Villa Door Station

User's Manual

V1.0.0

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

Revision History

Version	Revision Content	Release Date
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, 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

⚠ WARNING

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

⚠ WARNING

- 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

1 Initializing the VTO

1.1 Web

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

Procedure

Step 1 Power on the VTO.

Step 2 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.

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

🕮

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

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

Step 5 Click **Next**.

Step 6 Click **OK** to go to the login page.

Step 7 Enter the username (admin by default) and password to log in to the webpage.

1.2 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

Step 1 Power on the VTO.

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

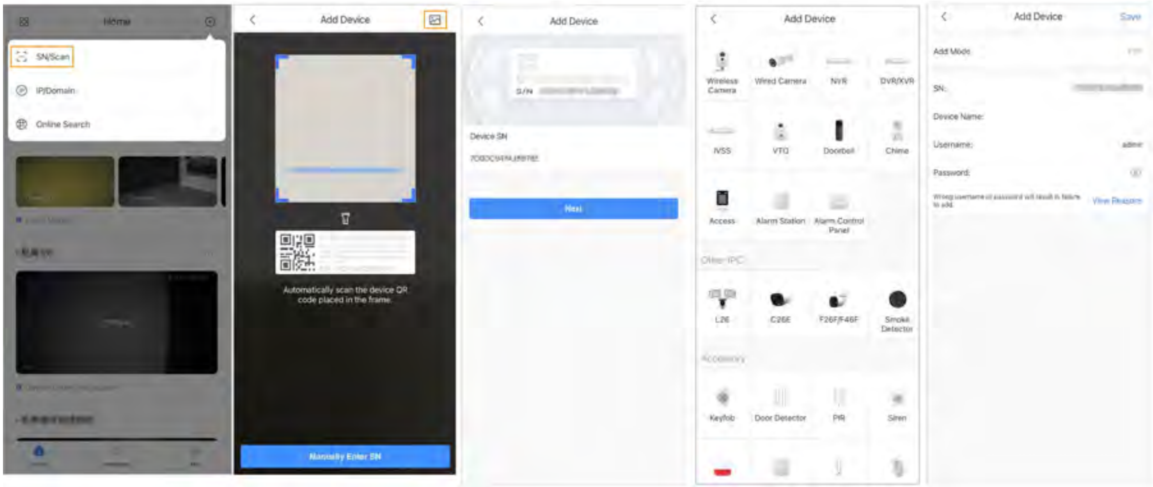
🕮

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

Step 3 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**.

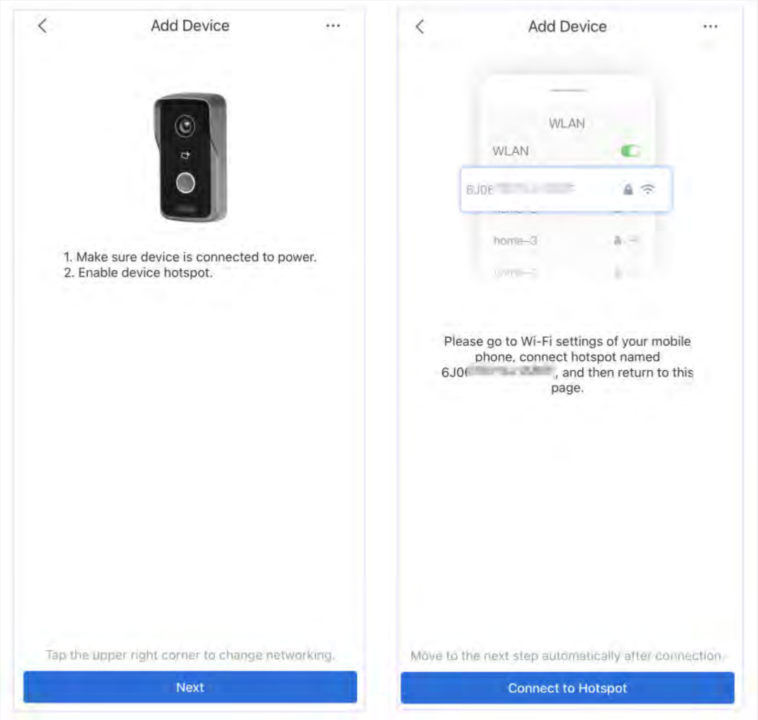
Figure 1-1 Add VTO to DMSS



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.

- The hotspot name is the SN number of your VTO.
- The current page will move on to the next step automatically after connection.

Figure 1-2 AP configuration



1. Make sure device is connected to power.
2. Enable device hotspot.

Tap the upper right corner to change networking.

Next

Please go to Wi-Fi settings of your mobile phone, connect hotspot named 6J0, and then return to this page.

Move to the next step automatically after connection.

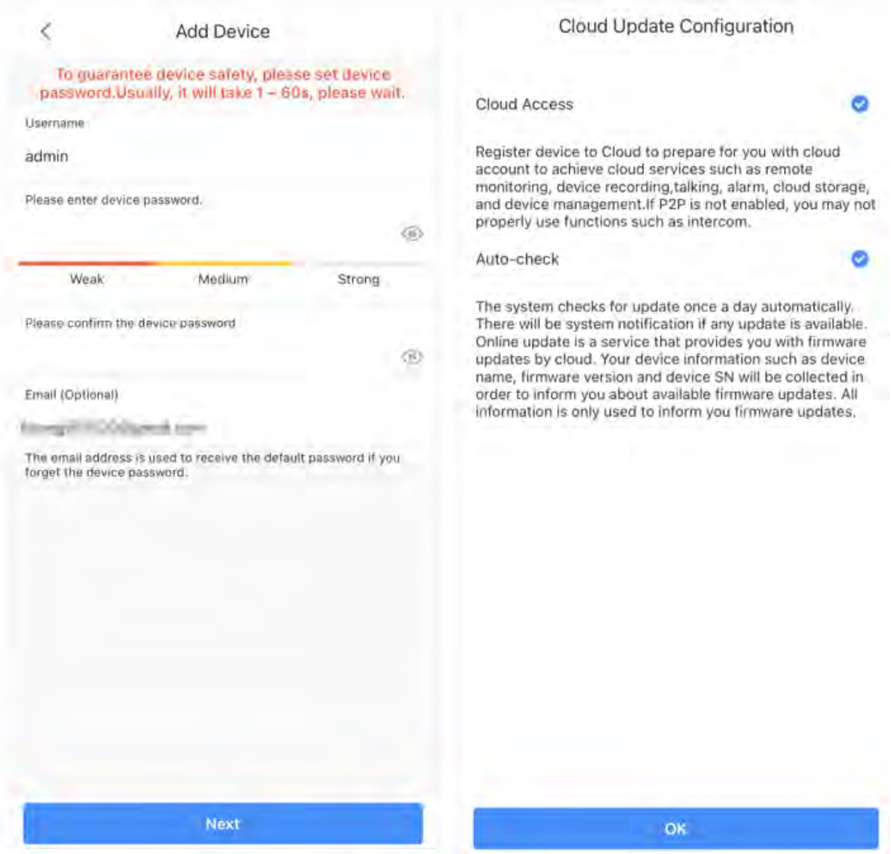
Connect to Hotspot

Step 4 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 1-3 Initialization



Add Device

To guarantee device safety, please set device password.Usually, it will take 1－60s, please wait.

Username

admin

Please enter device password.

Weak Medium Strong

Please confirm the device password

Email (Optional)

The email address is used to receive the default password if you forget the device password.

Next

Cloud Update Configuration

Cloud Access ☑

Register device to Cloud to prepare for you with cloud account to achieve cloud services such as remote monitoring, device recording,talking, alarm, cloud storage, and device management.If P2P is not enabled, you may not properly use functions such as intercom.

Auto-check ☑

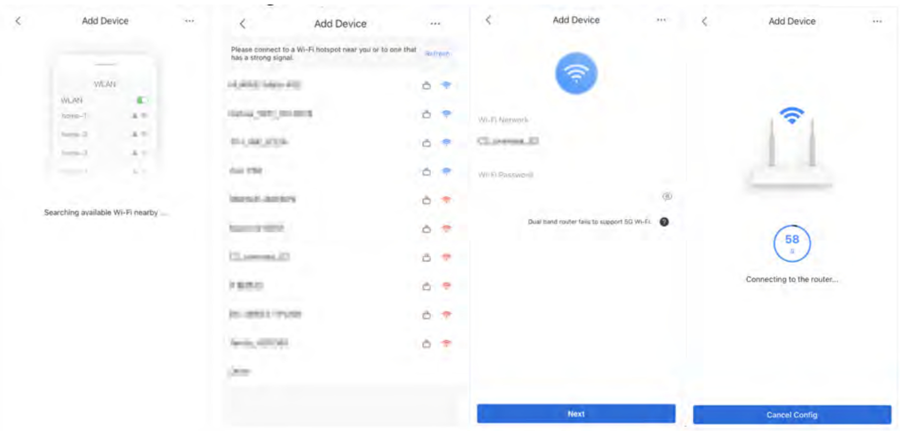
The system checks for update once a day automatically. There will be system notification if any update is available. Online update is a service that provides you with firmware updates by cloud. Your device information such as device name, firmware version and device SN will be collected in order to inform you about available firmware updates. All information is only used to inform you firmware updates.

OK

Step 5 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 1-4 Wi-Fi connection



Add Device

Searching available Wi-Fi nearby ...

Add Device

Please connect to a Wi-Fi hotspot near you or to one that has a strong signal.

Add Device

Wi-Fi Network

Wi-Fi Password

Dual band router fails to support 5G Wi-Fi.

Next

Add Device

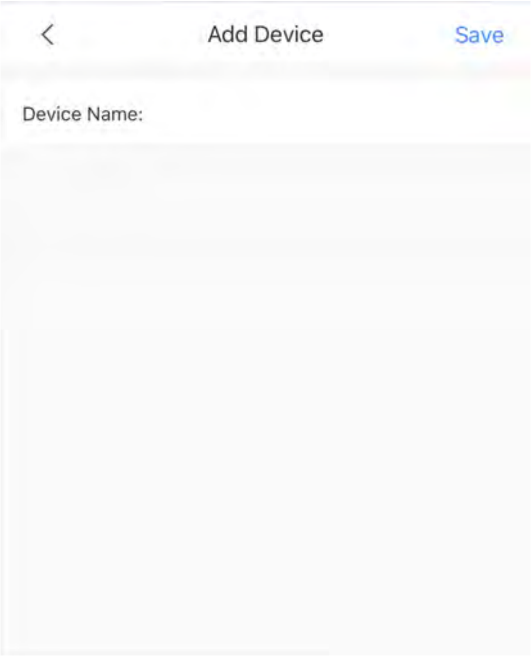
58 s

Connecting to the router...

Cancel Config

Step 6 Configure device name, and tap **Save**.

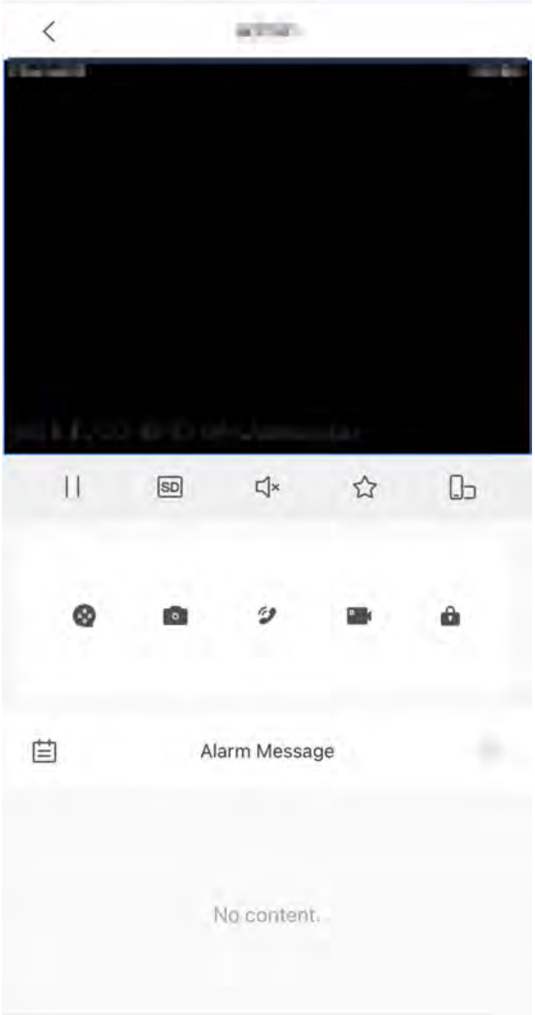
Figure 1-5 Configure device name



Device Name:

Step 7 View monitoring video from the camera on the VTO.

Figure 1-6 Monitor



No content.

2 Login and Resetting Password

2.1 Login

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

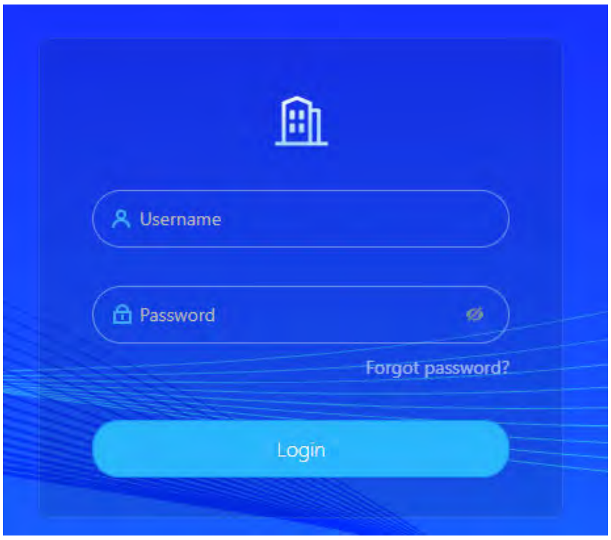
Procedure

Step 1 Go to the IP address of the VTO in the browser.

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

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

Figure 2-1 Login



2.2 Resetting Password

Procedure

Step 1 On the login page, click **Forgot Password?** , and then click **Next**.

Step 2 Scan the QR code, and then you will get a string of numbers and letters.

Step 3 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.

Step 4 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.

Step 5 Enter and confirm the new password, and then click **OK**.

3 Home Page

Figure 3-1 Home Page

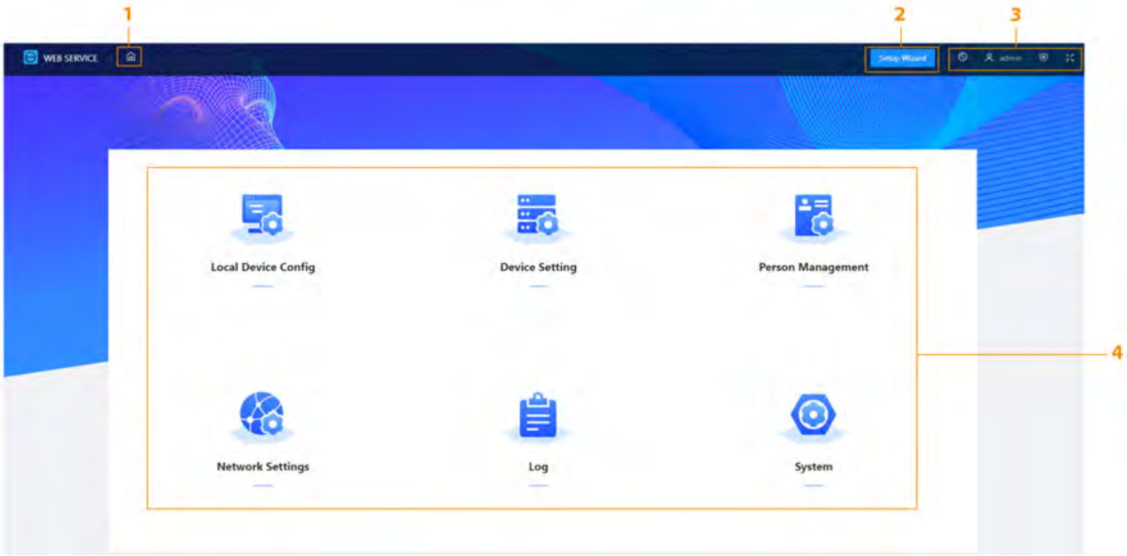


Table 3-1 Home page introduction

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. ● admin: Change password, log out of the current device, restart the system, and restore the device to factory settings. ● 🛡: View and configure the security settings. ● ⛶: View the webpage in full screen mode.
4	VTO function	Different function areas of the VTO.

4 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.

4.1 Setting as SIP Server

Set the VTO as the SIP server.

Prerequisites

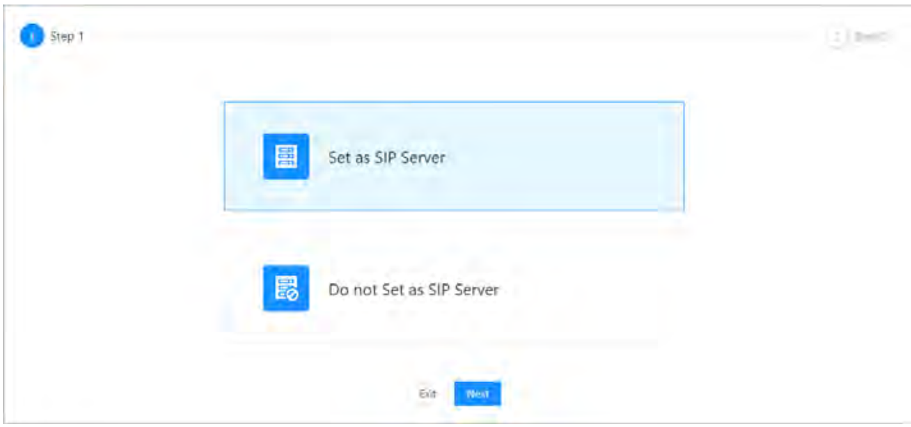
You have added VTOs on the webpage. If not, you can add them in **Set as SIP Server** page or in the **Device Setting** section.

Procedure

Step 1 Log in to the webpage of the VTO.

