Digital VTS

User's Manual

V1.0.0

Foreword

This manual introduces the configurations on local VTS and webpage. Read carefully before using the VTS, 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 Time
V1.0.0	First release.	November 2024

Privacy Protection Notice

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

About the Manual

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

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important 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

- Do not connect the power adapter to the device while the adapter is powered on.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Please follow the electrical requirements to power the device.
  - Following are the requirements for selecting a power adapter.
    - 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.
  - We recommend using the power adapter provided with the device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.

- 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.

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

1 Device Structure

1.1 Front Panel

Figure 1-1 Front panel

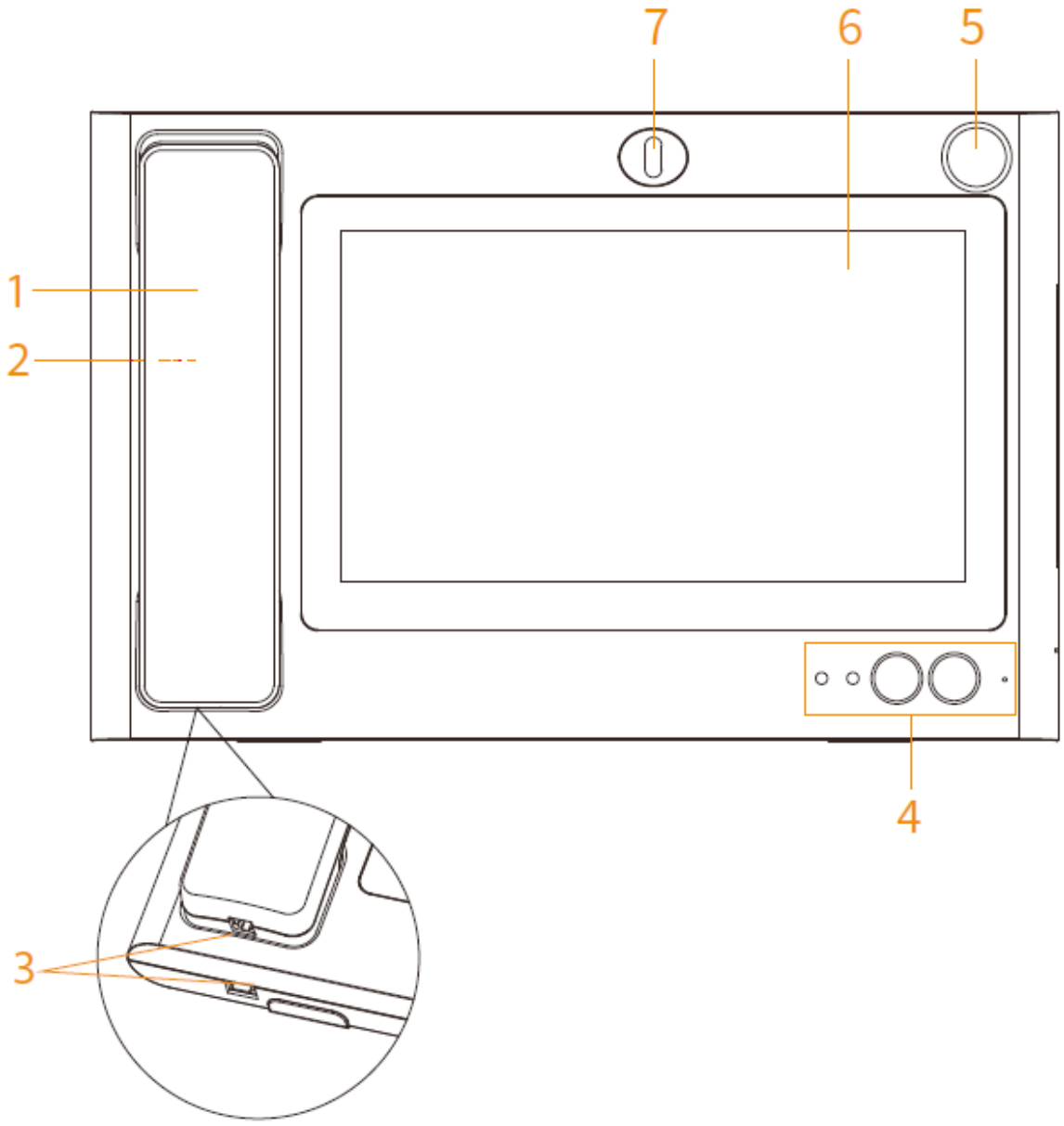


Table 1-1 Front panel description

No.	Name	Description
1	MIC	If you lift MIC, audio and pickup are both converted into MIC.
2	Speaker	Outputs sound.
3	RJ-11 Port	Connects VTS and MIC using the telephone cord.

