Villa Door Station

User Manual



V1.0.1

Foreword

General

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

Symbols

The following symbols might appear in the manual.

Symbol	Description
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
V1.0.1	Updated the cable connection.	October 2026
V1.0.0	First release.	September 2026

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Important Safeguard 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.

Installation Requirements

WARNING

- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- The power supply must meet the rated voltage requirements as indicated on the device label.
- If the device uses a power adapter, ensure it meets the following requirements:
  - If a power adapter was shipped with your device, we recommend you use it. If you need to buy a separate adapter, make sure it meets the following requirements.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - Do not connect the power adapter to the device while the adapter is powered on.

- 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 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.
- The device must be installed at a height of 2 meters or below.

Operation Requirements

DANGER

Battery Pack Precautions

Preventive measures (including but not limited to):

- Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
- Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
- Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.



- 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.

Table of Contents

Foreword.....I
Important Safeguard and Warnings.....III
1 Appearance and Interface.....1
2 Initializing the VTO.....5
2.1 Webpage.....5
2.2 DMSS App.....5
3 Logging In and Resetting the Password.....7
3.1 Logging In.....7
3.2 Resetting the Password.....7
4 Home Page.....9
5 Setup Wizard.....10
5.1 Setting as the SIP Server.....10
5.2 Not Setting as the SIP Server.....11
6 Local Device Configuration.....12
6.1 Basic Settings.....12
6.2 Access Control.....14
6.2.1 Configuration.....14
6.2.2 Extension Function.....17
6.3 Light Control.....21
6.4 Card Settings.....21
6.5 Intelligent.....23
6.5.1 Video Intelligence.....23
6.5.2 Audio Intelligence.....28
6.5.3 Linkage Configuration.....29
6.6 Port Configuration.....30
7 Device Setting.....32
7.1 VTO Management.....32
7.2 VTH Management.....33
7.3 VTS Management.....35
8 Person Management.....36
9 Network Settings.....38
9.1 TCP/IP.....38
9.2 Port.....39
9.3 SIP Server.....40
9.4 Cloud Service.....44
9.5 UPnP.....45
9.6 Basic Services.....45

9.7 Auto Registration....48
10 System....49
10.1 Alarm....49
10.1.1 Alarm Linkage Setting....49
10.1.2 Configuring Alarm....49
10.2 Video....51
10.3 Audio....56
10.4 Time....58
10.5 ONVIF User....60
11 Maintenance Center....62
11.1 One-Click Diagnosis....62
11.2 System Information....62
11.2.1 Version Information....63
11.2.2 Legal Information....63
11.3 Data Capacity....63
11.4 Log Management....63
11.4.1 Call History....64
11.4.2 Alarm Logs....64
11.4.3 Unlock Records....64
11.4.4 Log....65
11.4.5 Intelligent Records....65
11.5 Maintenance Management....66
11.5.1 Config....66
11.5.2 Maintenance....67
11.6 Update....67
11.7 Advanced Maintenance....68
12 Security Management....70
12.1 Security Status....70
12.2 System Service....70
12.3 Attack Defense....71
12.3.1 Firewall....71
12.3.2 Account Lockout....72
12.3.3 Anti-DoS Attack....73
12.4 CA Certificate....73
12.5 Video Encryption....74
12.6 Security Warning....74
12.7 Security Authentication....75
Appendix 1 Security Recommendation....76

1 Appearance and Interface

Figure 1-1 Appearance and interface (with one camera) (unit: mm [inch])

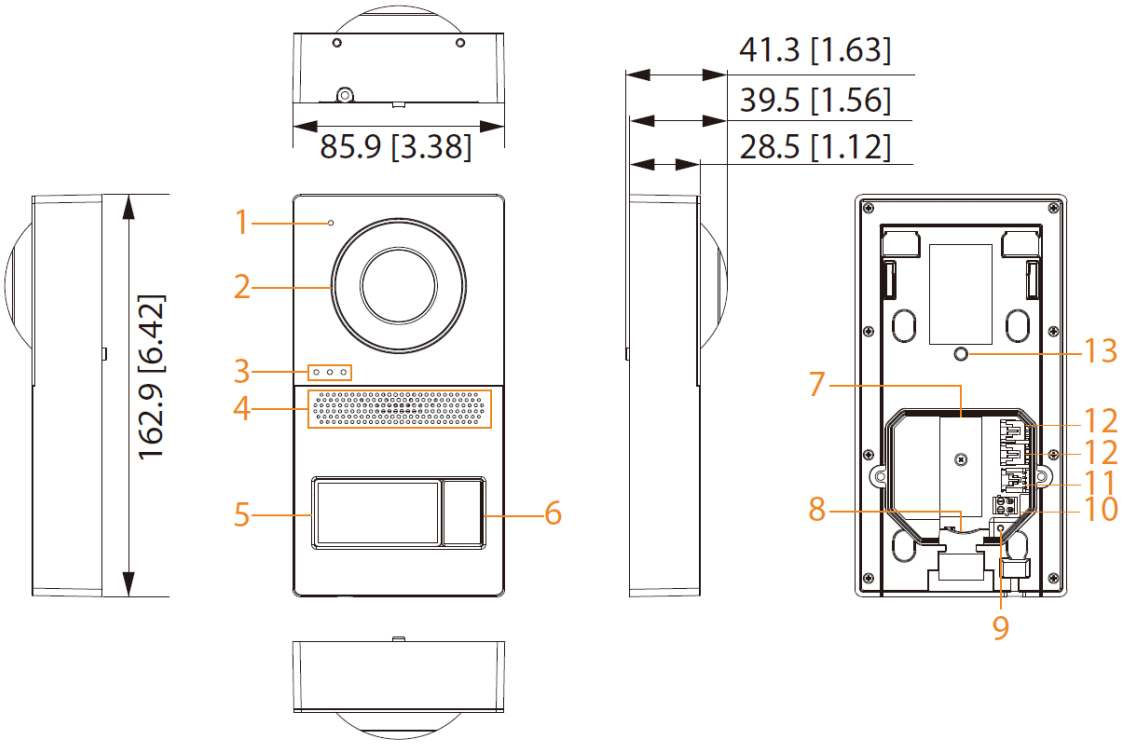


Figure 1-2 Appearance and interface (with two cameras) (unit: mm [inch])

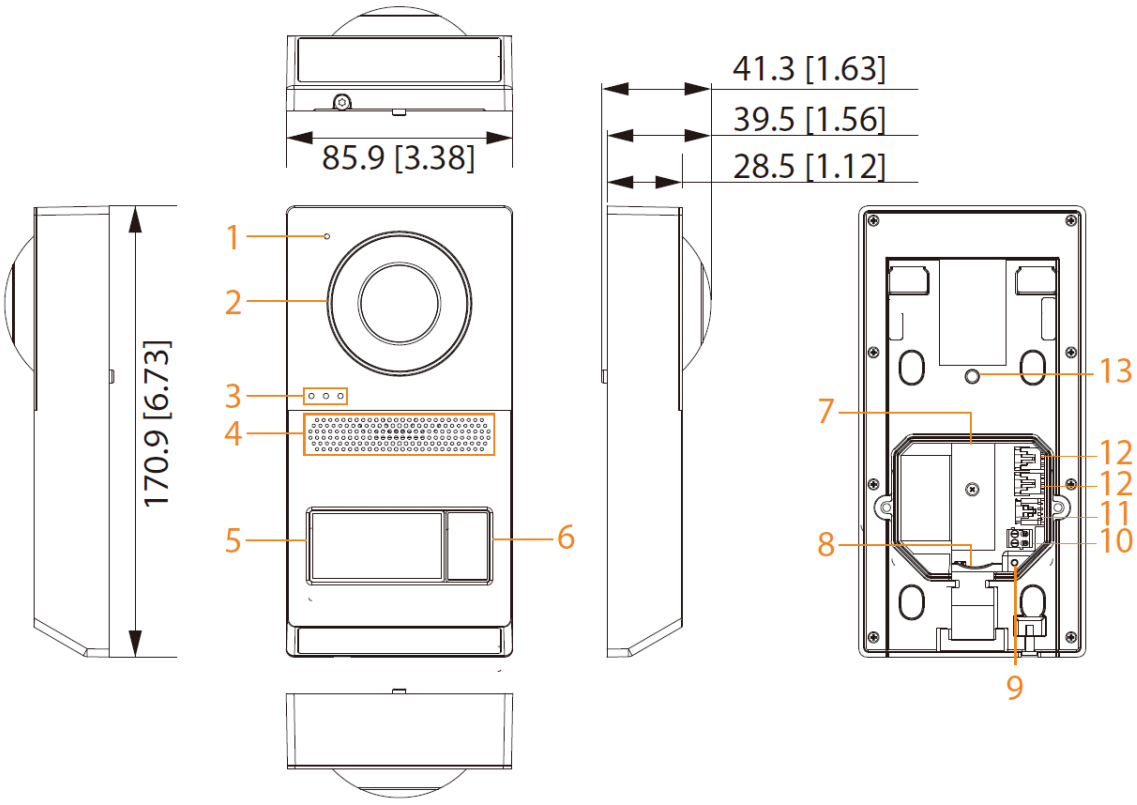


Table 1-1 Appearance and interface description

No.	Item	Description
1	MIC	Audio input.
2	Camera	Captures images or records videos for the VTO.
3	Indicators	From left to right: • Ring: VTO is calling the VTH. • Talking: The VTO is in a two-way talk with the VTH. • Unlocking: The VTO unlocks successfully.
4	Speaker	Audio output.
5	Nameplate	Displays custom information and supports backlight. Supports and swiping cards on the area of No.5 and No.6.
6	Call button	Press it to call the VTH. • Supports swiping cards on the area of No.5 and No. 6. • Within 5 minutes after the VTO is powered on and started up, press the call button for 5 seconds, and the VTO will broadcast its IP address.
7	Network port	Connects to the network.
8	SD card slot	Used to insert an SD card so that data such as images and videos can be stored.
9	Reset button	Press and hold the button for 8 seconds to reset to factory settings.
10	Power input port	Connects to the power supply (12V).
11	RS-485 port / Power output	—
12	Multi-function port	For the upper unit: Door magnetic detector 2 (alarm input 2), door unlocking button 2 (alarm input 4), lock 2 (alarm output 2). For the lower unit: Door magnetic detector 1 (alarm input 1), door unlocking button 1 (alarm input 3), lock 1 (alarm output 1).

No.	Item	Description
13	Tamper button	• After the device is removed from the wall or other mounting locations, the device beeps and generates an alarm record. • Within 10 minutes after the device is powered on, if you press the tamper button 5 times within 8 seconds, the device beeps and deletes the account information, and an alarm record is generated.

Figure 1-3 Cable connection (1)

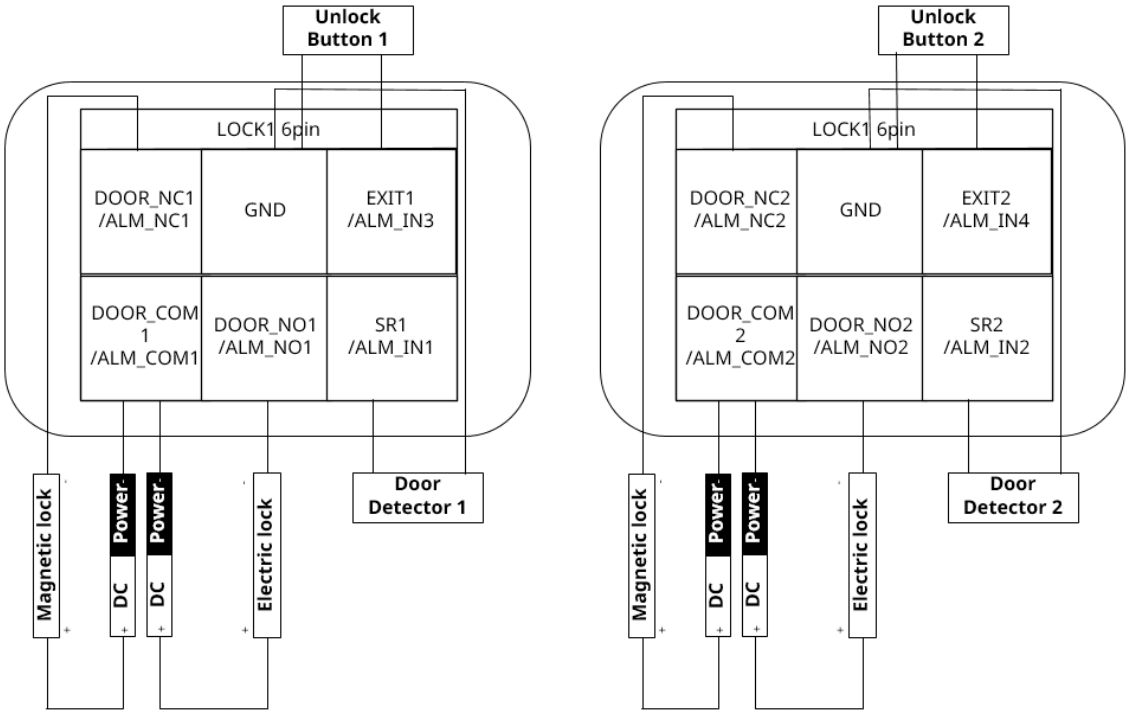
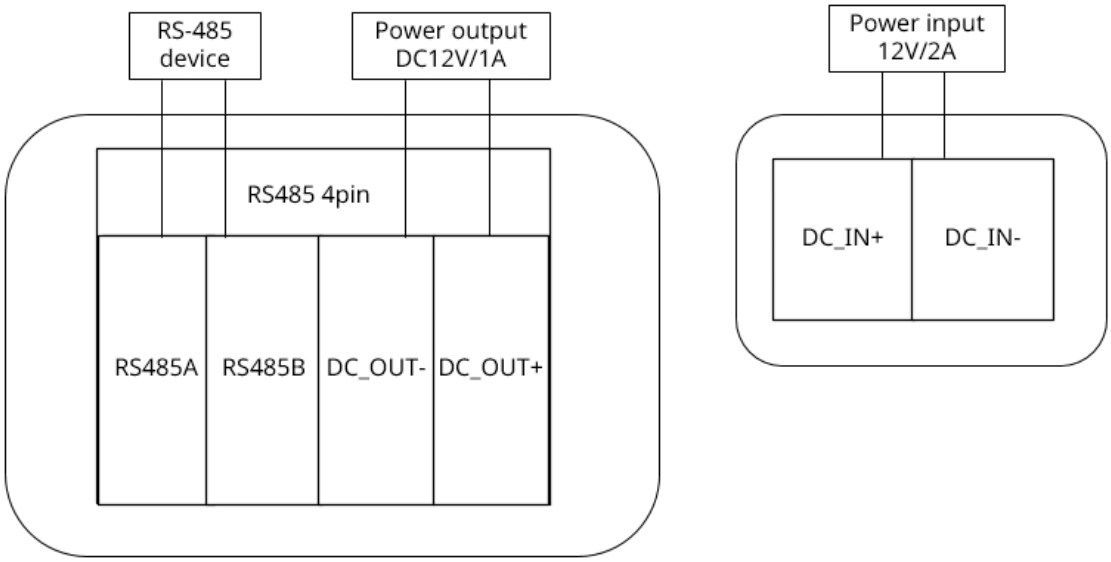


Figure 1-4 Cable connection (2)



2 Initializing the VTO

2.1 Webpage

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

Procedure

Step 1 Power on the VTO.

Step 2 Open a web browser, and then 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 the password.

Step 5 Click **Next**.

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

Step 7 Enter the user name (it is admin by default) and the password to log in to the web manager of the VTO.

2.2 DMSS App

Initialize the device through the DMSS App. For details, see its user manual.

Before the initialization, make sure the followings have been done.

- The device is powered on.
- Your phone and the device are on the same LAN.

Add the Device by SN/QR Code

You can add devices by scanning the QR code or manually entering the SN.

1. On the **Home** screen, tap , and then select **Scan the QR Code**.
2. Add the device.
   - Scan the device QR code directly, or tap , import the QR code picture to add a device.

- Tap , and then enter the device SN to manually add a device.

3. Make sure the device and the phone meet the requirements, and then click **Next**.
4. Set the device password, and then click **Next**.
5. Configure the cloud access service and the auto-check update service, and then click **OK**.
6. Configure the device information, and then click **OK**.

Add the Device Automatically

1. On the **Home** screen, tap **Add Device** or select  > **Add Device**.
2. The phone will detect the device nearby. Wait for the detecting result, and then select the device you want to add.
3. Set the device password, and then click **Next**.
4. Configure the cloud access service and the auto-check update service, and then click **OK**.
5. Configure the device information.

3 Logging In and Resetting the Password

3.1 Logging In

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

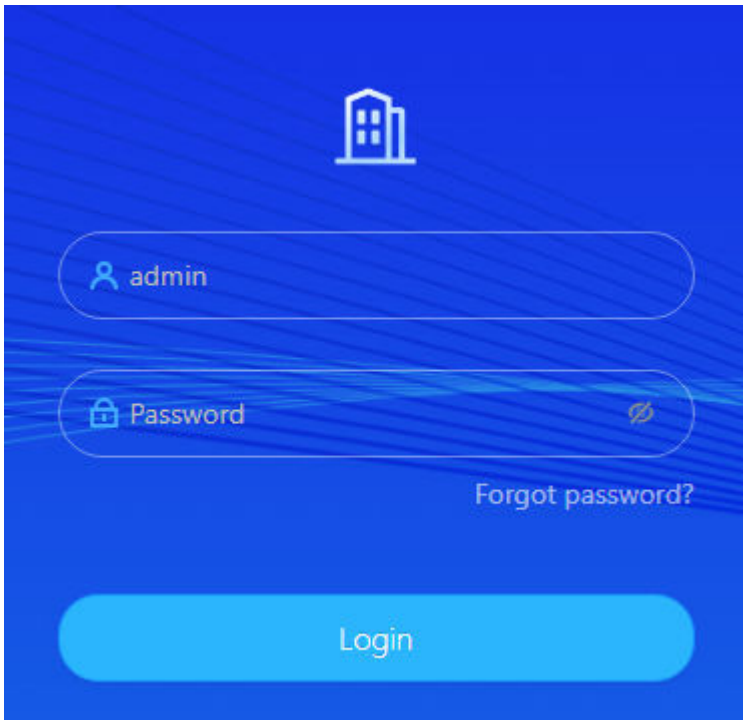
Procedure

Step 1 Enter 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 to avoid IP address conflicts.

Step 2 Enter the user name **admin** and the password you set during initialization, and then click **Login**.

Figure 3-1 Login



3.2 Resetting the Password

Procedure

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

Step 2 Scan the QR code to obtain a string of numbers and letters.

Step 3 Send the string to the email account displayed on the page. The security code is then 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 the local dealer or technical support for help.
- The security code is valid for only 24 hours after 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**.

4 Home Page

Figure 4-1 Home page

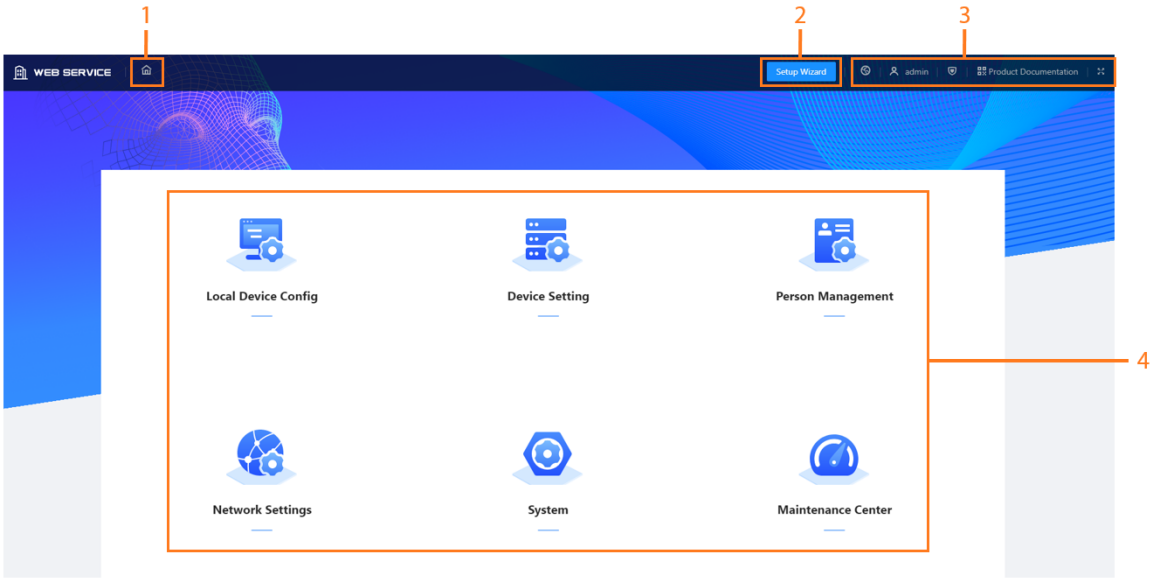


Table 4-1 Home page introduction

No.	Function	Description
1	Home button	Go back to the home page.
2	Setup Wizard	Configure the VTO SIP server.
3	Navigation bar	• : Change the language of the VTO webpage. • 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. • Product Documentation: Scan the QR code to access the product information. • : View the webpage in full-screen mode.
4	VTO functions	Access different VTO function areas.

5 Setup Wizard

- Through the setup wizard, you can finish the process of adding VTO/VTH or a specific VTO as the SIP server. You can also cancel its operation as a SIP server.
- If the device has been added to the DoLynk Pro, the setup wizard will not be available.

5.1 Setting as the SIP Server

Set the VTO as the SIP server.

Prerequisites

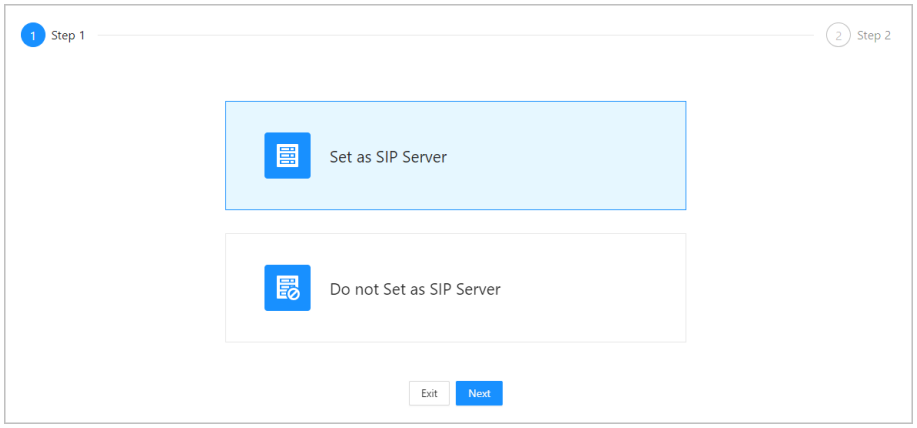
You have added VTOs on the webpage. If not, you can add them on **Set as SIP Server** page or in the **Device Setting** section.

Procedure

Step 1 Log in to the webpage of the VTO.

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

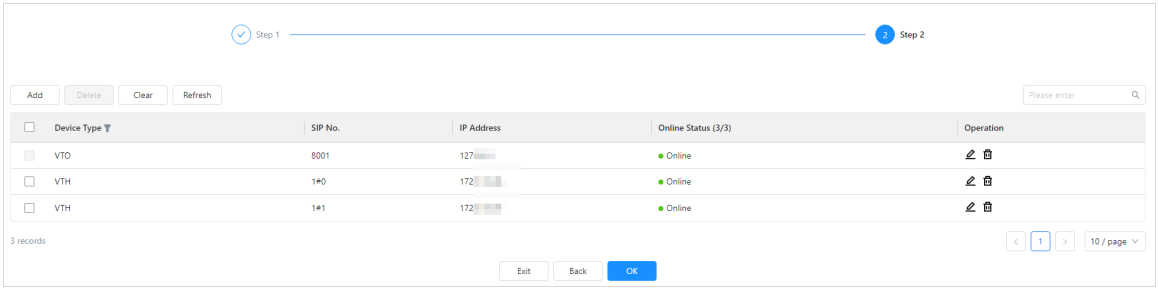
Figure 5-1 Set as SIP server



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 there is no VTO as the SIP server.