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

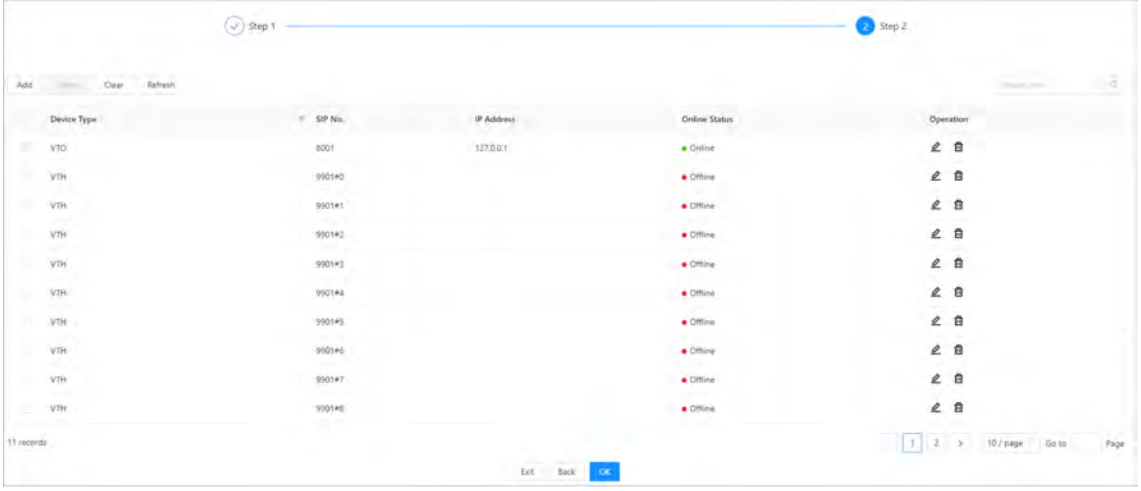
Figure 4-1 Set as SIP server



Step 3 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 4-2 Select the SIP server



Device Type	SIP No.	IP Address	Online Status	Operation
VTO	8001	127.0.0.1	● Online	
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	
VTH	9901#7		● Offline	
VTH	9901#8		● Offline	

11 records

4.2 Not Setting as SIP Server

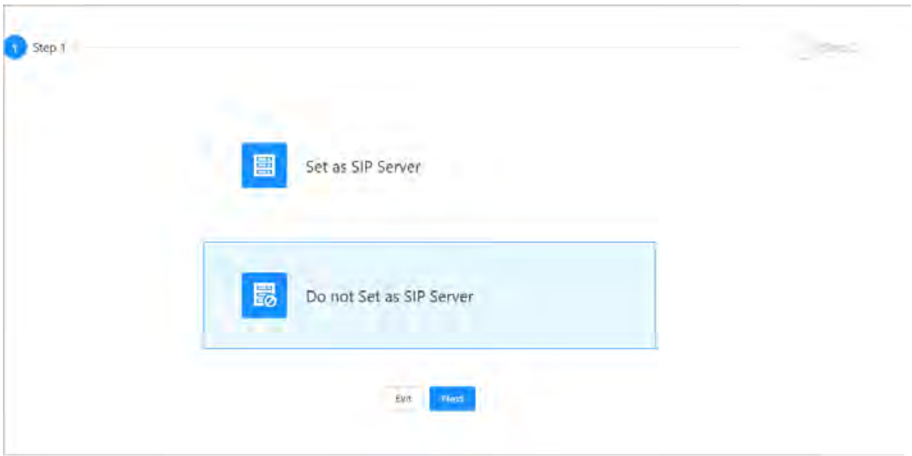
If you want to change the SIP server, you need to remove the current one from the list.

Procedure

Step 1 Log in to the webpage of the VTO.

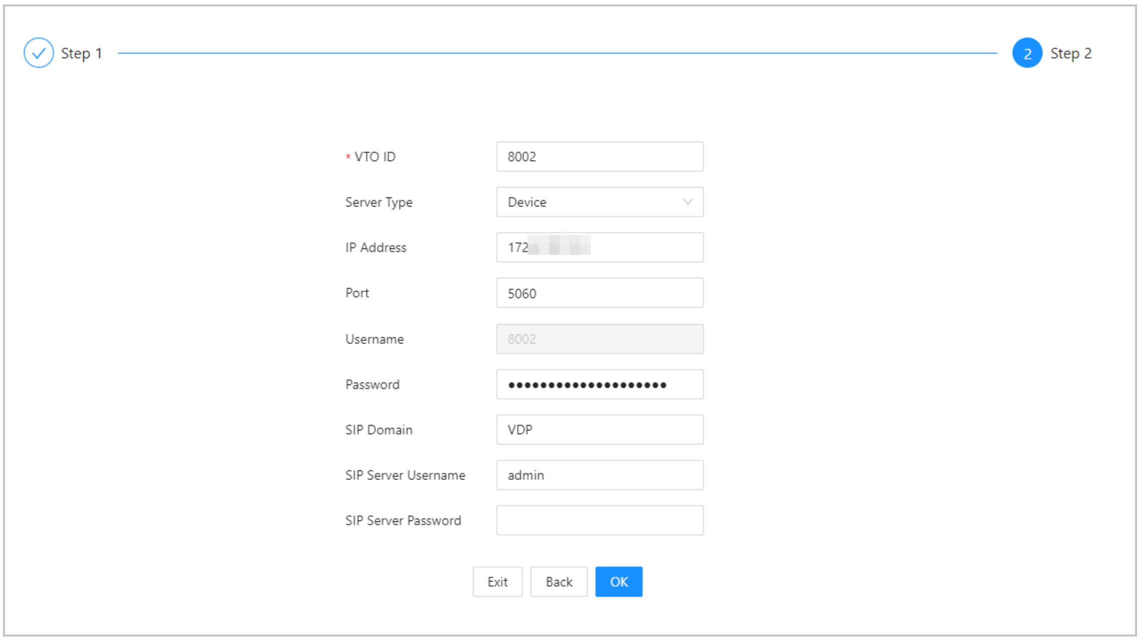
Step 2 Select **Setup Wizard** > **Do not Set as SIP Server**, and then click **Next**.

Figure 4-3 Do not set as SIP server



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

Figure 4-4 Configure information



* VTO ID	8002
Server Type	Device
IP Address	172[redacted]
Port	5060
Username	8002
Password	•••••••••••••••••••
SIP Domain	VDP
SIP Server Username	admin
SIP Server Password	

5 Local Device Configuration

This chapter introduces the detailed configuration of the VTO.

Slight differences might be found in different models.

5.1 Basic Settings

Configure basic settings of the device.

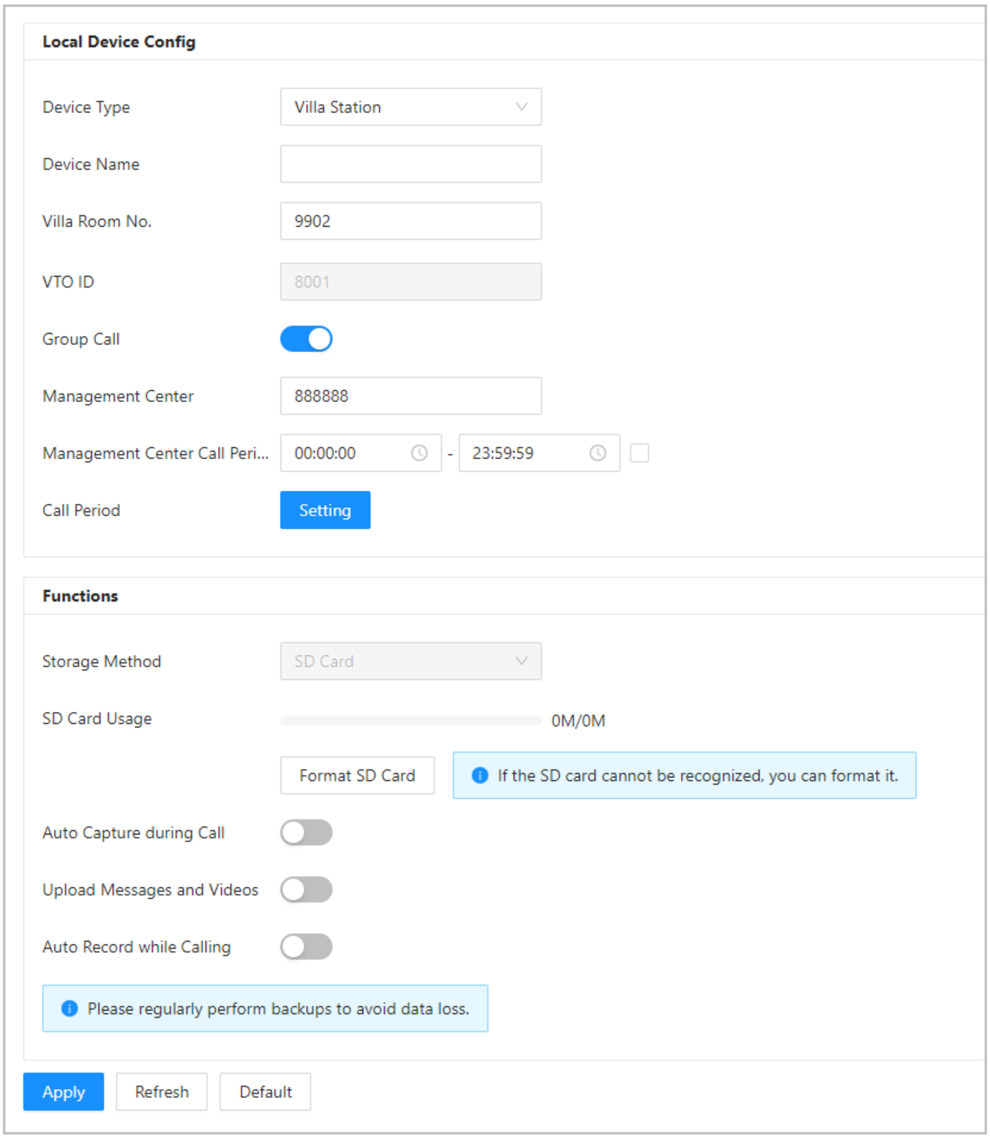
5.1.1 Villa Door Station

Procedure

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

Step 2 Configure the parameters.

Figure 5-1 Basic settings (Villa station)



Local Device Config

Device Type: Villa Station

Device Name:

Villa Room No.: 9902

VTO ID: 8001

Group Call: on

Management Center: 888888

Management Center Call Peri...: 00:00:00 - 23:59:59 □

Call Period: Setting

Functions

Storage Method: SD Card

SD Card Usage: 0M/0M

Format SD Card

If the SD card cannot be recognized, you can format it.

Auto Capture during Call: off

Upload Messages and Videos: off

Auto Record while Calling: off

Please regularly perform backups to avoid data loss.

Table 5-1 Basic parameter description

Parameter	Description
Device Type	Select **Villa 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.

Parameter	Description
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.
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 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**.

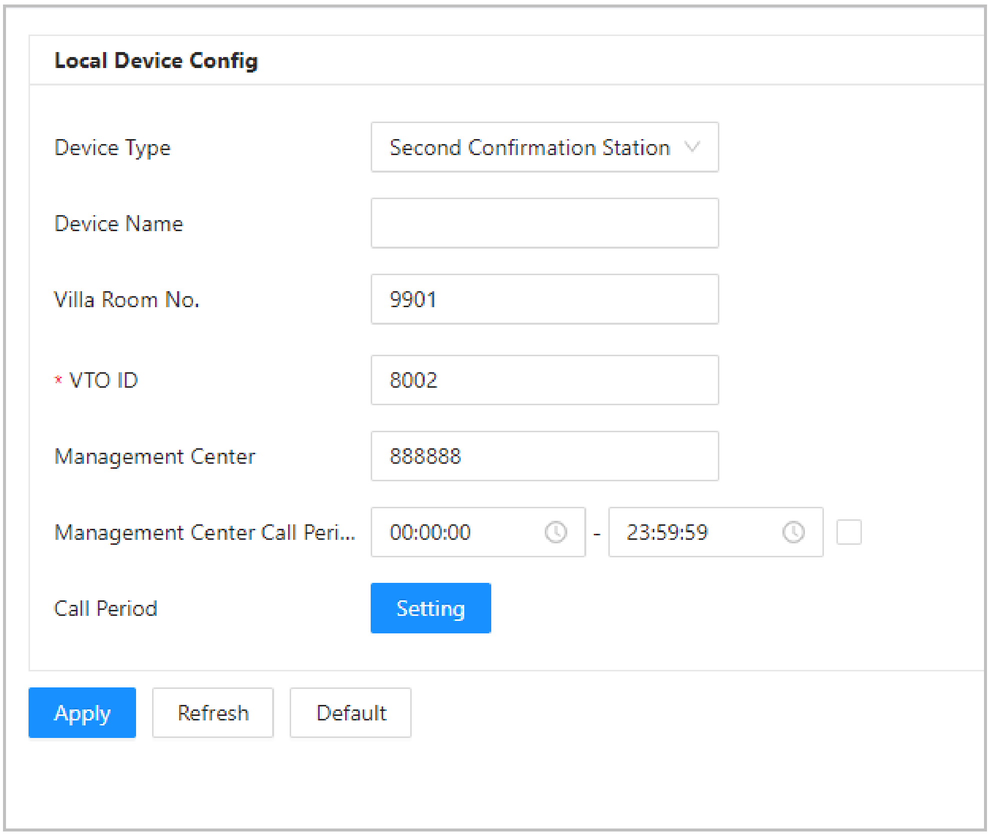
5.1.2 Second Confirmation Station

Procedure

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

Step 2 Configure the parameters.

Figure 5-2 Basic settings (Second confirmation station)



Local Device Config

Device Type: Second Confirmation Station

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

Table 5-2 Basic parameter description

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**.

5.2 Access Control

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

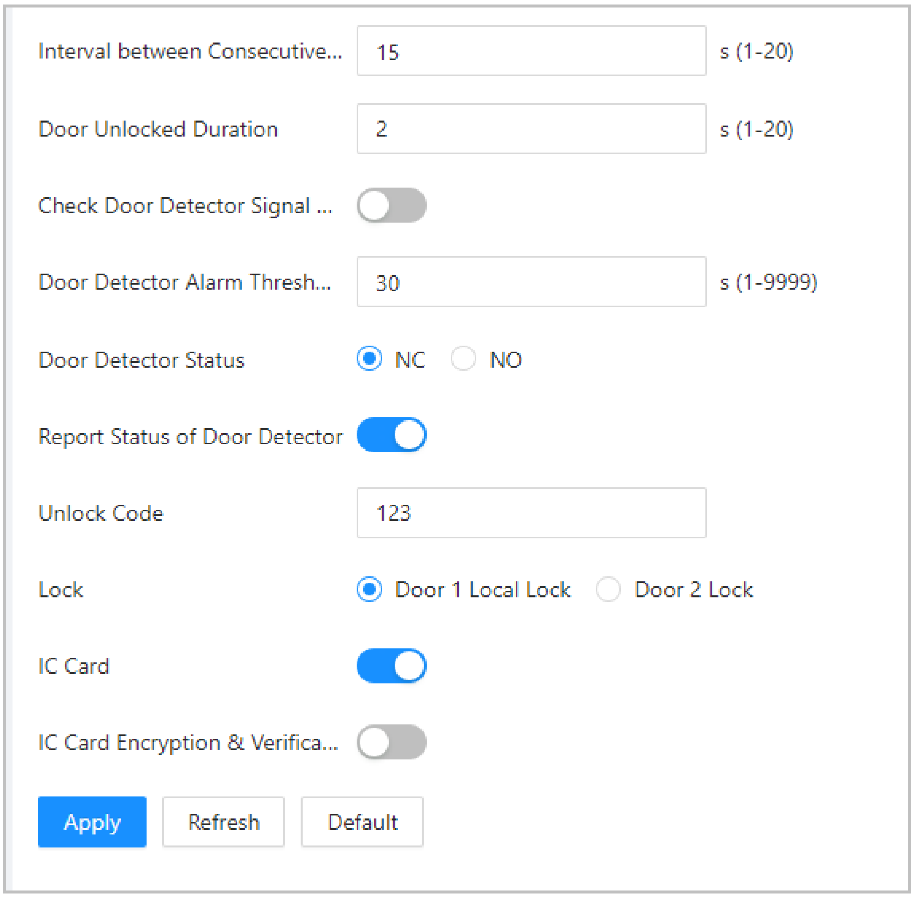
5.2.1 Config

Procedure

Step 1 Select **Local Device Config** > **Access Control** > **Config**.

Step 2 Configure the parameters.

Figure 5-3 Access control



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 ○ Door 2 Lock

IC Card ●

IC Card Encryption & Verifica... ○

Table 5-3 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**: 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**.

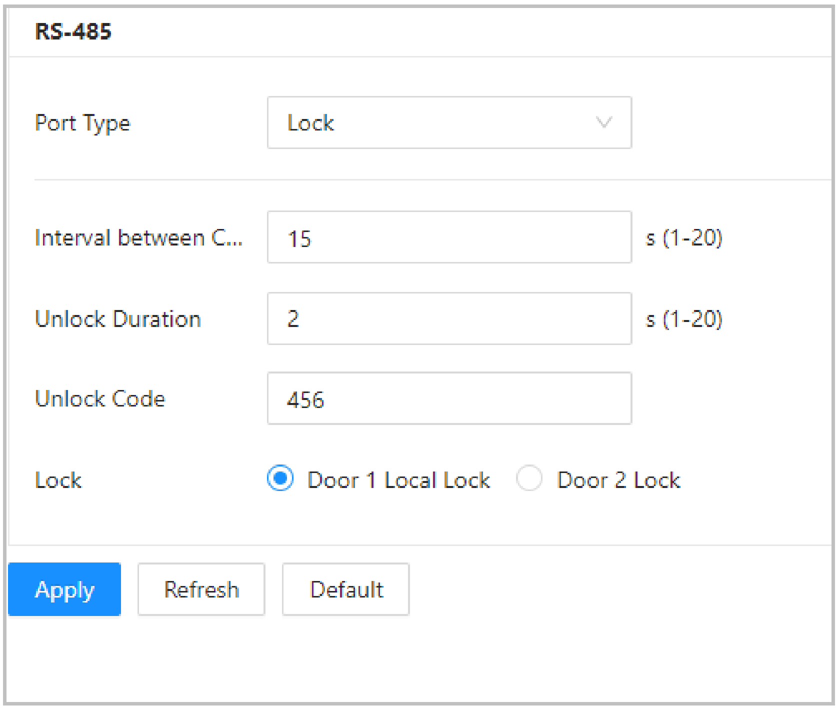
5.2.2 RS-485

Procedure

Step 1 Select **Local Device Config** > **Access Control** > **RS-485**.