No.	Name	Description
4	Indicator/Button	From left to right: • Power indicator ◇ On: The device is powered on. ◇ Off: The device is not connected to the power supply. • Information indicator ◇ On: There is a missed call. ◇ Off: The missed call has been processed or there is no missed call. In the industrial scene, if the indicator is on, it indicates that the device has unread alarm records. • Unlock button When you are making calls, watching videos, or talking to others through the VTS, press the unlock button, you can remotely open the door of some front-end devices that support unlocking function. • Hands-free button Used to answer incoming calls. You can select hands free mode or handset mode. • Built-in MIC Inputs sound.
5	Gooseneck Microphone Port	Connects to a gooseneck microphone. The port is available on select models.
6	Display and Touch	Screen and touch area.
7	Camera	Used to talk with another VTS or the platform. The camera is available on select models.

1.2 Rear Panel

Figure 1-2 Rear panel

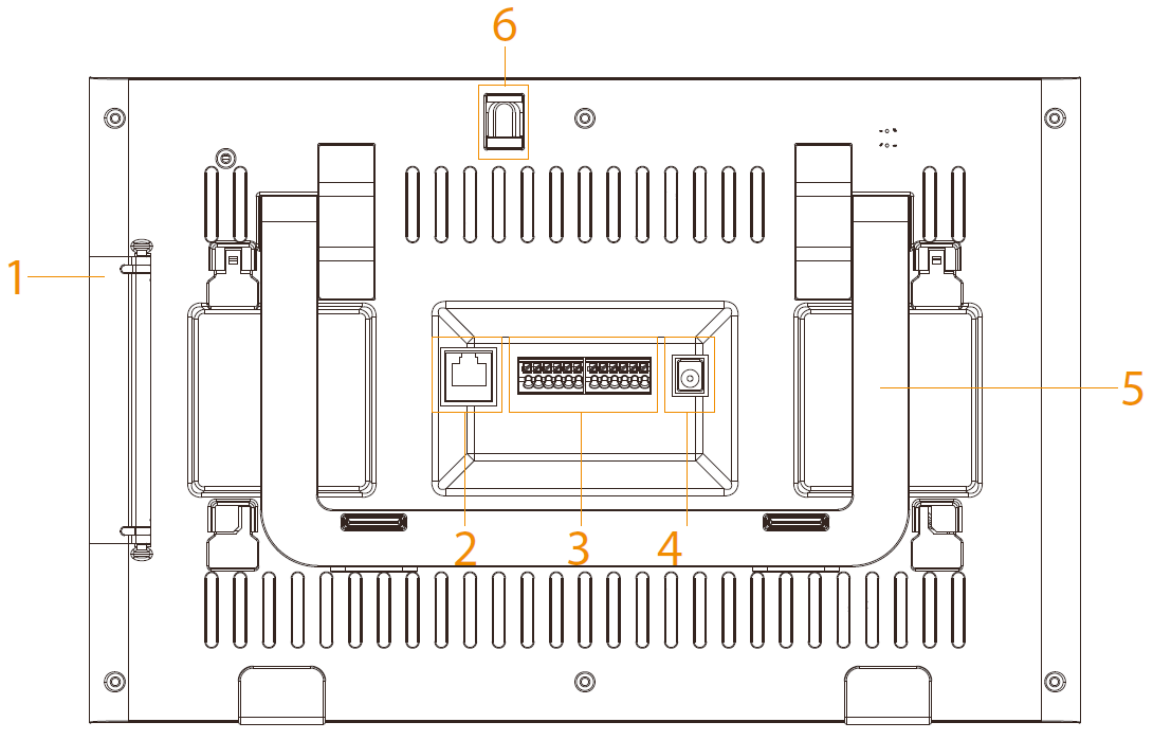


Table 1-2 Rear panel description

No.	Name	Description
1	Port	Open the rear panel and the ports from top to bottom are: ● HDMI video transmission port, for video transmission only. ● USB port. ● USB port. ● SD card slot.
2	Network Port	Connects RJ-45 cable. We recommend you use FTP (Foil Twisted-Pair).

No.	Name	Description
3	12-pin Port	Ports from left to right are: • Power output port. • GND. • Alarm input port 1. • Alarm input port 2. • Alarm input port 3. • Alarm input port 4. • Power input port. • GND. • RS-485A port. • RS-485B port. • Alarm output port NO. • Alarm output port COM.
4	Power Port	12 VDC power.
5	Bracket	Place VTS on the desk. You can adjust the bracket angle to an appropriate position for monitoring.
6	Camera Knob	You can adjust the knob to an appropriate angel for monitoring. You can also hide the camera by adjusting the knob. The knob is available on select models.

2 Initializing VTS

You can initialize VTS through the local device or through the webpage.

2.1 Initialization through Local Device

Procedure

Step 1 Power on the VTS.

Step 2 Select the language.

Step 3 Enter the password and e-mail address.

Step 4 Select **I have read and agree to all the terms Privacy, Software License Agreement** , and then tap **Next**.

Step 5 Select the scene depending on your needs.

Figure 2-1 Initialization through local device

Step 6 Tap **Complete**.

2.2 Initialization through Webpage

Prerequisites

Make sure that the computer is on the same network segment as VTS.

Procedure

Step 1 Enter the IP address of VTS in a browser, and then click **Enter**.

Step 2 Select the language.

Step 3 If there are agreements, select **I have read and agree to the terms and conditions and accept privacy policy and license agreement** , and then click **Next**.