Figure 5-2 Select the SIP server



5.2 Not Setting as the SIP Server

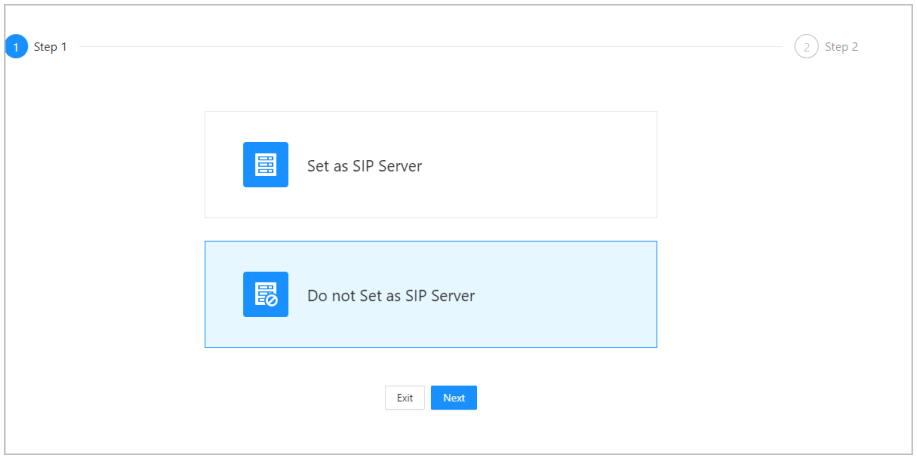
If you want to change the SIP server, you need to remove the current one from the list.

Procedure

Step 1 Log in to the webpage of the VTO.

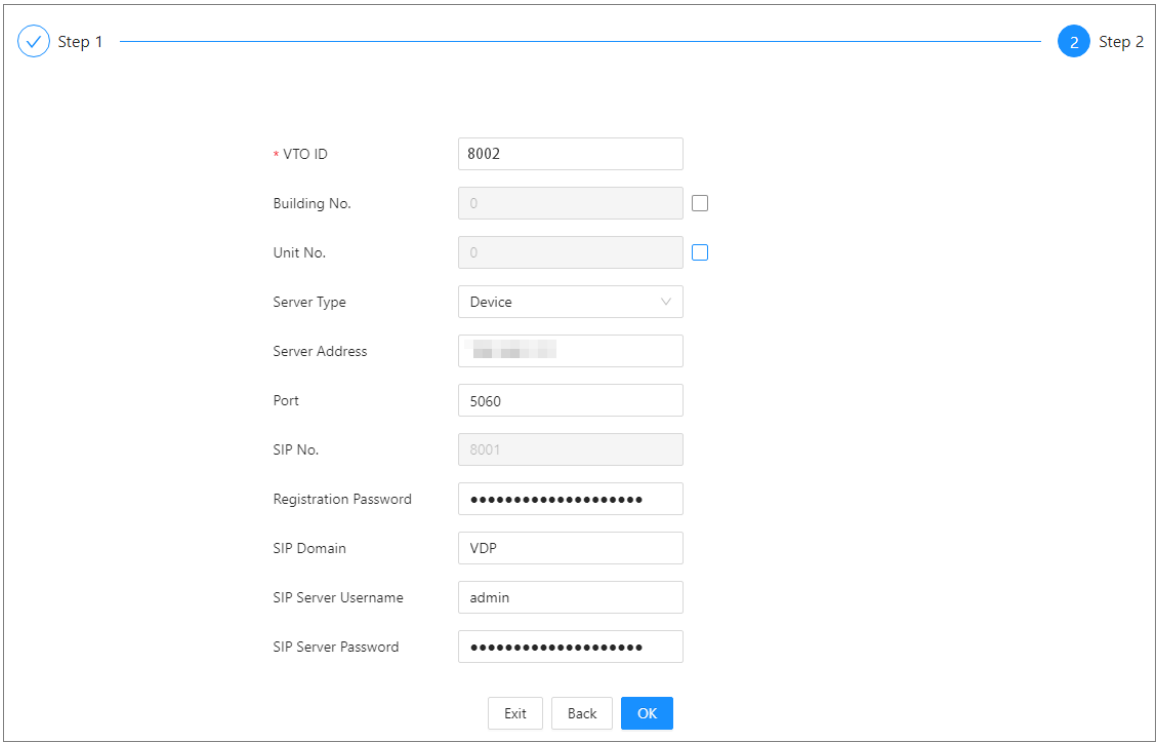
Step 2 Select **Setup Wizard** > **Do not Set as SIP Server**, and then click **Next**.

Figure 5-3 Do not set as SIP server



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

Figure 5-4 Configure information



6 Local Device Configuration

6.1 Basic Settings

Configure basic settings of the device.

Procedure

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

Step 2 Configure the parameters.

Figure 6-1 Basic settings

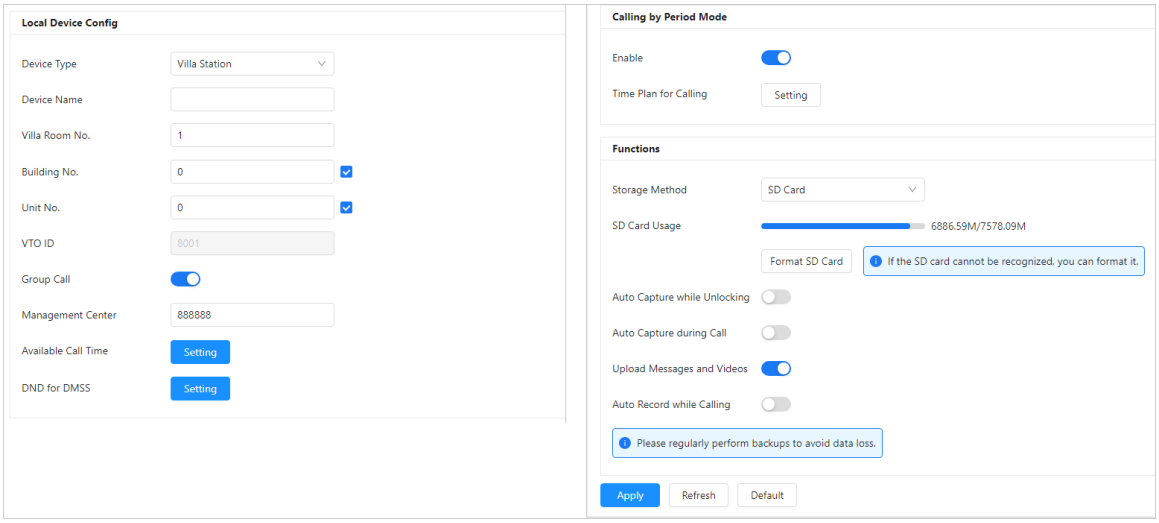


Table 6-1 Basic parameter description

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.
Building No.	Configuring the building and unit number where the device is. If you clear the **Building No.** and **Unit No.** check box, it means that there is just only 1 building and unit.
Unit No.	

Parameter	Description
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.
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.
Management Center	888888 by default.
Available Call Time	The time period in which the VTO's calling to other devices is limited. Click **Setting** to set the time plan for calling.
DND for DMSS	The time period in which the calling to DMSS is limited. Click **Setting** to set the time plan for calling.
Calling by Period Mode	• If you enable the **Calling by Period Mode**, the specified number can be called in the specified period and the default number in other period. • Click **Setting** to set the time plan for calling. Only available when the mode is villa door station and second confirmation station.
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 while Unlocking	Take a snapshot and save it in the SD card of the VTO when the VTO is unlocking. If the VTO is unlock through local unlock button, the snapshot will not be taken.
Auto Capture during Call	Take a snapshot and save it in the SD card of the VTO when the VTO is calling.

Parameter	Description
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. • When the call time is less than 5 seconds, no video file will be generated. • If there is a conflict between **Auto Record while Calling** and **Leave Videos**, **Leave Videos** prevails.

Step 3 Click **Apply**.

6.2 Access Control

6.2.1 Configuration

Procedure

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

Step 2 Select **Local Lock 1** or **Local Lock 2** to configure the parameters of the local lock.

The parameters of the **Local Lock 1** and **Local Lock 2** are the same. Use **Local Lock 1** as an example.

Figure 6-2 Access control

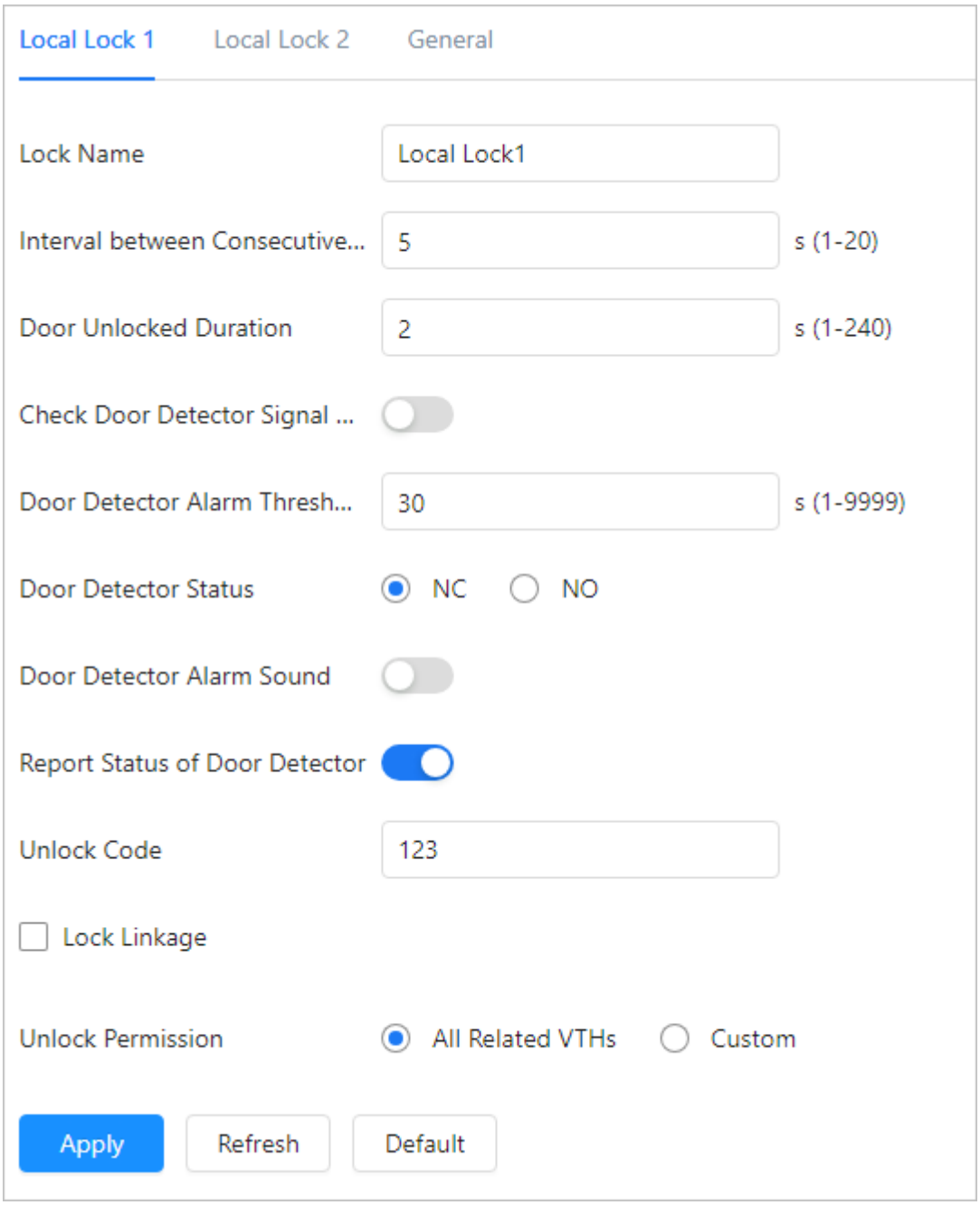


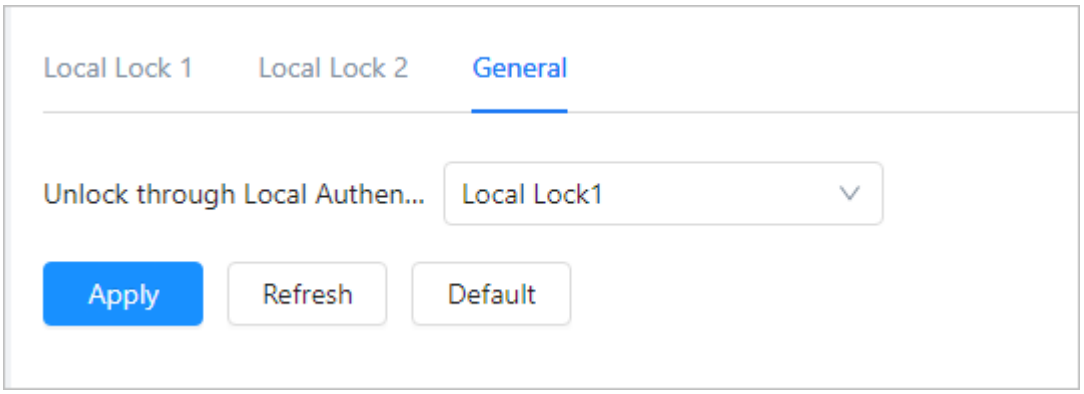
Table 6-2 Access control parameter description

Parameter	Description
Local Name	Enter the name of the local lock.
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.

Parameter	Description
Check Door Detector Signal Before Locking	Enable the function based on your needs. When it is enabled, the door detector signal will be checked before locking. For example, when there is door detector signal, it will not be locked.
Door Detector Alarm Threshold	The threshold time when the door detector alarm is triggered.
Door Detector Status	• **NC** : Normally closed. • **NO** : Normally open.
Door Detector Alarm Sound	It is disabled by default. When it is enabled: • **Door Detector Status** is **NO**: If the door opening time exceeds the set door detector alarm threshold, the VTO will beep. And when the door detector is closed, the VTO does not beep again. • **Door Detector Status** is **NC**: If the door closing time exceeds the set door detection alarm threshold, the VTO will beep. And when the door detector is open, the VTO does not beep again.
Report Status of Door Detector	After it is enabled, the status of the door detector will be reported.
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 Linkage	After enabling it, select the lock from the drop-down list to link with this lock.
Unlock Permission	Supports sending the unlock permission to the related VTHs. • **All Related VTHs** : Send the unlock permission to all related VTHs. • **Custom** : Select the VTHs to which you want to send the unlock permission.

Step 3 Select the **General** tab to configure the general parameters.

Figure 6-3 General settings



Unlock through Local Authentication: Select the local lock for authentication.

Step 4 Click **Apply**.

6.2.2 Extension Function

Procedure

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

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

Figure 6-4 RS-485 (connecting to the lock)

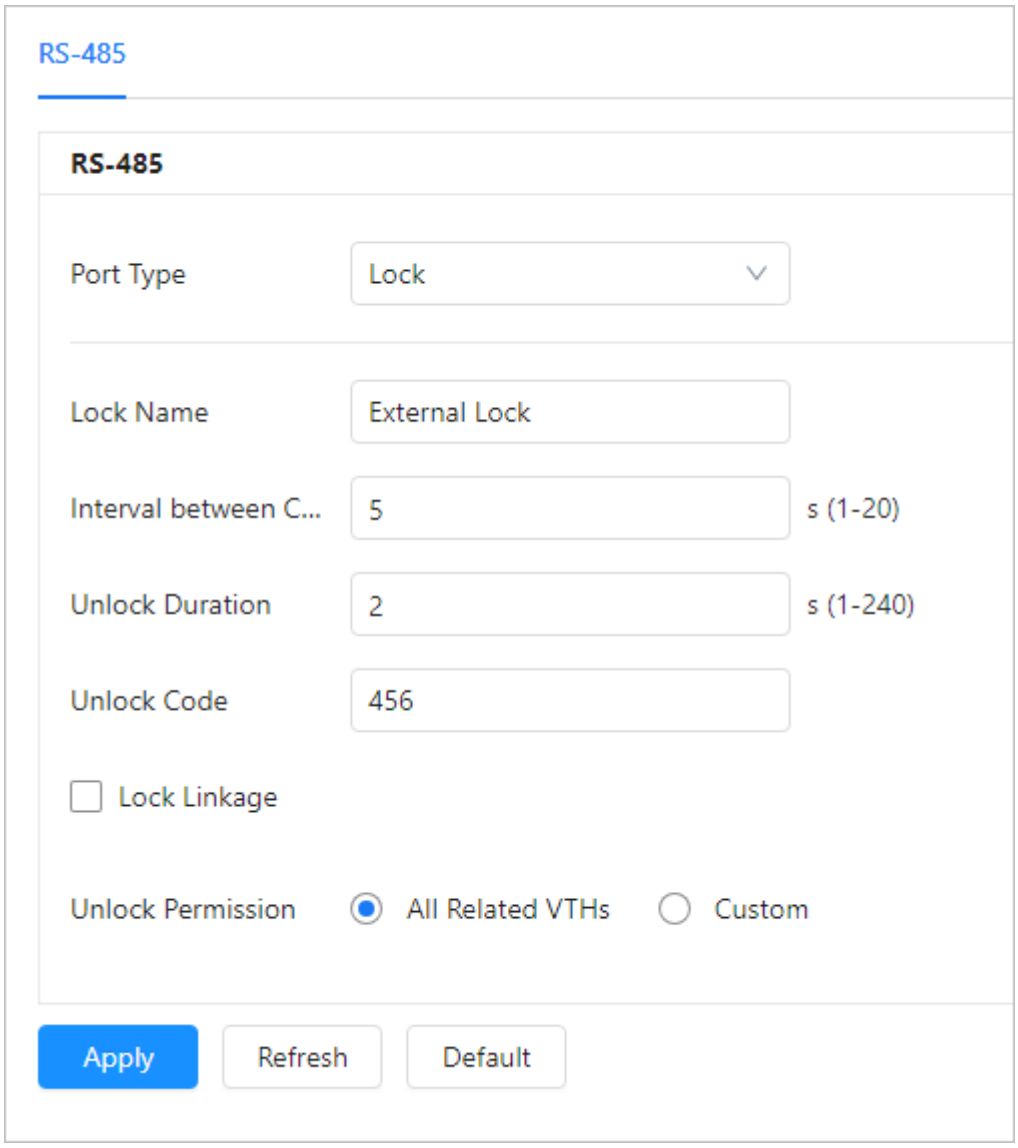


Figure 6-5 RS-485 (connecting to the card reader)

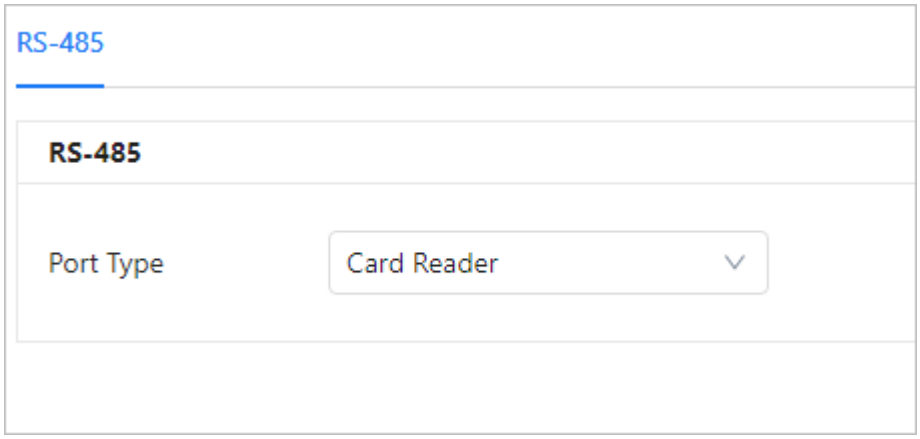


Figure 6-6 RS-485 (connecting to the expansion module-external lock)

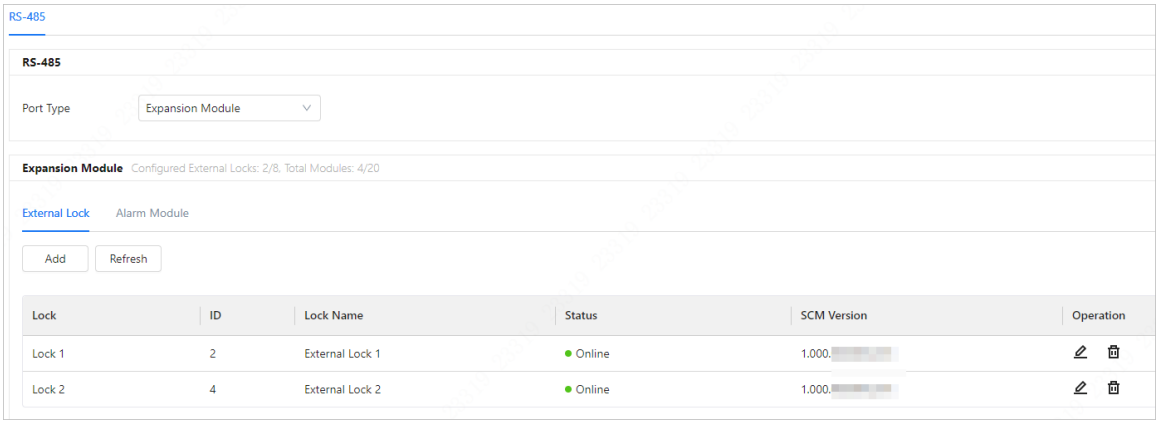


Figure 6-7 RS-485 (connecting to the expansion module-alarm module)

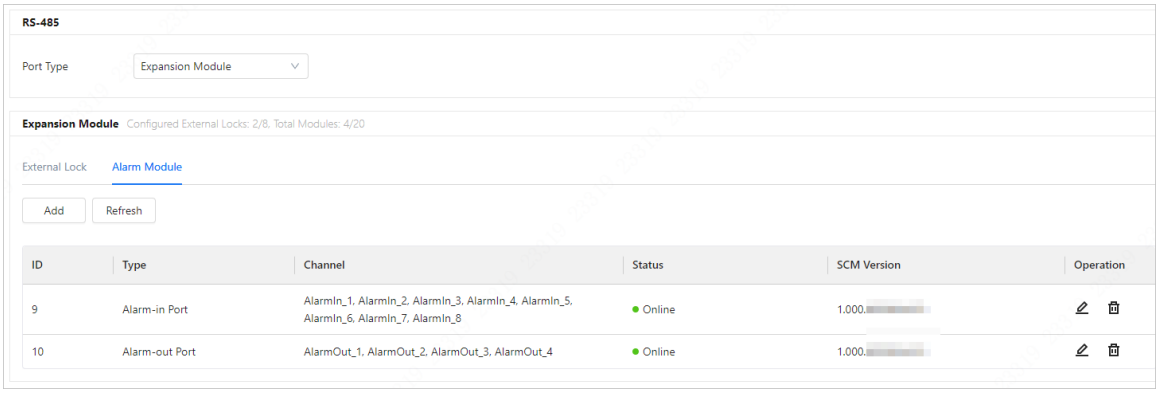


Table 6-3 RS-485 description

Parameter	Description
Port Type	Select **Lock** , **Card Reader**, or **Expansion Module** as the port type. It is **Lock** by default. When **Card Reader** is selected, fingerprint card readers and QR card readers are not supported.
Lock Name	Customize the lock name. Fill it with 1 to 32 characters and it cannot be empty.
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 unlock code to open the door remotely. The default unlock code is 456.