Step 2 Configure the parameters of the lock connected through the RS-485 port.

Figure 5-4 RS-485



RS-485

Port Type: Lock

Interval between C...: 15 s (1-20)

Unlock Duration: 2 s (1-20)

Unlock Code: 456

Lock: ● Door 1 Local Lock ○ Door 2 Lock

Table 5-4 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.
Lock	Select the **Lock** type to unlock the lock you select. ● **Door 1 Local Lock**: Local lock. ● **Door 2 Lock**: 485 lock.

Step 3 Click **Apply**.

5.3 Layout

This function is only available for Q series 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

Step 1 Log in to the webpage of the VTO.

Step 2 Select **Local Device Config** > **Layout**.

Step 3 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.

- 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 "7.2 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 web page. 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 web page. Keep the above configuration rule when you install 2 buttons or 4 buttons on the VTO and configure the corresponding room numbers on the web page.

Figure 5-5 Fourth button installation

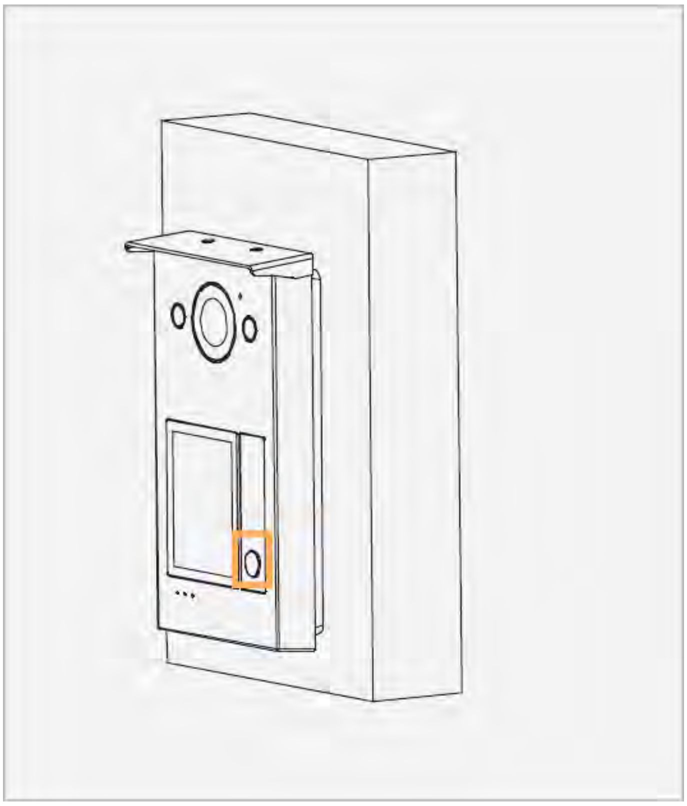
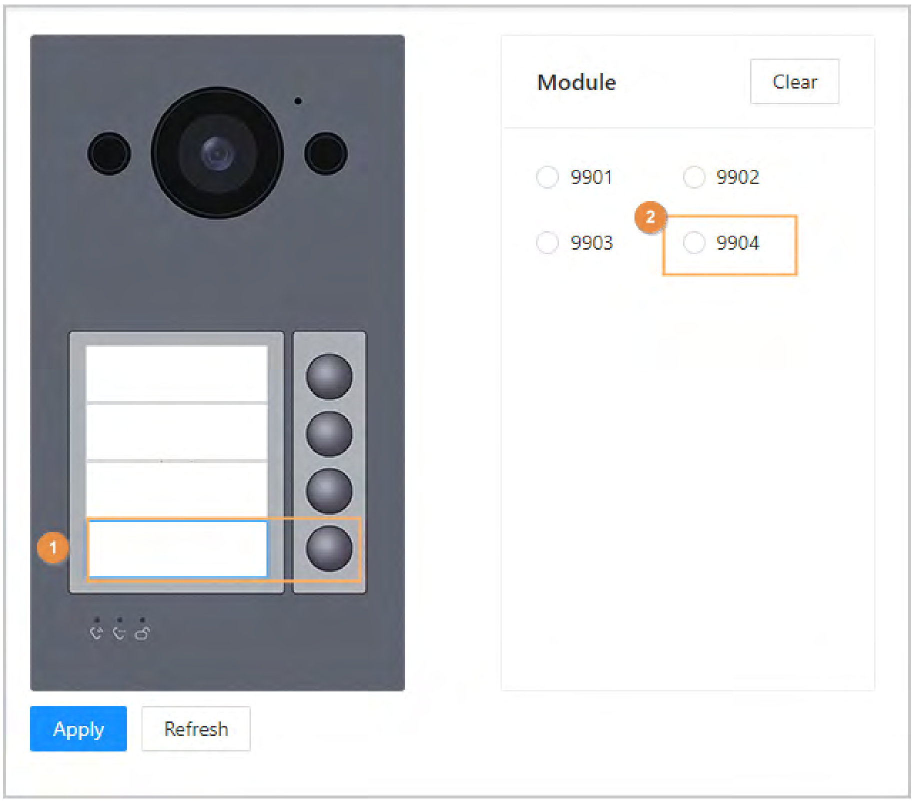
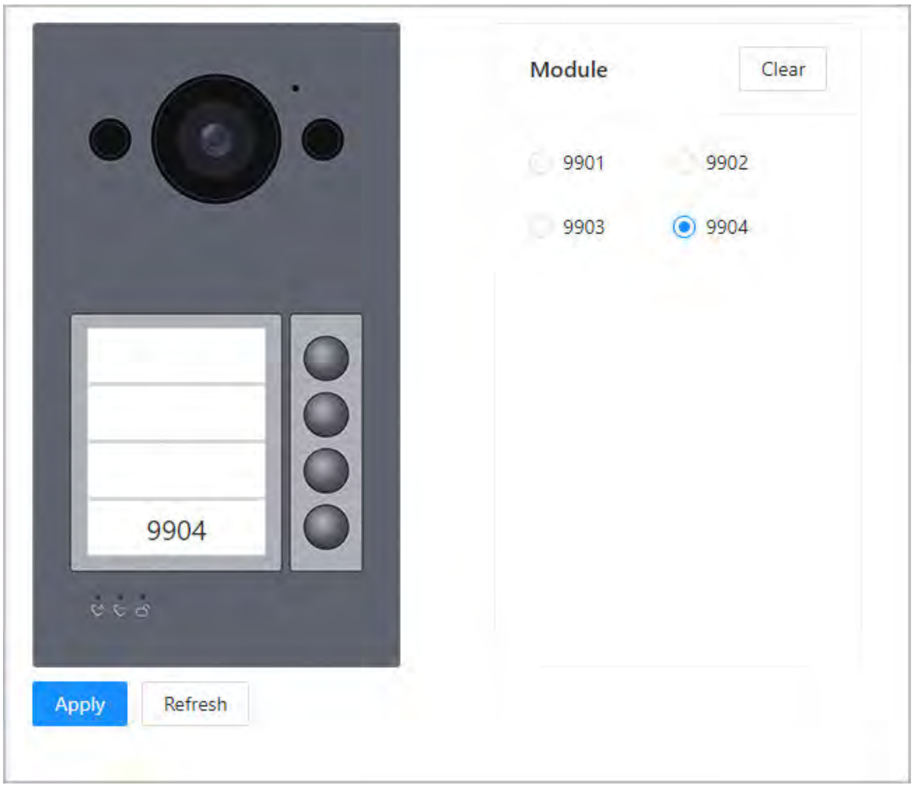


Figure 5-6 Configure the fourth nameplate (1)



Step 4 Click **Apply** to save the selected room number.

Figure 5-7 Configure the fourth nameplate



Module

○ 9901 ○ 9902

○ 9903 ● 9904

Step 5 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 System

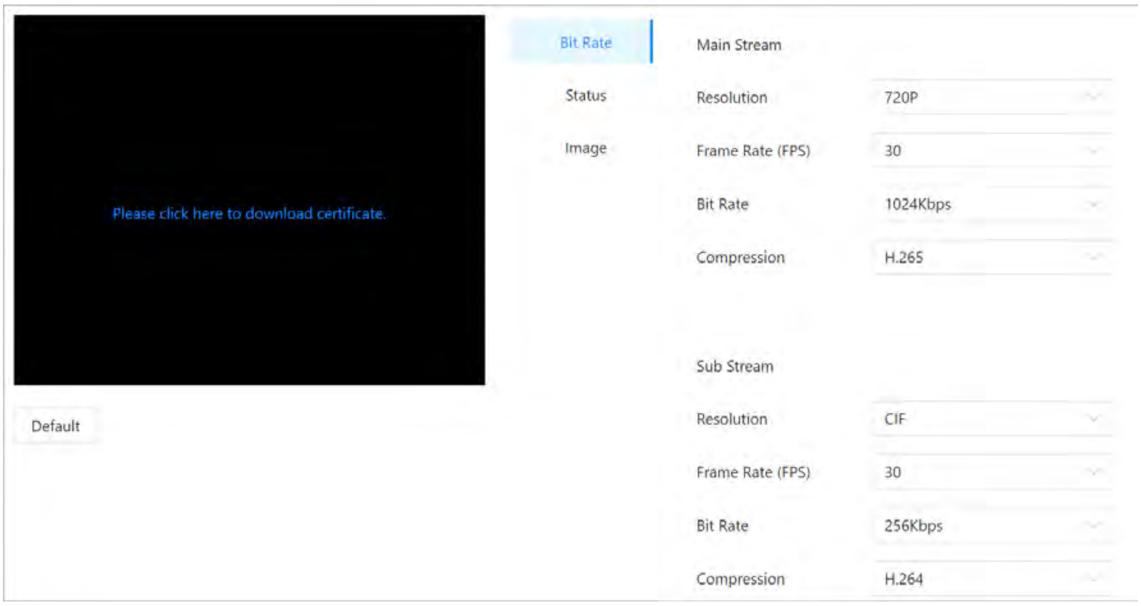
6.1 Video

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

Procedure

Step 1 Select **System** > **Video**.

Figure 6-1 Video



Main Stream

Resolution: 720P

Frame Rate (FPS): 30

Bit Rate: 1024Kbps

Compression: H.265

Sub Stream

Resolution: CIF

Frame Rate (FPS): 30

Bit Rate: 256Kbps

Compression: H.264

Step 2 Configure the parameters, which will take effect upon change.

Table 6-1 Video parameter description

Parameter		Description
Bit Rate	Resolution (Main Stream)	● **720P** : 1280 × 720. ● **WVGA** : 800 × 480. ● **D1** : 720 × 480. ● **CIF** : 352 × 288.
	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** : 720 × 480. ● **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.
Status	Scene Mode	Select from **Auto** , **Disable**, **Sunny** and **Night**. **Auto** is selected by default.
	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.
Image	Brightness	The larger the value, the brighter the image.
	Contrast	Larger value for more contrast between bright and dark areas.
	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.

Parameter		Description
	Gain Adjustment	Amplify the video signal to increase image brightness. If the value is too large, there will be more noise in the image.
	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.

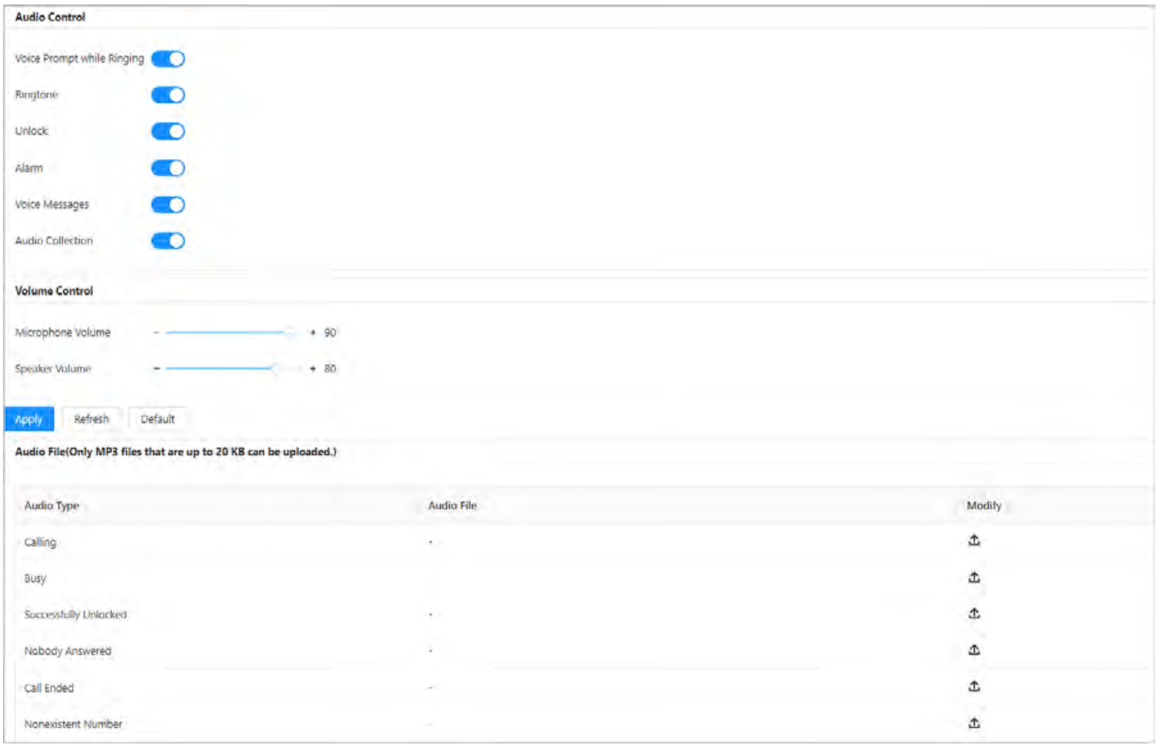
6.2 Audio

Procedure

Step 1 Select **System** > **Video**.

Step 2 Configure the parameters, which will take effect upon change.

Figure 6-2 Audio



Audio Control

Voice Prompt while Ringing: on

Ringtone: on

Unlock: on

Alarm: on

Voice Messages: on

Audio Collection: on

Volume Control

Microphone Volume: 90

Speaker Volume: 80

Audio File(Only MP3 files that are up to 20 KB can be uploaded.)

Audio Type	Audio File	Modify
Calling	-	⇧
Busy		⇧
Successfully Unlocked	-	⇧
Nobody Answered	-	⇧
Call Ended	-	⇧
Nonexistent Number	-	⇧

Table 6-2 Audio parameter description

Parameter		Description
Audio Control	Voice Prompt while Ringing	Turn on or off each type of sound.
	Ringtone	
	Alarm	
	Voice Messages	
	Unlock	
	Audio Collection	

Parameter		Description
Volume Control	Microphone Volume	Adjust the volume.
	Speaker Volume	

Step 3 Click **Apply**.

Step 4 (Optional) Upload audio file by clicking ⤒ next to the corresponding audio type (including calling, busy, successfully unlocked, nobody answered, call ended and nonexistent number).

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

6.3 Time

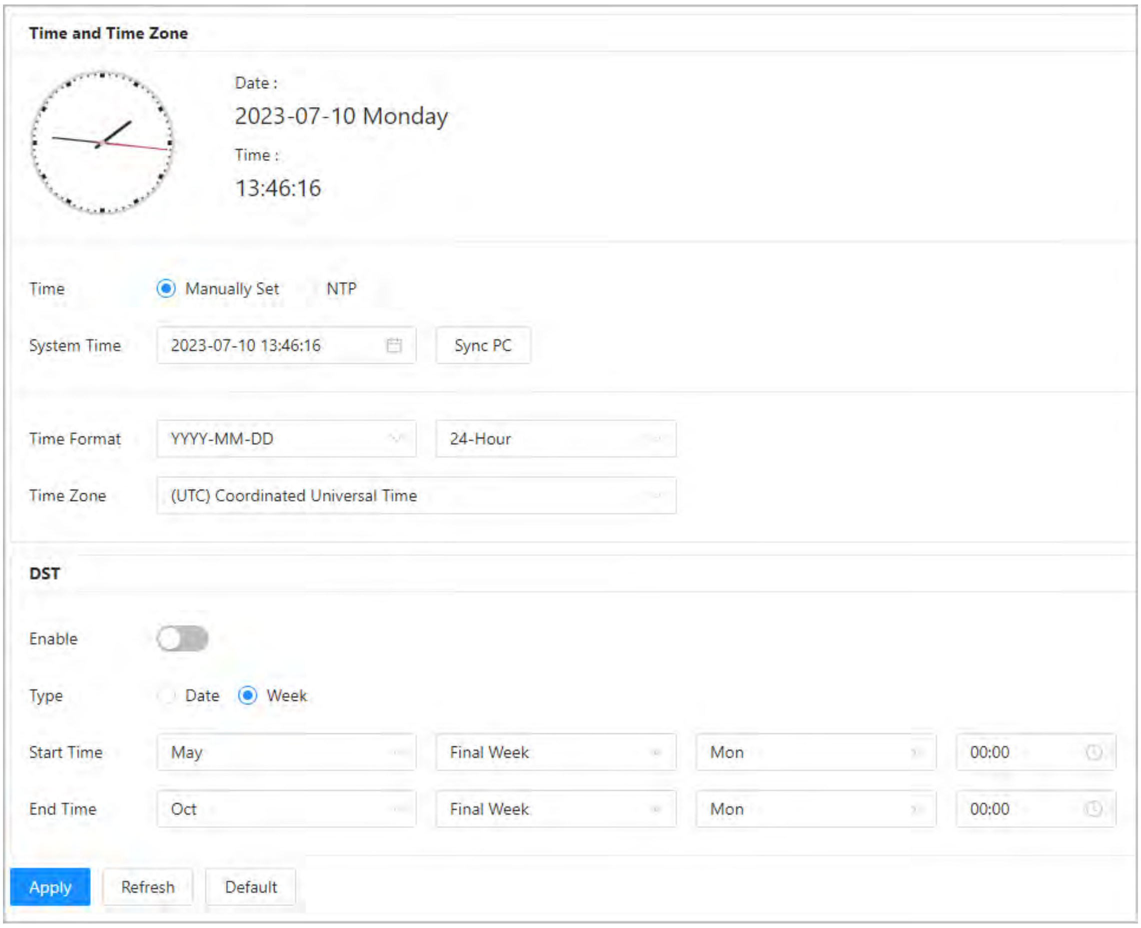
Configure the time zone and day light saving parameters.