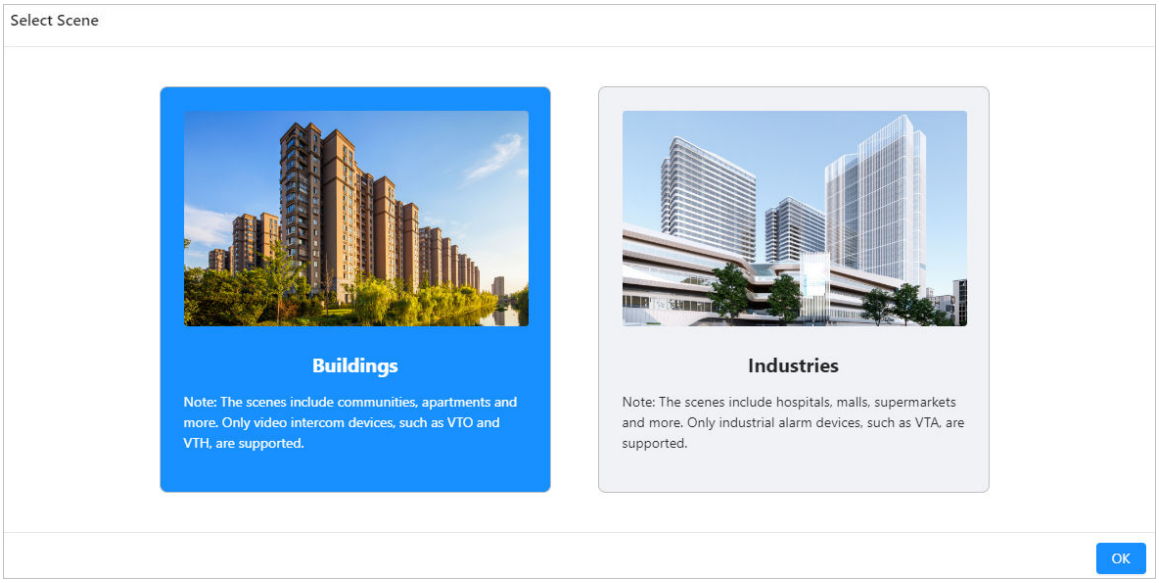
Step 4 Enter the password and e-mail address, and then click **Completed**.

Step 5 (Optional) Select **Auto Check for Updates** and **Cloud Service** as needed, and then click **Completed**.

Step 6 Enter the username and password, and then click **Login**.

Step 7 Select the scene, and then click **OK**.

Figure 2-2 Select scene



3 Building Scenes

3.1 Operations on Local Device

3.1.1 Local Screen

Figure 3-1 Local screen

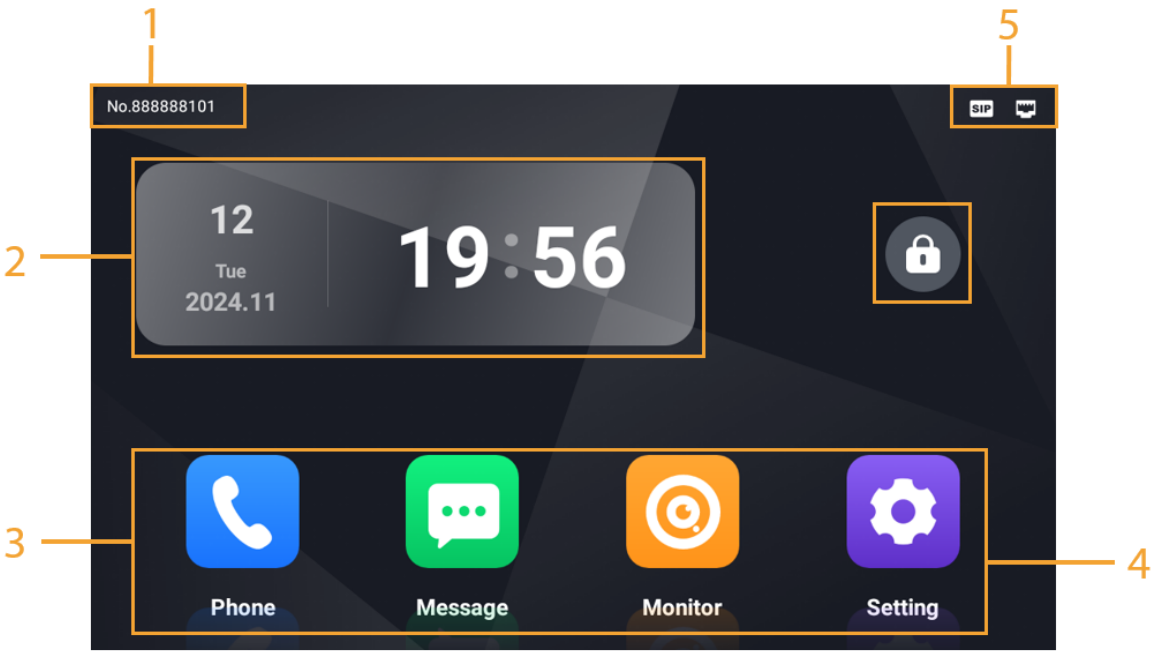


Table 3-1 Home screen introduction

No.	Description
1	The number of VTS.
2	Date and time.
3	Function buttons. • Phone: Call VTH and check the call history. For details, see "3.1.8.1 Call". • Message: Check the video playback and screenshots. For details, see "3.1.8.2 Checking the Information". • Monitor: Monitor VTH, VTO and IPC. For details, see "3.1.8.3 Monitoring". • Setting: Enter the setting screen of VTS.

