of the IPC/VNR/XVR/HCVR device.
Protocol Type	Select from Local and ONVIF according to the device you add.
Stream Type	Select from Main Stream and Sub Stream.
Device Type	Select the type according to the actual devices.
Channel No.	 If you add the IPC, it is 1 by default. If you add the NVR/XVR/HCVR, it is the channel of IPC that was configured on the VNR/XVR/HCVR device.
Encryption	Keep consistent with the encryption status of the terminal device.
Username	Enter the username and the password that used to log in to the
Password	webpage of the IPC/VNR/XVR/HCVR device.
Port	The value is 554 by default.

Table 6-6 Parameters description of the video monitoring device

Step 4 Click OK.

6.5.2 Exporting the IPC Information in Batches

Export the IPC information and save the information to the local computer.

Procedure

- Step 1 Click Export.
- <u>Step 2</u> Enter the login password, and then click **OK**.

The IPC configuration file is saved to the local computer.

6.5.3 Importing the IPC Information in Batches

Import the IPC information to the system.

Procedure

<u>Step 1</u> Click **Import**, and then enter the login password.

```
Figure 6-16 Import
```

Import			Х
	Select File	Import	

<u>Step 2</u> Select the file, and then click **Import**.

7 System

7.1 Video

Configure the video format and quality, and audio of the VTO. **Procedure**

<u>Step 1</u> Select **System** > **Video**.

	Bit Rate	Main Stream	
	Status	Resolution	720P V
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Image	Frame Rate (FPS)	25 🗸
ALC: NOT THE REAL PROPERTY OF		Bit Rate	1024Kbps 🗸
the second second second		Compression	H.264 V
		Sub Stream	
Video Clip		Resolution	CIF V
Left Right Reset		Frame Rate (FPS)	25 ~
Default		Bit Rate	256Kbps 🗸
		Compression	H.264 V

<u>Step 2</u> Configure the parameters, which will take effect upon change.

Table 7-1 Video parameter description

Parameter		Description		
	Resolution (Main Stream)	 720P: 1280 × 720. WVGA: 800 × 480. D1: 704 × 576. CIF: 352 × 288. 		
Bit Rate	Frame Rate (FPS) (Main Stream)	 If select the Video Standard as PAL: The range is 1 to 25. If select the Video Standard as NTSC: The range is 1 to 30). The larger the value, the smoother the video, but it requires more bandwidth. 		
	Bit Rate (Main Stream)	Include 768 Kbps, 896 Kbps, 1024 Kbps, 1.25 Mbps, 1.5 Mbps, 1.75 Mbps, 2 Mbps and 4 Mbps and more. The larger the value, the better the video quality, but it requires more bandwidth.		

Parameter		Description
	Compression (Main Stream)	H.264. H.265. Compared with H.264, H.265 requires smaller bandwidth.
	Resolution (Sub Stream)	 1080P: 1920 × 1080. WVGA: 800 × 480. QVGA: 320 × 240. D1: 704 × 576. CIF: 352 × 288.
	Frame Rate (FPS) (Sub Stream)	The range is 1 to 25. The larger the value, the smoother the video, but it requires more bandwidth.
	Bit Rate (Sub Stream)	Include 224 Kbps, 256 Kbps, 320 Kbps, 384 Kbps, 448 Kbps, 512 Kbps, 640 Kbps, 768 Kbps. The larger the value, the better the video quality, but it requires more bandwidth.
	Compression (Sub Stream)	H.264. H.265.
	Scene Mode	Select from Auto , Disable , Sunny and Night . Auto is selected by default.
Status	Compensation Mode	 BLC : Back light compensation. Improve the clarity of the target in the image. WDR : Wide dynamic range. Enhance the brightness of dark areas, and reduce the brightness of bright areas to improve the image. HLC : High light compensation. Reduce the brightness of the strong spots to improve the overall image. Disable: Do not use any compensation mode.
	Day/Night	Select from Color , Auto and B/W .
	Video Standard	Select PAL or NTSC according to your area.
	Illuminator Sensitivity	 Configure the sensitivity value. If the illumination intensity is lower than the configured value, the illuminator will be turned on. If the illumination intensity is higher than the configure value, the illuminator will be turned off.
	Brightness	The larger the value, the brighter the image.
Image	Contrast	Larger value for more contrast between bright and dark areas.

Parameter		Description
	Hue	Make the color brighter or darker. The default value is made by the light sensor, and we recommend keeping it default.
	Saturation	The larger the value, the thicker the color.
	Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. The larger the value, the brighter the image.
		This function is available on select models.
	Mirror	Display the image with left and right side reversed.
	Flip	Display the image upside down.
	Display Time	Display the current time and date on the video image.

Related Operations

Click Left or Right to adjust the video image.

Click **Reset** or **Default** to reset the video configurations or restore to default configurations.

7.2 Audio

Procedure

<u>Step 1</u> Select **System** > **Audio**.

<u>Step 2</u> Configure the parameters, which will take effect upon change.