Procedure

Step 1 Select **System** > **Time**.

Step 2 Configure the time and time zone and DST.

Figure 6-3 Time



Time and Time Zone

Date : 2023-07-10 Monday

Time : 13:46:16

Time ● Manually Set ○ NTP

System Time 2023-07-10 13:46:16 Sync PC

Time Format YYYY-MM-DD 24-Hour

Time Zone (UTC) Coordinated Universal Time

DST

Enable

Type ○ Date ● Week

Start Time May Final Week Mon 00:00

End Time Oct Final Week Mon 00:00

Table 6-3 Parameter description

Module	Parameter	Description
Time and Time Zone	Time	● Manually Set ● NTP
	System Time	The time of the VTO system. ⚠ 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.
	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.
DST	Enable	Click to enable the **DST** function.

Module	Parameter	Description
	Type	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**.

6.4 ONVIF User

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

Procedure

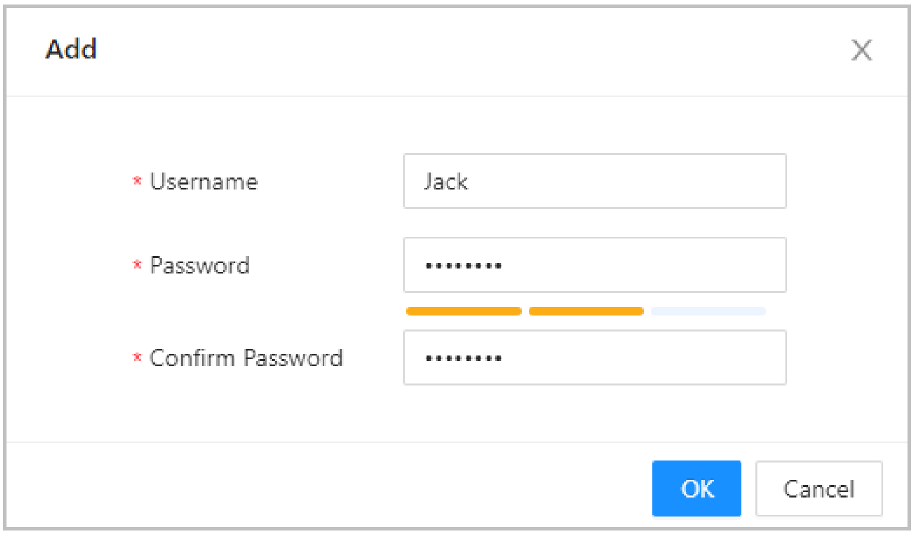
Step 1 Select **System** > **ONVIF User**.

Step 2 Click **Add**.

Step 3 Enter the information, and then click **OK**.

ONVIF devices can monitor the VTO by using the account.

Figure 6-4 ONVIF user



Add

* Username: Jack

* Password: •••••••••

* Confirm Password: •••••••••

6.5 Config

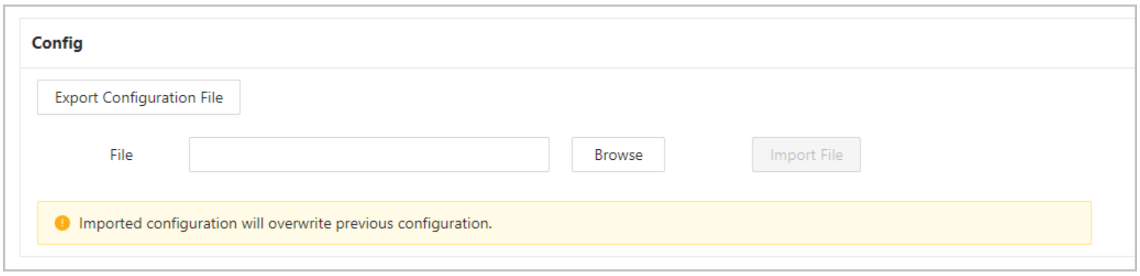
You can export and import the configuration file.

Procedure

Step 1 Select **System** > **Config**.

Step 2 Click **Export Configuration File**, or click **Browse** to select the file from local computer, and then click **Import file**.

Figure 6-5 Config



Config

Export Configuration File

File

Browse

Import File

Imported configuration will overwrite previous configuration.

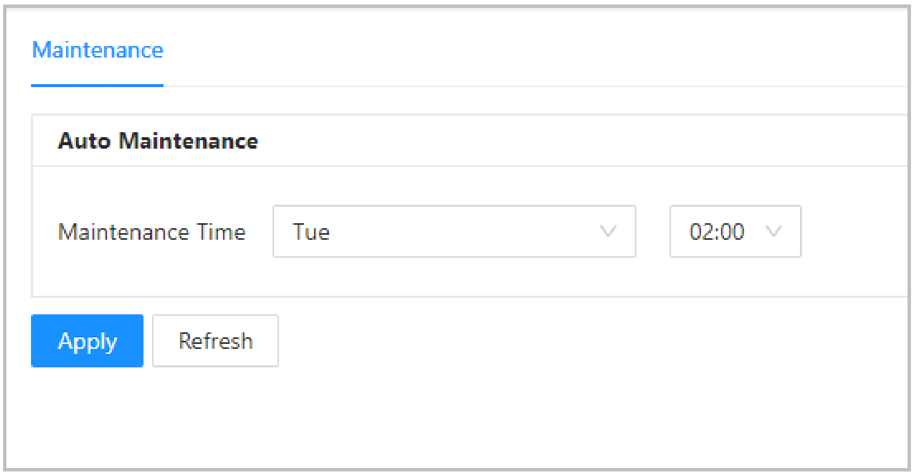
6.6 Maintenance

Procedure

Step 1 Select **System** > **Maintenance**.

Step 2 Configure the auto maintenance time.

Figure 6-6 Auto Maintenance



Maintenance

Auto Maintenance

Maintenance Time: Tue, 02:00

Step 3 Click **Apply**.

6.7 Updating

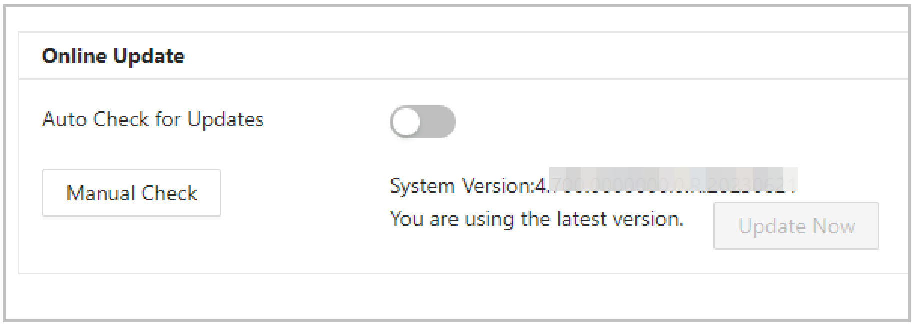
Procedure

Step 1 Select **System** > **Update**.

Step 2 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 6-7 Update



Online Update

Auto Check for Updates

Manual Check

System Version:4.[redacted]

You are using the latest version.

Update Now

6.8 Legal Information

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

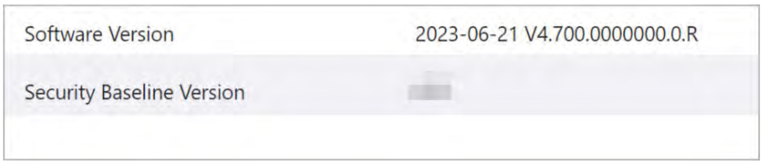
6.9 System Information

Procedure

Step 1 Select **System** > **System Info**.

Step 2 View the software version and security baseline version.

Figure 6-8 System information



Software Version	2023-06-21 V4.700.0000000.0.R
Security Baseline Version	[redacted]

7 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.

7.1 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

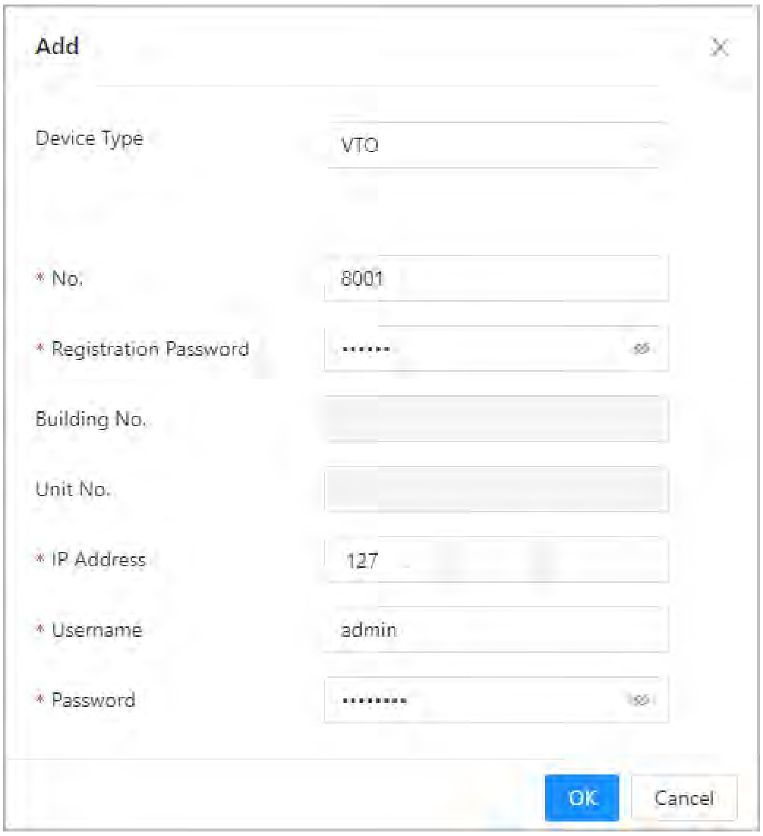
Step 1 Log in to the web page of the VTO that works as the SIP server.

Step 2 Select **Device Setting**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 7-1 Add VTO



Add

Device Type: VTO

* No.: 8001

* Registration Password: ••••••

Building No.:

Unit No.:

* IP Address: 127

* Username: admin

* Password: •••••••••

Table 7-1 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**.

📖

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

7.2 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.

Procedure

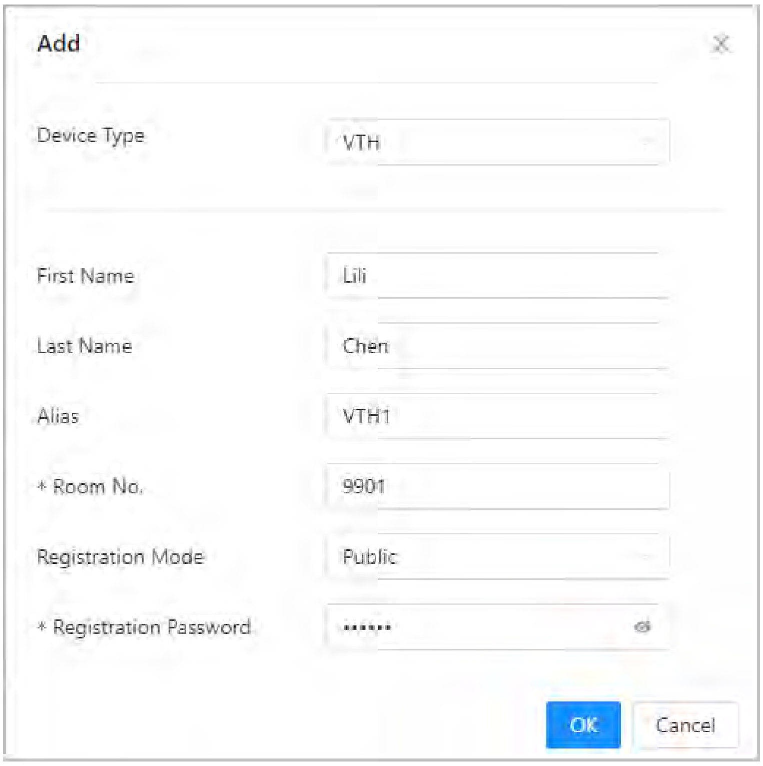
Step 1 Log in to the webpage of the SIP server.

Step 2 Select **Device Setting**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 7-2 Add VTH



Add

Device Type: VTH

First Name: Lili

Last Name: Chen

Alias: VTH1

* Room No.: 9901

Registration Mode: Public

* Registration Password: ••••••

Table 7-2 Room information

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

Step 5 Click **Save**.

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

7.3 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.

Procedure

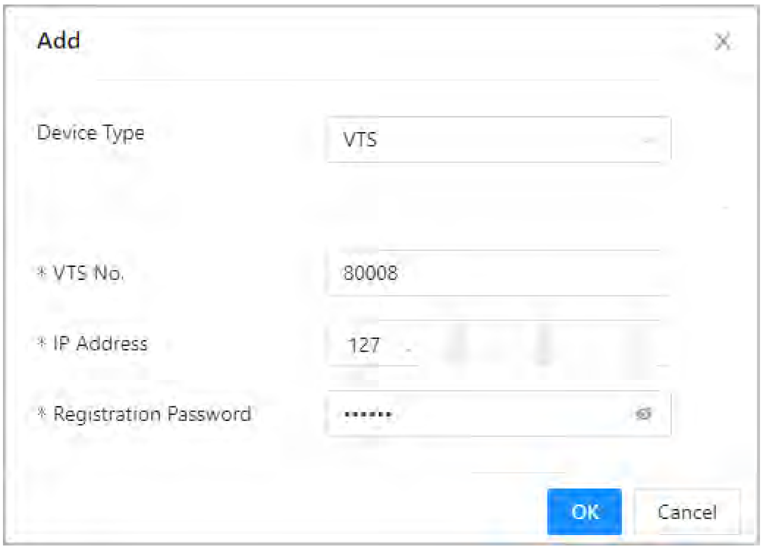
Step 1 Log in to the web page of the VTO that works as the SIP server.

Step 2 Select **Device Setting**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 7-3 Add VTS



Add

Device Type: VTS

* VTS No.: 80008

* IP Address: 127 .

* Registration Password: ••••••

Table 7-3 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**.

8 Person Management

Adding personnel information.

Background Information

Some VTO series support card issuing function in the person management. Issue an access card to unlock the door of a room. To use this function, the VTO must have a card reader.

Procedure

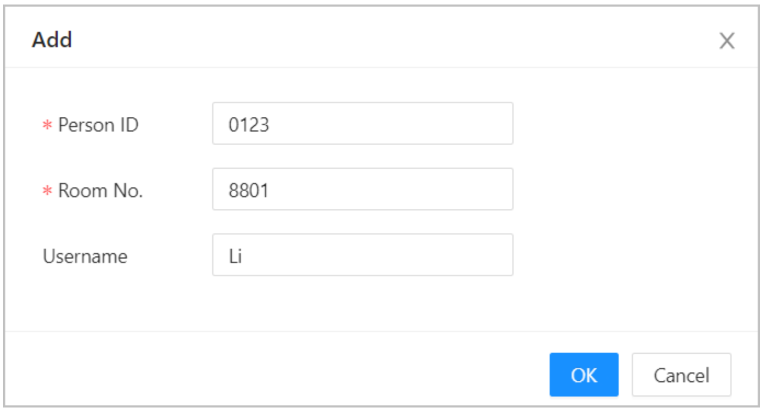
Step 1 Log in to the webpage of the VTO.

Step 2 Select **Person Management**.

Step 3 Click **Add**.

- VTO that do not have card issuing function: Enter the room ID, room number, username, and then click **OK**.

Figure 8-1 Add person



Add

* Person ID: 0123

* Room No.: 8801

Username: Li

- VTO that has card issuing function:

  a. Enter the room ID, room number, username and select the lock permission.

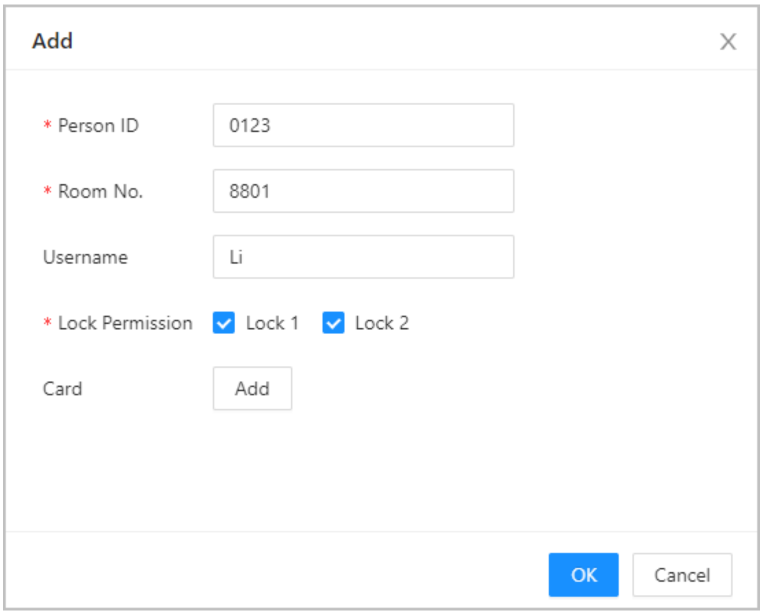
  ◇ Lock1: Local lock.

  ◇ Lock 2: 485 lock.

  📖

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

Figure 8-2 Add a person



Add

* Person ID: 0123

* Room No.: 8801

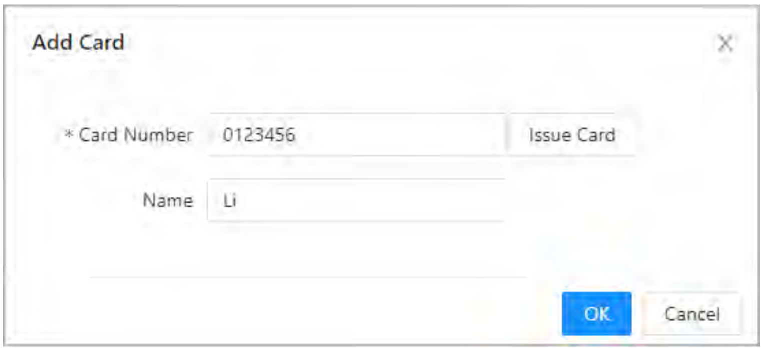
Username: Li

* Lock Permission: ☑ Lock 1 ☑ Lock 2

Card: Add

b. Click **Add** next to **Card**, and enter the card number and name.