No.	Description
4	Tap  to lock the screen. If you select **Setting** > **Display Settings**, and turn on **Lock Screen** , you need to enter the default password **123456** to unlock the screen when you lock it after the configuration.
5	The connection status of the network, the SIP server, and the SD card.

3.1.2 Configuring the Display Parameters

Configure the brightness and screen turn-off time. Turn on or turn off **Lock Screen**.

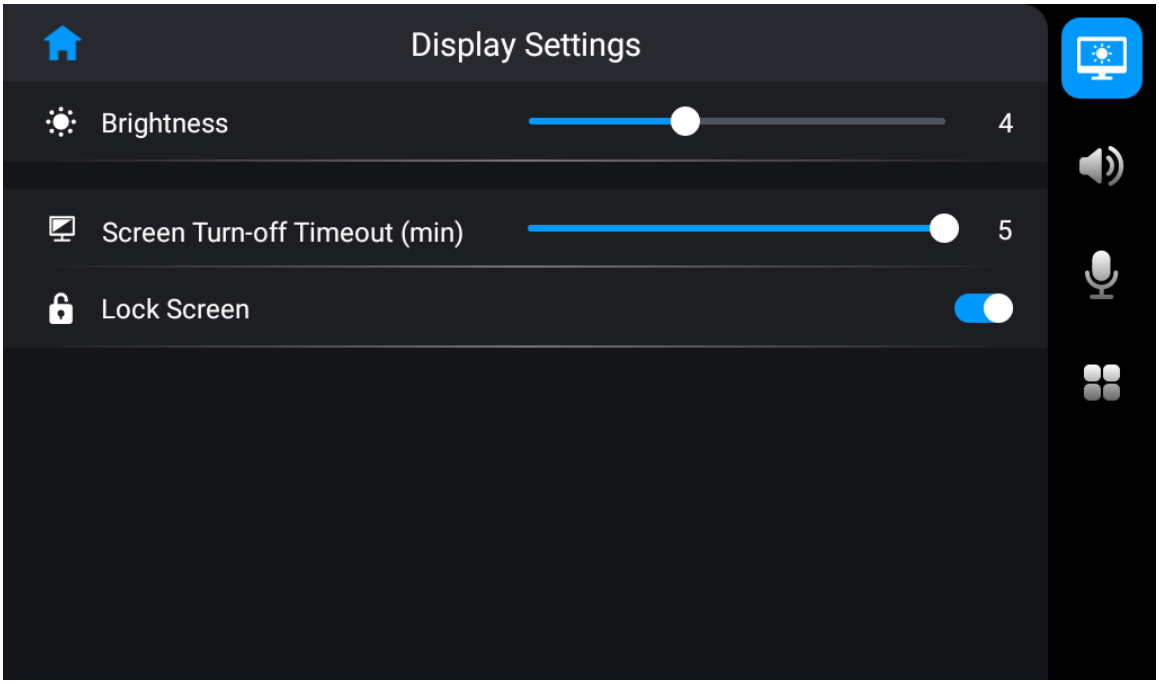
Procedure

Step 1 On the home screen, select **Setting** >  .

Step 2 Configure the parameters.

Lock screen: After turning on the function, if you need to unlock the screen again, enter the default password **123456**.