Figure 7-2 Audio

Audio Control		
Voice Prompt while Ringing		
Ringtone		
Unlock		
Alarm		
Voice Messages		
Audio Collection		
Volume Control		
Microphone Volume – — — + 90		
Speaker Volume – — + 80		
Apply Refresh Default		
Audio File(Only MP3 files that are up to 20 KB can be uploaded.)		
Audio Type	Audio File	Modify
Calling		Δ
Busy		
Successfully Unlocked	-	<u></u>
Nobody Answered		£
Call Ended		£
Nonexistent Number	-	£

Parameter		Description	
	Voice Prompt while Ringing		
	Ringtone		
Audia Cantual	Alarm	Turn on or off each type of	
Audio Control	Voice Messages sound.		
	Unlock		
	Audio Collection		
Values Control	Microphone Volume		
Volume Control	Speaker Volume	Adjust the volume.	

Table 7-2 Audio parameter description

Step 3 Click **Apply**.

<u>Step 4</u> (Optional) Upload audio file by clicking [▲] next to the corresponding audio type (including calling, busy, successfully unlocked, nobody answered, call ended and nonexistent number).

 \square

Only MP3 files that are up to 20 KB can be uploaded.

7.3 Time

Configure the time zone and day light saving parameters.

- <u>Step 1</u> Select **System** > **Time**.
- <u>Step 2</u> Configure the time and time zone and DST.

Figure 7-3 Time

Time and Time	Zone							
	Date : 2023-0 Time : 13:46:10	7-10 Monday 6						
Time	Manually Set	NTP						
System Time	2023-07-10 13:46:1	6 🛱 Sy	nc PC					
Time Format	YYYY-MM-DD	∨ 24-	Hour	\sim				
Time Zone	(UTC) Coordinated Universal Time							
DST								
Enable								
Туре	🔵 Date 💿 Week							
Start Time	May	∨ Fin	al Week	\vee	Mon	\vee	00:00	0
End Time	Oct	∨ Fin.	al Week	~	Mon	\vee	00:00	0
Apply Ref	fresh Default							

Table 7-3 Parameter description

Module	Parameter	Description		
	Time	Manually SetNTP		
		The time of the VTO system.		
Time and Time Zone	System Time	Changing system time might cause problems on video searching and information publication. Turn off video recording and auto snapshot before changing it.		
		Only applicable under the Manually Set mode.		
	Sync PC	Synchronize the VTO system time with your PC.		
		Only applicable under the Manually Set mode.		

Module	Parameter	Description
	Server	The address of the NTP server.
		Only applicable under the NTP mode.
	Manual Update	Click the icon and the device time of the VTO will be automatically synchronized with server.
		Only applicable under the NTP mode.
	Port	NTP server port number.
		Only applicable under the NTP mode.
	Interval	VTO time update cycle. 30 minutes at most.
		Only applicable under the NTP mode.
	Time Format	 For the date format, select from one of the following: YYYY-MM-DD MM-DD-YYYY DD-MM-YYYY For the time format, select from one of the following: 24-Hour 12-Hour
	Time Zone	Select the time zone for the VTO system.
	Enable	Click to enable the DST function.
DST	Туре	Select Date or Week as needed, and then configure the specific period.
	Start Time	Configure the start time and end time of DST.
	End Time	

Step 3 Click **Apply**.

7.4 ONVIF User

Add accounts for devices to monitor the VTO through the ONVIF protocol.

Procedure

- <u>Step 1</u> Select **System** > **ONVIF User**.
- Step 2 Click Add.
- <u>Step 3</u> Enter the information, and then click **OK**.

ONVIF devices can monitor the VTO by using the account.

Figure 7-4 ONVIF user

Add				Х
∗ Us	ername	Jack		
* Pa	ssword			
* Co	nfirm Password			
			ОК	Cancel

7.5 Config

You can export and import the configuration file.

Procedure

- <u>Step 1</u> Select System > Config.
- <u>Step 2</u> Click **Export Configuration File**, or click **Browse** to select the file from local computer, and then click **Import file**.

Figure 7-5 Config

n File			
	Browse	Import File	
		Browse	Browse Import File

7.6 Maintenance

<u>Step 1</u>	Select System > Maintenance.
<u>Step 2</u>	Configure the auto maintenance time.

Figure 7-6 Auto Maintenance

Auto Maintenan	ce		
Maintenance Tim	e Tue	\vee	02:00 ∨
Apply Refree			



7.7 Updating

Procedure

<u>Step 1</u> Select **System** > **Update**.

<u>Step 2</u>

- Select ways to check the update.
 - **Auto Check** : Select the function to check automatically whether there is a new system version.
 - Manual Check : Select the function to check whether there is a new system version.

Figure 7-7 Update

Auto Check for Updates		
Manual Check	System Version:4	
mandar encer	You are using the latest version.	Update Now

7.8 Legal Information

Select **System** > **Legal Info**. You can view related legal information notices in this section.

7.9 System Information

<u>Step 1</u>	Select System > System Info.
<u>Step 2</u>	View the software version, SCM version and security baseline version.

Figure 7-8 System information

Software Version	
SCM Version	
Security Baseline Version	

8 Device Setting

This chapter introduces how to add, modify, and delete VTO, VTH, VTS, and IPC, and how to send messages from the SIP server to VTOs and VTHs when the VTO works as the SIP server. If you are using other servers as the SIP server, see the corresponding manual for details.

8.1 VTO No. Management

You can add VTOs to the SIP server, and all the VTOs connected to the same SIP server can call each other.

Procedure

- <u>Step 1</u> Log in to the webpage of the VTO that works as the SIP server.
- Step 2 Select **Device Setting**.
- Step 3 Click Add.
- <u>Step 4</u> Configure the parameters.