Parameter	Description
Lock Linkage	Enable the **Lock Linkage**, and then select the lock to be linked from the drop-down list.
Unlock Permission	Supports sending the unlock permission to the related VTHs. • All Related VTHs: Send the unlock permission to all related VTHs. • Custom: Select the VTHs to which you want to send the unlock permission.
Expansion Module	• External Lock: Up to 8 extremal locks can be added. 1. Select **External Lock** tab 2. Click **Add** to add the external lock. 3. Select the lock number and configure the lock ID, and then click **Search** to add the lock.  • Alarm Module 1. Select **Alarm Module** tab 2. Click **Add** to add the alarm module. 3. Configure the module ID, and then click **Search** to add the module.   Up to 8 external locks can be added, and the total number of the external locks and alarm modules is 20 at most.

Step 3 Click **Apply**.



- When the RS-485 module of VTO linked with security module (DEE1010B) connects to card reader, the security module has a limit on the length of the entered password (10 digits supported). Therefore, room number (6 digits) + personal password (6 digits) cannot unlock the door.
- When the RS-485 module of VTO linked with security module (DEE1010B) connects to QR card reader or fingerprint card reader, the door cannot be unlocked because the RS-485 of VTO does not support QR code and fingerprint transmission.
- When the RS-485 module of VTO linked with security module (DEE1010B) connects to card reader, cards cannot be issued through the RS-485 module and security module DEE1010B, because the 485 module does not support bidirectional command interaction.

6.3 Light Control

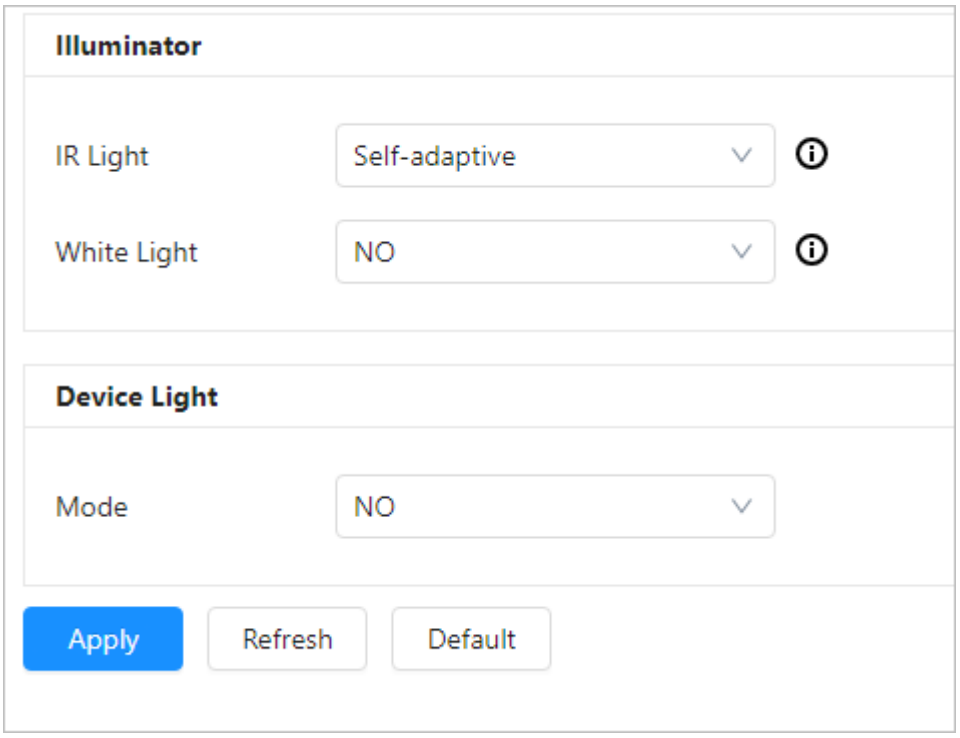
Configure the illuminator mode as needed.

Procedure

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

Step 2 Configure the IR light, white light, and device light mode according to the actual needs.

Figure 6-8 Light control configuration



- **NO** : The light is always on.
- **NC** : The light is always off.
- **Self-adaptive** : The light adapts to the environment and automatically sets a suitable brightness.
- **Period** : The light will be open during the defined period.

Step 3 Click **Apply**.

6.4 Card Settings

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Card Settings**.

Step 3 Configure the card parameters.

Figure 6-9 Card settings

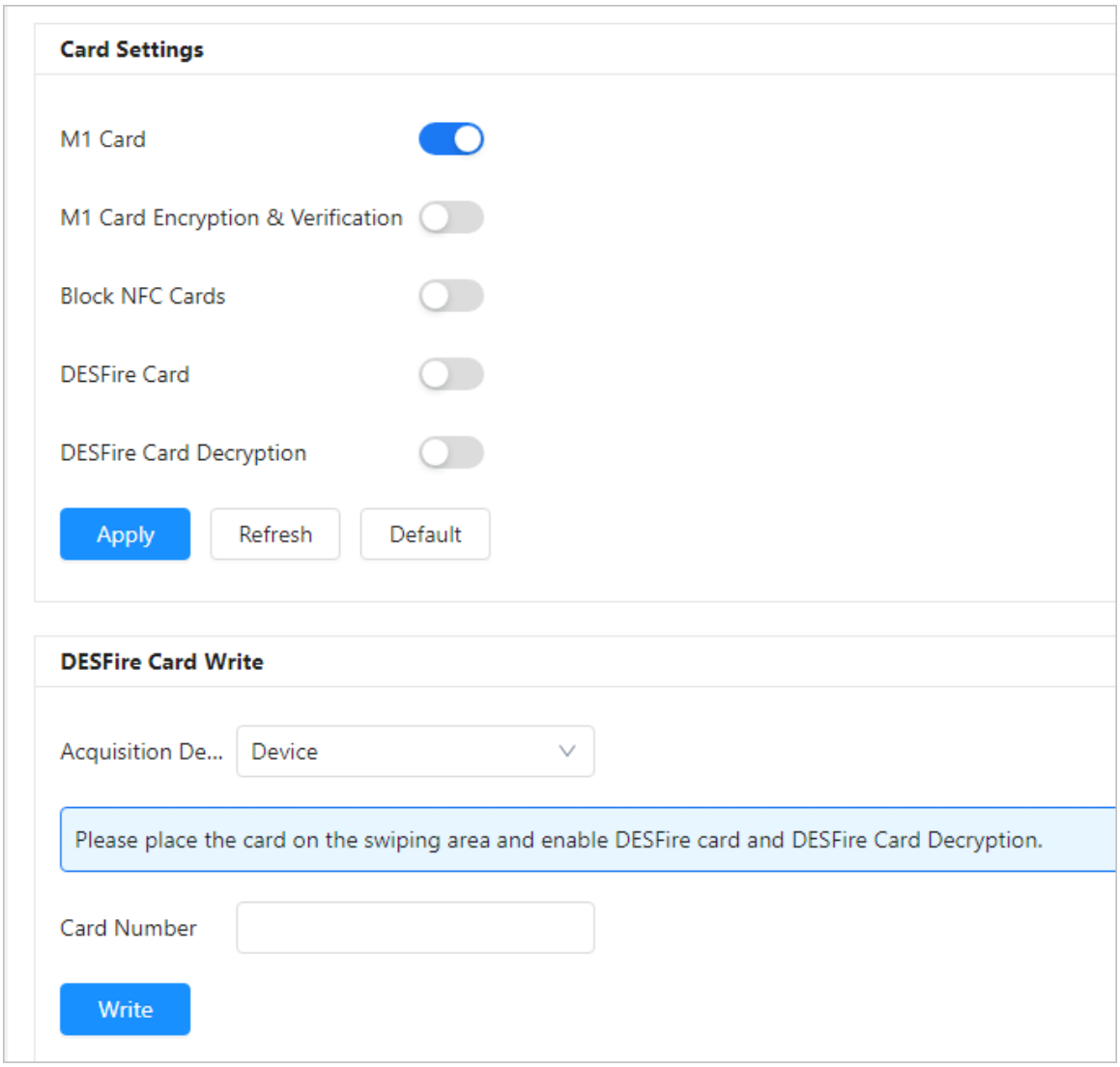


Table 6-4 Description of card parameters

Parameter	Description
M1 Card	When enabled, M1 card can be used to open the door.
M1 Card Encryption & Verification	When enabled, M1 cards are encrypted. Swipe the correct card, if encryption verification succeeds, the door opens.
Block NFC Cards	When it is enabled, NFC function is unavailable.
DESFire Card	When enabled, DESFire card number can be read.
DESFire Card Decryption	When enabled, a DESFire card that is encrypted by the card manufacturer can be decrypted, allowing the card content to be read.

Parameter	Description
Acquisition Device	Select the acquisition device, place the card on the swiping area, enter the card number, and then click **Write**. Enable **DESFire Card** and **DESFire Card Decryption** first.
Card Number	

External card readers do not support encrypted IC cards.

Step 4 Click **Apply**.

6.5 Intelligent

The device with one camera supports one channel, and the device with 2 cameras supports 2 channels. The intelligent configurations for Channel 1 and Channel 2 are the same. This topic uses the Channel 1 configuration of the device with 2 cameras as an example.

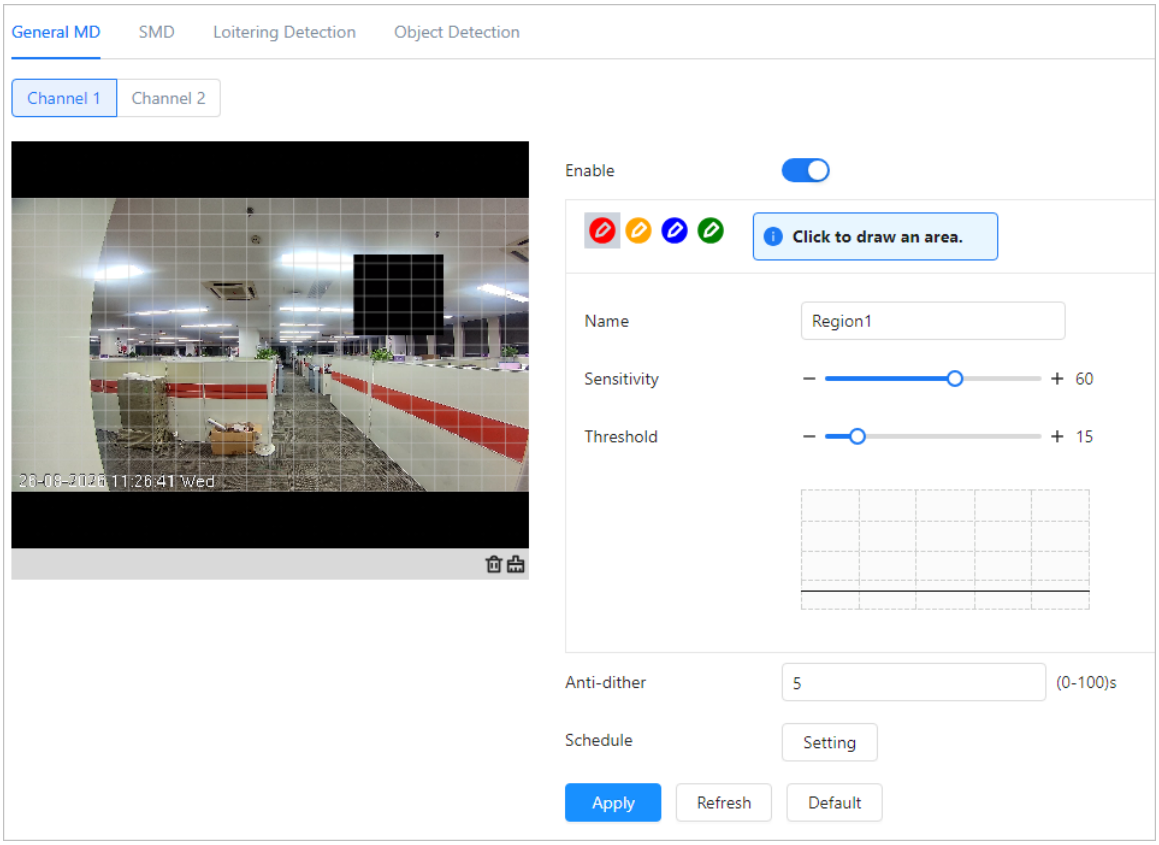
If you need to query the intelligent records and recordings, an SD card must be configured. It is recommended that the write speed of the SD card be greater than 10 MB/s.

6.5.1 Video Intelligence

General MD

1. Log in to the webpage.
2. Select **Local Device Config** > **Intelligent** > **Video Intelligence**, and then select the **General MD** tab.
3. Click to enable the function.

Figure 6-10 General MD configuration



4. Select the brushes with different colors to draw regions.

- One color represents one region, and up to 4 regions can be added.
- Only the regions you have drawn can trigger the motion detection.

5. Configure the parameters of each region, and then click **Apply**.

Table 6-5 Parameter description

Parameter	Description
Name	Enter the name of the region.
Sensitivity	Configure the sensitivity of the region detection. The larger the value, the more likely it is to trigger a motion detection.
Threshold	Adjust the accuracy level of detection. Higher threshold means higher accuracy and lower false detection rate. The larger the value, the less likely it is to trigger a motion detection.
Anti-dither	Configure the period of the anti-dither. An alarm is triggered only when movement continues for the set period, such as 5 seconds.

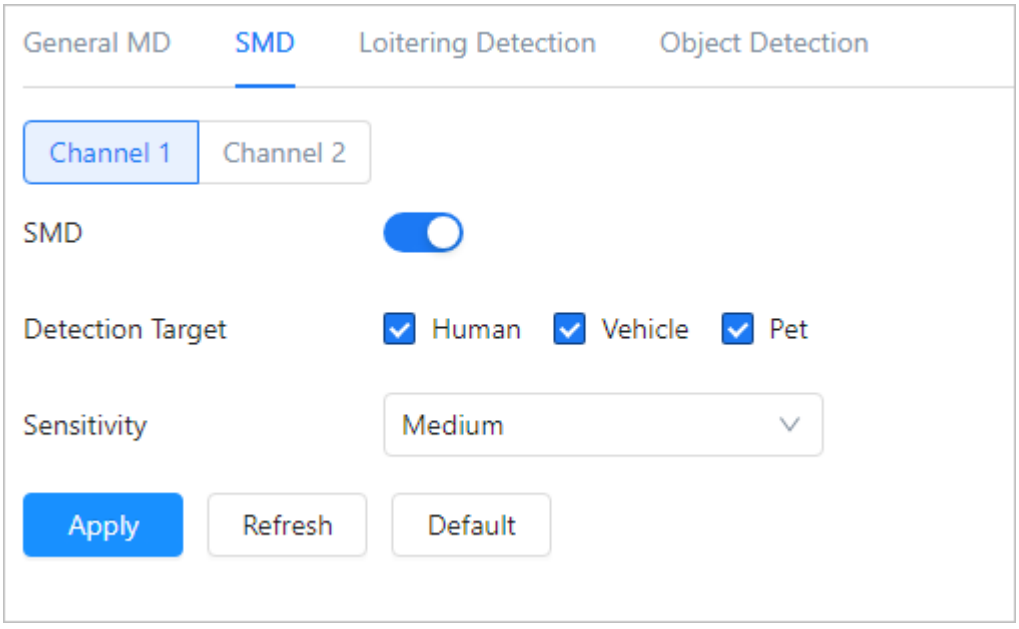
Parameter	Description
Schedule	Click **Setting** to configure the period of the motion detection, and then click **OK**. If the motion detection issue occurs outside the specified period, it will not be reported.

SMD

By default, detection covers the entire area and supports targets such as people, four-wheeled vehicles, and animals (including cats, dogs, and others, but excluding kangaroos, mice, snakes, birds, chickens, and ducks).

1. Log in to the webpage.
2. Select **Local Device Config** > **Intelligent** > **Video Intelligence**, and then select the **SMD** tab.
3. Click to enable the function.

Figure 6-11 SMD configuration



4. Select the detection target, including human, vehicle, and pet.

   At least one target should be selected.

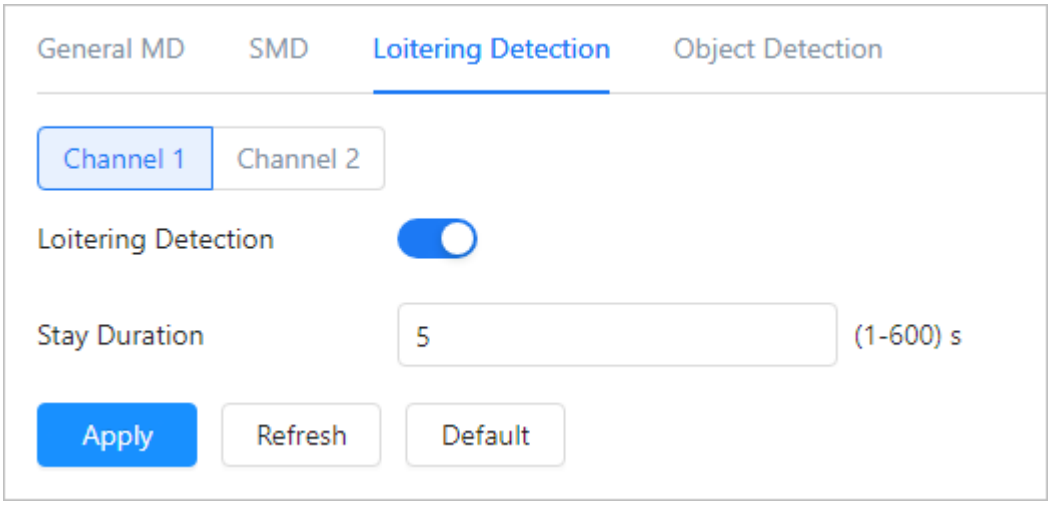
5. Configure the sensitivity of detection, including low, medium, and high, and then click **Apply**.

Loitering Detection

Supports detecting the loitering and configuring the stay duration. When the loitering time exceeds the configured stay duration, an alarm will be generated.

1. Log in to the webpage.
2. Select **Local Device Config** > **Intelligent** > **Video Intelligence**, and then select the **Loitering Detection** tab.
3. Click to enable the function.

Figure 6-12 Loitering detection configuration



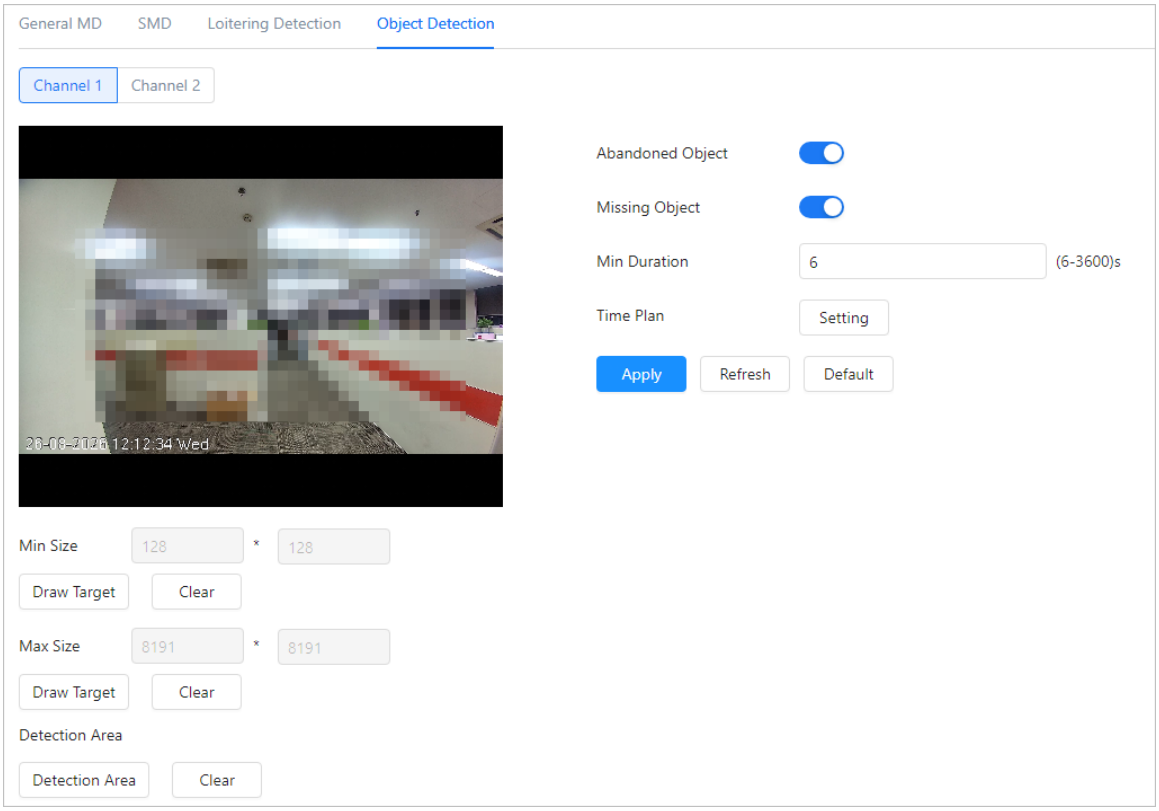
4. Configure the stay duration of detection, and then click **Apply**.

Object Detection

Only available on devices with two cameras.

1. Log in to the webpage.
2. Select **Local Device Config** > **Intelligent** > **Video Intelligence**, and then select the **Object Detection** tab.
3. Click to enable the function.

Figure 6-13 Object detection configuration



4. Configure the parameters of object detection, and then click **Apply**.

Table 6-6 Parameter description

Parameter	Description
Abandoned Object	After it is enabled, when the left time of an object in the area reaches the set time, an alarm will be generated.
Missing Object	After it is enabled, when the missing time of an object in the area reaches the set time, an alarm will be generated.
Min Duration	An alarm will be generated when the duration of an item or its disappearance time exceeds the configured duration. It is recommended that the configured duration be less than the pre-record time configured in the **Linkage Configuration** ; otherwise, the whole process of placing the package or missing the package cannot be found in the corresponding video.
Time Plan	Click **Setting** to configure the time plan of the detection, and then click **OK**.
Min Size	Click **Draw Target**, and then draw the minimum size of the detection target. If the size of the detected objects is smaller than the minimum size, it will not be reported.

Parameter	Description
Max Size	Click **Draw Target**, and then draw the maximum size of the detection target. If the size of the detected objects is bigger than the maximum size, it will not be reported.
Detection Area	Click **Detection Area**, and then draw the detection target area. The objects outside the detection area will not be reported.

6.5.2 Audio Intelligence

6.5.2.1 AI Event

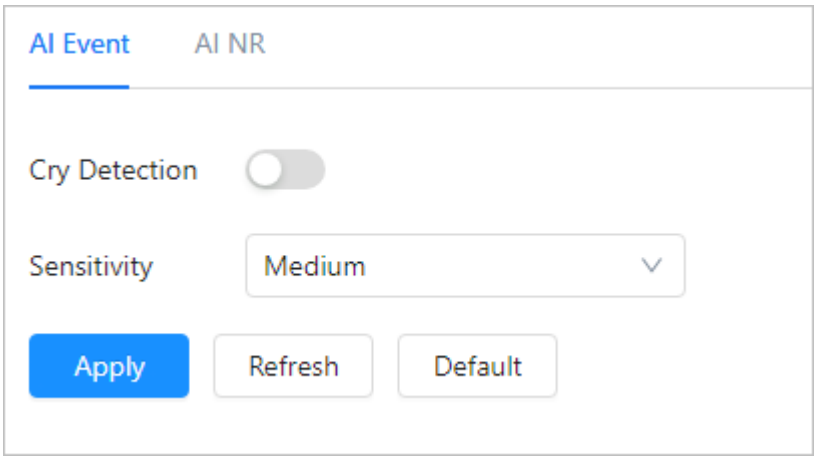
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Intelligent** > **Audio Intelligence**.