Figure 8-3 Issue card



Add Card

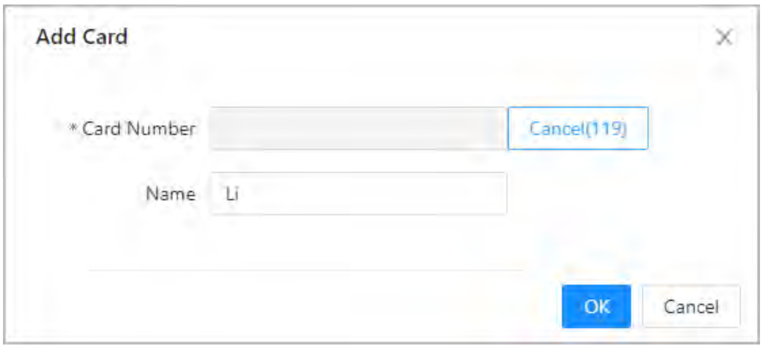
* Card Number: 0123456

Name: Li

c. Click **Issue Card**.

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

Figure 8-4 Countdown



Add Card

* Card Number:

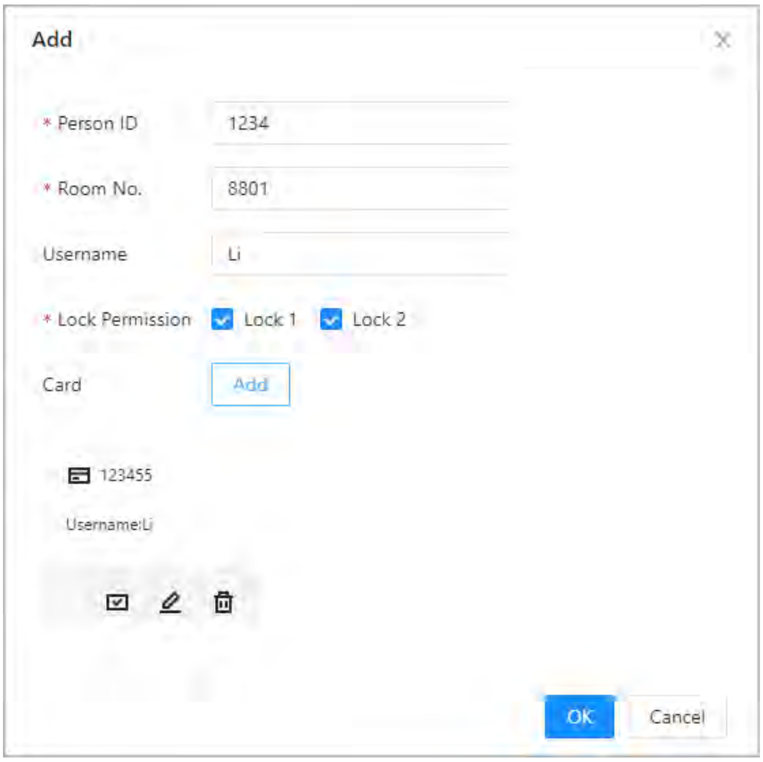
Name: Li

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

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

- ◇ ☑: Report lost card. After clicking the icon, it becomes 🔒.
- ◇ ✎: Edit the card information.
- ◇ 🗑: Delete the added card.

Figure 8-5 Card issued



* Person ID: 1234

* Room No.: 8801

Username: Li

* Lock Permission: ☑ Lock 1 ☑ Lock 2

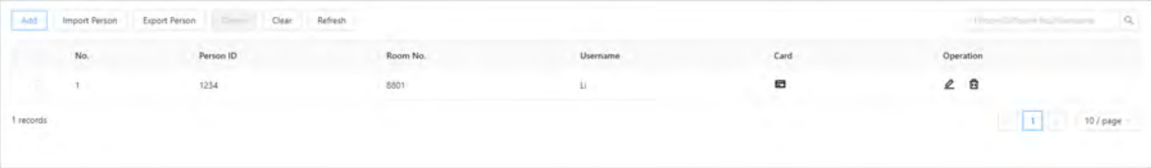
Card: Add

123455

Username:Li

e. Click **OK**.

Figure 8-6 Card added successfully



No.	Person ID	Room No.	Username	Card	Operation
1	1234	8801	Li	▭	✎ 🗑

1 records

Related Operations

- Click **Import Person**, and enter the password to log into the webpage of the VTO to import the person information.
- Click **Export Person**, and enter the password to log into the webpage of the VTO to export the person information.

9 Network Settings

This chapter introduces how to configure the network parameters.

9.1 TCP/IP

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

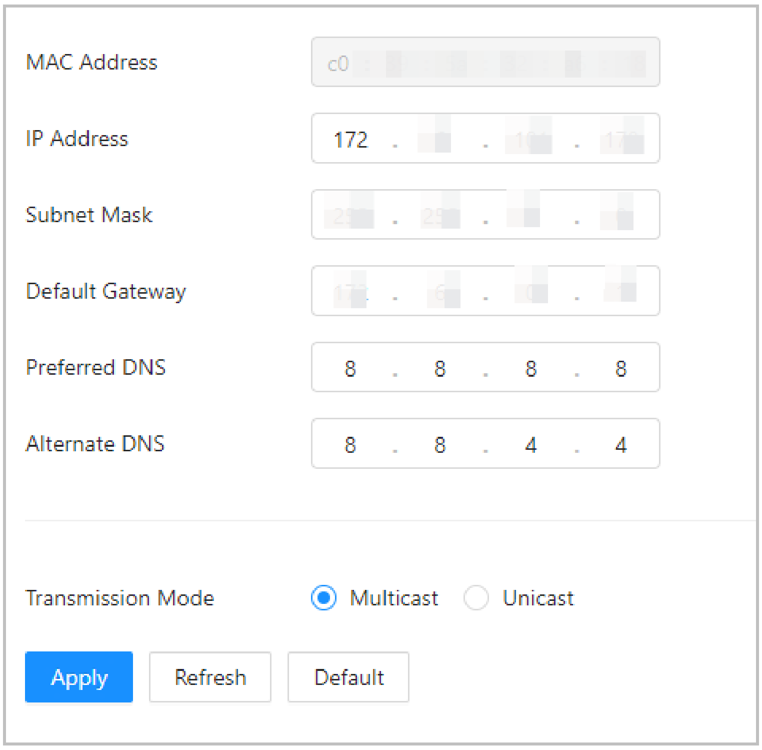
Procedure

Step 1 Log in to the webpage of the VTO.

Step 2 Select **Network Settings** > **TCP/IP**.

Step 3 Configure the TCP/IP parameters.

Figure 9-1 TCP/IP



MAC Address: c0 [redacted]

IP Address: 172 . [redacted] . [redacted] . [redacted]

Subnet Mask: [redacted] . [redacted] . [redacted] . [redacted]

Default Gateway: [redacted] . [redacted] . [redacted] . [redacted]

Preferred DNS: 8 . 8 . 8 . 8

Alternate DNS: 8 . 8 . 4 . 4

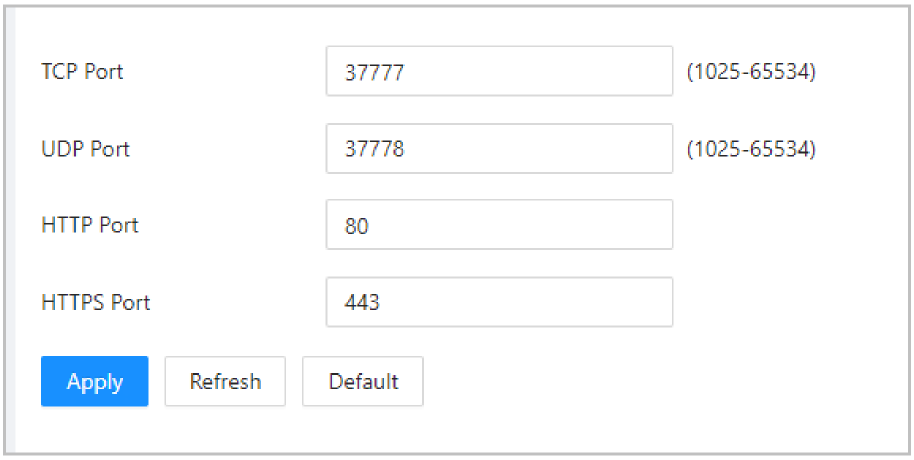
Transmission Mode: ● Multicast ○ Unicast

Table 9-1 Parameter description

Parameter	Description
IP Address	Your planned IP address for the VTO.
Preferred DNS	It is 8.8.8.8 by default.
Alternate DNS	It is 8.8.4.4 by default.
Transmission Mode	● Multicast. ● Unicast. 🕮 Unicast is preferred when the switch does not support multicast function, or when the network connection is not good.

9.2 Port

Figure 9-2 Port



TCP Port 37777 (1025-65534)

UDP Port 37778 (1025-65534)

HTTP Port 80

HTTPS Port 443

Table 9-2 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.

9.3 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

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

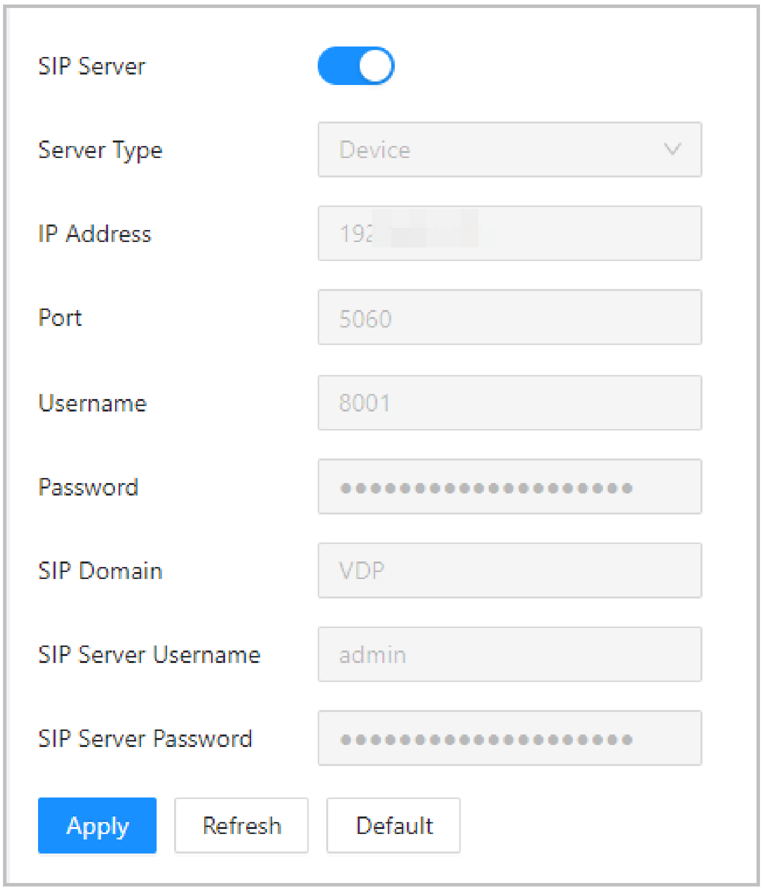
Step 2 Select a server type.

- 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.

Figure 9-3 Current VTO as SIP server

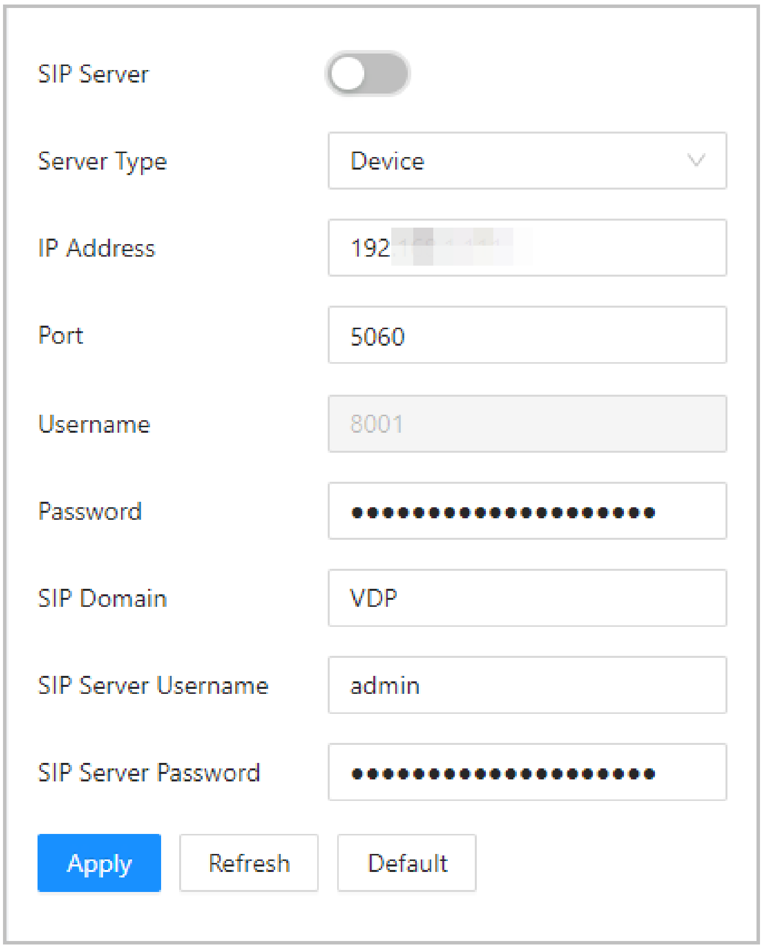


SIP Server	●
Server Type	Device
IP Address	19[redacted]
Port	5060
Username	8001
Password	•••••••••••••••••••••
SIP Domain	VDP
SIP Server Username	admin
SIP Server Password	•••••••••••••••••••••

- 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 9-4 Another VTO as SIP server



SIP Server: ○

Server Type: Device

IP Address: 192[redacted]

Port: 5060

Username: 8001

Password: ••••••••••••••••••••

SIP Domain: VDP

SIP Server Username: admin

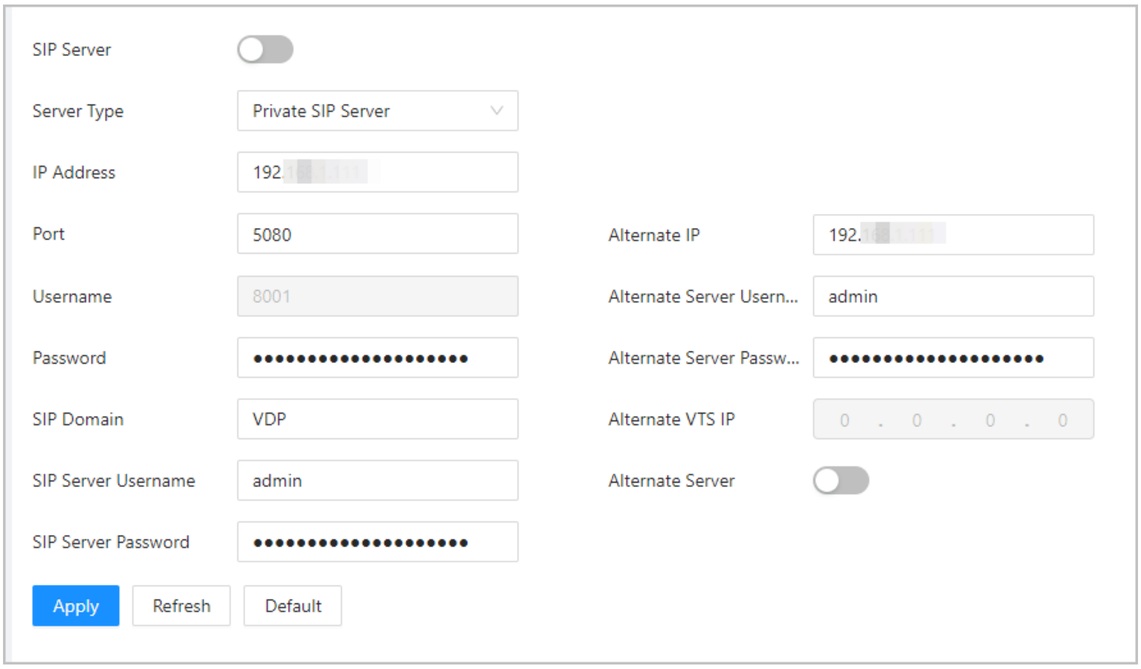
SIP Server Password: ••••••••••••••••••••

Table 9-3 SIP server configuration (VTO as the SIP server)

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

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

Figure 9-5 Private SIP server



SIP Server: ○ (off)

Server Type: Private SIP Server

IP Address: 192[redacted]

Port: 5080

Username: 8001

Password: ••••••••••••••••••••

SIP Domain: VDP

SIP Server Username: admin

SIP Server Password: ••••••••••••••••••••

Alternate IP: 192.[redacted]

Alternate Server Usern...: admin

Alternate Server Passw...: ••••••••••••••••••••

Alternate VTS IP: 0 . 0 . 0 . 0

Alternate Server: ○ (off)

Table 9-4 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**.