Add		×
Device Type	VTO V	
* No.	8001	
* Registration Password	····· Ø	
Building No.		
Unit No.		
* IP Address	127 .	
* Username	admin	
* Password		
	ОК Са	ncel

Figure 8-1 Add VTO

Table 8-1 Add VTO configuration

Parameter	Description	
Device Type	Select VTO .	
No.	The VTO number you configured.	
Registration Password	Leave it as default.	

Parameter	Description	
Building No.	Available only when the platform servers work as the SIP server.	
Unit No.		
IP Address	IP address of the VTO.	
Username	Username and password used to log in to the webpage of the VTO.	
Password		

Step 5 Click **OK**.

 \square

Click *to* edit the VTO, or *to* to delete added VTOs, but the one that you have logged in to cannot be modified or deleted.

8.2 VTH Management

You can add room numbers to the SIP server, and then configure the room number on the VTHs to connect them to the network.

- <u>Step 1</u> Log in to the webpage of the SIP server.
- Step 2 Select **Device Setting**.
- Step 3 Click Add.
- <u>Step 4</u> Configure the parameters.
 - Select the add mode as Add One by One.

Add		Х
Device Type	VTH	~
Add Mode	Add One by One	\sim
First Name	Please enter	
Last Name	Please enter	
Alias	Please enter	
* Room No.	Please enter	
Registration Mode	Public	\sim
* Registration Password	•••••	ø
		OK Cancel

Figure 8-2 Add VTH one by one

Table 8-2 Parameters description

Parameter	Description	
First Name		
Last Name	Enter the information you need to differentiate each room.	
Alias		
Room No.	Enter a room number, and then configure the number on a VTH to connect it to the network.	
Registration Mode	Select Public.	
Registration Password	Leave it as default.	

• Select the add mode as **Add in Batches**.

Add		Х
Device Type	VTH \vee	
Add Mode	Add in Batches \lor	
Floors in Unit	5	
Rooms on Each Floor	4	
First Room No. on 1st Floor	101	
First Room No. on 2nd Floor	201	
	OK Cance	el

Figure 8-3 Add VTH in batches

Table 8-3 Parameters description

Parameter	Description	
Floors in Unit	– Configure the number of floors, rooms.	
Rooms on Each Floor		
First Room No. on 1st Floor	Configure the first room number on the first and second floor, the room number will be automatically generated.	
First Room No. on 2nd Floor		
Step 5 Click OK .		

Click *L* to edit the VTH, or *L* to delete added VTHs, but the one that you have logged in to cannot be modified or deleted.

8.3 VTS Management

You can add a VTS to the SIP server, and then it can be used as the management center. It can also manage, call, or receive calls from all the VTOs and VTHs in the network. See the corresponding user's manual for details.

- <u>Step 1</u> Log in to the webpage of the VTO that works as the SIP server.
- Step 2 Select **Device Setting**.
- Step 3 Click Add.
- <u>Step 4</u> Configure the parameters.

Figure 8-4 Add VTS

Add		Х
Device Type	VTS	~
* VTS No.	Please enter	
* IP Address		
* Registration Password		ø
	OK	Cancel

Table 8-4 Add VTS configuration

Parameter	Description
Device Type	Select VTS .
VTS No.	The number of the VTS.
Registration Password	Leave it as default.
IP Address	VTS IP address.

Step 5 Click OK.

9 Person Management

Adding personnel information.

\square

The card and fingerprint functions are available on select models or when the device is connect to the corresponding modules.

Procedure

- <u>Step 1</u> Log in to the webpage of the VTO.
- Step 2 Select **Person Management**.
- Step 3 Click Add.
 - VTO that do not have other functions or modules: Enter the room ID, room number, username, and then click **OK**.

Add		×
* Person ID	0123	
* Room No.	8801	
Username	Li	
		OK Cancel

Figure 9-1 Add person

- VTO that has card issuing function or module:
 - 1. Enter the room ID, room number, username and select the lock permission.
 - ♦ Lock1: Local lock.
 - Lock 2: 485 lock.

Only models that have 485 ports support 2 types of locks.

Figure 9-2 Add a person

Add			Х
* Person ID	0123		
* Room No.	8801		
Username	Li		
* Lock Permission	🗸 Lock 1 🔽 Lock 2		
Card	Add		
		С	K Cancel

2. Click Add next to Card, and then enter the card number and name.

Figure 9-3 Issue card

Add Card			×
* Card Number	0123456	Issue Card	
Name	Li		
		ОК	Cancel

3. Click Issue Card.

The webpage displays the countdown prompt (120 seconds). 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.



Add Card			Х
* Card Number		Cancel(119)]
Name	Li		
		ОК	Cancel

4. Click **OK** after swiping to complete the issuing process.

Then the window goes back to the **Add**, with a card being added.

\diamond	Report lost card. After clicking the icon, it becomes	£.
\diamond	: Edit the card information.	
\diamond	Delete the added card.	