Figure 3-2 Display settings



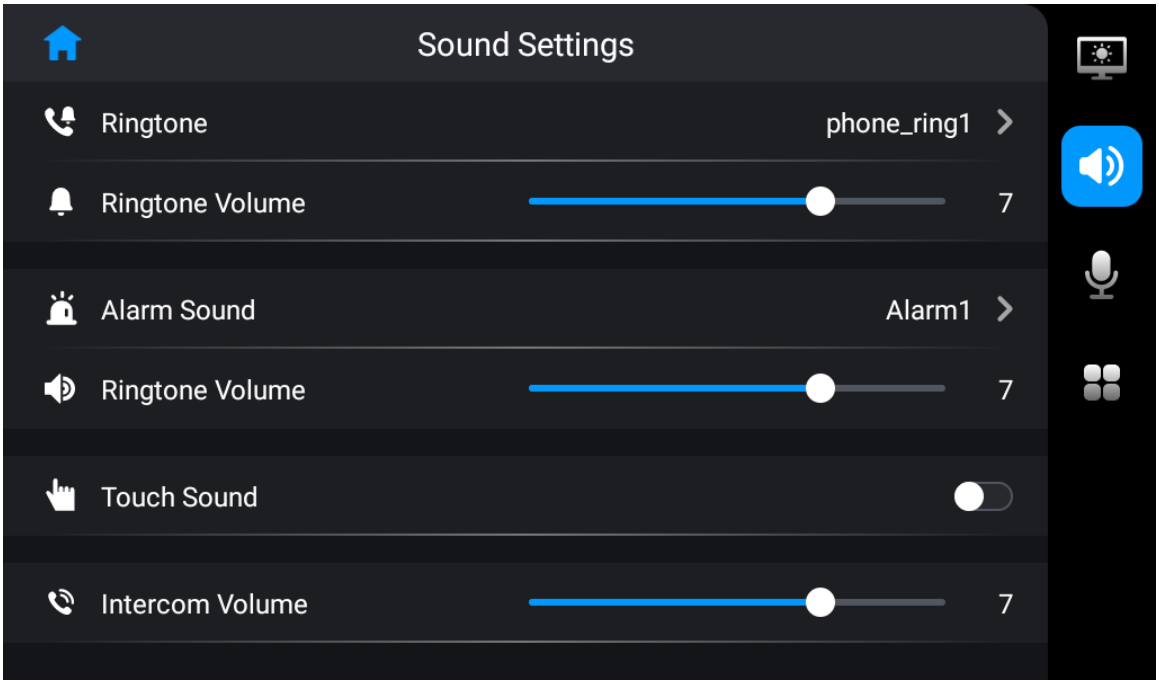
3.1.3 Configuring the Sound Parameters

Procedure

Step 1 On the home screen, select **Setting** >  .

Step 2 Configure the parameters.

Figure 3-3 Sound settings



3.1.4 Configuring the Intercom Parameters

Configure the ringtone and call limit of VTO and VTH, and the monitoring time.

Procedure

Step 1 On the home screen, select **Setting** >  .

Step 2 Configure the parameters.

Figure 3-4 Intercom settings

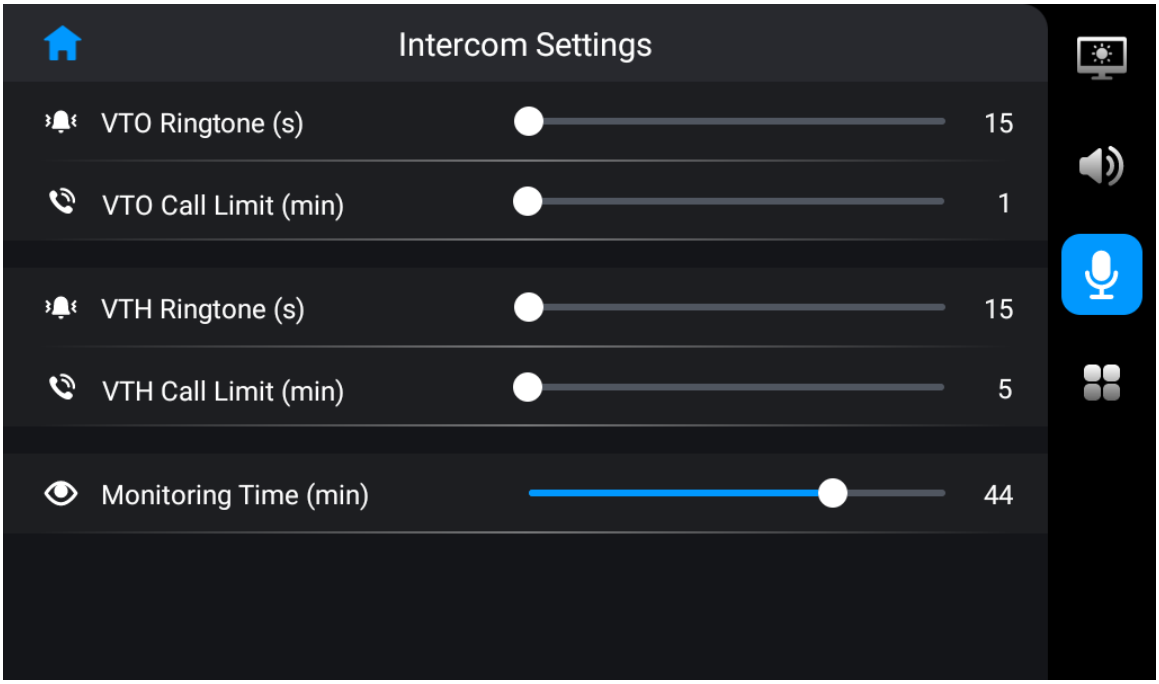


Table 3-2 Description of intercom parameters

Parameter	Description
VTO Ringtone (s)	The call from VTO stops ringing after the time you set.
VTO Call Limit (min)	VTO automatically hangs up the call to VTS after the time you set.
VTH Ringtone (s)	The call from VTH stops ringing after the time you set.
VTH Call Limit (min)	VTH automatically hangs up the call to VTS after the time you set.
Monitoring Time (min)	The time that VTS monitor VTO and other devices.

3.1.5 Configuring the Advanced Parameters

Procedure

Step 1 On the home screen, select **Setting** > .

Step 2 Configure the parameters.