9.4 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

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

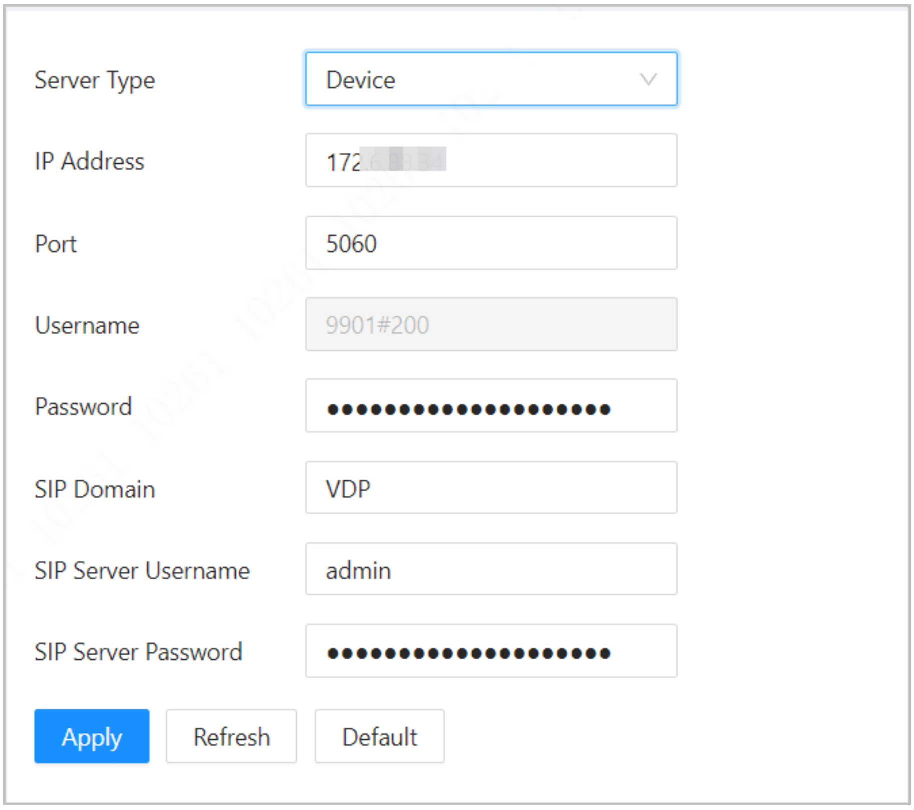
Step 2 Configure the second confirmation station information in **Local Device Config** > **Basic Settings**.

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

Step 3 Set **Server Type** as **Device**, and then configure the parameters.

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

Figure 9-6 SIP server configuration (VTH as the SIP server)



Server Type: Device

IP Address: 172[redacted]

Port: 5060

Username: 9901#200

Password: ●●●●●●●●●●●●●●●●●●●●

SIP Domain: VDP

SIP Server Username: admin

SIP Server Password: ●●●●●●●●●●●●●●●●●●●●

Table 9-5 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	Leave it as default.
Password	
SIP Domain	

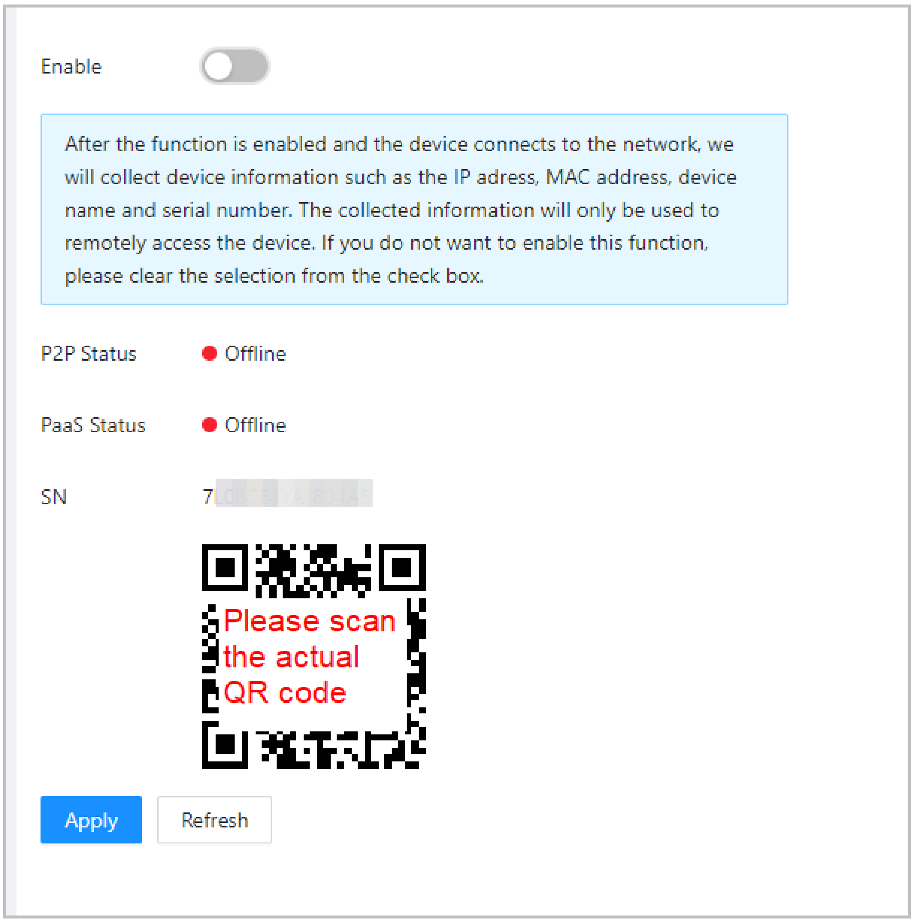
Parameter	Description
SIP Server Username	Username and password used to log into the VTH that serves as the SIP server.
SIP Server Password	

Step 4 Click **Apply**.

9.5 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.

Figure 9-7 Cloud service



Enable ○

After the function is enabled and the device connects to the network, we will collect device information such as the IP adress, MAC address, device name and serial number. The collected information will only be used to remotely access the device. If you do not want to enable this function, please clear the selection from the check box.

P2P Status ● Offline

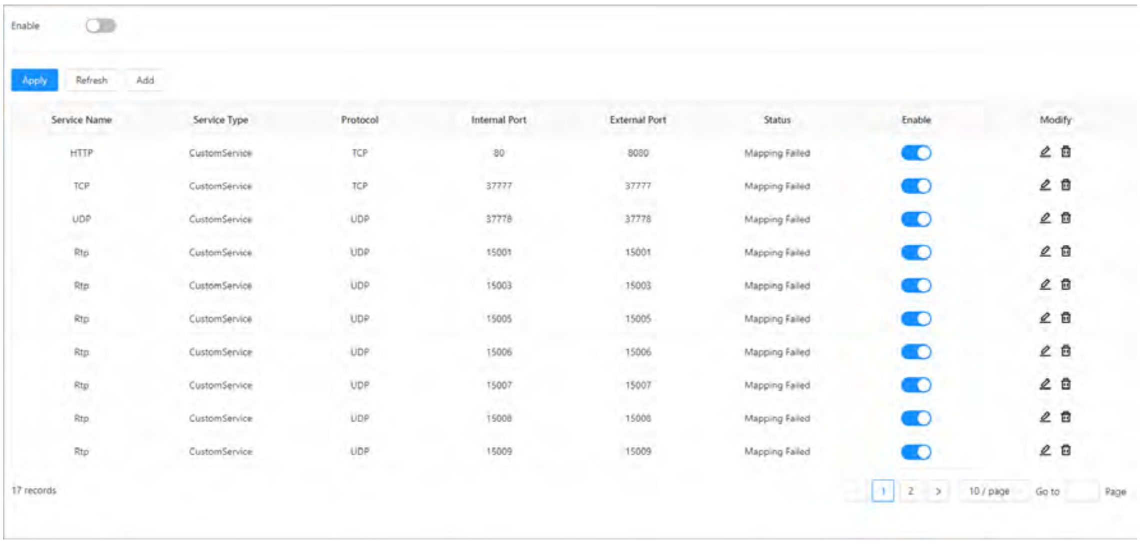
PaaS Status ● Offline

SN 7[redacted]

9.6 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 9-8 UPnP



Enable ○

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	●	✎ 🗑

17 records

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.

9.6.1 Enabling UPnP Services

Procedure

Step 1 Select **Network Settings** > **UPnP**.

Step 2 Enable the services listed.

Step 3 Select **Enable**.

Step 4 Click **Save**.

9.6.2 Adding UPnP Services

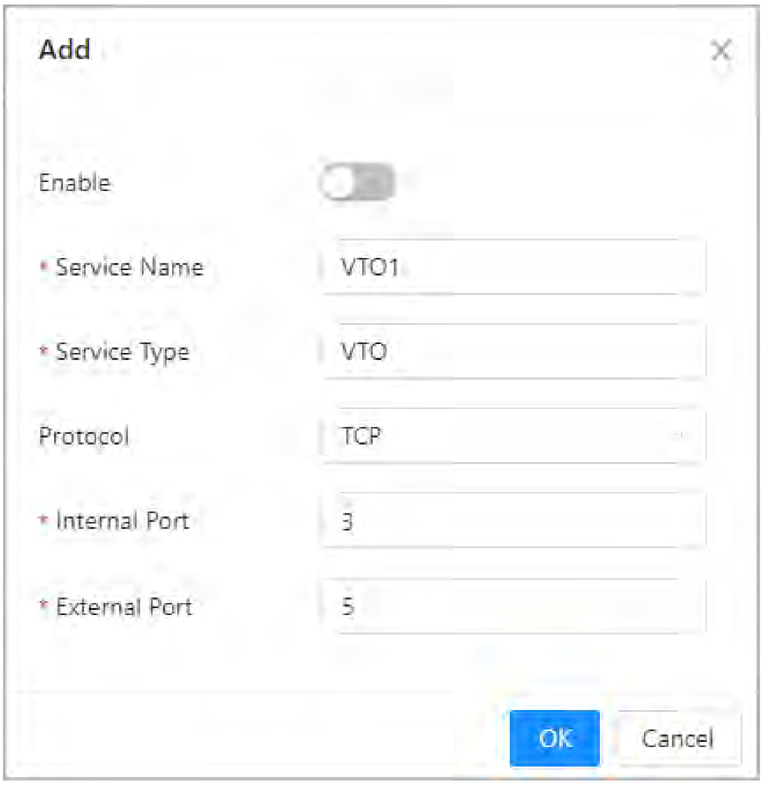
Procedure

Step 1 Select **Network Settings** > **UPnP**.

Step 2 Click **Add**.

Step 3 Configure the parameters, and then click **OK**.

Figure 9-9 Add a UPnP service



Add

Enable

* Service Name: VTO1

* Service Type: VTO

Protocol: TCP

* Internal Port: 3

* External Port: 5

Table 9-6 Parameter description

Parameter	Description
Service Name	Enter the name and type of the service.
Service Type	
Protocol	Select **TCP** or **UDP**.
Internal Port	Internal port of the service. ● 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	External port of the service. ● 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.

9.7 Wi-Fi

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

Procedure

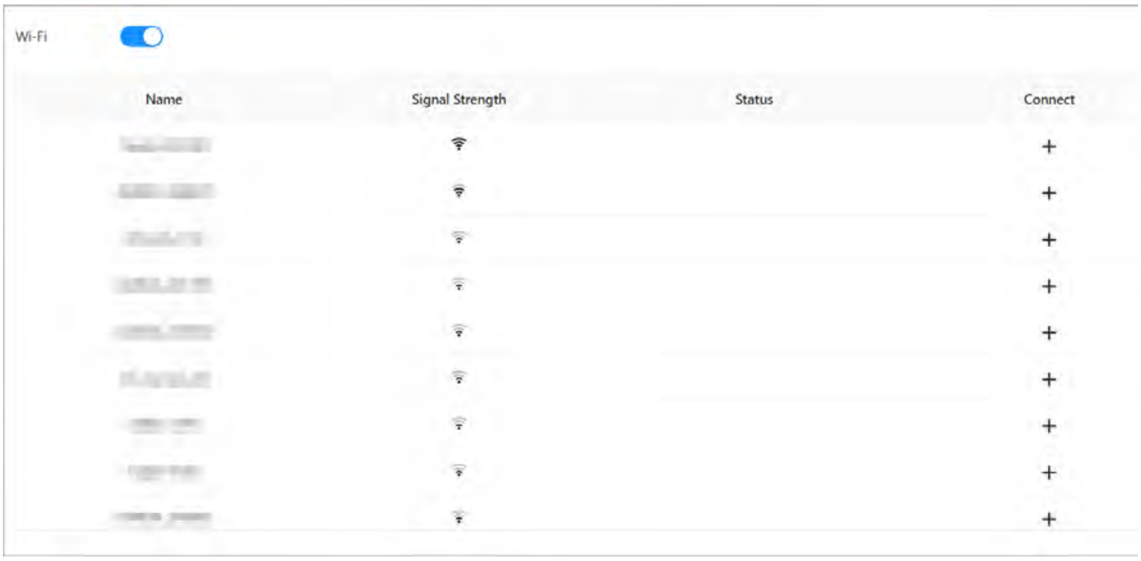
Step 1 Log in to the webpage of the VTO.

Step 2 Select **Network Settings** > **Wi-Fi**.

Step 3 Set the **Wi-Fi** status as **On**.

All the networks available are displayed.

Figure 9-10 Wi-Fi



Wi-Fi

Name	Signal Strength	Status	Connect
[illegible]			+
[illegible]			+
[illegible]			+
[illegible]			+
[illegible]			+
[illegible]			+
[illegible]			+
[illegible]			+
[illegible]			+

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

9.8 Basic Services

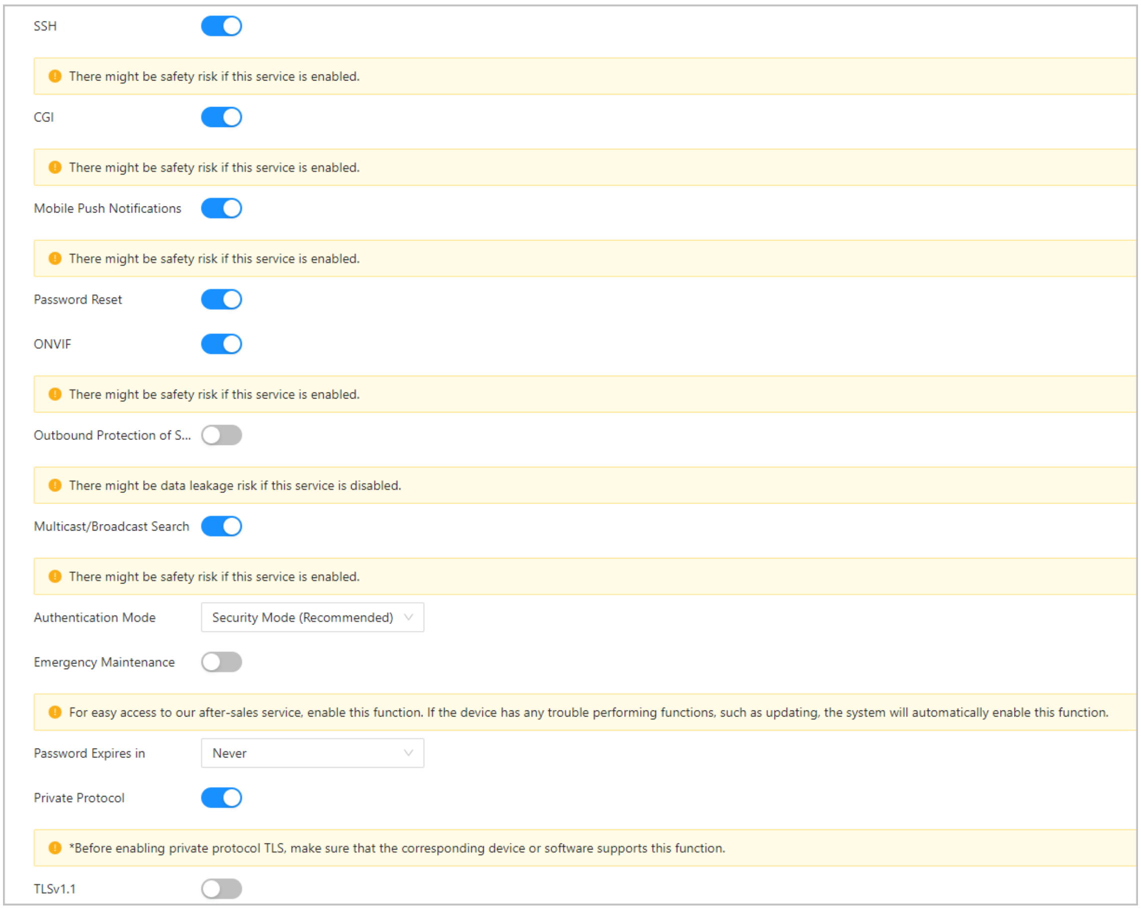
Configure functions that involve device security.

Procedure

Step 1 Select **Network Settings** > **Basic Services**.

Step 2 Enable the security functions based on your needs.

Figure 9-11 Basic services



SSH

There might be safety risk if this service is enabled.

CGI

There might be safety risk if this service is enabled.

Mobile Push Notifications

There might be safety risk if this service is enabled.

Password Reset

ONVIF

There might be safety risk if this service is enabled.

Outbound Protection of S...

There might be data leakage risk if this service is disabled.

Multicast/Broadcast Search

There might be safety risk if this service is enabled.

Authentication Mode: Security Mode (Recommended)

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

Table 9-7 Security parameter description

Parameter	Description
SSH	A secure alternative to unsecured remote protocols. 📖 We recommend you turn it off because there might be safety risk if this service is enabled.
CGI	The use of CGI command. 📖 We recommend you turn it off. Otherwise, the VTO might be exposed to security risks and data leakage.
Mobile Push Notification	Send information to the app on the phone. 📖 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.
Outbound Service Information Protection	Protect your passwords. 📖 We recommend you turn it on. Otherwise, the VTO might be exposed to security risks and data leakage.
Multicast/Broadcast Search	Enable it so that the VTO will be found by other devices. 📖 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**.