Figure 9-5 Card issued

Add		×
* Person ID	1234	
* Room No.	8801	
Username	Li	
* Lock Permission	🗸 Lock 1 🔽 Lock 2	
Card	Add	
123455		
Username:Li		
v <u>/</u>	<u>ڨ</u>	
		OK Cancel

5. Click **OK**.

Figure 9-6 Card added successfully

No. Person ID Room No. Username Card Operation 1 1234 8801 Li E 2 1 2 2 1 2 1 2 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1 1 1 2 1 1 1 2 1 </th <th>oom No./Username</th>	oom No./Username
🗌 1 1234 8801 Li 🖬 🖄 🖄	
cods	1 > 10 / page >

- VTO that has fingerprint function or module:
 - 1. Enter the room ID, room number, username and select the lock permission.
 - 2. Click **Add** next to **Fingerprint**, and then press your finger according to the prompt.

Figure 9-7 Issue card

Fingerprint	×
Please press your finger on the scanner three times continuous	sly.
<i>M</i>	
ОК Сало	el

3. Click **OK**.

Then the window goes back to the **Add**, with a fingerprint being added. You can edit the name of the fingerprint.

4. Click **OK**.

Related Operations

- Click **Export Person**, and then enter the encryption password for the file to export the person information.
- Click **Import Person**, and then select the file to import the person information.

10 Network Settings

This chapter introduces how to configure the network parameters.

10.1 TCP/IP

You need to configure the TCP/IP information to connect the VTO to the network. **Procedure**

- <u>Step 1</u> Log in to the webpage of the VTO.
- <u>Step 2</u> Select **Network Settings** > **TCP/IP**.
- <u>Step 3</u> Configure the TCP/IP parameters.

MAC Address	c0 :
IP Address	172
Subnet Mask	29 . 29
Default Gateway	17 . 6 . 0 .
Preferred DNS	8 . 8 . 8 . 8
Alternate DNS	8 . 8 . 4 . 4
Transmission Mode	Multicast Unicast
Apply Refresh	Default

Figure 10-1 TCP/IP

Table 10-1 Parameter description

Parameter	Description	
IP Address	Your planned IP address for the VTO.	
Preferred DNS	It is 8.8.8 by default.	
Alternate DNS	It is 8.8.4.4 by default.	
Transmission Mode	 Multicast. Unicast. Unicast. 	
	Unicast is preferred when the switch does not support multicast function, or when the network connection is not good.	

10.2 Port

		_
TCP Port	37777	(1025-65534)
UDP Port	37778	(1025-65534)
HTTP Port	80	
HTTPS Port	443	
Apply Refresh	Default	

Figure 10-2 Port

Table 10-2 Parameter description

Parameter	Description
HTTP Port	You can now enter http://VTO IP address: HTTPS Port to log in to the VTO.
TCP/UDP Port	Used for accessing the VTO with devices in other networks.
HTTPS Port	You can now enter https://VTO IP address: HTTPS Port to log in to the VTO.

10.3 SIP Server

There must be a SIP server in the network for all connected VTOs and VTHs to call each other. You can use a VTO or other servers as the SIP server.

Procedure

- <u>Step 1</u> Select **Network Settings** > **SIP Server**.
- <u>Step 2</u> Select a server type.
 - The VTO you have logged in as the SIP server: Select the SIP type as **Device**, and configure the parameters for the VTO, and then click
 next to **SIP Server**.

The parameters would become grey after enabling the SIP Server function.

SIP Server	
Server Type	Device \vee
IP Address	192
Port	5060
Username	8001
Password	•••••
SIP Domain	VDP
SIP Server Username	admin
SIP Server Password	•••••
Apply Refresh	Default

Figure 10-3 Current VTO as SIP server

If another VTO works as the SIP server: Select the SIP type as **Device**, and configure the parameters for the VTO working as the SIP.

If the VTO you have logged in does not work as the SIP server, do not enable **SIP Server**. Otherwise, the connection would fail.

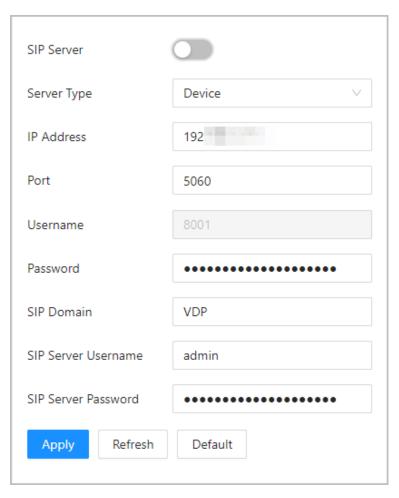


Figure 10-4 Another VTO as SIP server

Table 10-3 SIP server configuration (VTO as the SIP server)

Parameter	Description	
IP Address	Planned IP address of the VTO.	
Port	5060 by default.	
Username		
Password	Leave it as default.	
SIP Domain		
SIP Server Username	Username and password used to log into the webpage of the	
SIP Server Password	SIP server.	

• The DSS platform works as the SIP server: Set **Server Type** as **Private SIP Server**, and then configure the parameters.

SIP Server			
Server Type	Private SIP Server \lor		
IP Address	192		
Port	5080	Alternate IP	192.
Username	8001	Alternate Server Usern	admin
Password	•••••	Alternate Server Passw	•••••
SIP Domain	VDP	Alternate VTS IP	0.0.0.0
SIP Server Username	admin	Alternate Server	
SIP Server Password	•••••		
Apply Refresh	Default		

Table 10-4 SIP server description (platform as the SIP server)

Parameter	Description
IP Address	IP address of the SIP server.
Port	5080 by default when the platform works as the SIP server.
Username/Password	Leave it as default.
SIP Domain	
SIP Server Username/ Password	Used to log in to the SIP server.
Alternate IP	The alternate server will be used as the SIP server when Express/DSS stops responding. We recommend you configure the alternate IP address.
	 If you enable Alternate Server, the current VTO you have logged in serves as the alternate server. If you want another VTO serve as the alternate server, you need to enter the IP address of that VTO in the Alternate IP textbox. Do not enable Alternate Server in this case.
Alternate Server Username/ Password	Used to log in to the alternate server.
Alternate VTS IP	IP address of the alternate VTS.
Alternate Server	Enable it so that you can configure the Alternate VTS IP.