Figure 3-5 Advanced settings

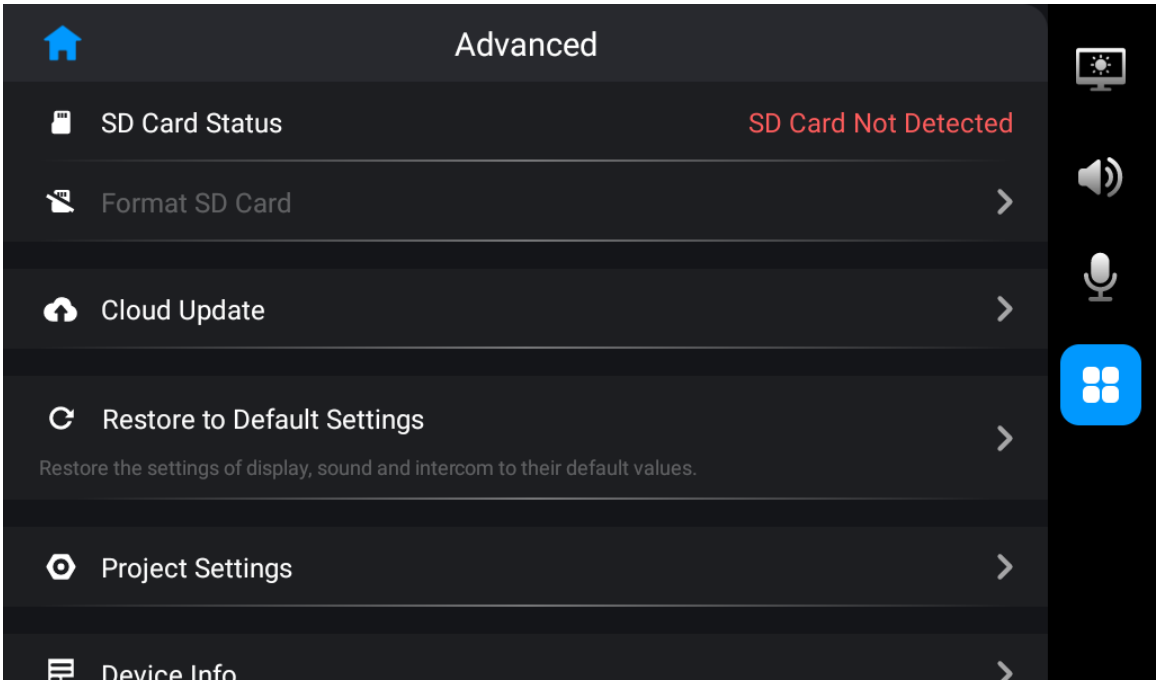


Table 3-3 Advanced settings description

Parameter	Description
SD Card Status	Check the used capacity and the total capacity of the SD card if there is a SD card in VTS. System of numeration differs in Android system and Windows system when converting the capacity. So the capacity of the SD card displayed on VTS is larger than that displayed on the computer.
Format SD Card	Supports formatting the SD card.
Cloud Update	Check the latest version through the interactions with the cloud, and then update online.
Restore to Default Settings	Restore the display, sound and intercom settings to default settings.
Project Settings	Enter the initial password to enter the project settings screen. For details, see "3.1.7 Project Settings".
Device Info	View the legal information, version and security baseline version of VTS.

3.1.6 Resetting Password

You can reset the password through the linked e-mail address.

Prerequisites

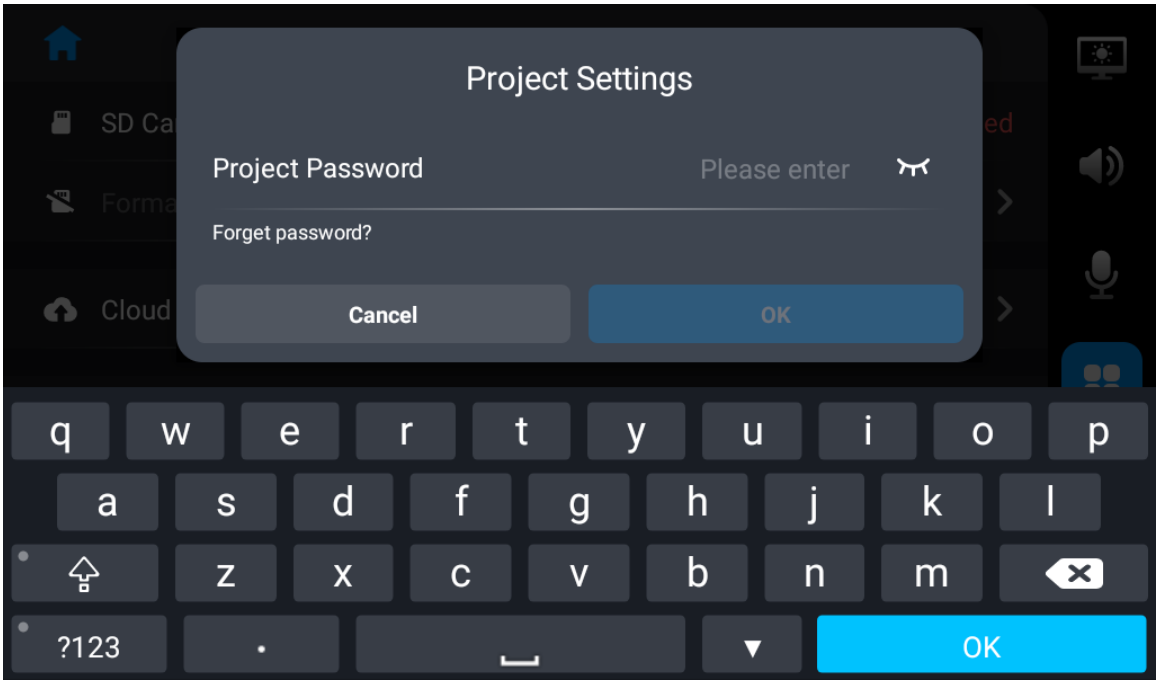
Make sure that you have turned on **Reset Info** in **Project Settings**. For details, see "3.1.7.2.2 Resetting Information".