Step 3 Select **AI Event** tab, and then configure the **Cry Detection** function.

Figure 6-14 Cry detection



Step 4 Click to enable cry detection. The function detects baby cries in the detection area.

The baby cries lasting for more then 5 seconds can be detected.

Step 5 Select the detection sensitivity from 3 levels: low, medium, and high.

Step 6 Click **Apply**.

- After it is enabled, an alarm will be triggered when a baby crying sound is detected. However, detection performance is highly dependent on the crying volume, and the sound may not be detected at long distances.

- The detection effect is related to the environment. It performs better in relatively quiet scenarios, but the effect cannot be guaranteed in the noisy environments.

6.5.2.2 AI NR

Procedure

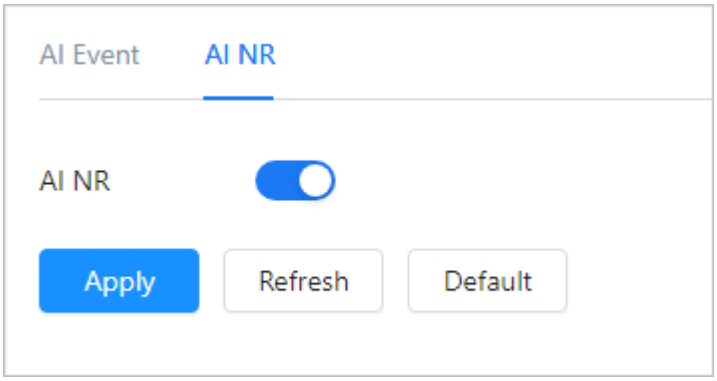
Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Intelligent** > **Audio Intelligence**.

Step 3 Select **AI NR** tab, click to enable the function.

When it is enabled, the noise can be reduced at the other end during intercom and improve the audio effect at the other end.

Figure 6-15 AI NR



Step 4 Click **Apply**.

6.5.3 Linkage Configuration

When intelligent events (such as motion detection) are triggered, the system starts recording automatically. This topic describes the configuration of linked recording parameters.

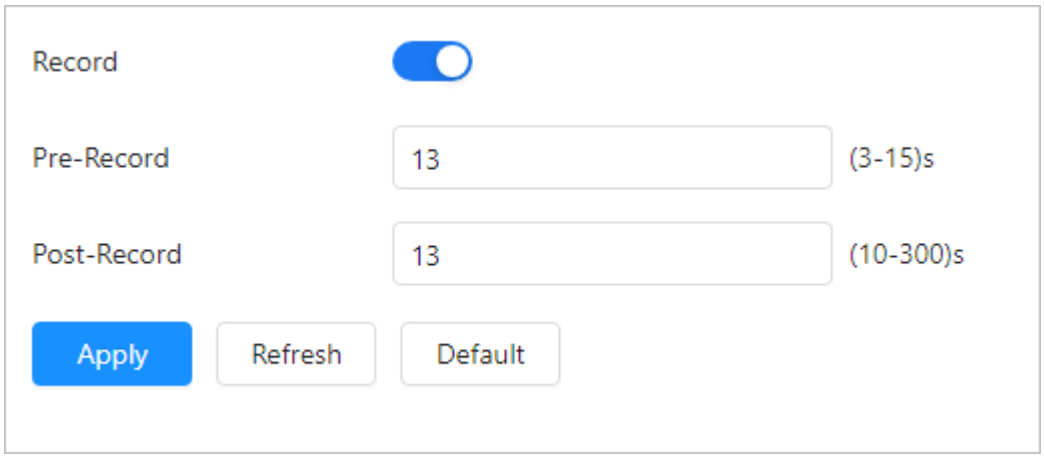
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Intelligent** > **Linkage Configuration**.

Step 3 Click to enable the **Record** function, and then configure the parameters.

Figure 6-16 Linkage parameters



- Pre-Record: When an event occurs, the video of the configured period (such as 13 seconds) before the event happens will be saved.
- Post-Record: After the event ends, the video of the configured period (such as 13 seconds) after the event ends will continue to be saved.

Step 4 Click **Apply**.

6.6 Port Configuration

Background Information

The device supports 2 channels of door magnetic input (which can also serve as the alarm inputs 1 and 2, and it is door magnetic mode by default), door unlocking button input (which can also serve as the alarm inputs 3 and 4, and it is door unlocking button input by default), and 2 channels of door lock control output (which can also serve as the alarm output, and it is door lock control output by default. For details about the wiring, see Figure 1-3 .

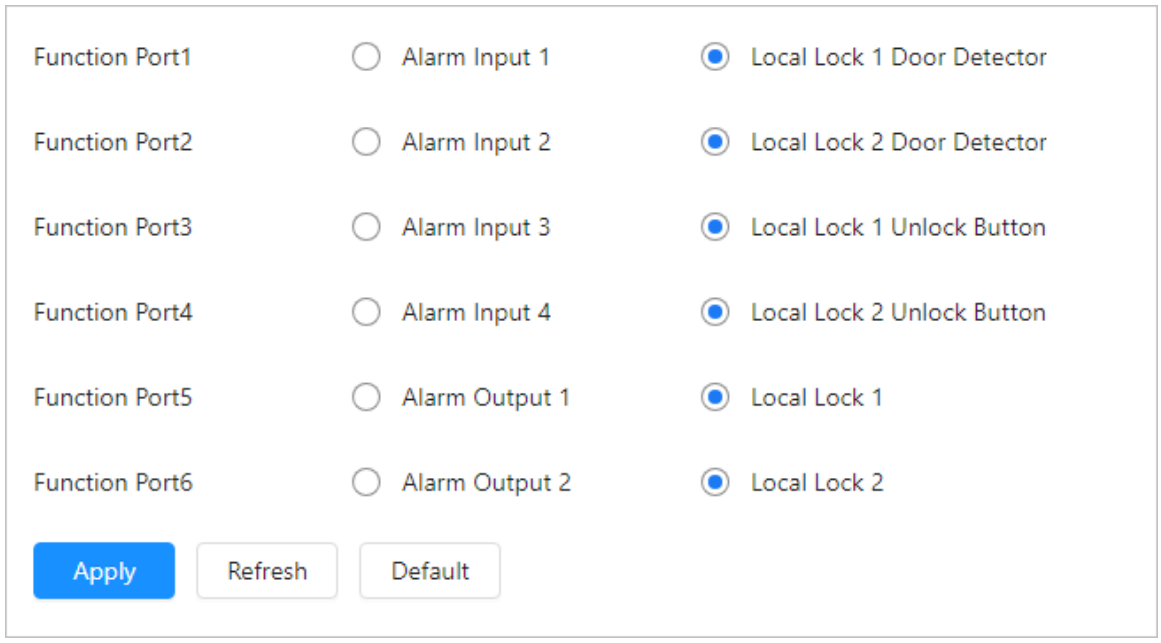
Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the function of ports, including alarm input, alarm output, and other functions.

Figure 6-17 Port configuration



Step 4 Click **Apply**.

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 a 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 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 webpage 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

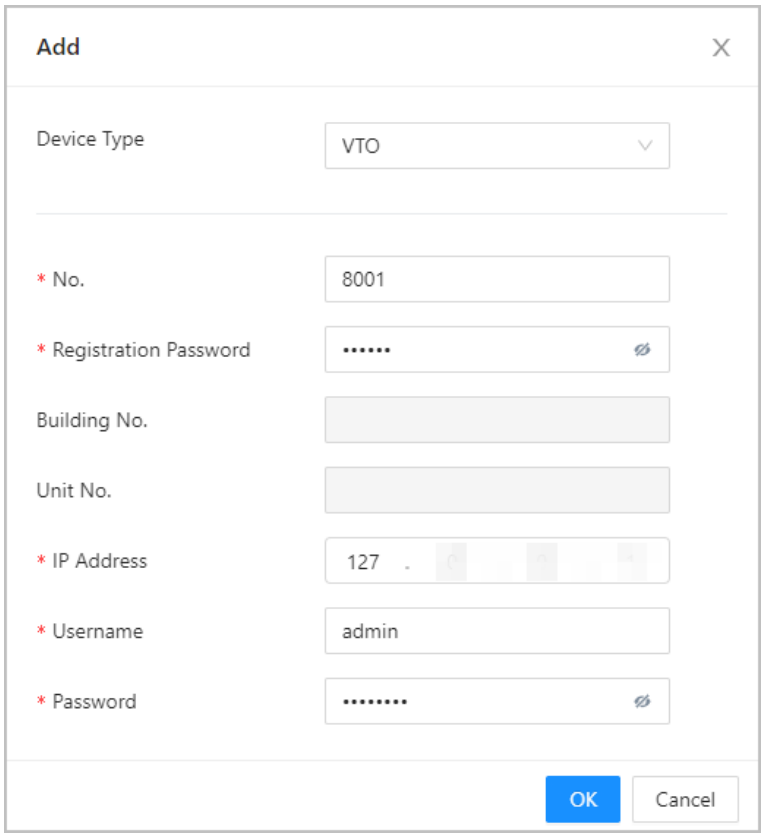


Table 7-1 Add VTO configuration

Parameter	Description
Device Type	Select **VTO**.

Parameter	Description
No.	The VTO number you configured.
Registration Password	Leave it as default.
Building No.	Available only when the platform servers or VTS work as the SIP server.
Unit No.	
IP Address	IP address of the VTO.
Username	User name and password used to log in to the webpage of the VTO.
Password	

Step 5 Click **OK**.

Related Operations

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

7.2 VTH Management

You can add room numbers to the SIP server, and then configure the room numbers on 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

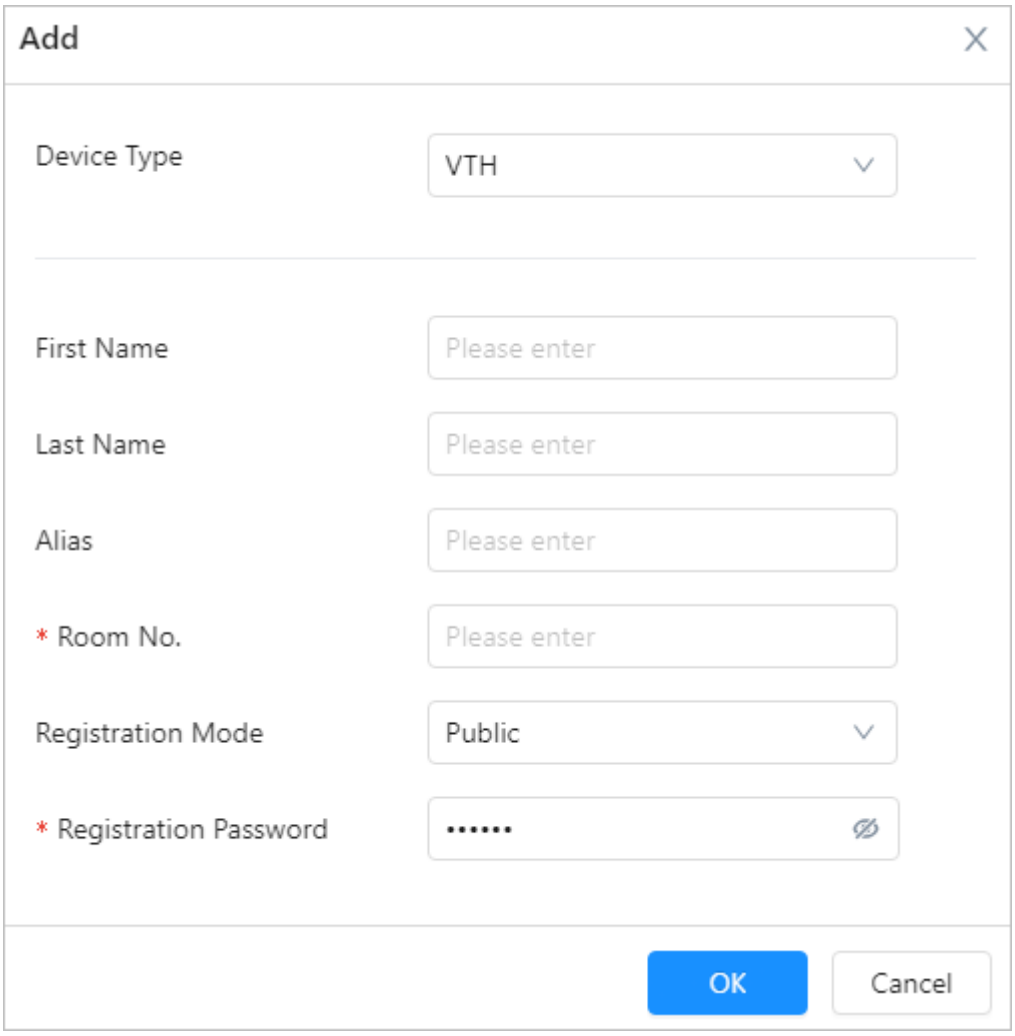


Table 7-2 Parameter description

Parameter	Description
First Name	Enter the information needed to differentiate rooms.
Last Name	
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.

Step 5 Click **OK**.

- Click to edit the VTH, or to delete added VTHs, but a VTH currently in use cannot be modified or deleted.

- Click or to call or hang up a VTH.
  - This function is available only when the SIP function is online.
  - If a group calling is enabled, a group call is performed when you call VTH #0 or -0.
  - The calling function is only available for VTHs.

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 all the VTOs and VTHs in the network, and make or receive calls from them. See the VTS user manual for details.

Procedure

Step 1 Log in to the web manager of the VTO that functions as the SIP server.

Step 2 Select **Device Setting**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 7-3 Add VTS

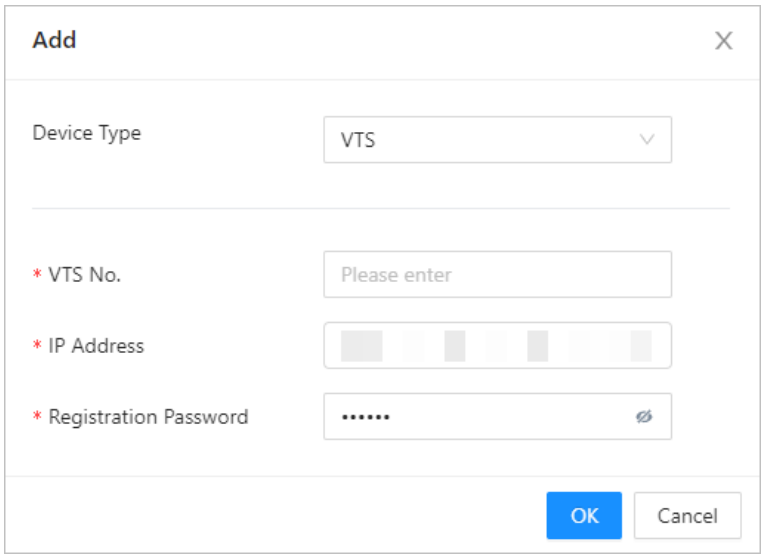


Table 7-3 Add VTS configuration

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

Step 5 Click **OK**.

8 Person Management

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Person Management**.

Step 3 Click **Add**.

Step 4 Configure the parameters, and then click **OK**.

Figure 8-1 Add person

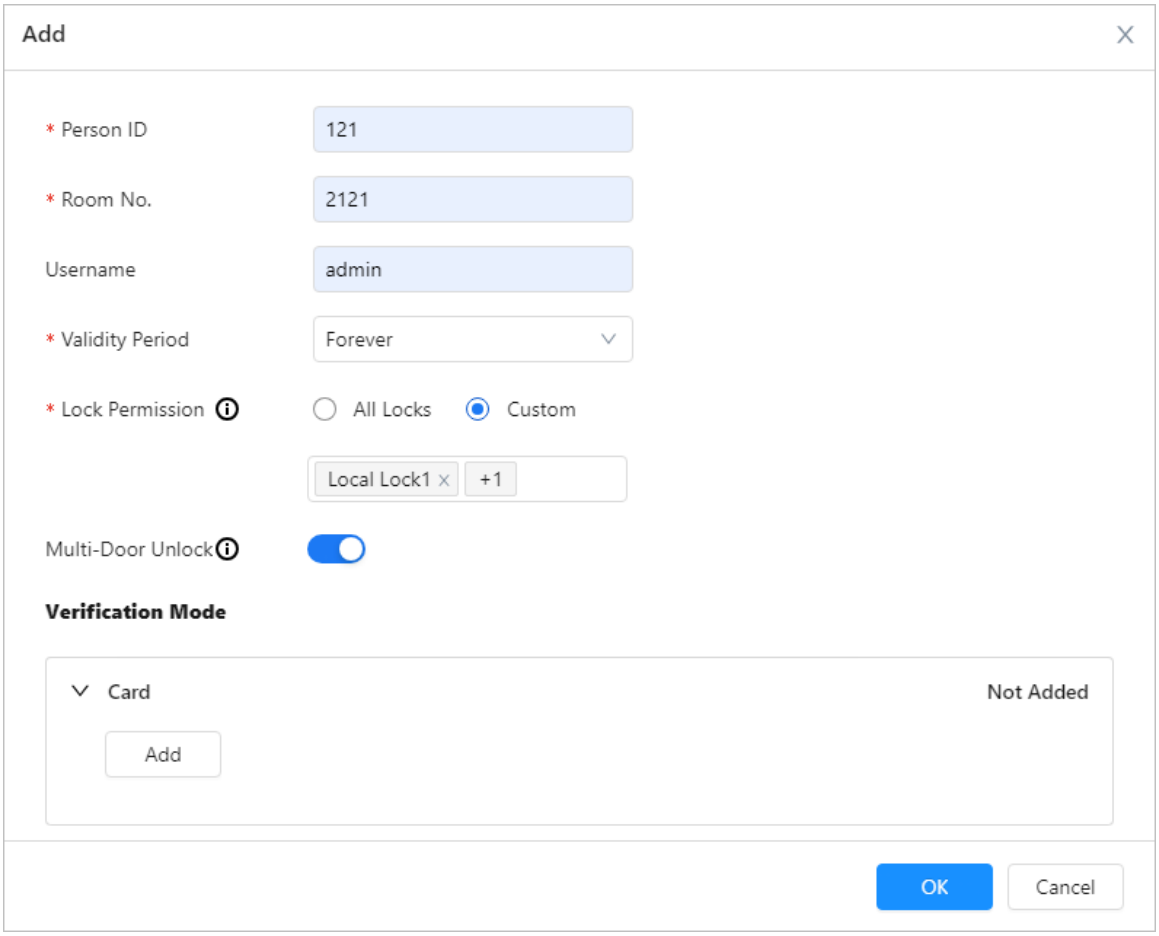


Table 8-1 Person parameter description

Parameter	Description
Person ID	Customize the ID number.
Room No.	Enter the corresponding room number of the VTH.
Username	Enter the user name.
Validity Period	Configure the validity period during which people have access permissions.

Parameter	Description
Lock Permission	Configure the lock permission. • **All Locks** : All locks, including local locks and external locks, are granted permissions. The user gets permission to access all existing locks, and will also automatically be allowed to access all newly added locks. • **Custom** : Select the locks to which you want to grant permissions. The user only gets permission to access the locks you select for them, and newly added locks have to be manually assigned to them.
Multi-Door Unlock	When verification is successful, all the locks that the user has permission for will open.
Card	1. Select **Card** > **Add**. 2. Enter the card number. Or you can click **Issue Card**, and then swipe the card on VTO. 3. Click **OK**. You can manage the cards through the following icons. • : If the card is lost, click it to report the loss. The icon becomes , and the card permission becomes invalid. • : It indicates that the card cannot be used to open the door. Click it to make the card valid. • : Edit the card name. • : Delete the card.

9 Network Settings

This chapter explains how to configure network parameters.

9.1 TCP/IP

Configure the TCP/IP information to connect the VTO to the network.

Procedure

Step 1 Log in to the web manager of the VTO.

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

Step 3 Configure the TCP/IP parameters.

Figure 9-1 TCP/IP

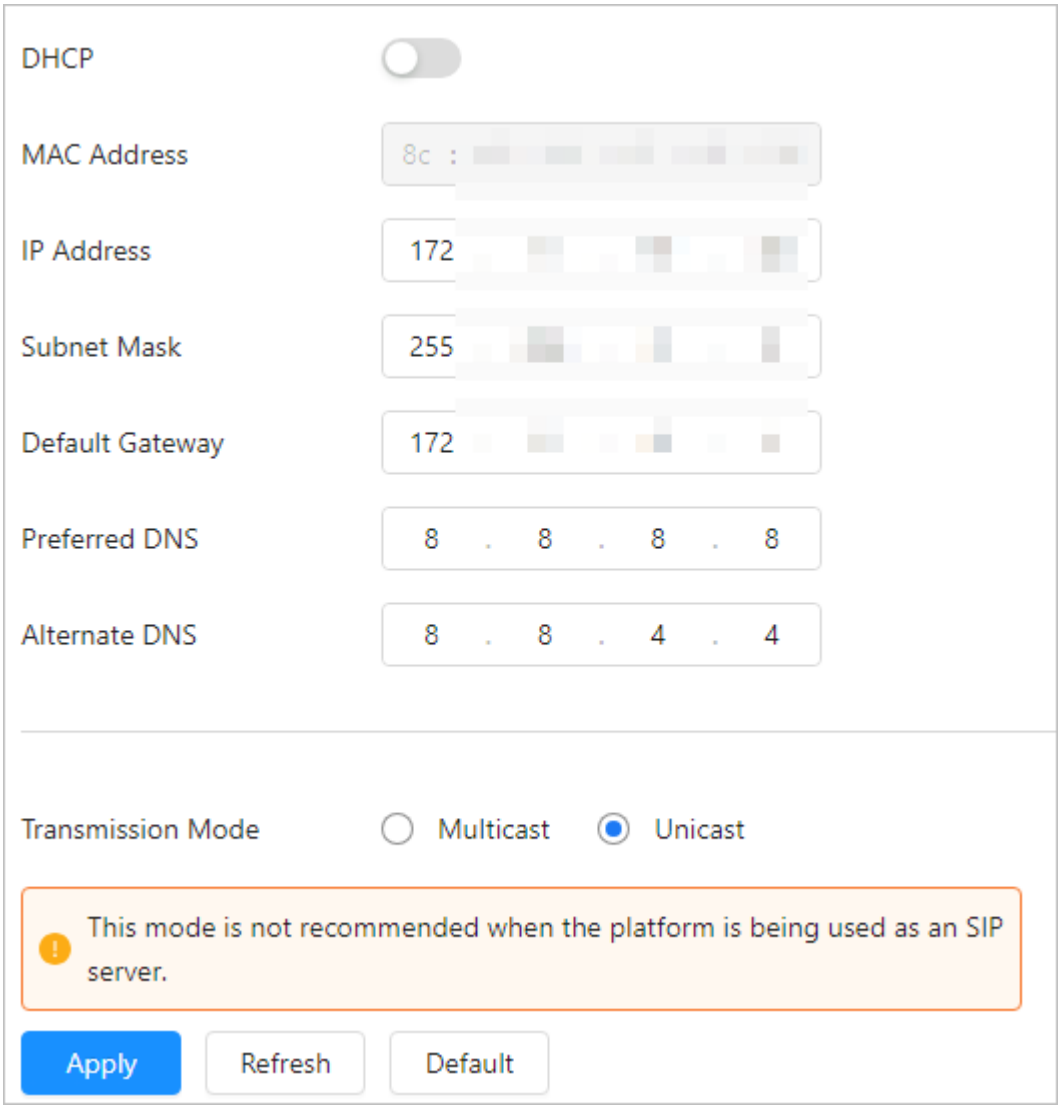


Table 9-1 Parameter description

Parameter	Description
DHCP	Automatically assigns IP addresses and other network configuration parameters.
IP Address	The IP address to configure 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: Ideal for video talk. • Unicast: Ideal for group call. Unicast is not recommended when the platform is being used as a SIP server.