Step 3 Click Apply.

10.4 Second Confirmation Station Cascading

It applied to the situation when the second confirmation station cascades to the VTH.

Prerequisites

The software version of the VTH must be V4.7 and later.

Procedure

- <u>Step 1</u> Select **Network Settings** > **SIP Server**.
- <u>Step 2</u> Configure the second confirmation station information in **Local Device Config** > **Basic** Settings.

The device type should be set as **Second Confirmation Station**.

<u>Step 3</u> Set **Server Type** as **Device**, and then configure the parameters.

In this cascading situation, the VTH works as the SIP server.

Figure 10-6 SIP server configuration (VTH as the SIP server)

Server Type	Device \lor
IP Address	172 6 1 2 3
Port	5060
Username	9901#200
Password	•••••
SIP Domain	VDP
SIP Server Username	admin
SIP Server Password	•••••
Apply Refresh	Default

Table 10-5 SIP server configuration description (VTH as the SIP server)

Parameter	Description
IP Address	Your planned IP address of the VTH.
Port	5060 by default.
Username	
Password	Leave it as default.
SIP Domain	

Parameter	Description	
SIP Server Username	Username and password used to log into the VTH that serves as	
SIP Server Password	the SIP server.	
Step 4 Click Apply .		

10.5 Cloud Service

Enable the **Cloud Service** function, and then you can scan the QR code with your phone to add the VTO to the app on your phone.

Enable	
will collect o name and so remotely ac	nction is enabled and the device connects to the network, we device information such as the IP adress, MAC address, device erial number. The collected information will only be used to cess the device. If you do not want to enable this function, the selection from the check box.
P2P Status	• Offline
PaaS Status	• Offline
SN	7.00054480445
Apply	Please scan the actual QR code

Figure 10-7 Cloud service

10.6 UPnP

When the VTO works as the SIP server, you can configure the UPnP function to allow WAN devices to log in to the VTO.

Figure 10-8 UPnP

able							
Apply Refresh Add							
Service Name	Service Type	Protocol	Internal Port	External Port	Status	Enable	Modify
HTTP	CustomService	TCP	80	8080	Mapping Failed		_ ₫
TCP	CustomService	TCP	37777	37777	Mapping Failed		_ ⊡
UDP	CustomService	UDP	37778	37778	Mapping Failed		∠ ⊡
Rtp	CustomService	UDP	15001	15001	Mapping Failed		∠ ⊡
Rtp	CustomService	UDP	15003	15003	Mapping Failed		∠ ⊡
Rtp	CustomService	UDP	15005	15005	Mapping Failed		_ ₫
Rtp	CustomService	UDP	15006	15006	Mapping Failed		_ ⊡
Rtp	CustomService	UDP	15007	15007	Mapping Failed		∠ ⊡
Rtp	CustomService	UDP	15008	15008	Mapping Failed		∠ ⊡
Rtp	CustomService	UDP	15009	15009	Mapping Failed		∠ ⊡
records						(1 2 > 10	/ page ∨ Go to

Preparation

- Enable the UPnP function on the router, and then configure a WAN IP address for the router.
- Connect the VTO to the LAN port of the router.

10.6.1 Enabling UPnP Services

Procedure

- <u>Step 1</u> Select **Network Settings** > **UPnP**.
- <u>Step 2</u> Enable the services listed.
- Step 3 Select Enable.
- Step 4 Click Save.

10.6.2 Adding UPnP Services

Procedure

- <u>Step 1</u> Select **Network Settings** > **UPnP**.
- Step 2 Click Add.
- <u>Step 3</u> Configure the parameters, and then click **OK**.

Add		Х
Enable		
* Service Name	VTO1	
* Service Type	VTO	
Protocol	ТСР	\sim
* Internal Port	3	
* External Port	5	
	ОК	Cancel
	OK	Lancel

Figure 10-9 Add a UPnP service

Table 10-6 Parameter description

Parameter	Description				
Service Name	- Enter the name and type of the service.				
Service Type	Enter the nume and type of the service.				
Protocol	Select TCP or UDP .				
	Internal port of the service.				
Internal Port	 If you need to configure this function for multiple devices, make sure that the ports are not the same. The port number you use must not be occupied. The internal and external port number must be the same. 				
	External port of the service.				
External Port	 If you need to configure this function for multiple devices, make sure that the ports are not the same. The port number you use must not be occupied. The internal and external port number must be the same. 				

10.7 Wi-Fi

If the VTO supports Wi-Fi function, then configure the parameters here.

Procedure

- <u>Step 1</u> Log in to the webpage of the VTO.
- <u>Step 2</u> Select **Network Settings** > **Wi-Fi**.
- Set the **Wi-Fi** status as **On**.

All the networks available are displayed.