Procedure

Step 1 On the home screen, select **Setting** >  > **Project Settings**.

Step 2 Tap **Forget password?** , and then tap **OK**.

Figure 3-6 Reset password



Step 3 Get the **Security Code** according to the instructions, and then enter the new password and security code.

Step 4 Tap **OK**.

3.1.7 Project Settings

3.1.7.1 Configuring VTS

Configure the number and network parameters of VTS.

Procedure

Step 1 Select **Settings** >  > **Project Setting** on the home screen.

Step 2 Enter the password that you configured during initialization and tap **OK**.

Step 3 Tap  and configure the parameters.

Figure 3-7 Configure the parameters

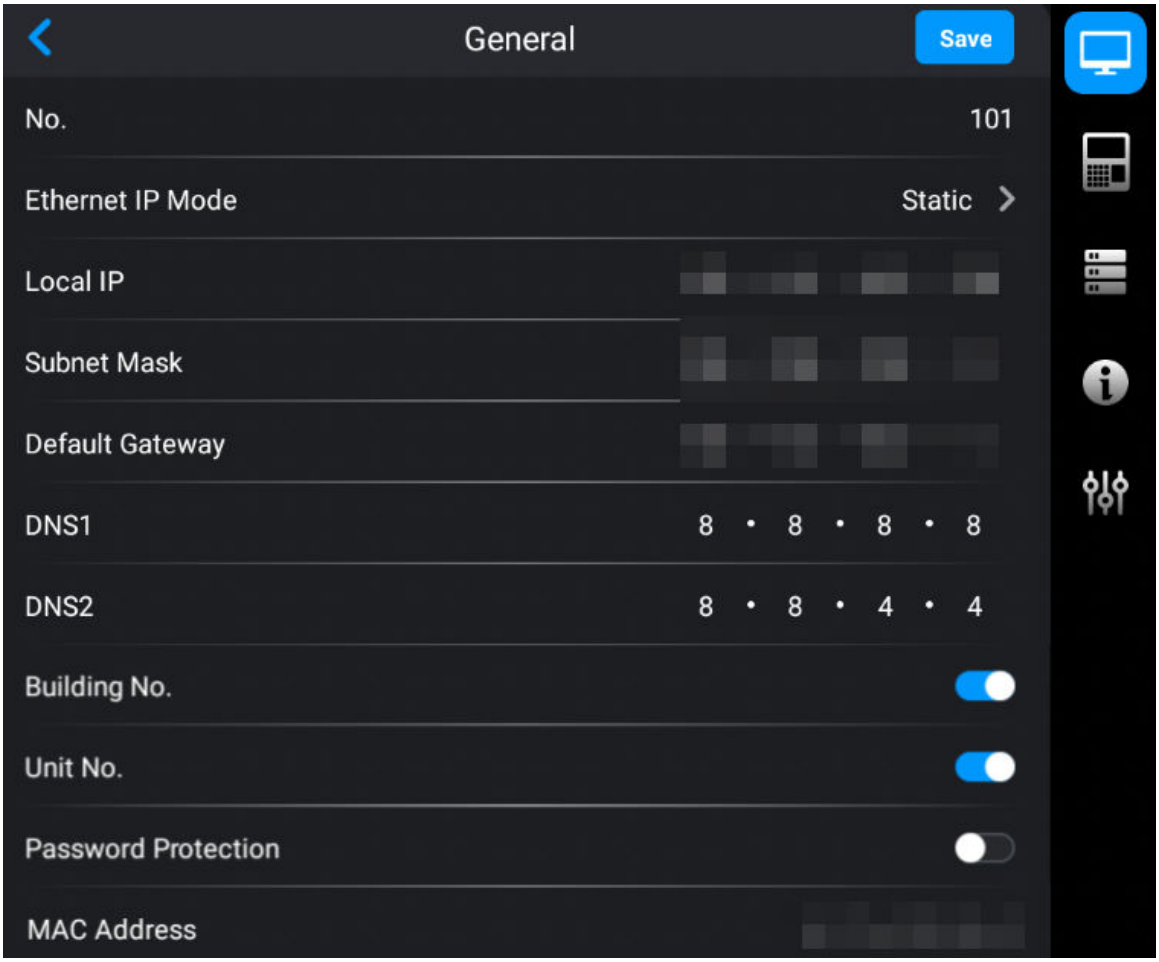


Table 3-4 Parameters description

Parameter	Description
No.	User-defined. You can configure the number from 101 to 999.
Ethernet IP Mode	Configure the mode to get the IP. ● Static: Manually set **Local IP** , **Subnet Mask** and **Default Gateway**. ● DHCP (Dynamic Host Configuration Protocol): Select **DHCP** if there is a DHCP server. The device automatically gets a dynamic IP address.
Local IP	If you select **Static** in **Ethernet IP Mode**, configure the IP address, subnet mask and default gateway according to the network planning.
Subnet Mask	
Default Gateway	
DNS 1	IP address of DNS server.
DNS 2	Standby IP address of DNS server.

Parameter	Description