Step 4 Click **Apply**.

9.2 Port

Procedure

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

Step 2 Configure the port parameters.

Figure 9-2 Port

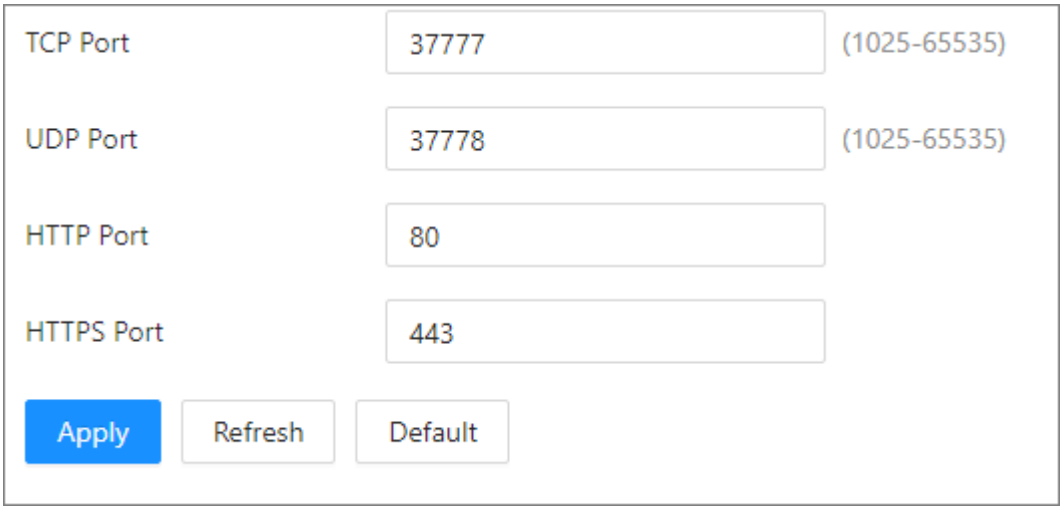


Table 9-2 Parameter description

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

Parameter	Description
HTTPS Port	You can enter https://VTO IP address: HTTPS Port to log in to the VTO.

Step 3 Click **Apply**.

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

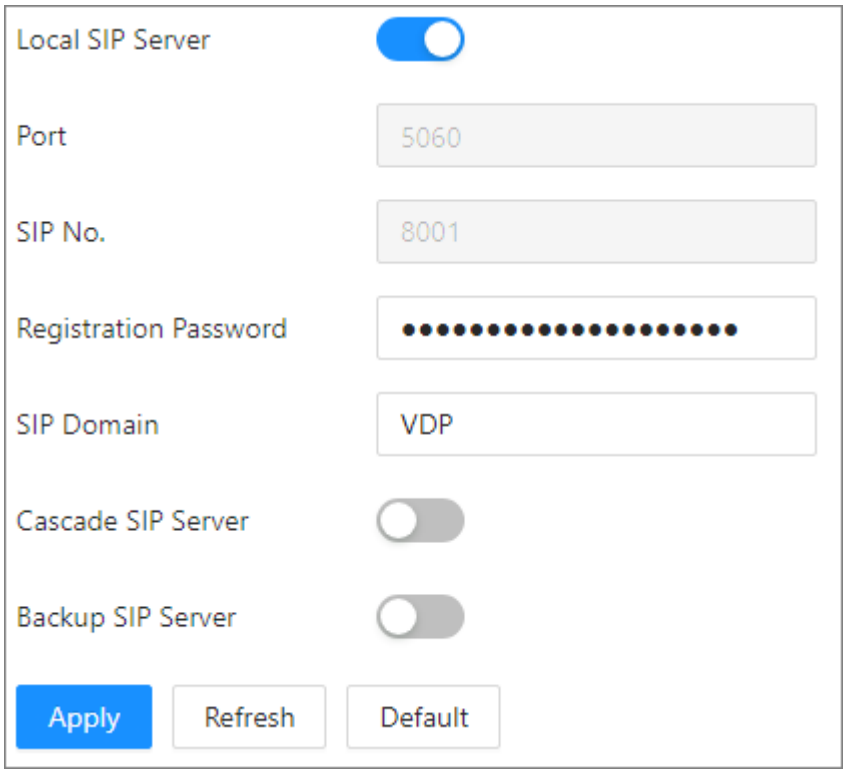
Step 1 Select **Network Settings** > **SIP Server**.

Step 2 Select a server type.

- The VTO you have logged in as the SIP server: Enable **Local SIP Server**, and then configure the parameters for the VTO.

  Some parameters would become grey after enabling the **Local SIP Server** function.

Figure 9-3 Current VTO as SIP server



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

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

Figure 9-4 Another VTO as SIP server

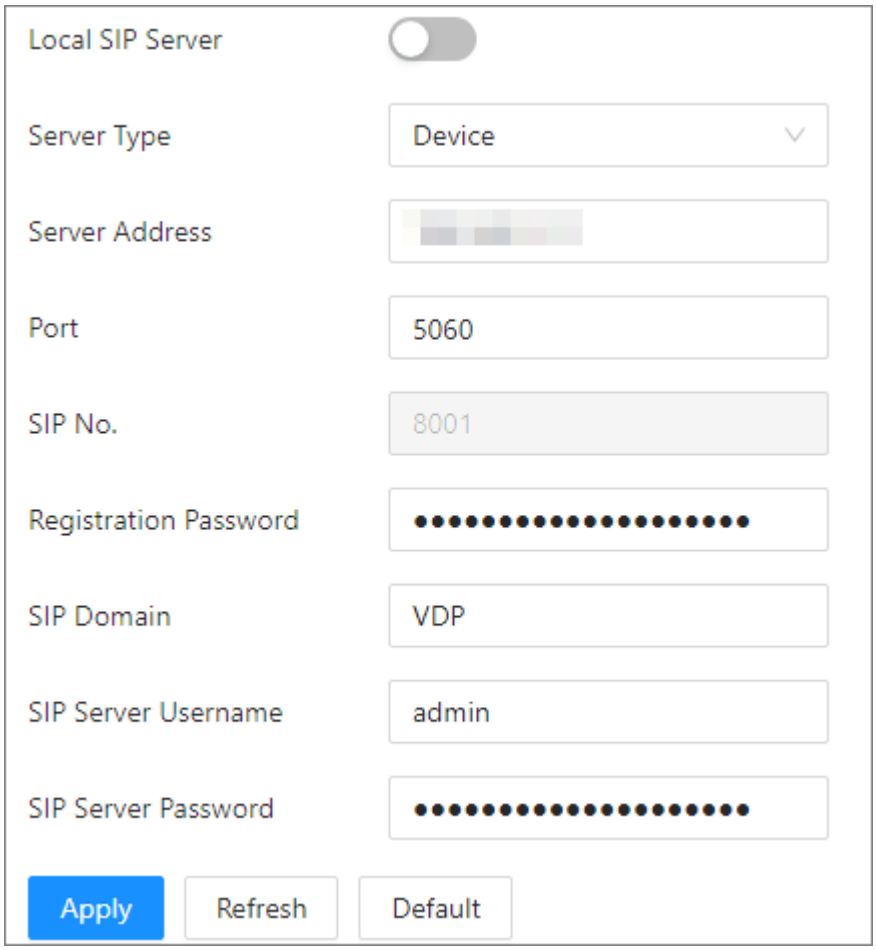


Table 9-3 SIP server parameter description (VTO as the SIP server)

Parameter	Description
Server Address	Planned IP address of the VTO.
Port	5060 by default.
SIP No.	Leave it as default.
Registration Password	
SIP Domain	
SIP Server Username	User name and password used to log into the webpage of the SIP server.
SIP Server Password	

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

Figure 9-5 Private SIP server

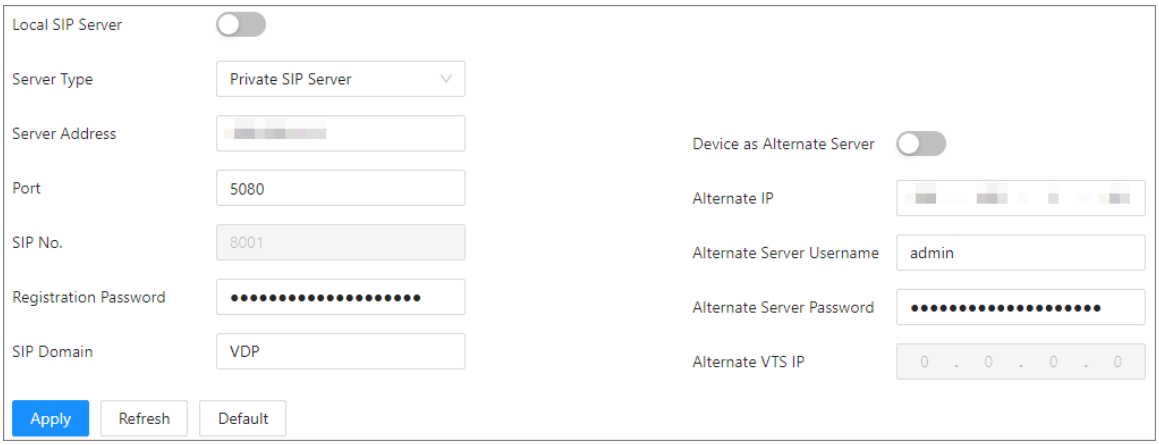


Table 9-4 SIP server description (platform as the SIP server)

Parameter	Description
Server Address	IP address of the SIP server.
Port	5080 by default when the platform works as the SIP server.
SIP No.	Leave it as default.
Registration Password	
SIP Domain	
Device as Alternate Server	Enable it so that you can configure the Alternate VTS IP.
Alternate IP	The alternate server will be used as the SIP server when Express or DSS stops responding. We recommend you configure the alternate IP address. ◇ If you enable **Device as Alternate Server**, the current VTO you have logged in serves as the alternate server. ◇ If you want another VTO to serve as the alternate server, you need to enter the IP address of that VTO in the **Alternate IP** textbox. Do not enable **Device as Alternate Server** in this case.
Alternate Server Username/ Password	Used to log in to the alternate server.
Alternate VTS IP	Enter the IP address of the alternate VTS.

- When third-party server works as the SIP server: Set **Third-party Server** as **Server Type**, and then configure the parameters.

Figure 9-6 Third-party server

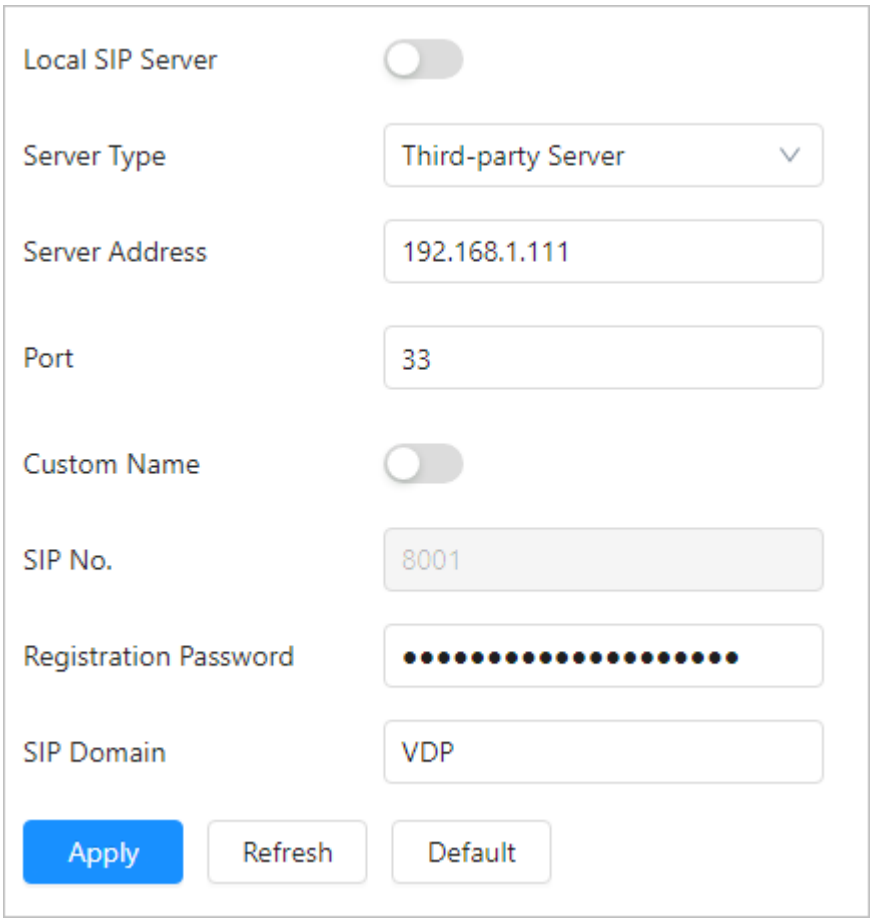


Table 9-5 Third-party server description

Parameter	Description
Server Address	The IP address of the third-party server.
Port	Enter the port of the SIP server, which is from 1 to 65535.
Custom Name	After enabling it, you can customize the **SIP No.**.
SIP No.	
Registration Password	Leave it as default.
SIP Domain	Keep default value VDP or leave it empty.

Step 3 Click **Apply**.

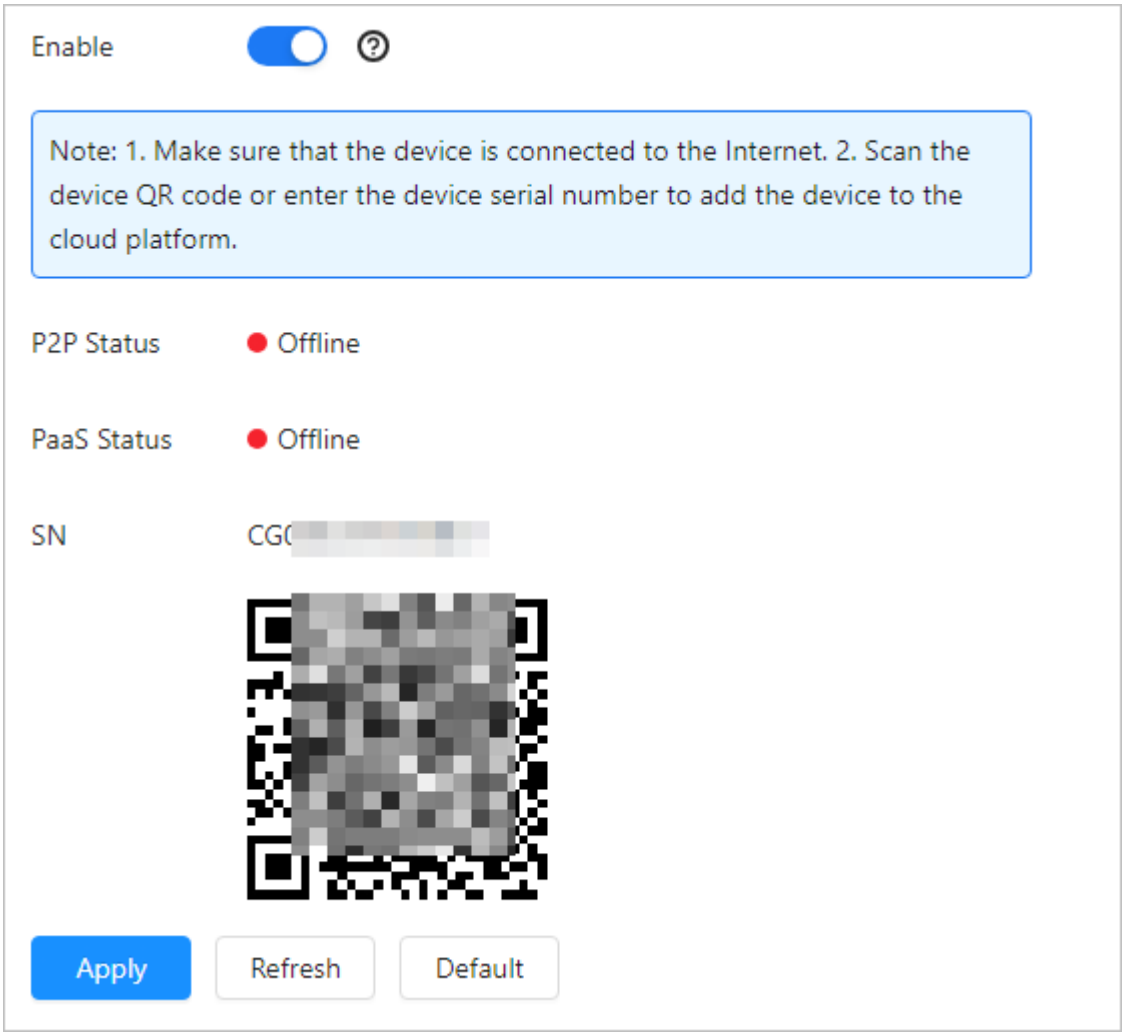
- For some third-party servers, if the intercom selects two unlocking methods of the **RFC 2833** and **SIP INFO** at the same time, the unlocking code will not available to unlock the intercom.

- When a third-party server is used to support a third-party intercom, the intercom exception or SIP offline may occur on some servers.
- If **Third-party Server-Asterisk** and **SIP Intercom** select two unlocking methods of the **RFC 2833** and **SIP INFO** at the same time, the unlocking code will not available to unlock the intercom.
- If IB intercom frequently disconnects from the 3CX server, the mapping relationship needs to be deleted.

9.4 Cloud Service

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

Figure 9-7 Cloud service



9.5 UPnP

This task describes how to enable UPnP to map intranet ports to the extranet.

Background Information

After enabling UPnP, the intranet services/ports of the device are mapped to the extranet.

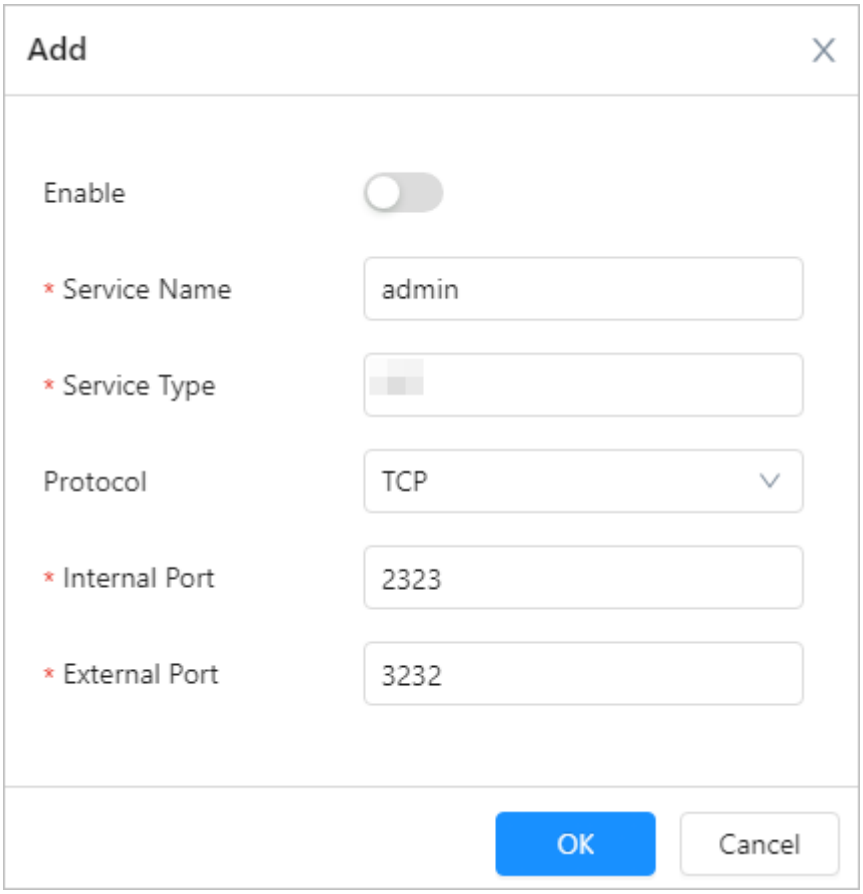
Procedure

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

Step 2 Select to enable the function.

Step 3 Click **Add** to add new services, configure the parameters, and then click **OK**.

Figure 9-8 Add a new service



Step 4 Click **Apply**.

9.6 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 9-9 Basic services

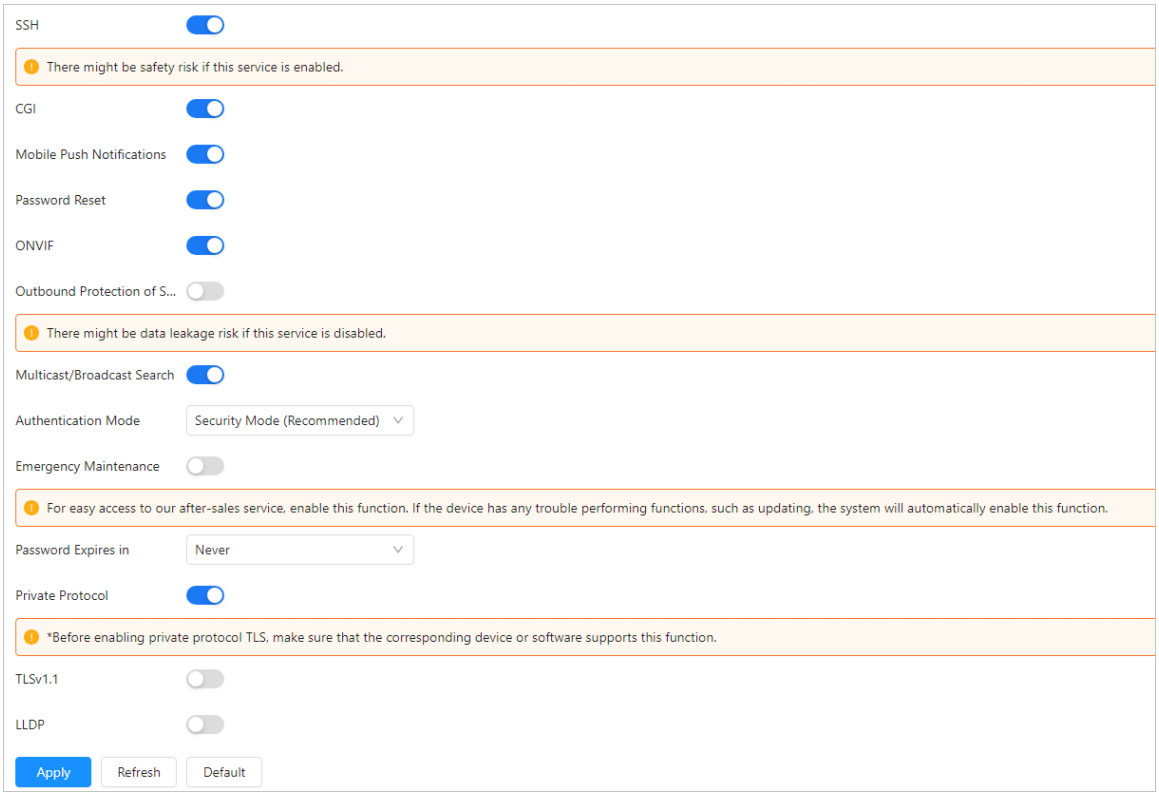


Table 9-6 Security parameter description

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	Enable the use of CGI commands. We recommend you turn it off. Otherwise, the VTO might be exposed to security risks and data leakage.
Mobile Push Notification	Sends information to the app on your 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 the password.