10 Log Management

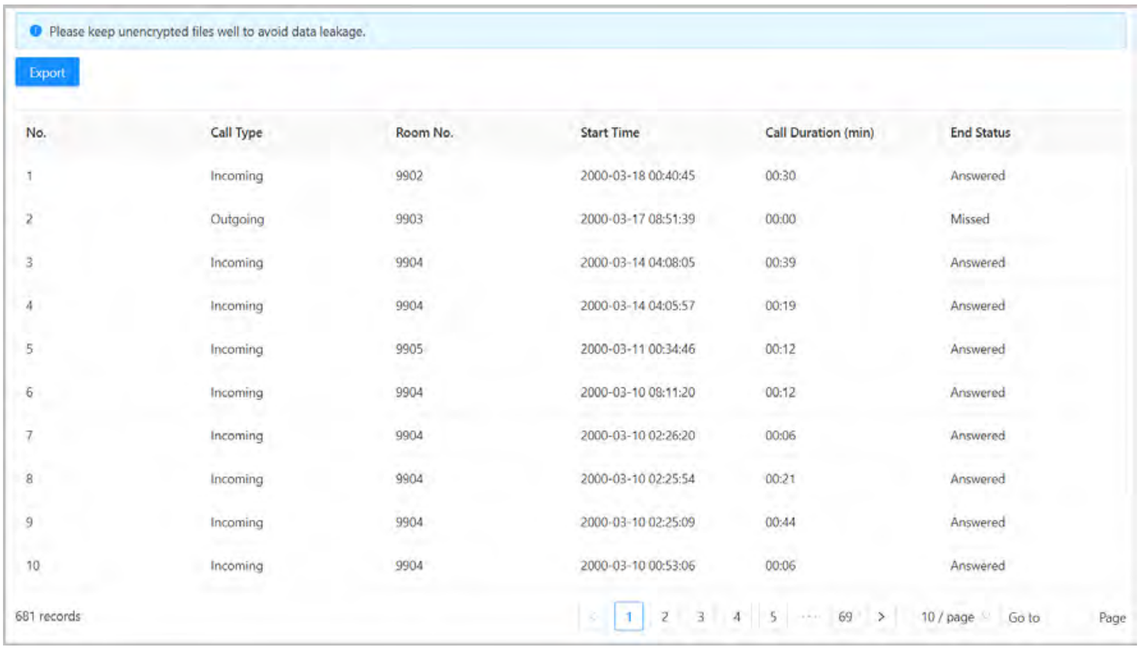
Select **Log**. You can search for different logs, and export them to your local computer.

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

10.1 Call History

Select **Log** > **Call History**.

Figure 10-1 Call history



Please keep unencrypted files well to avoid data leakage.

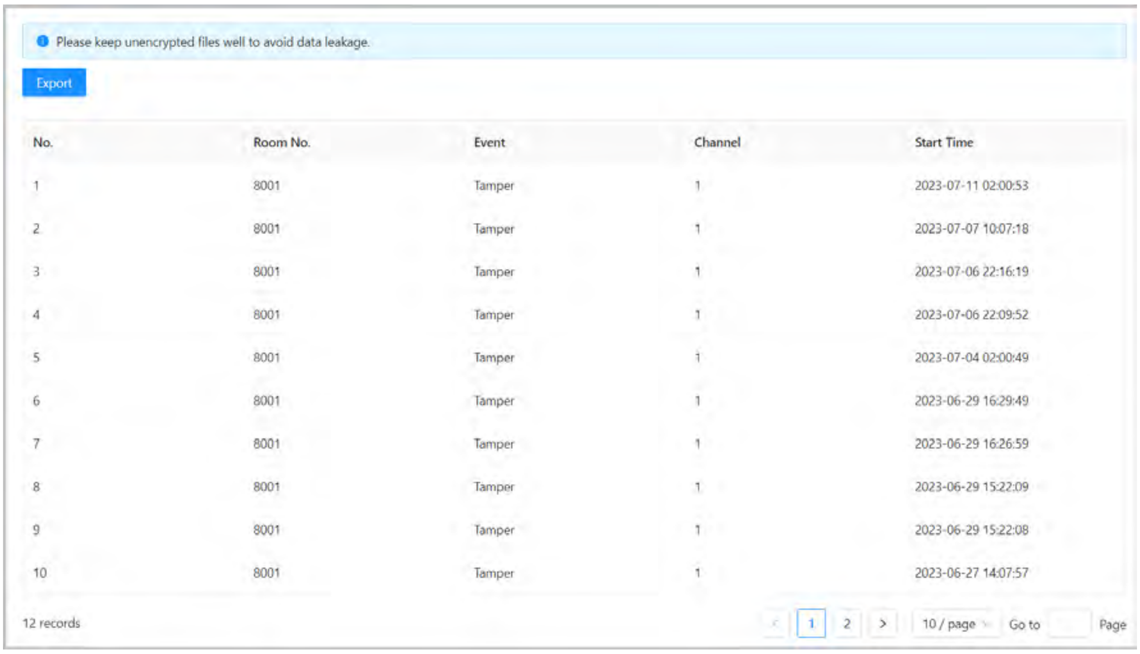
No.	Call Type	Room No.	Start Time	Call Duration (min)	End Status
1	Incoming	9902	2000-03-18 00:40:45	00:30	Answered
2	Outgoing	9903	2000-03-17 08:51:39	00:00	Missed
3	Incoming	9904	2000-03-14 04:08:05	00:39	Answered
4	Incoming	9904	2000-03-14 04:05:57	00:19	Answered
5	Incoming	9905	2000-03-11 00:34:46	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

681 records

10.2 Alarm Logs

Select **Log** > **Alarm Logs**.

Figure 10-2 Alarm



Please keep unencrypted files well to avoid data leakage.

Export

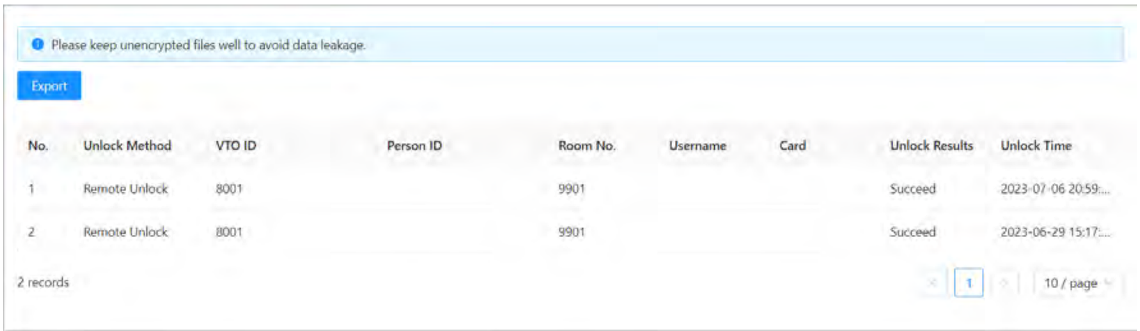
No.	Room No.	Event	Channel	Start Time
1	8001	Tamper	1	2023-07-11 02:00:53
2	8001	Tamper	1	2023-07-07 10:07:18
3	8001	Tamper	1	2023-07-06 22:16:19
4	8001	Tamper	1	2023-07-06 22:09:52
5	8001	Tamper	1	2023-07-04 02:00:49
6	8001	Tamper	1	2023-06-29 16:29:49
7	8001	Tamper	1	2023-06-29 16:26:59
8	8001	Tamper	1	2023-06-29 15:22:09
9	8001	Tamper	1	2023-06-29 15:22:08
10	8001	Tamper	1	2023-06-27 14:07:57

12 records

10.3 Unlock Records

Select **Log** > **Unlock Records**.

Figure 10-3 Unlock



Please keep unencrypted files well to avoid data leakage.

Export

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

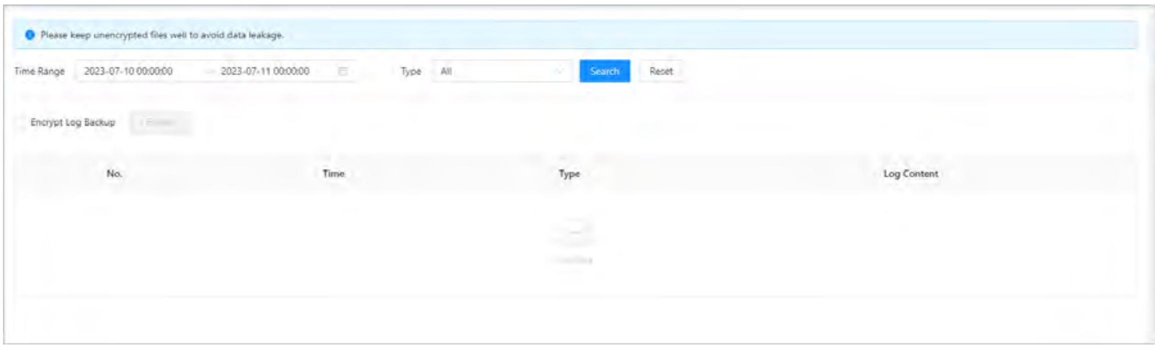
2 records

10.4 Log

Select **Log** > **Log**.

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

Figure 10-4 Log



Please keep unencrypted files well to avoid data leakage.

Time Range 2023-07-10 00:00:00 – 2023-07-11 00:00:00

Type All

□ Encrypt Log Backup

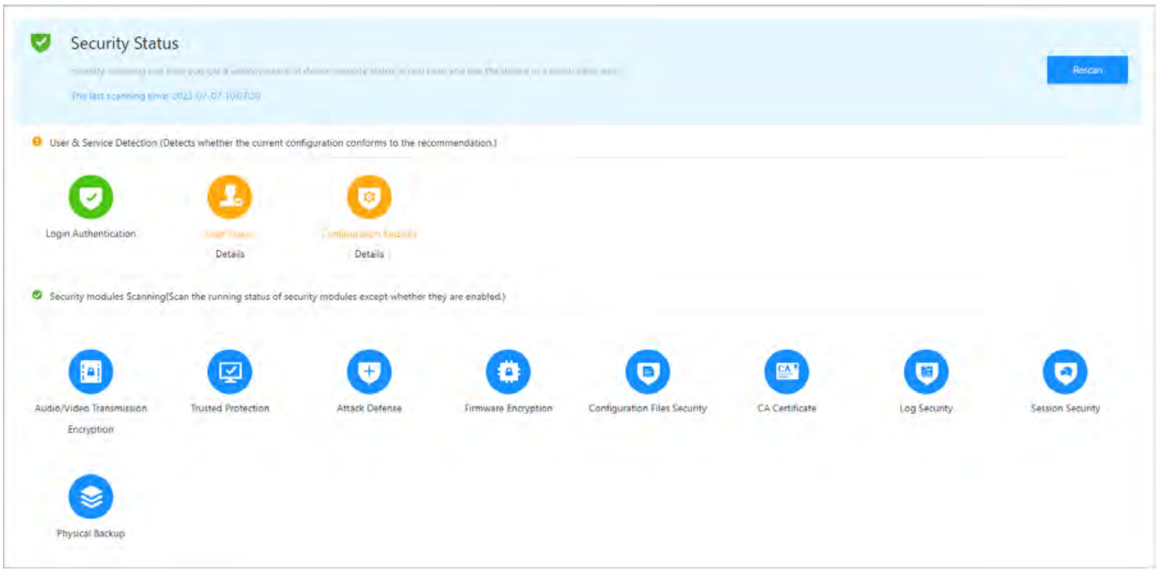
No.	Time	Type	Log Content

11 Security Management

11.1 Security Status

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

Figure 11-1 Security status



Security Status

[illegible]

The last scanning time: 2023-07-07 10:07:20

User & Service Detection (Detects whether the current configuration conforms to the recommendation.)

Security modules Scanning(Scan the running status of security modules except whether they are enabled.)

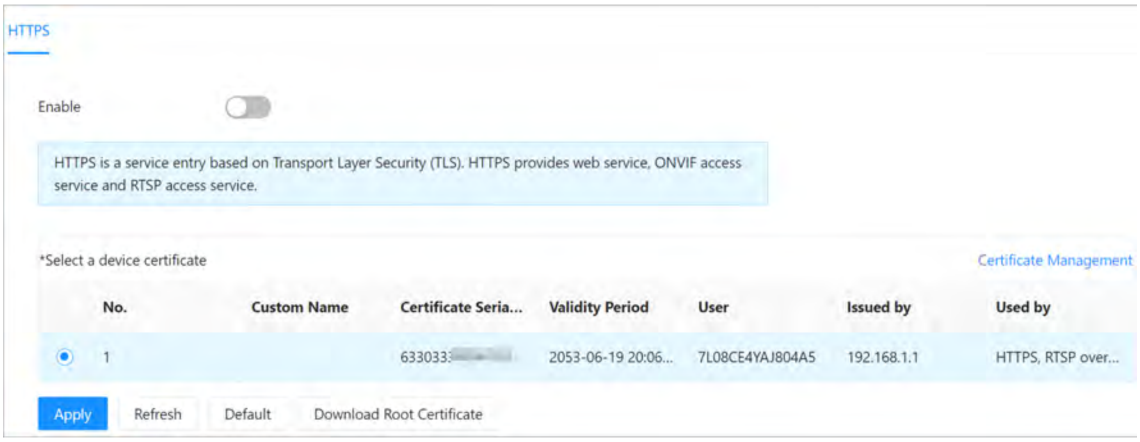
11.2 System Service

Procedure

Step 1 On the home page, click 🛡, and then select **System Service**.

Step 2 Select a device certificate, and then enable the HTTPS function.

Figure 11-2 System service



Enable ○

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

*Select a device certificate

	No.	Custom Name	Certificate Seria...	Validity Period	User	Issued by	Used by
●	1		633033[redacted]	2053-06-19 20:06...	7L08CE4YAJ804A5	192.168.1.1	HTTPS, RTSP over...

Step 3 Click **Apply**.

11.3 Attack Defense

11.3.1 Firewall

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

Procedure

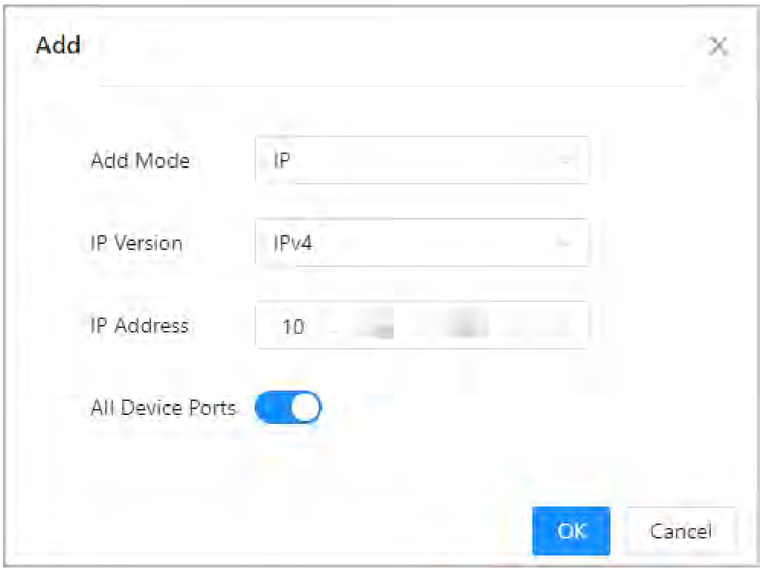
Step 1 On the home page, click 🛡, and then select **Attack Defense** > **Firewall**.

Step 2 Select the **Mode** as either **Allowlist** or **Blocklist**.

- Allowlist: Devices that have been granted an access.
- Blocklist: Devices that have been forbidden an access.

Step 3 Click **Add** to add the IP address for allowlist or blocklist.

Figure 11-3 Add



Add

Add Mode: IP

IP Version: IPv4

IP Address: 10

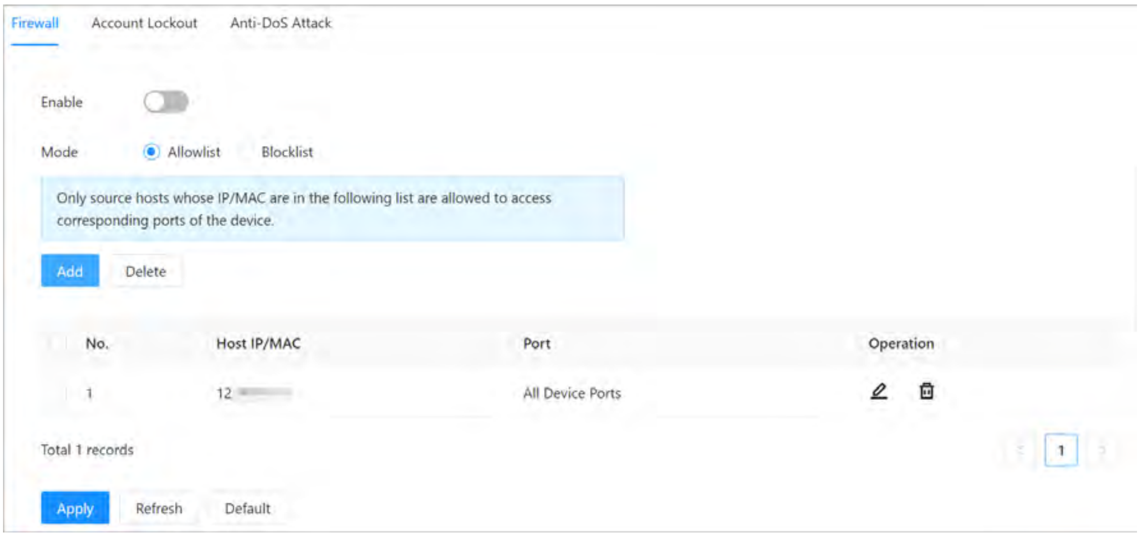
All Device Ports: ●

Step 4 Click **OK**.

Step 5 Click ○ next to **Enable**.

Step 6 Select an added IP address for allowlist or blocklist, and then click **Apply**.

Figure 11-4 Apply



Enable

Mode ● Allowlist ○ Blocklist

Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.