Figure 10-10 Wi-Fi

Name	Signal Strength	Status	Connect
Sec. (1988)	Ś		+
100.007	ই		+
1045-75	ি		+
100.00	(î		+
100.000	(?		+
1.000	(î		+
100.00	(î		+
10000	?		+
	(r		+

<u>Step 4</u> Click + of the Wi-Fi you chose, enter the password of it, and then connect to the network.

10.8 Basic Services

Configure functions that involve device security.

Procedure

- <u>Step 1</u> Select Network Settings > Basic Services.
- <u>Step 2</u> Enable the security functions based on your needs.

SSH O There might be safety risk if this service is enabled. CGI O There might be safety risk if this service is enabled. Mobile Push Notifications Intere might be safety risk if this service is enabled. Password Reset ONVIF One of the safety risk if this service is enabled. Outbound Protection of S... One of the second se Multicast/Broadcast Search O There might be safety risk if this service is enabled. Authentication Mode Emergency Maintenance • For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function. Password Expires in Never Private Protocol • *Before enabling private protocol TLS, make sure that the corresponding device or software supports this function. TLSv1.1

Figure 10-11 Basic services

Table 10-7 Security parameter description

Parameter	Description
CC11	A secure alternative to unsecured remote protocols.
SSH	We recommend you turn it off because there might be safety risk if this service is enabled.
	The use of CGI command.
CGI	We recommend you turn it off. Otherwise, the VTO might be exposed to security risks and data leakage.
Mobile Push	Send information to the app on the phone.
Notification	We recommend you turn it off if you do not need this function. Otherwise, the VTO might be exposed to security risks and data leakage.
Password Reset	If turned off, you will not be able to reset password.

Parameter	Description
ONVIF	Allow third-party to pull video stream of the VTO through the ONVIF protocol.
	We recommend turning it off. Otherwise, the VTO might be exposed to security risks and data leakage.
	Protect your passwords.
Outbound Service	
Information Protection	We recommend you turn it on. Otherwise, the VTO might be exposed to security risks and data leakage.
	Enable it so that the VTO will be found by other devices.
Multicast/Broadcast	
Search	We recommend you turn it off. Otherwise, the VTO might be exposed to security risks and data leakage.
Authentication Mode	 Security Mode (recommended): Support logging in with Digest authentication. Compatibility Mode : Use the old login method.
	We recommend you use the security mode. Compatible mode might expose the VTO to security risks and data leakage.
Emergency Maintenance	For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.
Password Expires in	 Select an expiration period from 30 days, 60 days, 90 days, 180 days, Custom and Never. If you select Custom, you need to configure an expiration day between 0 and 180.
Private Protocol	Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.
TLSv1.1	We recommend you turn it off because there might be safety risk if this service is enabled.

Step 3 Click Apply.

11 Log Management

Select Log. You can search for different logs, and export them to your local computer.

If storage is full, the oldest records will be overwritten. Back up the records in time.

11.1 Call History

Select Log > Call History.

Please keep uner Export	ncrypted files well to avoid data lea	kage.			
No.	Call Type	Room No.	Start Time	Call Duration (min)	End Status
1	Incoming	9902	2000-03-18 00:40:45	00:30	Answered
2	Outgoing	9903	2000-03-17 08:51:39	00:00	Missed
3	Incoming	9904	2000-03-14 04:08:05	00:39	Answered
4	Incoming	9904	2000-03-14 04:05:57	00:19	Answered
5	Incoming	9905	2000-03-11 00:34:46	00:12	Answered
6	Incoming	9904	2000-03-10 08:11:20	00:12	Answered
7	Incoming	9904	2000-03-10 02:26:20	00:06	Answered
8	Incoming	9904	2000-03-10 02:25:54	00:21	Answered
9	Incoming	9904	2000-03-10 02:25:09	00:44	Answered
10	Incoming	9904	2000-03-10 00:53:06	00:06	Answered
581 records			< 1 2 3	4 5 69 >	10 / page ∨ Go to Page

Figure 11-1 Call history

11.2 Alarm Logs

Select Log > Alarm Logs.

Export				
No.	Room No.	Event	Channel	Start Time
I	8001	Tamper	1	2023-07-11 02:00:53
2	8001	Tamper	1	2023-07-07 10:07:18
3	8001	Tamper	1	2023-07-06 22:16:19
L .	8001	Tamper	1	2023-07-06 22:09:52
5	8001	Tamper	1	2023-07-04 02:00:49
5	8001	Tamper	1	2023-06-29 16:29:49
,	8001	Tamper	1	2023-06-29 16:26:59
3	8001	Tamper	1	2023-06-29 15:22:09
)	8001	Tamper	1	2023-06-29 15:22:08
0	8001	Tamper	1	2023-06-27 14:07:57

Figure 11-2 Alarm

11.3 Unlock Records

Select Log > Unlock Records.

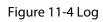
Figure	1	1-3	Un	lock
inguic	•		011	i o ci

xport								
lo.	Unlock Method	VTO ID	Person ID	Room No.	Username	Card	Unlock Results	Unlock Time
	Remote Unlock	8001		9901			Succeed	2023-07-06 20:59:
	Remote Unlock	8001		9901			Succeed	2023-06-29 15:17:

11.4 Log

Select Log > Log.

Select time range and type, and then you can see all the log information.