Parameter	Description
ONVIF	Allows communication between devices from different brands or series.
Outbound Protection of Service Information	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): Supports login with Digest authentication. • **Compatibility Mode** : Use the old login method. We recommend you use the **Security Mode** . **Compatibility 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 VTO has any problems 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 period between 0 and 180.
Private Protocol	Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.
TLSv1.1	Enables or disables TLS 1.1. We recommend you turn it off because there might be a security risk if this service is enabled.
LLDP	Improves the efficiency of information exchange among network devices.

Step 3 Click **Apply**.

9.7 Auto Registration

The VTO automatically registers with the server and reports its IP address to the designated server.

Procedure

Step 1 Log in to the web manager of VTO.

Step 2 Select **Network Settings** > **Auto Registration**.

Step 3 Enable the function. Enter the server address, port number and registration ID.

Figure 9-10 Auto registration

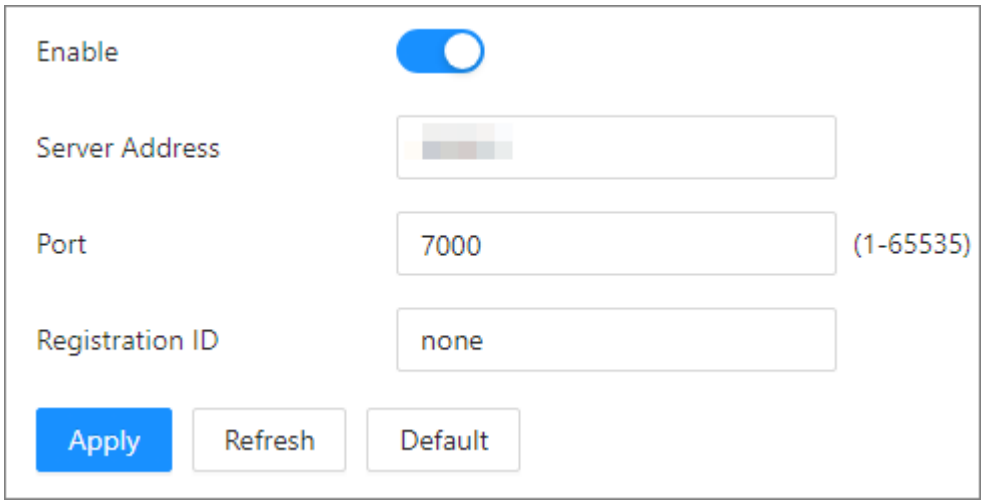


Table 9-7 Parameter description

Parameter	Description
Server Address	The IP address or domain name of the server required for registration.
Port	Port number used by the server for automatic registration.
Registration ID	The server distributes an ID for the device. Keep it consistent with the ID registered on the server.

Step 4 Click **Apply**.

10 System

10.1 Alarm

10.1.1 Alarm Linkage Setting

View the local alarm list and the expansion module list.

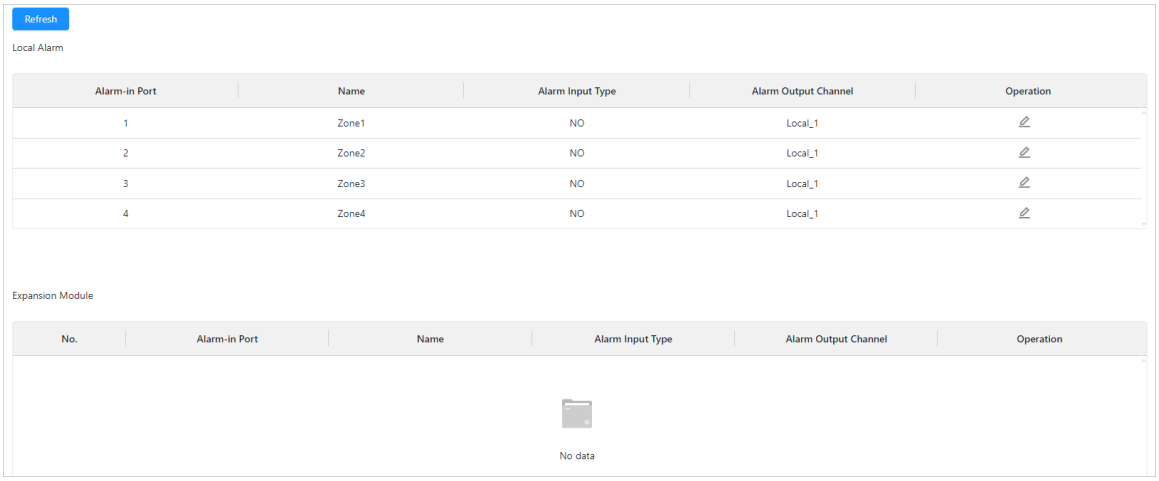
Procedure

Step 1 Select **System** > **Alarm** > **Alarm Linkage Setting**.

Step 2 View the local alarm list and the expansion module list.

Click **Refresh** to update the list.

Figure 10-1 Alarm linkage list



10.1.2 Configuring Alarm

Procedure

Step 1 Select **System** > **Alarm** > **Alarm**.

Step 2 Configure the parameters.

Figure 10-2 Alarm

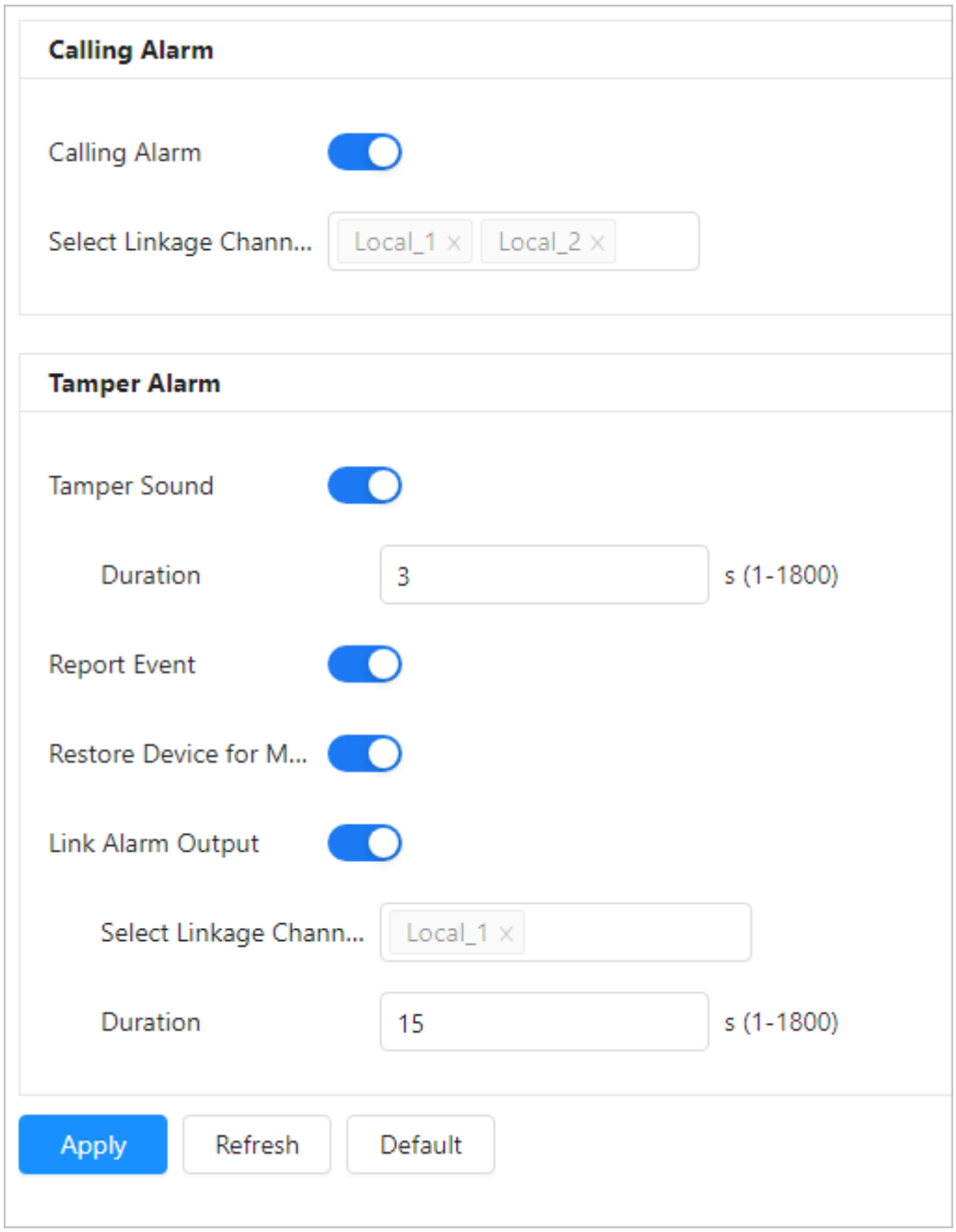


Table 10-1 Alarm parameter description

Parameter	Description
Calling Alarm	When the call is initiated, the alarm output will be linked. If the alarm output interface is connected to a buzzer, it will beep.
Select Linkage Channel	After the **Calling Alarm** is enabled, select the linkage channels.

Parameter	Description
Tamper Sound	Configure whether the device whistles locally or not. It is enabled by default.
Duration	After the **Tamper Sound** is enabled, configure the tamper sound period, which is 3 seconds by default.
Report Event	Configure whether the device reports the tamper alarm to the App, indoor monitor, and platform backend. It is enabled by default.
Restore Device for Multiple Tamper Alarms	Within 10 minutes of powering on the device, if you press the tamper button 5 times within 8 seconds, the device beeps and deletes the account information.
Link Alarm Output	When it is enabled, configure the linkage channels and the duration, which is 15 seconds by default.

Step 3 Click **Apply**.

10.2 Video

Configure the video format and quality of the VTO.

Procedure

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

Step 2 Select different channel tabs to configure their parameters, which will take effect upon change.

Channel 1 of the device with two cameras is used as an example.

- For devices with one camera, you can configure the image ratio from 16:9 or 1:1.
- For devices with two cameras, the image ratio is 16:9 by default and cannot be configured.

Figure 10-3 Channel 1 video configuration

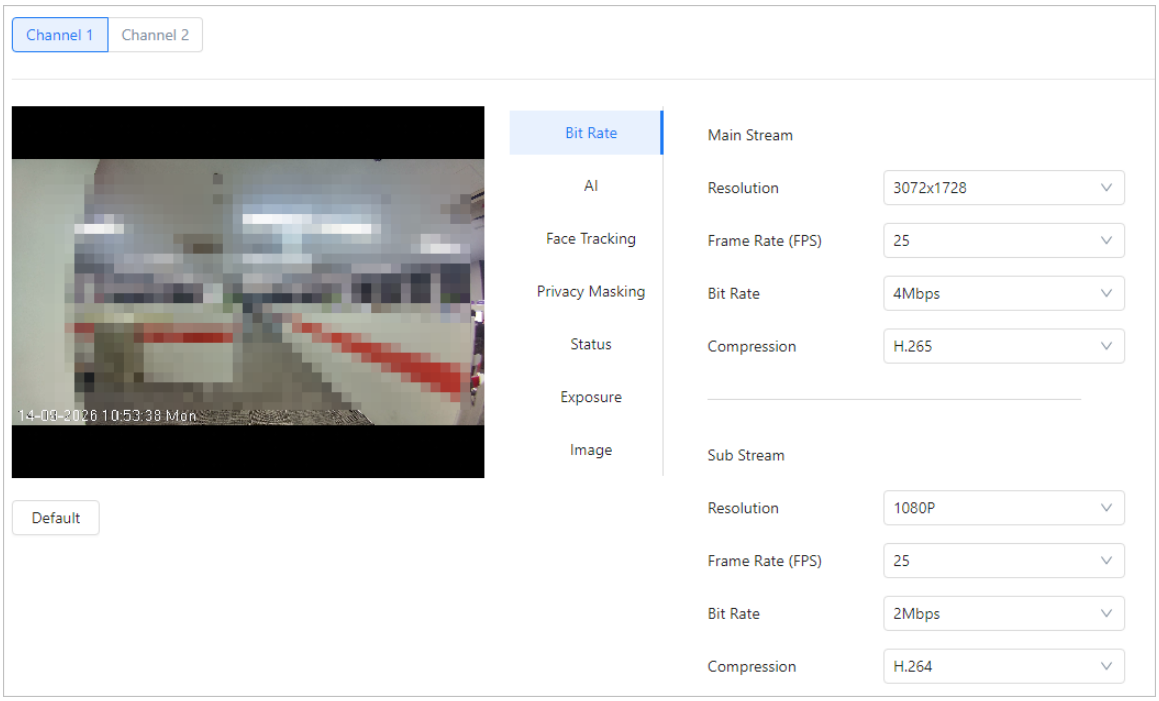


Table 10-2 Video parameter description

Parameter		Description
Bit Rate (Main Stream/Sub Stream)	Resolution	Select the resolution. • The resolution of the upper camera for the device with 2 cameras: ◇ Main stream: 3072 × 1728 (default), 2688 × 1520, 1080P, 720P, and WVGA. ◇ Sub stream: 1080P (default), 720P, D1, WVGA, and CIF. • The resolution of the lower camera for the device with 2 cameras: ◇ Main stream: 1080P (default), 720P, D1, WVGA, and CIF. ◇ Sub stream: 720P (default), D1, WVGA, CIF, and QVGA. • The resolution of the device with one camera, when its length-width ratio of the image is configured as 1:1. ◇ Main stream: 2144 × 2144 (default), 1920 × 1920, 1440 × 1440, 960 × 960, and 720 × 720. ◇ Sub stream: 1440 × 1440 (default), 960 × 960, 720 × 720, 640 × 640, and 320 × 320. • The resolution of the device with one camera, when its length-width ratio of the image is configured as 16:9. ◇ Main stream: 3072 × 1728 (default), 2688 × 1520, 1080P, 720P, and WVGA. ◇ Sub stream: 1080P (default), 720P, D1, WVGA, and CIF. Some VTHs with low-performance do not support decoding at a resolution of 3072 × 1728, which will result in a black screen during video playback. In such cases, the resolution must be manually adjusted to 720P, and the compression to H.264.

Parameter		Description
	Frame Rate (FPS)	• If the **Video Standard** in the **Status** is configured as **PAL**: The range is from 1 to 25. When the **AI BLC** is enabled, the range is from 1 to 20. • If the **Video Standard** in the **Status** is configured as **NTSC**: The range is from 1 to 30. When the **AI BLC** is enabled, the range is from 1 to 20. The larger the value, the smoother the video, but it requires more bandwidth.
	Bit Rate	The larger the value, the better the video quality, and the more bandwidth.
	Compression	Compared with H.264, H.265 requires smaller bandwidth.  Some devices with low-performance do not support H.265, and the video screen will be in black. At this time, manually adjust it to H.264.
AI	AI BLC	When it is enabled, the image quality can be ensured.  Only available in the daytime but not nighttime.
Face Tracking		During a call, the VTO automatically adjusts the body in the middle of the video frame.  The camera at the bottom of the device with 2 cameras does not support this function.
Privacy Masking		Supports masking the privacy area. When it is enabled, click **Add**, and then draw the privacy area on the video. After the configuration, the private area will be displayed as a black block in the preview or call on the peer device.  Up to 4 privacy areas are supported.
Status	Scene Mode	Select from **Auto** , **Disable**, **Sunny** and **Night**. **Auto** is selected by default.
	Day/Night	Select from **Color** , **Auto** and **B/W**.

Parameter		Description
	Compensation Mode When **AI BLC** is enable, it is unavailable.	• **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.
	Video Standard	Select **PAL** or **NTSC** according to your area.
Exposure When **AI BLC** is enable, it is unavailable.	Anti-flicker	• **50Hz** : The system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. • **60Hz** : The system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. • **Outdoor** : If you select **Outdoor**, the exposure mode can be set to **Gain Priority**, **Shutter Priority** and **Iris Priority**. Different devices support different exposure modes.
	Exposure Mode	• **Auto** : Exposure is automatically adjusted according to scene brightness if the overall brightness of images is in the normal exposure range. • **Manual** : You can adjust the **Gain** and **Shutter** value manually. • **Shutter Priority** : The camera automatically adjusts the aperture size based on the selected shutter speed to ensure proper exposure.
	Exposure Compensation	You can set the exposure compensation value. The value ranges from 0 to 100. The higher the value is, the brighter the image will be.
	3D NR	Reduce the noise of multiple-frame (at least two frames) images by using inter-frame information between two adjacent frames in a video. The higher the level is, the lower the noise will be, and the larger the trailing smear will be.
	NR Level	Noise reduction grade. The value ranges from 0 to 100. The larger the value is, the less the noise will be.
Image	Brightness	The larger the value, the brighter the image.

Parameter		Description
	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.
	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 **Default** to restore to default configurations.

10.3 Audio

Procedure

Step 1 Select **System** > **Audio**.

Step 2 Configure the parameters.

Figure 10-4 Audio configuration

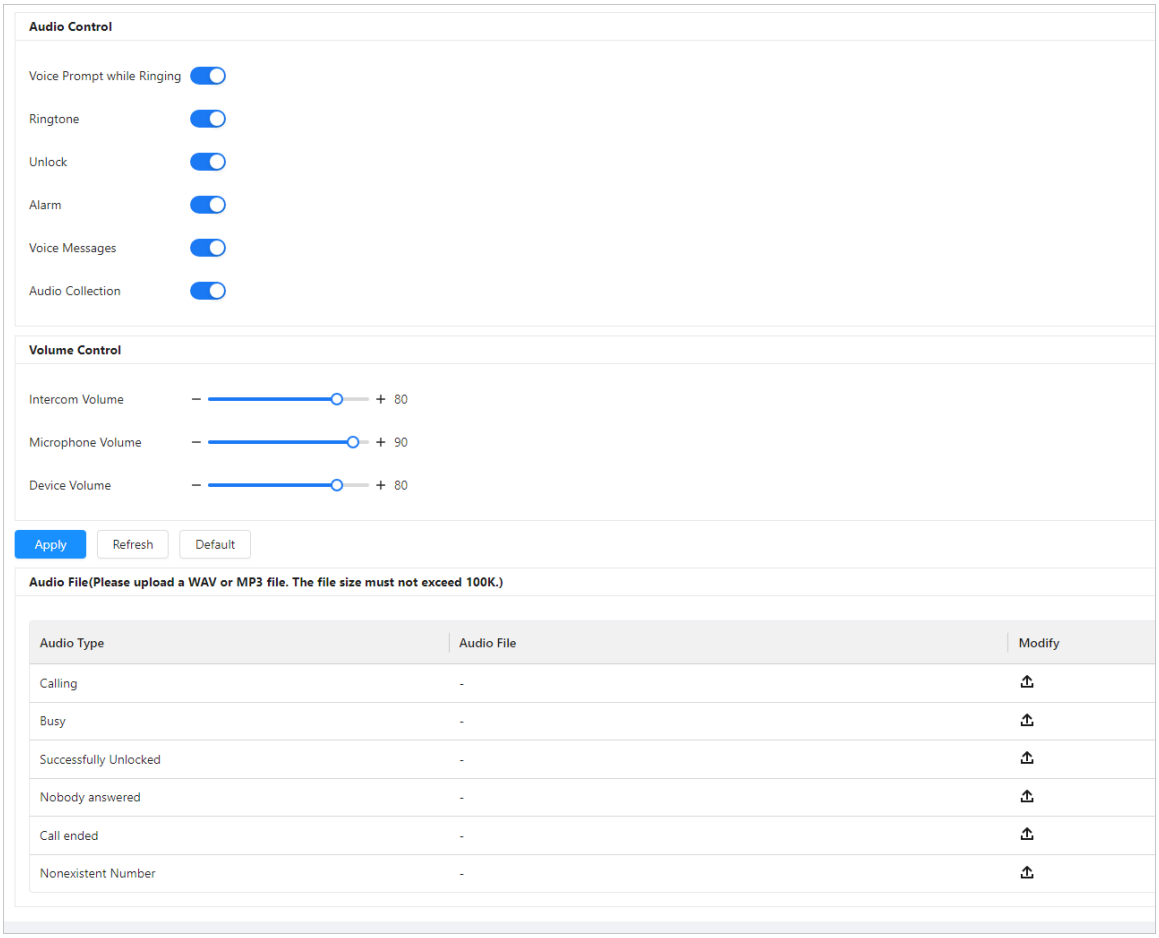


Table 10-3 Audio parameter description

Parameter		Description
Audio Control	Voice Prompt while Ringing	Enable or disable the corresponding audio feature or sound.
	Ringtone	
	Alarm	
	Voice Messages	
	Unlock	
	Audio Collection	
Volume Control	Microphone Volume	Adjust the microphone volume of the VTO. The higher the value is, the higher the volume will be.
	Intercom Volume	Adjust the speaker volume. The higher the value is, the higher the volume will be.

Parameter		Description
	Device Volume	Adjust the device volume. The higher the value is, the higher the volume will be.

Step 3 Click **Apply**.

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

Upload a WAV or MP3 file. The file size must not exceed 100 KB.

10.4 Time

Configure the time zone and daylight saving parameters.

Procedure

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

Step 2 Configure the time, time zone, and DST.

Figure 10-5 Time

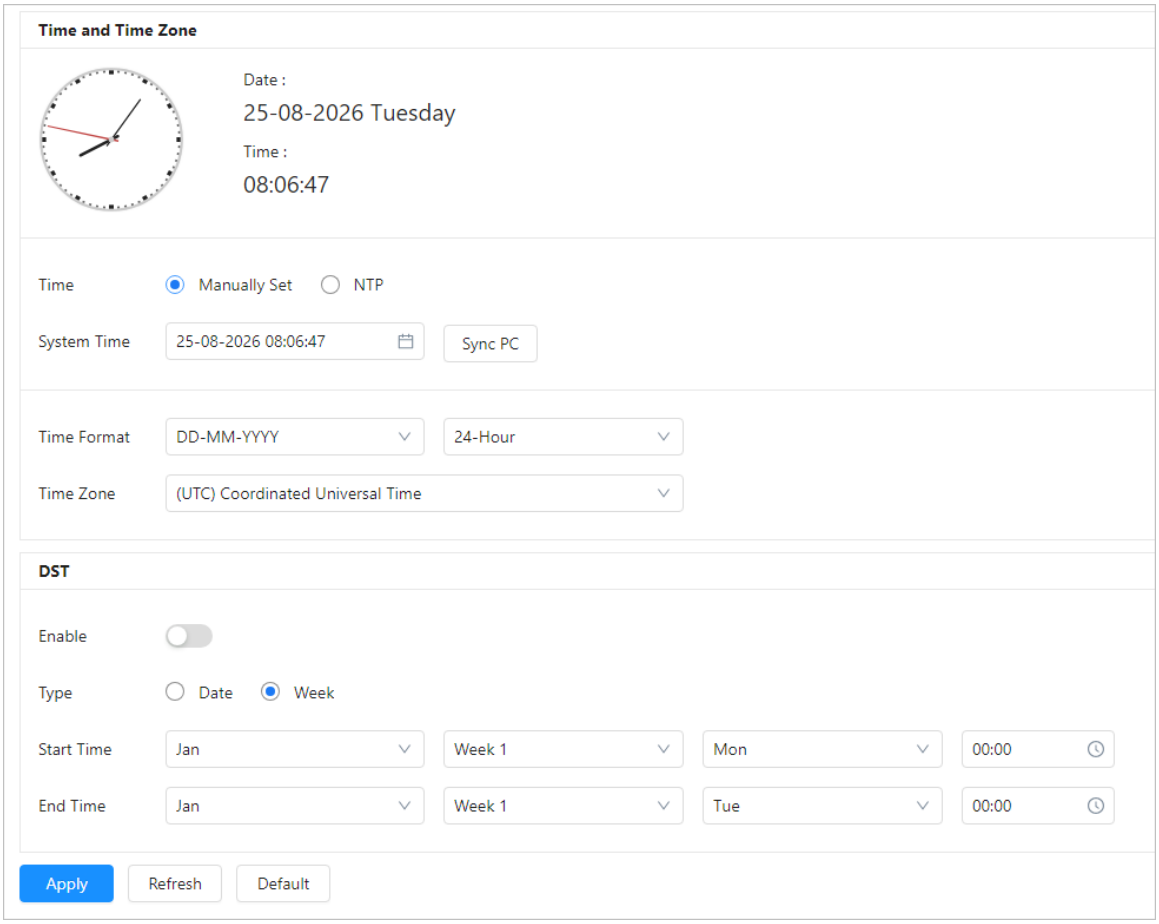


Table 10-4 Parameter description

Module	Parameter	Description
Time and Time Zone	Time	• Manually Set: Configure the time manually or synchronize with your computer. • NTP: Configure the NTP server parameters, and the time will be synchronized.
	System Time	The time of the VTO system. ⚠ Changing system time might cause problems with video searching and information publication. Turn off video recording and auto snapshot before changing it. 🕮 Only applicable in the **Manually Set** mode.
	Sync PC	Synchronize the VTO system time with your PC. 🕮 Only applicable in the **Manually Set** mode.
	Server	The address of the NTP server. 🕮 Only applicable in the **NTP** mode.
	Manual Update	Click the icon to automatically synchronize the VTO time with the NTP server. 🕮 Only applicable in the **NTP** mode.
	Port	NTP server port number. 🕮 Only applicable in the **NTP** mode.
	Interval	The VTO time synchronization interval. Maximum interval is 30 minutes. 🕮 Only applicable in the **NTP** mode.