No.	Host IP/MAC	Port	Operation
1	12[redacted]	All Device Ports	

Total 1 records

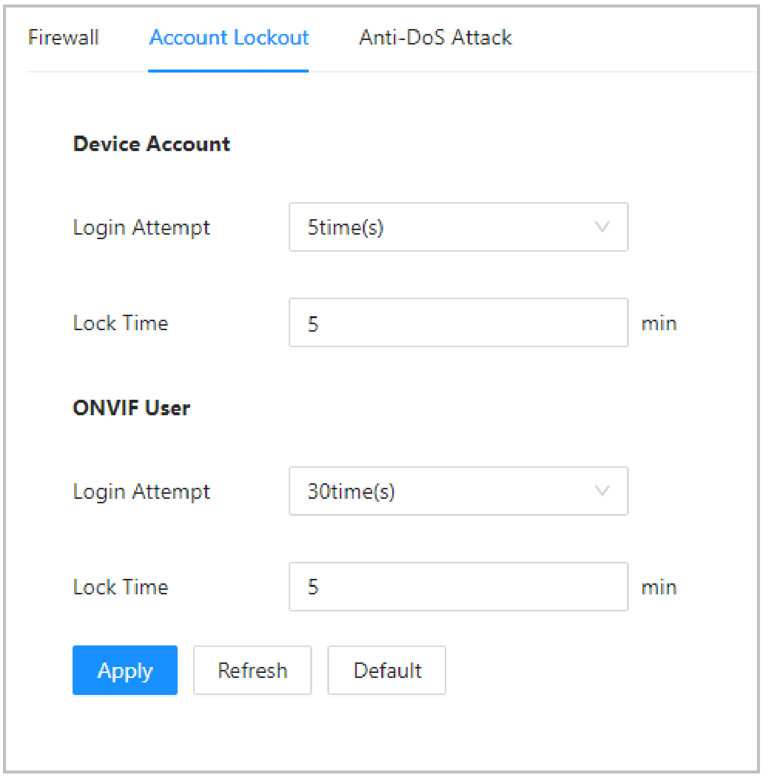
11.3.2 Account Lockout

Procedure

Step 1 On the home page, click 🛡, and then select **Attack Defense** > **Account Lockout**.

Step 2 Configure the login attempts and lock time.

Figure 11-5 Account lockout



Device Account

Login Attempt: 5time(s)

Lock Time: 5 min

ONVIF User

Login Attempt: 30time(s)

Lock Time: 5 min

Step 3 Click **Apply**.

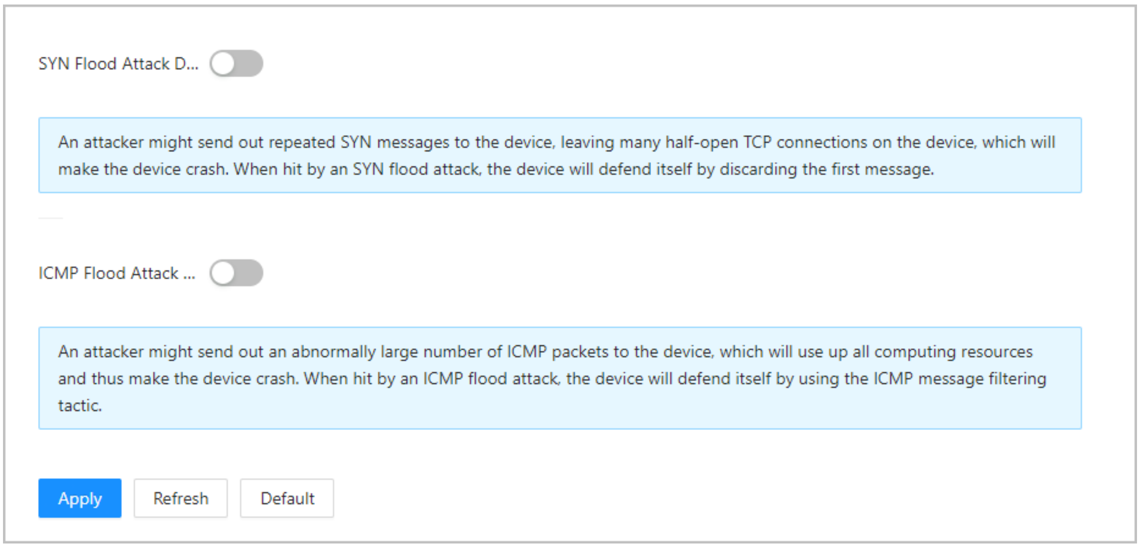
11.3.3 Anti-DoS Attack

Procedure

Step 1 On the home page, click 🛡, and then select **Attack Defense** > **Anti-DoS Attack**.

Step 2 Enable or disable the **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** function.

Figure 11-6 Anti-DoS attack



SYN Flood Attack D...

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack ...

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

Step 3 Click **Apply**.

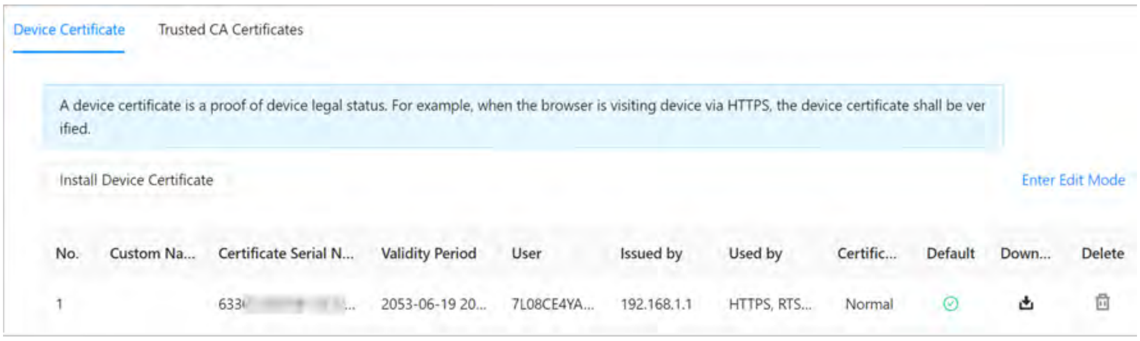
11.4 CA Certificate

Procedure

Step 1 On the home page, click 🛡, and then select **CA Certificate**.

- Device Certificate

Figure 11-7 Device Certificate

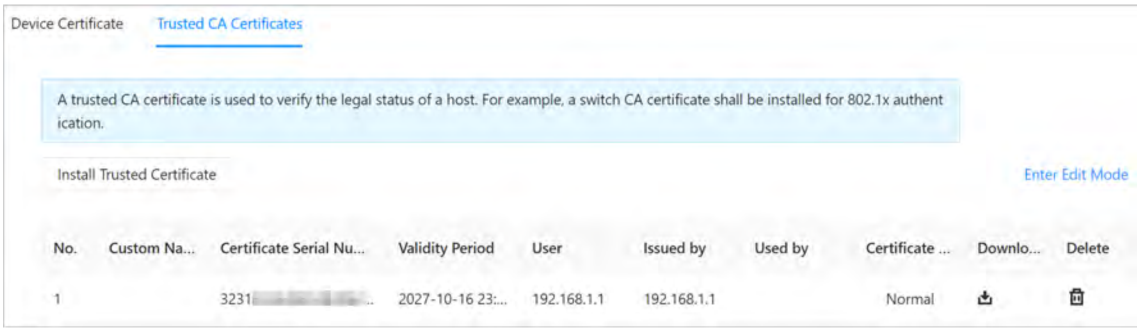


A device certificate is a proof of device legal status. For example, when the browser is visiting device via HTTPS, the device certificate shall be ver ified.

No.	Custom Na...	Certificate Serial N...	Validity Period	User	Issued by	Used by	Certific...	Default	Down...	Delete
1		633[redacted]...	2053-06-19 20...	7L08CE4YA...	192.168.1.1	HTTPS, RTS...	Normal	✓	⤓	🗑

- Trusted CA Certificates

Figure 11-8 Trusted CA Certificates



Device Certificate | Trusted CA Certificates

A trusted CA certificate is used to verify the legal status of a host. For example, a switch CA certificate shall be installed for 802.1x authentication.

Install Trusted Certificate

Enter Edit Mode

No.	Custom Na...	Certificate Serial Nu...	Validity Period	User	Issued by	Used by	Certificate ...	Downlo...	Delete
1		3231[redacted]...	2027-10-16 23:...	192.168.1.1	192.168.1.1		Normal		

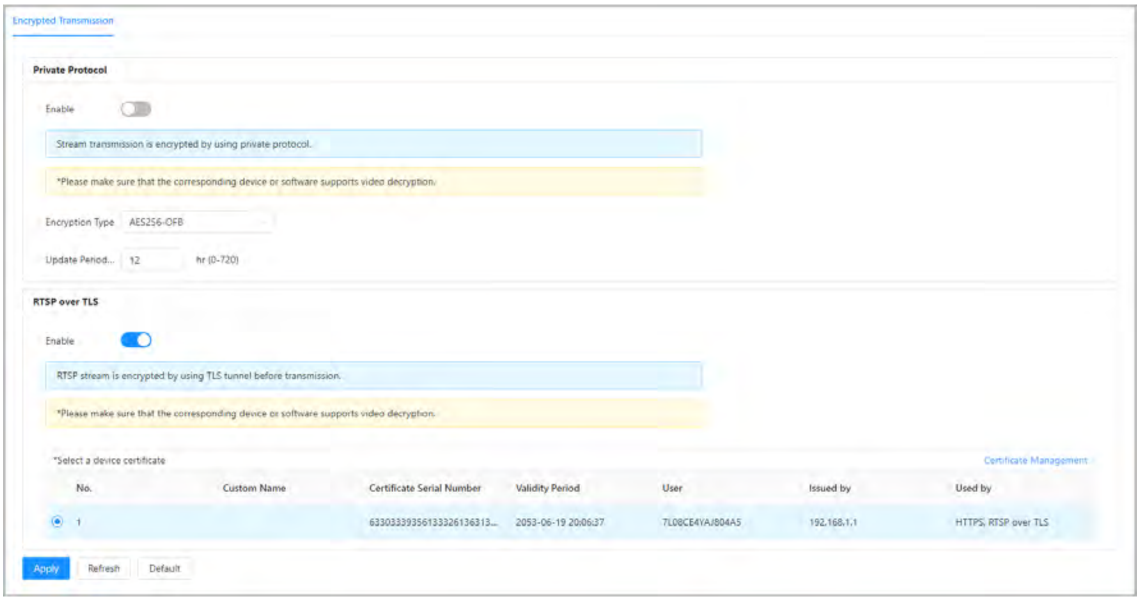
11.5 Video Encryption

Procedure

Step 1 On the home page, click , and then select **Video Encryption**.

Step 2 Configure **Private Protocol** and **RTSP over TLS** parameters.

Figure 11-9 Video encryption



Encrypted Transmission

Private Protocol

Enable ○

Stream transmission is encrypted by using private protocol.

*Please make sure that the corresponding device or software supports video decryption.

Encryption Type: AES256-OFB

Update Period...: 12 hr (0-720)

RTSP over TLS

Enable ●

RTSP stream is encrypted by using TLS tunnel before transmission.

*Please make sure that the corresponding device or software supports 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	192.168.1.1	HTTPS, RTSP over TLS

Step 3 Click **Apply**.

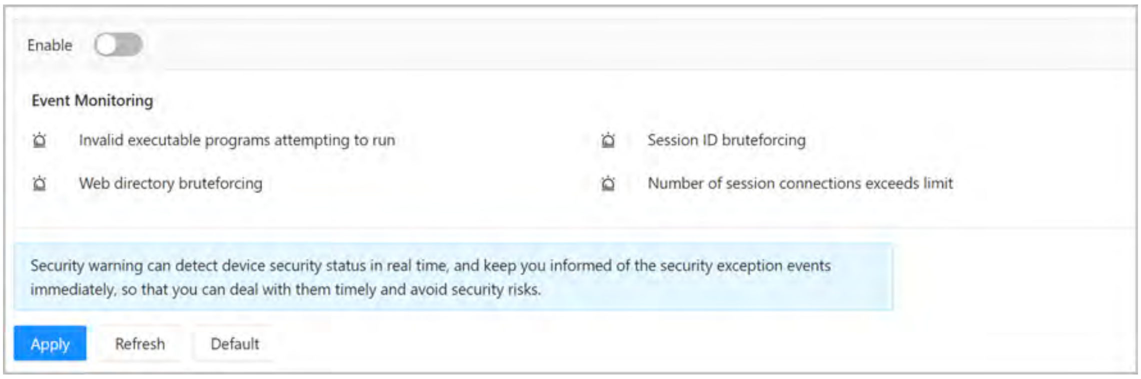
11.6 Security Warning

Procedure

Step 1 On the home page, click , and then select **Security Warning**.

Step 2 Enable event monitoring function, and then click **Apply**.

Figure 11-10 Security warning



Enable
Event Monitoring
Invalid executable programs attempting to run
Session ID bruteforcing
Web directory bruteforcing
Number of session connections exceeds limit
Apply
Refresh
Default

Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

12 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.

12.1 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 12-1 Button model

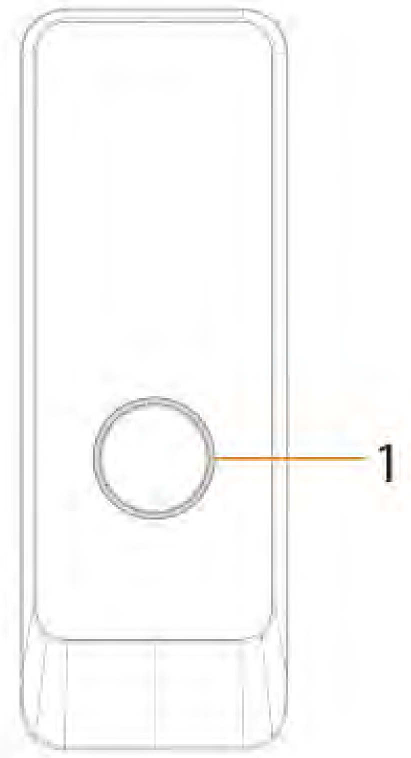
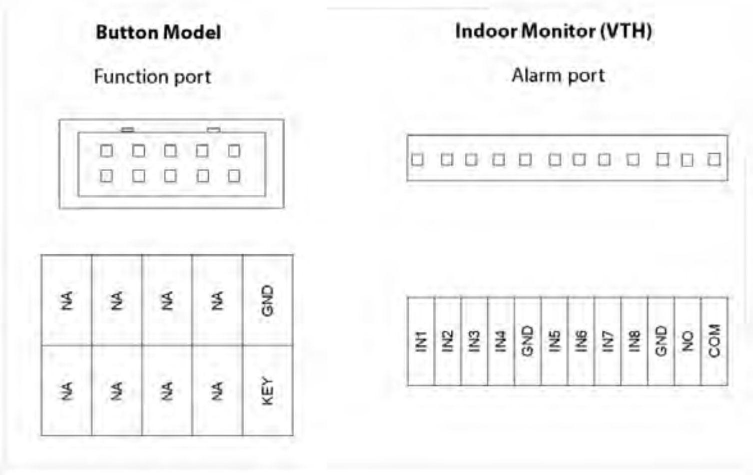


Table 12-1 Component

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.

Figure 12-2 Cable connection



12.2 VTH Configuration

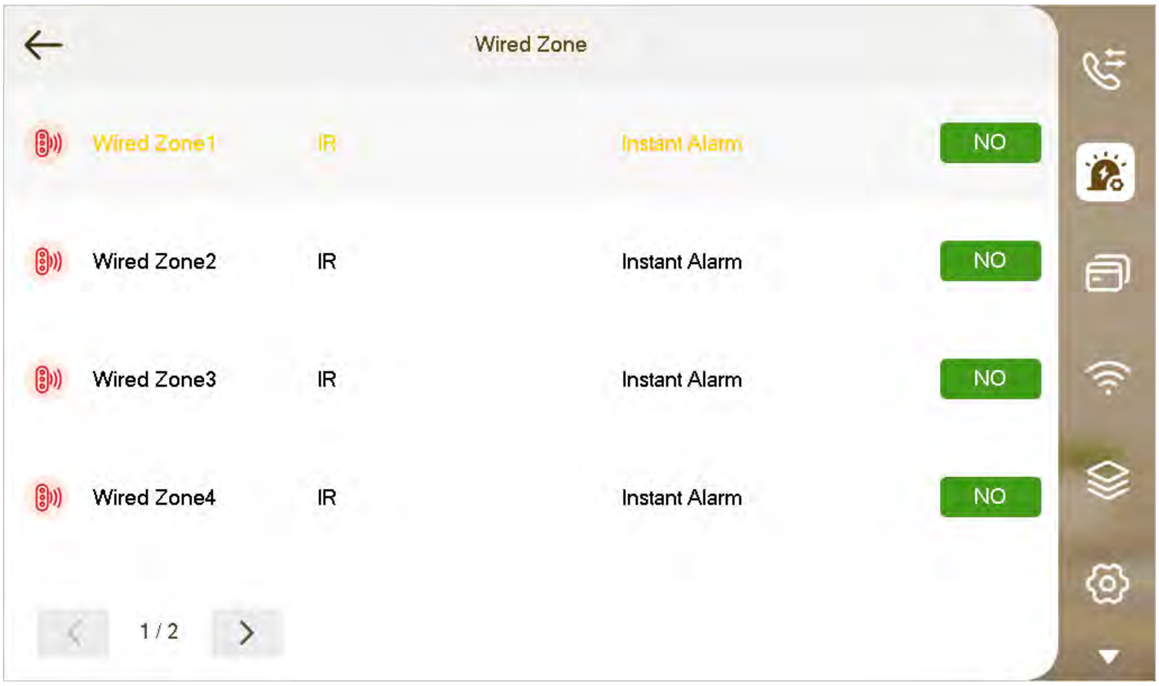
After completing cable connection, you need to set the **wired zone type** as **Doorbell** on the VTH to receive alarm signals once you press the button model.

Procedure

Step 1 Power on the VTH.

Step 2 Select **Setting** > **Alarm** > **Wired Zone** on the VTH.

Figure 12-3 Wired zone setting



Wired Zone

Wired Zone1	IR	Instant Alarm	NO
Wired Zone2	IR	Instant Alarm	NO
Wired Zone3	IR	Instant Alarm	NO
Wired Zone4	IR	Instant Alarm	NO

1 / 2

Step 3 Set the **Type** as **Doorbell**, and configure the rest of the parameters.

Table 12-2 Parameter description

Parameter	Description	
Area	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.	
Type	Select corresponding type according to detector type.	
Status	● **Instant Alarm** : After armed, if an alarm is triggered, the device produces siren at once and enters alarm status. ● **Delay Alarm** : After armed, if an alarm is triggered, the device enters alarm status after a specified time, during which you can disarm and cancel the alarm. ● **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. A zone in **Remove** status cannot be bypassed.	
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.	Delay is only valid to the areas of **Delay Alarm**.
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.	

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.
2. **Update Firmware and Client Software in Time**
   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.
2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.
4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.
5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.
6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.
7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.
8. **Assign Accounts and Privileges Reasonably**

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

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.