• Please keep unencrypted files	well to avoid data leakage.					
ime Range 2023-07-10 00:00:00	→ 2023-07-11 00:00:00	🗎 Туре	All	✓ Search Re	set	
Encrypt Log Backup Expor						
No.		Time		Туре		Log Content
				No Data		

12 Security Management

12.1 Security Status

On the home page, click , and then select **Security Status**.

Figure 12-1 Security status

Security Statu	15						
•		f device security status in real ti	me and use the device in a muc	h safer way.			Rescan
The last scanning time	: 2023-07-07 10:07:30						
User & Service Detection (I	etects whether the current co	nfiguration conforms to the reco	ommendation.)				
	2	0					
Login Authentication	User Status	Configuration Security					
	Details	Details					
Security modules Scanning	¥	Ţ	0	D			Ø
Audio/Video Transmission	Trusted Protection	Attack Defense	Firmware Encryption	Configuration Files Security	CA Certificate	Log Security	Session Security
Encryption							

12.2 System Service

Procedure

- <u>Step 1</u> On the home page, click , and then select **System Service**.
- <u>Step 2</u> Select a device certificate, and then enable the HTTPS function.

Figure 12-2 System service

Enable								
	HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access							
convic	service and RTSP access service.							
servic	e and RTSP acce	ess service.						
servic	e and RTSP acce	ess service.						
	a device certifica						Certificate Manag	
			Certificate Seria	Validity Period	User	Issued by	Certificate Manag	
*Select a	a device certifica	ate	Certificate Seria	Validity Period 2053-06-19 20:06	User 7L08CE4YAJ804A5	Issued by 192.168.1.1		

Step 3 Click Apply.

12.3 Attack Defense

12.3.1 Firewall

You can enable different firewall types to control network access to the VTO. **Procedure**



<u>Step 1</u> On the home page, click *mail*, and then select **Attack Defense** > **Firewall**.

<u>Step 2</u> Select the **Mode** as either **Allowlist** or **Blocklist**.

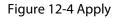
- Allowlist: Devices that have been granted an access.
- Blocklist: Devices that have been forbidden an access.
- <u>Step 3</u> Click **Add** to add the IP address for allowlist or blocklist.

Add		×
Add Mode	IP	\vee
IP Version	IPv4	~
IP Address	10	
All Device Ports		
		OK Cancel

Figure 12-3 Add

Step 4 Click **OK**.

- Step 5 Click Onext to Enable.
- <u>Step 6</u> Select an added IP address for allowlist or blocklist, and then click **Apply**.



Firewall Account L	ockout Anti-DoS Attack		
Enable			
Mode	Allowlist OBlocklist		
	sts whose IP/MAC are in the following lis ports of the device.	st are allowed to access	
Add Dele	te		
No.	Host IP/MAC	Port	Operation
1	12	All Device Ports	<u> </u>
Total 1 records			< 1
Apply Ret	fresh Default		

12.3.2 Account Lockout

Procedure

- <u>Step 1</u> On the home page, click , and then select **Attack Defense** > **Account Lockout**.
- <u>Step 2</u> Configure the login attempts and lock time.

Figure 12-5 Account lockout

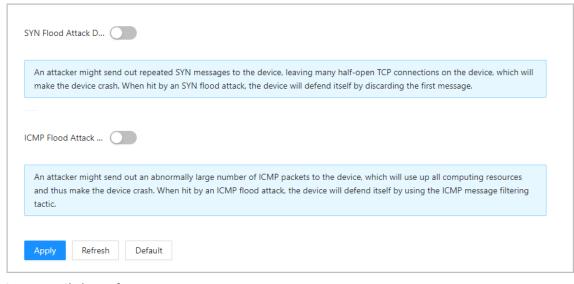
Device Account		
Login Attempt	5time(s) V	
Lock Time	5	min
ONVIF User		
Login Attempt	30time(s) V	
Lock Time	5	min
		mi

Step 3 Click **Apply**.

12.3.3 Anti-DoS Attack

Procedure

- Step 1On the home page, clickImage: and then select Attack Defense > Anti-DoS Attack.Step 2Enable or disable the SYN Flood Attack Defense or ICMP Flood Attack Defense function.
 - Figure 12-6 Anti-DoS attack



Step 3 Click Apply.

12.4 CA Certificate

Procedure

- <u>Step 1</u> On the home page, click , and then select **CA Certificate**.
 - Device Certificate

Figure 12-7 Device Certificate

A dev	vice certificate is a	proof of device legal sta	tus For example wh	en the browser is	visiting device v	ia HTTPS the dev	ice certificate	shall be ver		
ified.		i proor or device legal sta	tus. For example, wit	en the browser is	visiting device v	ia mirs, tie dev	ice certificate	shall be ver		
Insta	II Device Certificat								Enter B	dit M
mata	In Device Certificat								Linter L	.urc Ivi
	Custom Na	Certificate Serial N	Validity Period	User	Issued by	Used by	Certific	Default	Down	De
No		Certificate Serial N	validity Feriod	User	issued by	Used by	cerunc	Delault	DOWII	De
No.	custom ru									
No.	custom ru	633	2053-06-19 20	7L08CE4YA		HTTPS, RTS		\odot	÷	

Trusted CA Certificates

Figure 12-8 Trusted CA Certificates

ce Certifi	cate Trust	ed CA Certifica	tes							
A trus		ate is used to v	rerify the legal s	status of a host. For	example, a switc	h CA certificate sh	all be installed t	for 802.1x authent		
Install	Trusted Certif	icate							Ente	r Edit Mc
No.	Custom Na.	Certificat	e Serial Nu	Validity Period	User	Issued by	Used by	Certificate	Downlo	Delete
		3231		2027-10-16 23:	192,168,1,1	192.168.1.1		Normal	њ.	Ō

12.5 Video Encryption

Procedure

<u>Step 1</u>	On the home page, click W , and then select Video Encryption .
<u>Step 2</u>	Configure Private Protocol and RTSP over TLS parameters.