Module	Parameter	Description
	Time Format	For the date format, Select one of the following date formats: • YYYY-MM-DD • MM-DD-YYYY • DD-MM-YYYY For the time format, select one of the following time formats: • 24-Hour • 12-Hour
	Time Zone	Select the time zone for the VTO system.
DST	Enable	Click to enable the **DST** function.
	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**.

10.5 ONVIF User

Add ONVIF user accounts so that devices can monitor the VTO through the ONVIF protocol.



Only Profile C and Profile S are supported, while encoding formats and image parameters are not supported.

Procedure

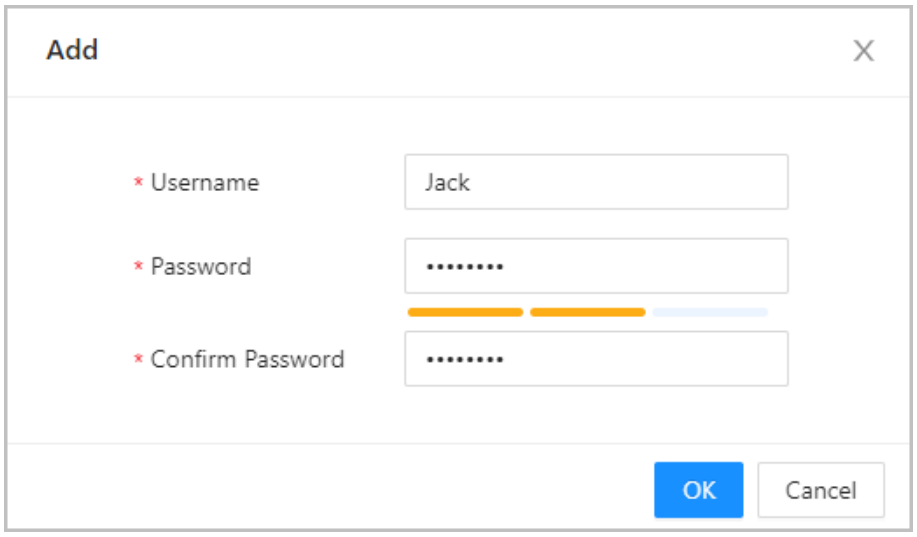
Step 1 Select **System** > **ONVIF User**.

Step 2 Click **Add**.

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

ONVIF devices can monitor the VTO using this account.

Figure 10-6 ONVIF user



11 Maintenance Center

11.1 One-Click Diagnosis

The system automatically diagnoses the configurations and the status of the device to help improve its performance.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **One-click Diagnosis**.

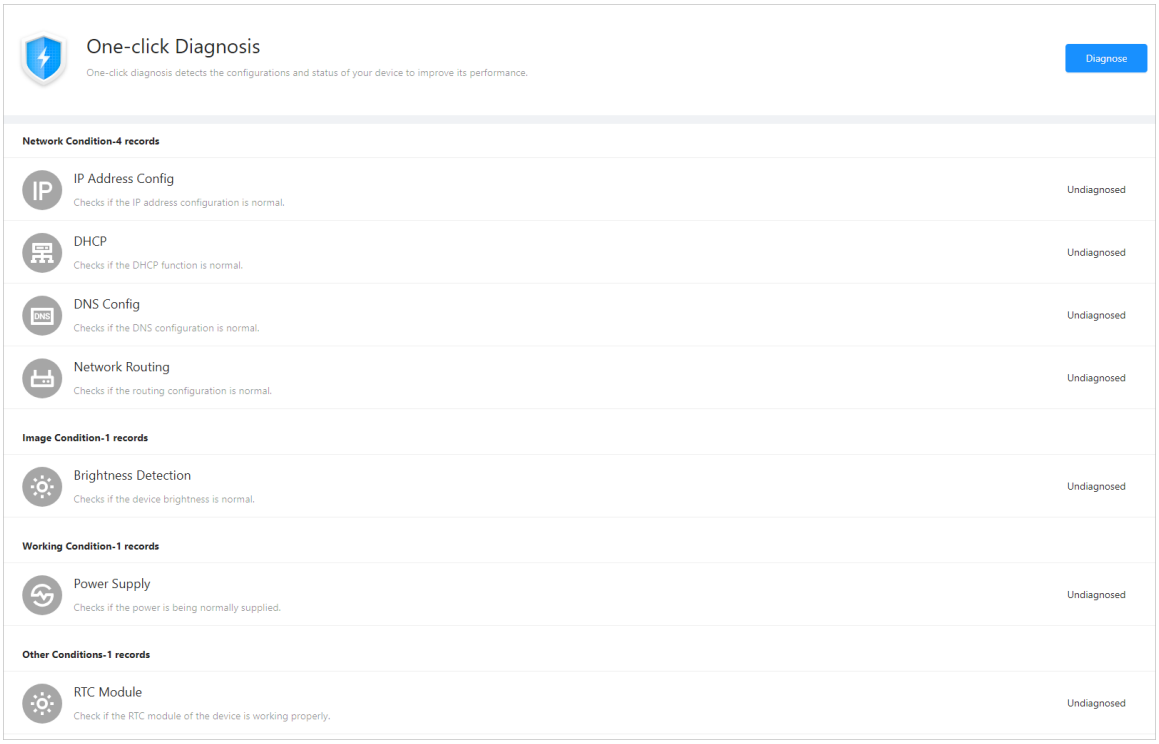
Step 3 Click **Diagnose**.

The system automatically diagnoses the configurations and the status of the device and displays the diagnostic results after the diagnosis is complete.

Step 4 (Optional) Click **Details** to view abnormal item details.

You can ignore the abnormality or optimize it. You can also click **Diagnose Again** to perform automatic diagnosis.

Figure 11-1 One-click diagnosis



11.2 System Information

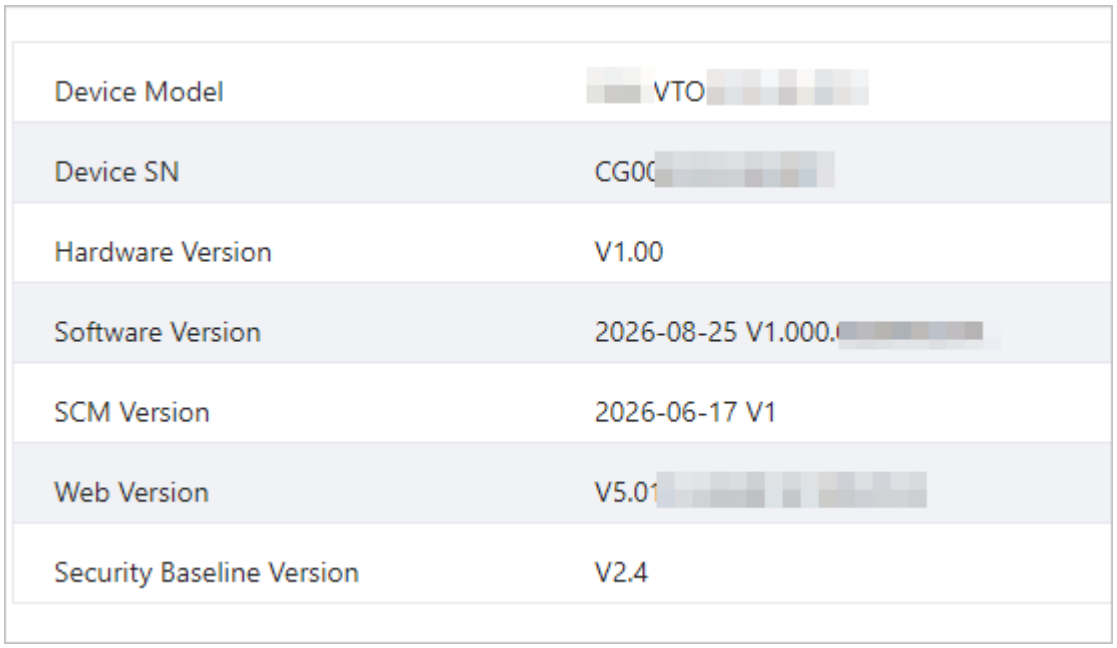
11.2.1 Version Information

Procedure

Step 1 Select **Maintenance Center** > **System Info** > **Version**.

Step 2 View the software version, SCM version and security baseline version.

Figure 11-2 System information



11.2.2 Legal Information

Select **Maintenance Center** > **System Info** > **Legal Info**. You can view related legal information notices.

11.3 Data Capacity

You can view the number of users and cards that the VTO can store.

Log in to the webpage and select **Maintenance Center** > **Data Capacity**.

11.4 Log Management

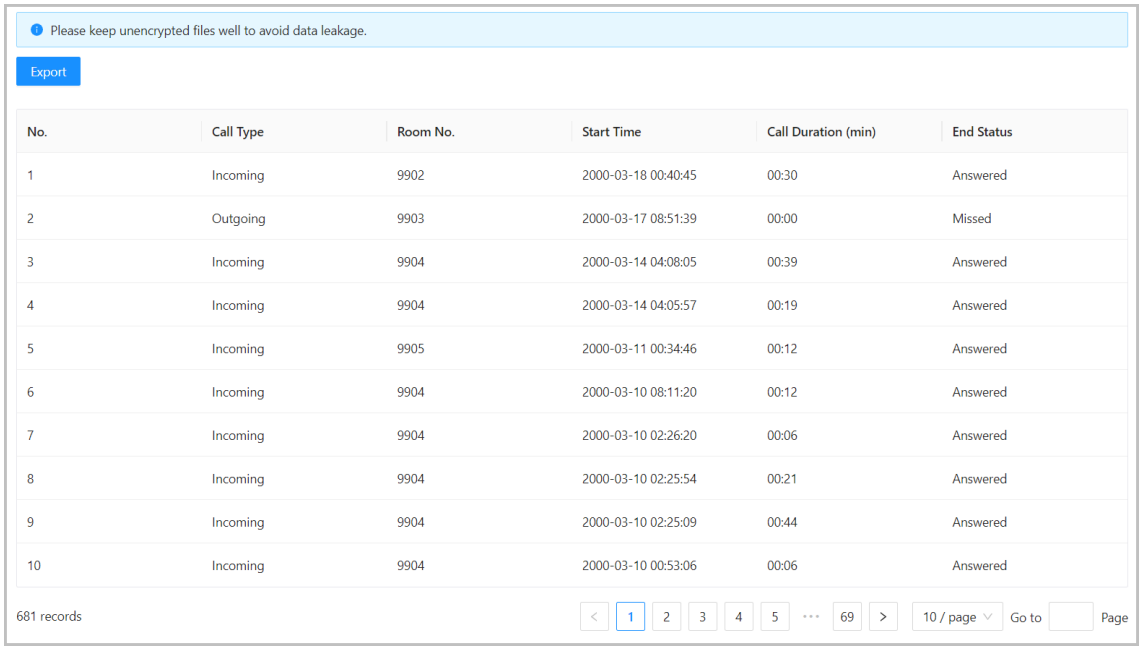
Select **Maintenance Center** > **Log**. You can search for different logs and export them to your local computer

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

11.4.1 Call History

Select **Maintenance Center** > **Log** > **Call History**.

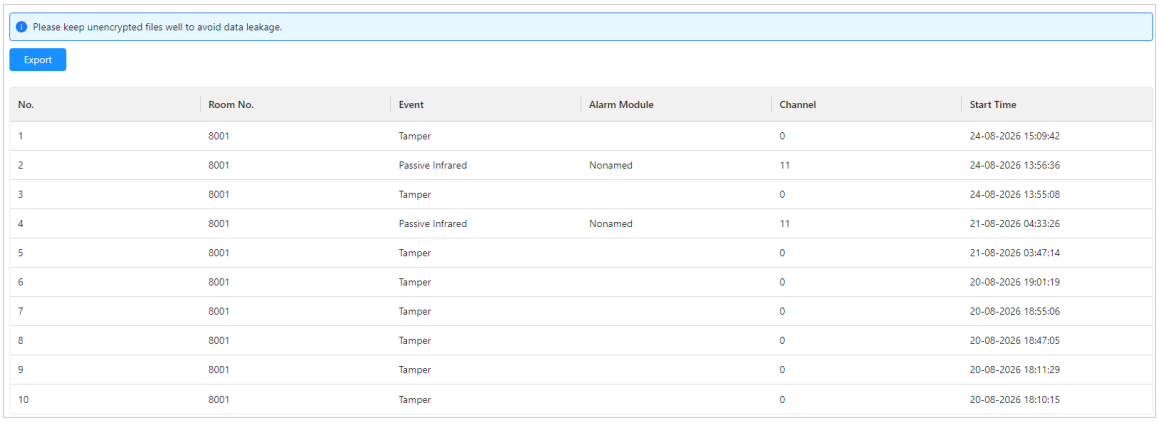
Figure 11-3 Call history



11.4.2 Alarm Logs

Select **Maintenance Center** > **Log** > **Alarm Logs**, and then view the alarm logs.

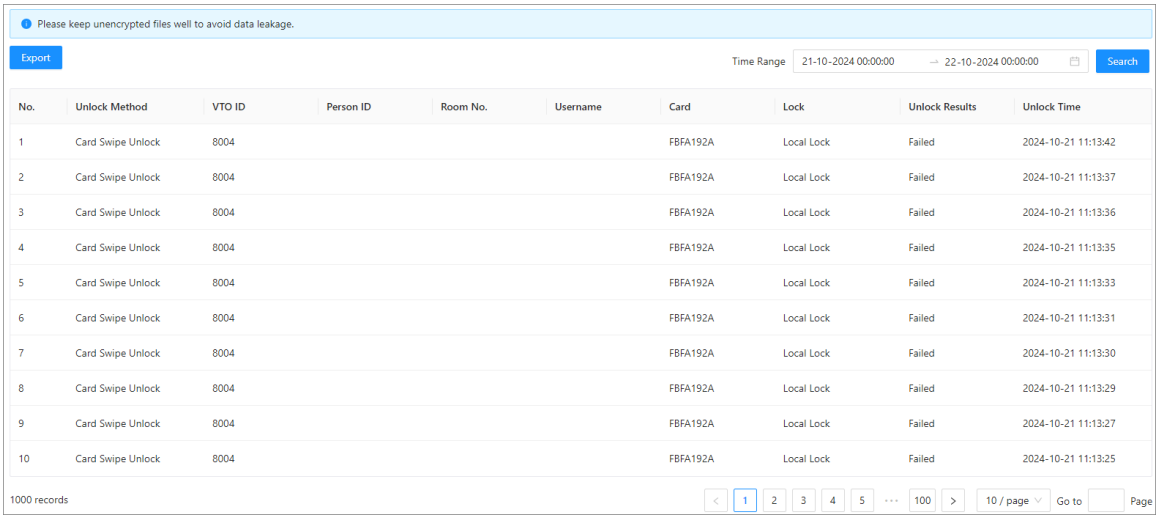
Figure 11-4 Alarm



11.4.3 Unlock Records

Select **Maintenance Center** > **Log** > **Unlock Records**, and then view the unlock records.

Figure 11-5 Unlock records



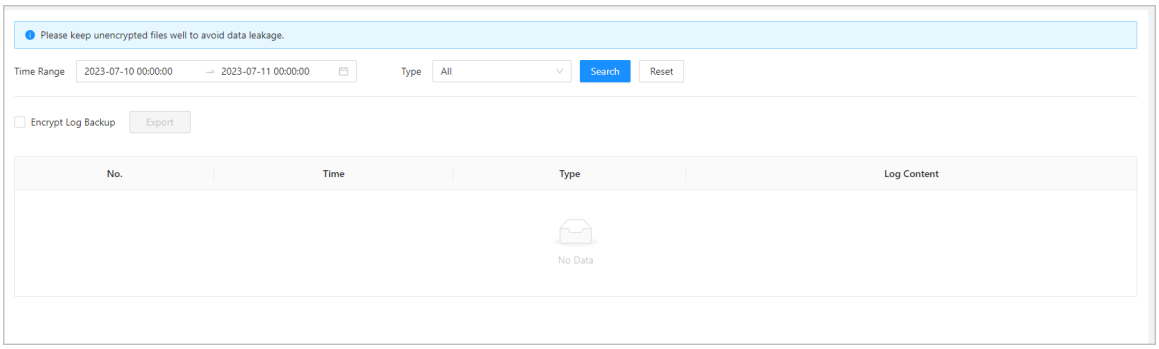
11.4.4 Log

Procedure

Step 1 Select **Maintenance Center** > **Log** > **Log**.

Step 2 Select a time range and a log type. The log information is displayed.

Figure 11-6 Log



11.4.5 Intelligent Records

Background Information

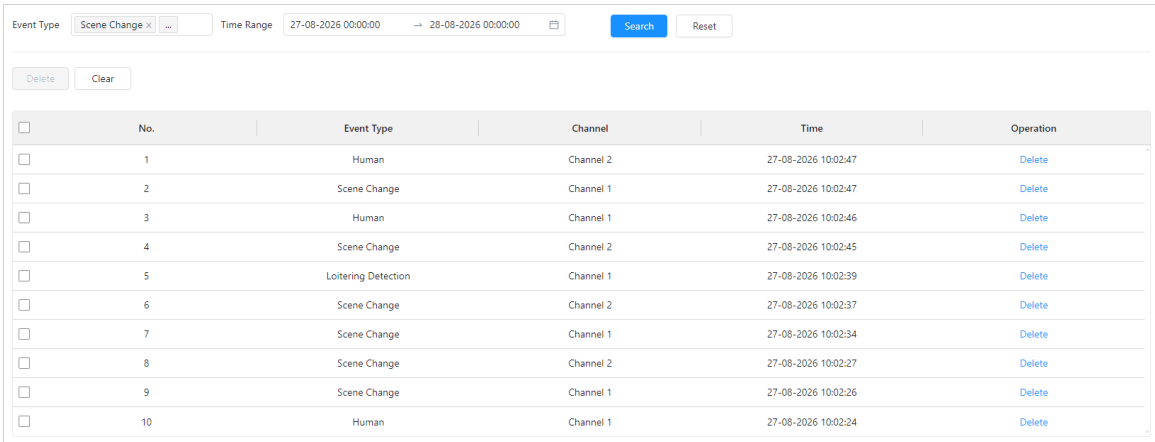
If you need to query the intelligent records and recordings, an SD card needs to be configured. It is recommended that the read and write speed of SD be greater than 10 MB/s. Otherwise, the records quality will be effected.

Procedure

Step 1 Select **Maintenance Center** > **Log** > **Intelligent Records**.

Step 2 Select the time range and type, click **Search** to view all intelligent records.

Figure 11-7 Intelligent records



Related Operations

- Delete one by one: Click **Delete** corresponding to the record to delete it.
- Delete in batches: Select more than one record, and then click **Delete** on the top to delete the selected records in batches.
- Clear the records: Click **Clear** to clear all records.

11.5 Maintenance Management

11.5.1 Config

You can import and export the configuration file for the device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

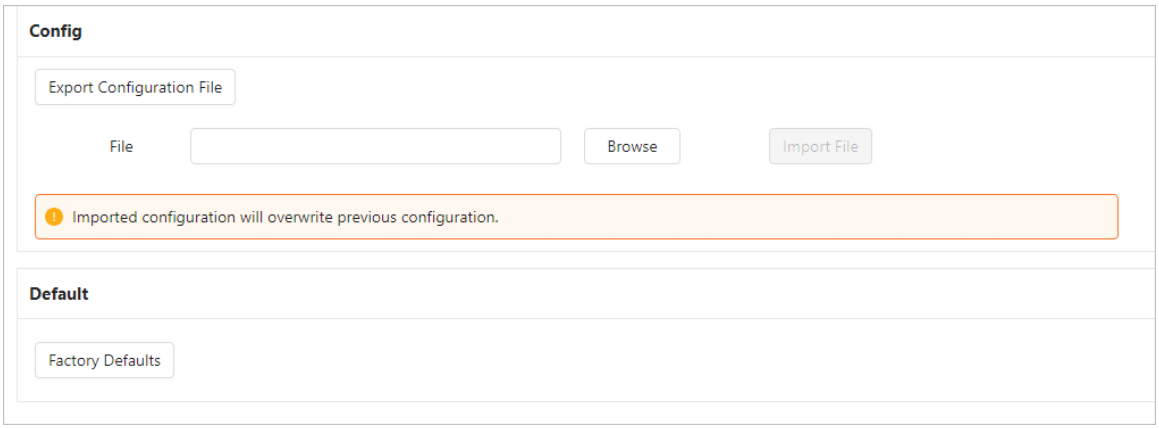
Step 1 Select **Maintenance Center** > **Maintenance Management** > **Config**.

Step 2 Export or import configuration files.

- Export the configuration file: Click **Export Configuration File** to download the file to the local computer.
- Import the configuration file:
  1. Click **Browse** to select the configuration file.
  2. Click **Import File**.

Configuration files can only be imported to devices that have the same model.

Figure 11-8 Configuration



Step 3 (Optional) Click **Factory Defaults** to set the device to its default settings.

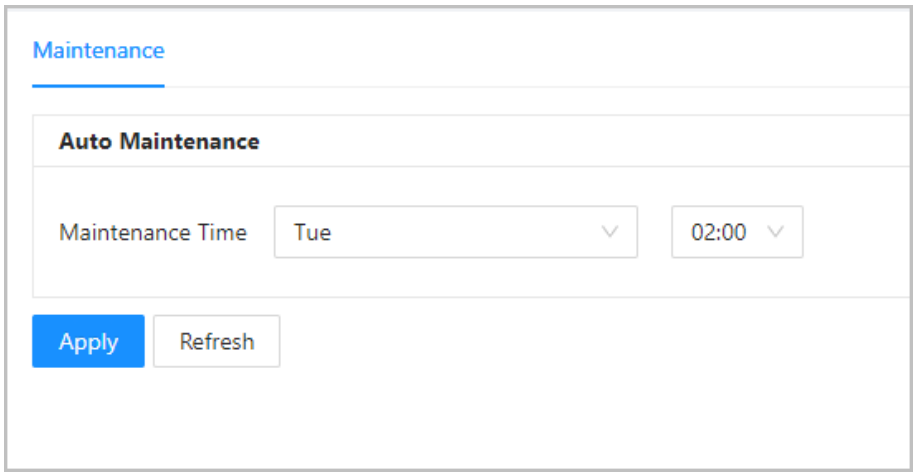
11.5.2 Maintenance

Procedure

Step 1 Select **Maintenance Center** > **Maintenance Management** > **Maintenance**.