Figure 12-9 Video encryption

oted Transmission								
Private Protocol								
Enable								
Stream transmission is encrypted by using private protocol.								
*Please make sure that the	corresponding device or software su	pports video decryption.						
Encryption Type AES256-C	FB V							
Update Period 12	hr (0-720)							
TSP over TLS								
Enable								
	y using TLS tunnel before transmissio							
*Please make sure that the	corresponding device or software su	pports video decryption.						
*Select a device certificate						Certificate Management		
No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by		
1		63303339356133326136313	2053-06-19 20:06:37	7L08CE4YAJ804A5	5 192.168.1.1	HTTPS, RTSP over TLS		
pply Refresh Defai	ult							

Step 3 Click Apply.

12.6 Security Warning

Procedure

Step 1On the home page, clickImage: and then select Security Warning.Step 2Enable event monitoring function, and then click Apply.

Figure 12-10 Security warning

Enable			
Event	Monitoring		
Ö	Invalid executable programs attempting to run	Ĭ	Session ID bruteforcing
Ö	Web directory bruteforcing		Number of session connections exceeds limit
	ity warning can detect device security status in real time, and keep you inforr diately, so that you can deal with them timely and avoid security risks.	ned of	the security exception events
Apply	Refresh Default		

13 Button Model Configuration

The button model can be connected to the VTH to work as an alarm input button. Press the button on the front panel of the model, and then the VTH receives an alarm signal.

13.1 Cable Connection

Connect the KEY port of the button model to any one of the alarm input ports of the indoor monitor (VTH) with a cable thread.

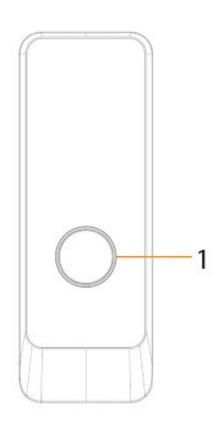
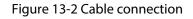
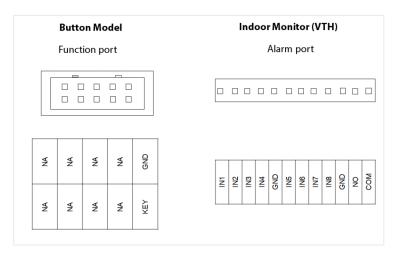


Figure 13-1 Button model

Table 13-1 Component

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.





13.2 VTH Configuration

After completing cable connection, you need to set the **wired zone type** as **Doorbell** on the VTH to receive alarm signals once you press the button model.

Procedure

- <u>Step 1</u> Power on the VTH.
- <u>Step 2</u> Select **Setting** > **Alarm** > **Wired Zone** on the VTH.

Figure 13-	-3 Wired zon	e setting
------------	--------------	-----------

\leftarrow		Wired Zone	C [‡]
(i)) Wired Zone1	IR	Instant Alarm	NO
(i)) Wired Zone2	IR	Instant Alarm	
谢 Wired Zone3	IR	Instant Alarm	NO
(B)) Wired Zone4	IR	Instant Alarm	NO
< 1/2 >			୍ ତ •

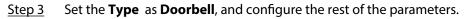


Table 13-2 Parameter description

Parameter	Description	Description		
Area	The number cannot be modified.	The number cannot be modified.		
NO/NC		Select NO (normally open) or NC (normally closed) according to detector type. It must be the same as detector type.		
Туре	Select corresponding type according to d	Select corresponding type according to detector type.		
Status	 produces siren at once and enters alarn Delay Alarm : After armed, if an alarm alarm status after a specified time, duri cancel the alarm. Bypass : Alarm will not be triggered in area will restore to normal working sta Remove : The area is invalid during arr 24 Hour : Alarm will be triggered all th arm or disarm. 	 Bypass : Alarm will not be triggered in the area. After disarmed, this area will restore to normal working status. Remove : The area is invalid during arm/disarm. 24 Hour : Alarm will be triggered all the time in the area regardless of arm or disarm. 		
Enter Delay	After entering delay, when armed area triggers an alarm, entering armed area from non-armed area within the delay time period will not lead to linkage alarm. Linkage alarm will be produced if delay time comes to an end and it is not disarmed.			
Exit Delay	After arm, Delay Alarm area will enter arm status at the end of Exit Delay . If multiple areas set the exit delay, screen prompt will conform to maximum delay time.	Delay is only valid to the areas of Delay Alarm .		

Appendix 1 Security Recommendation

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

- SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up complex passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
- 4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. Enable Allow list

It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

2. MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. Build a secure network environment

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. Check online users

It is recommended to check online users regularly to identify illegal users.

2. Check device log

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. Configure network log

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

Software Security

1. Update firmware in time

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. Update client software in time

It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).