Step 2 Configure the auto maintenance time.

Figure 11-9 Auto maintenance



Step 3 Click **Apply**.

11.6 Update

Procedure

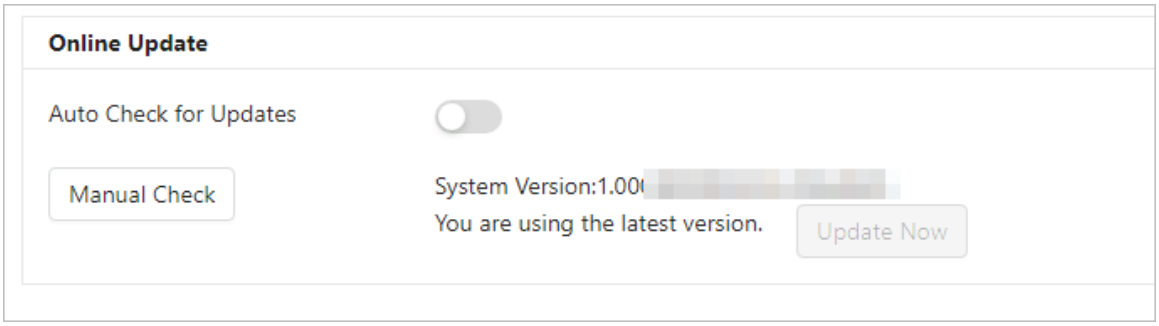
Step 1 Select **Maintenance Center** > **Update**.

Step 2 Select an update method.

- **File Update** : Click **Browse** to add an update file, and then click **Update**.
- **Online Update**

- **Auto Check for Updates** : Enable it to automatically check for new system versions.
- **Manual Check** : Select **Manual Check** to check for new system versions.

Figure 11-10 Online update



11.7 Advanced Maintenance

Export

Select **Maintenance Center** > **Advanced Maintenance** > **Export**, and then click **Export** to export the serial number, firmware version, device operation logs and configuration information.

Packet Capture

1. Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.
2. Enter the device port.
3. Click ▶ to start the packet capture.

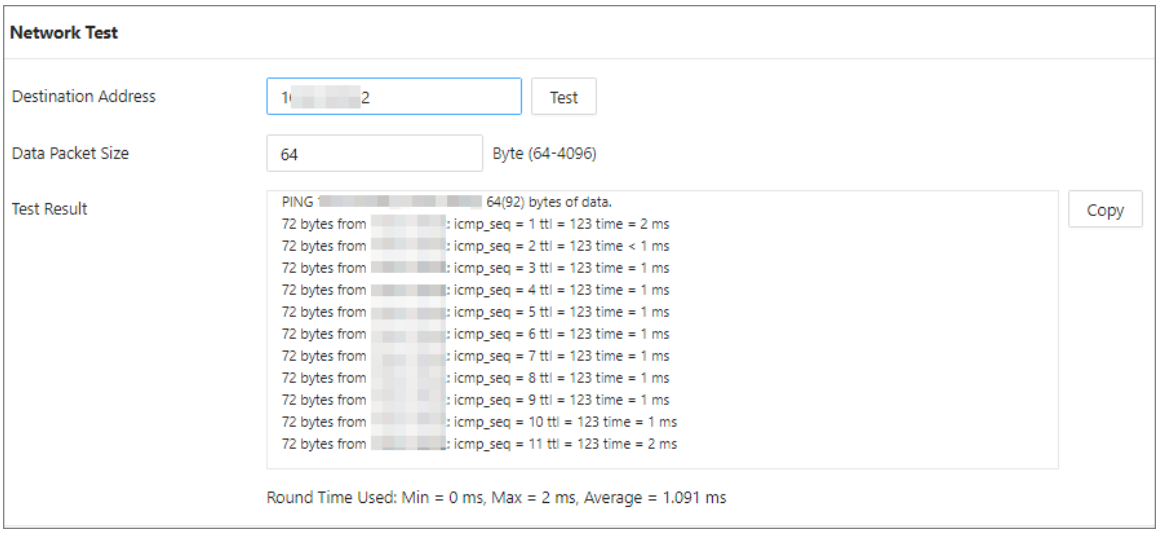
Figure 11-11 Packet capture



Network Test

1. Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.
2. In the **Network Test** area, test the network as needed.
   a. Enter the destination address in the destination address box, and then click **Test**.
   b. After you have collected enough data, click **Stop** and view the test result in the result box.
   c. Click **Copy** to copy the test result.

Figure 11-12 Test network

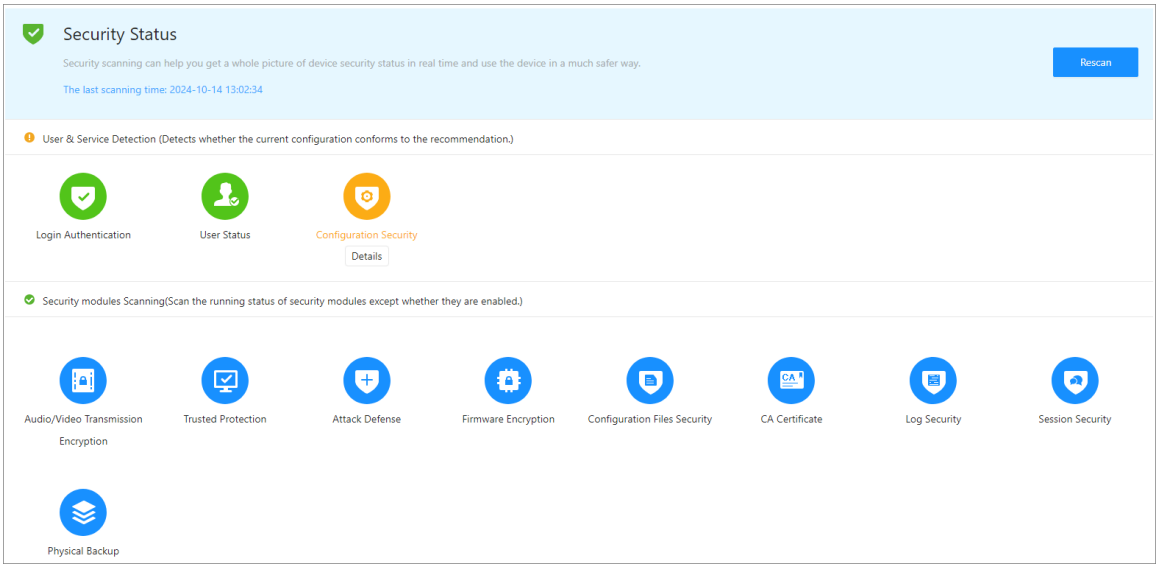


12 Security Management

12.1 Security Status

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

Figure 12-1 Security status



12.2 System Service

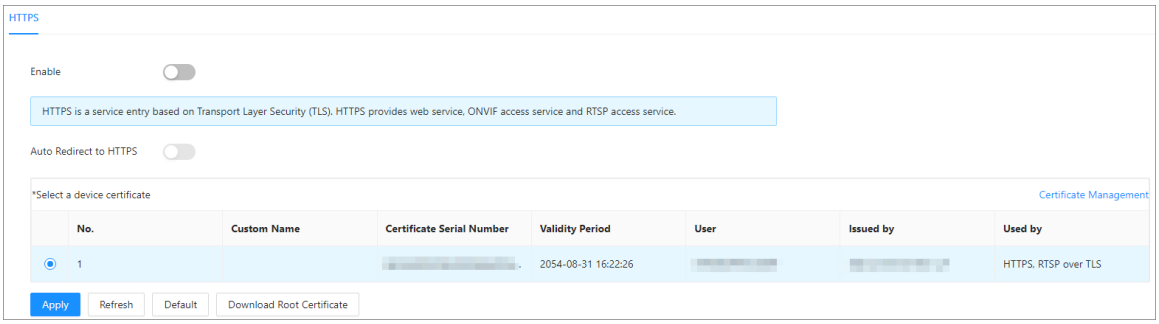
Procedure

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

Step 2 Select a device certificate.

Step 3 Enable the HTTPS function.

Figure 12-2 System service



Step 4 Click **Apply**.

12.3 Attack Defense

12.3.1 Firewall

You can configure firewall modes to control network access to the VTO.

Procedure

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

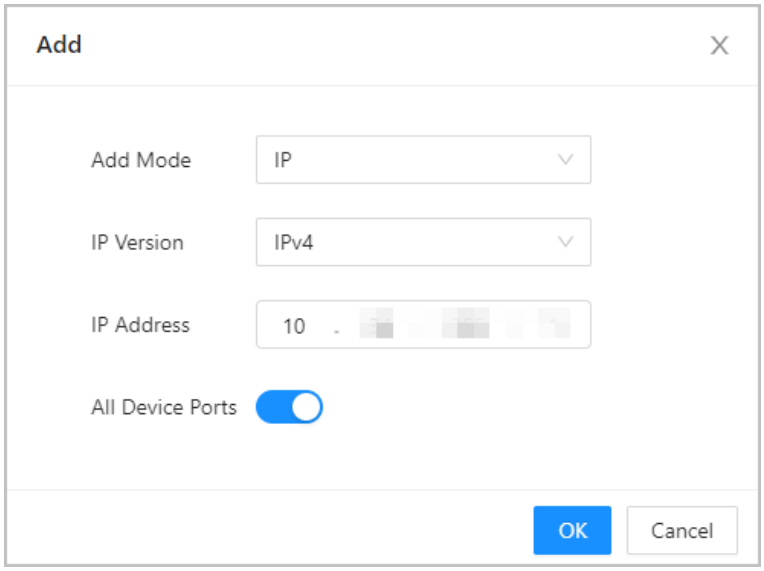
Step 2 Click next to **Enable**.

Step 3 Set the **Mode** to **Allowlist** or **Blocklist**.

- Allowlist: Devices that have been granted access.
- Blocklist: Devices that have been denied access.

Step 4 Click **Add** to add an IP address to the allowlist or blocklist.

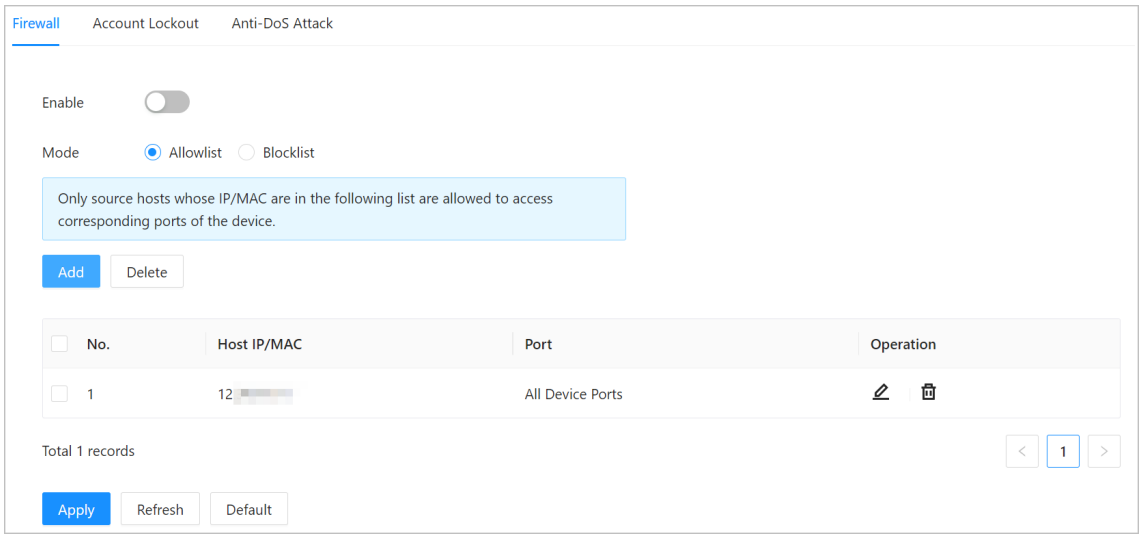
Figure 12-3 Add



Step 5 Click **OK**.

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

Figure 12-4 Apply



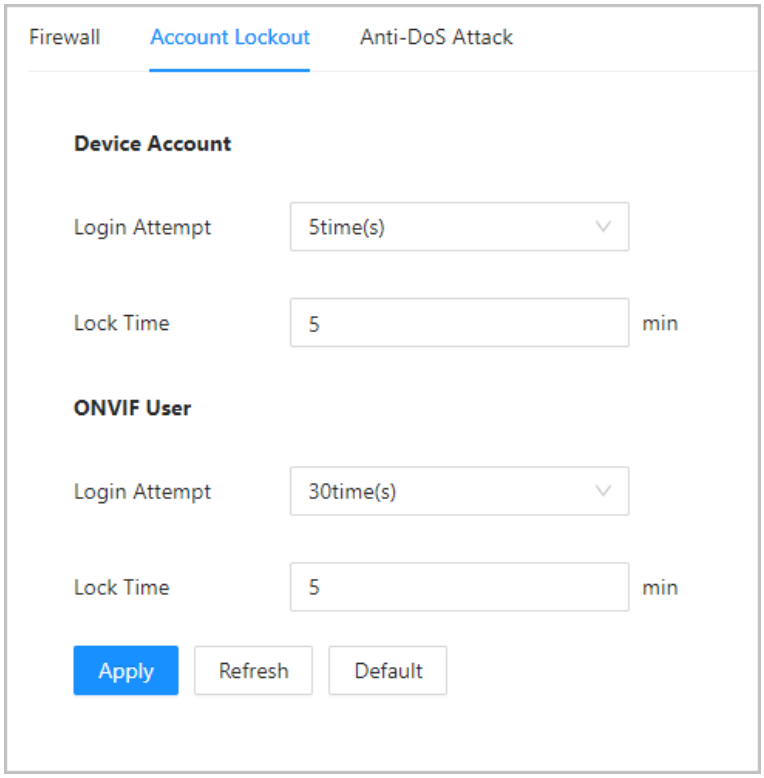
12.3.2 Account Lockout

Procedure

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

Step 2 Configure the login attempts and lock time for the device account and the ONVIF user.

Figure 12-5 Account lockout



Step 3 Click **Apply**.

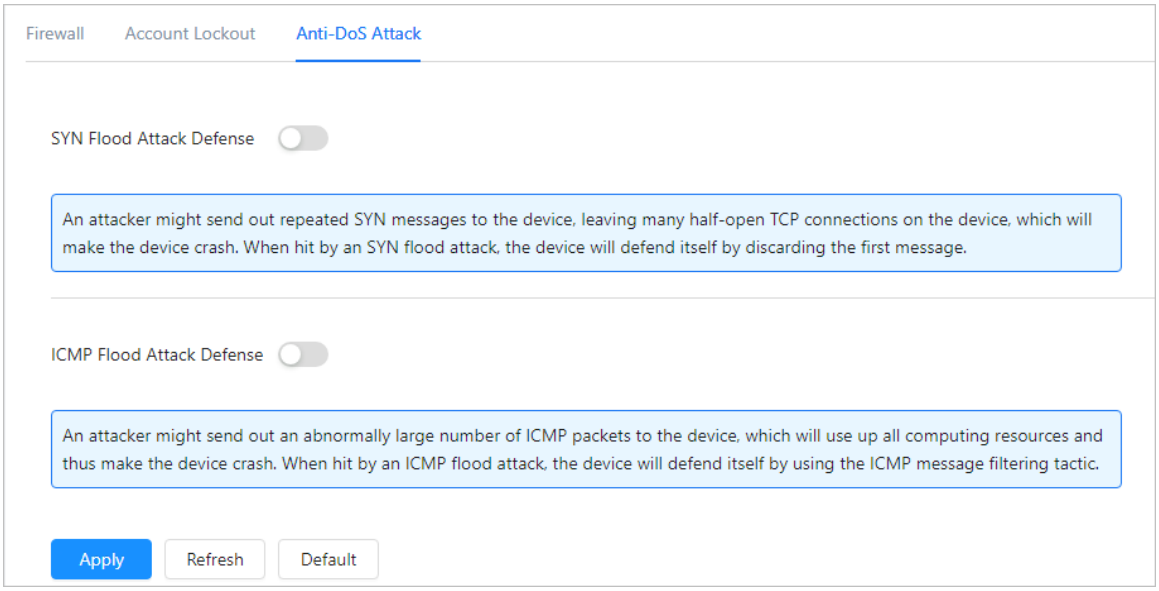
12.3.3 Anti-DoS Attack

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** functions.

Figure 12-6 Anti-DoS attack



Step 3 Click **Apply**.

12.4 CA Certificate

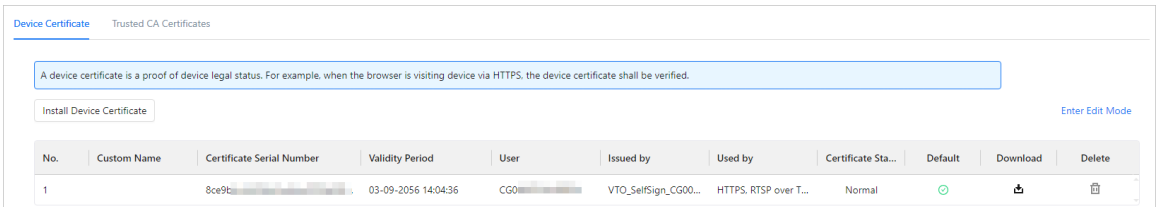
Procedure

Step 1 Log in to the web manager.

Step 2 On the home page, click , and then select **CA Certificate**.

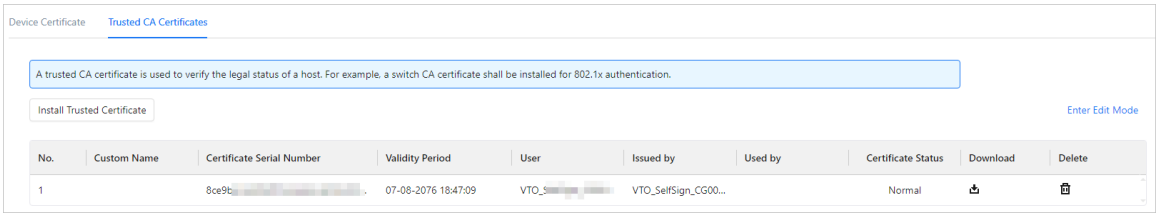
- Device certificate

Figure 12-7 Device certificate



- Trusted CA certificates

Figure 12-8 Trusted CA certificates



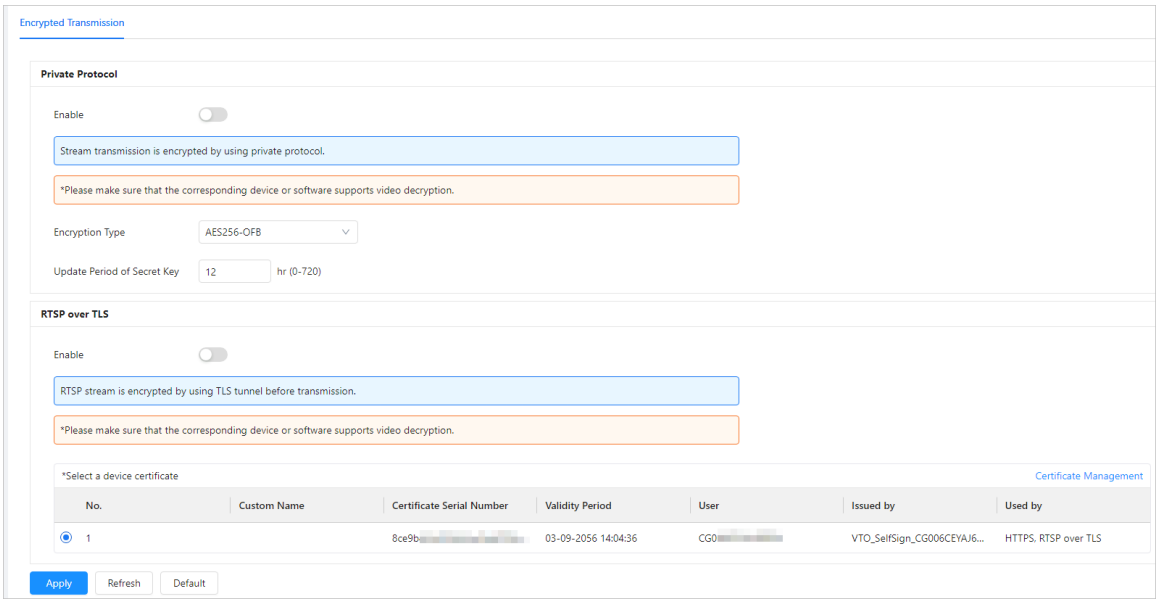
12.5 Video Encryption

Procedure

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

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

Figure 12-9 Video encryption



Step 3 Click **Apply**.

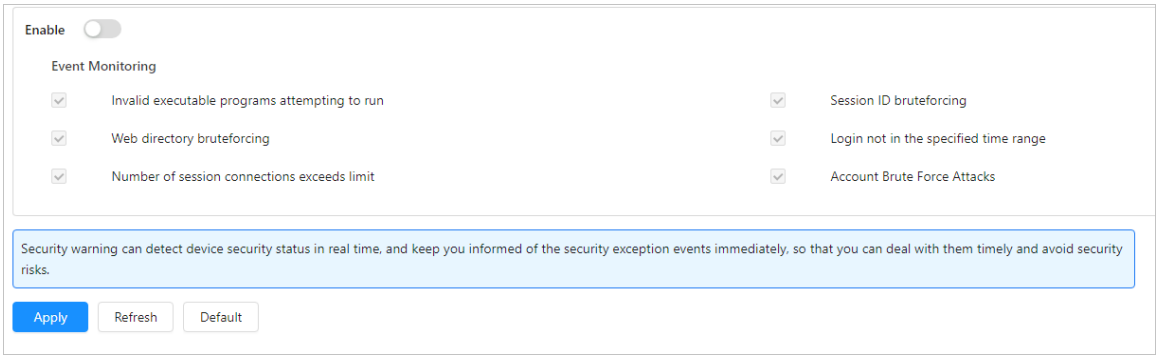
12.6 Security Warning

Procedure

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

Step 2 Enable the event monitoring function.

Figure 12-10 Security warning



Step 3 Click **Apply**.

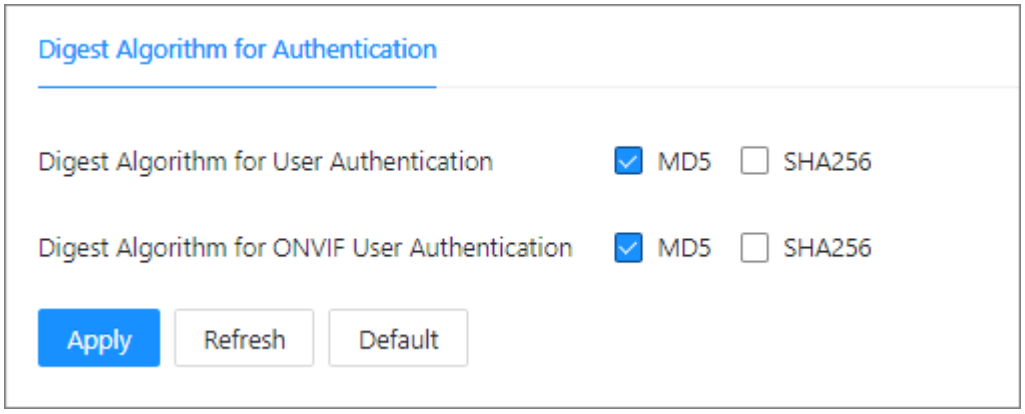
12.7 Security Authentication

Procedure

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

Step 2 Configure the digest algorithm for authentication, and then click **Apply**.

Figure 12-11 Security authentication



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 Allowlist**

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

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;
   - Establish 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).