Building No.	• If the platform or VTS is used as the SIP server, make sure that the configuration status of building and unit number is the same on the platform, VTS and VTO. • If the VTO is used as the SIP server, make sure that the enable/disable status of building and unit number is the same on VTS and VTO. You cannot get the device information of VTO on the monitoring screen.
Unit No.	
Password Protection	Turn on password protection. The password is transferred in encryption when the device is registered on the platform through SIP.
MAC Address	MAC (Media Access Control) address of the device.

3.1.7.2 Configuring SIP Server

Configure the parameters of SIP server. Connect to VTO through SIP agreement to achieve video intercom.

Procedure

Step 1 Select **Setting** >  > **Project Setting** on the home screen.

Step 2 Enter the password and tap **OK**.

Step 3 Tap  and configure the parameters.

Step 4 Click  to enable the VTS as the SIP server.

Figure 3-8 Configure the parameters

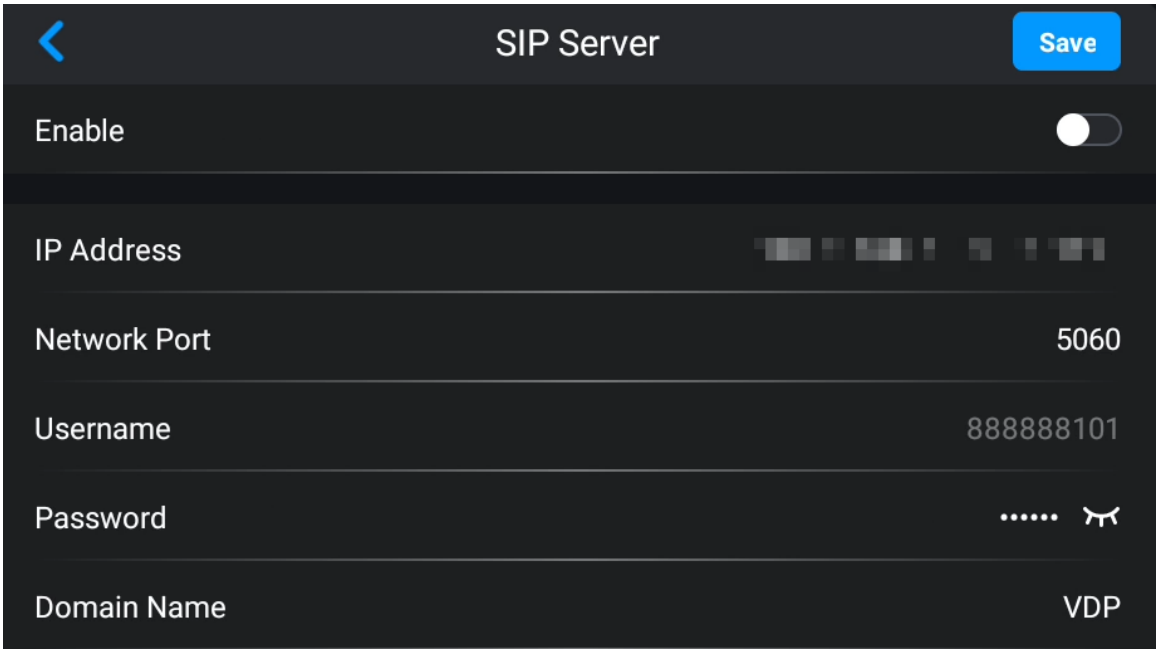


Table 3-5 Parameters description

Parameter	Description
IP Address	IP address of SIP server.
Network Port	Network port number of SIP server. • VTO as the SIP server: 5060. • VTS as the SIP server: 5060. • The platform as the SIP server: 5080.
Username	Default.
Password	Default.
Domain Name	Keep consistent with the SIP server. Domain name is VDP by default.

Step 5 Tap **Save**.

3.1.7.2.1 Adding Devices

Add VTO, fence station or IPC to the VTS, and then you can monitor VTO, fence station or IPC, remotely unlock and talk to VTO or fence station on the VTS.

Procedure

Step 1 Select **Settings** >  > **Project Setting** on the home screen.

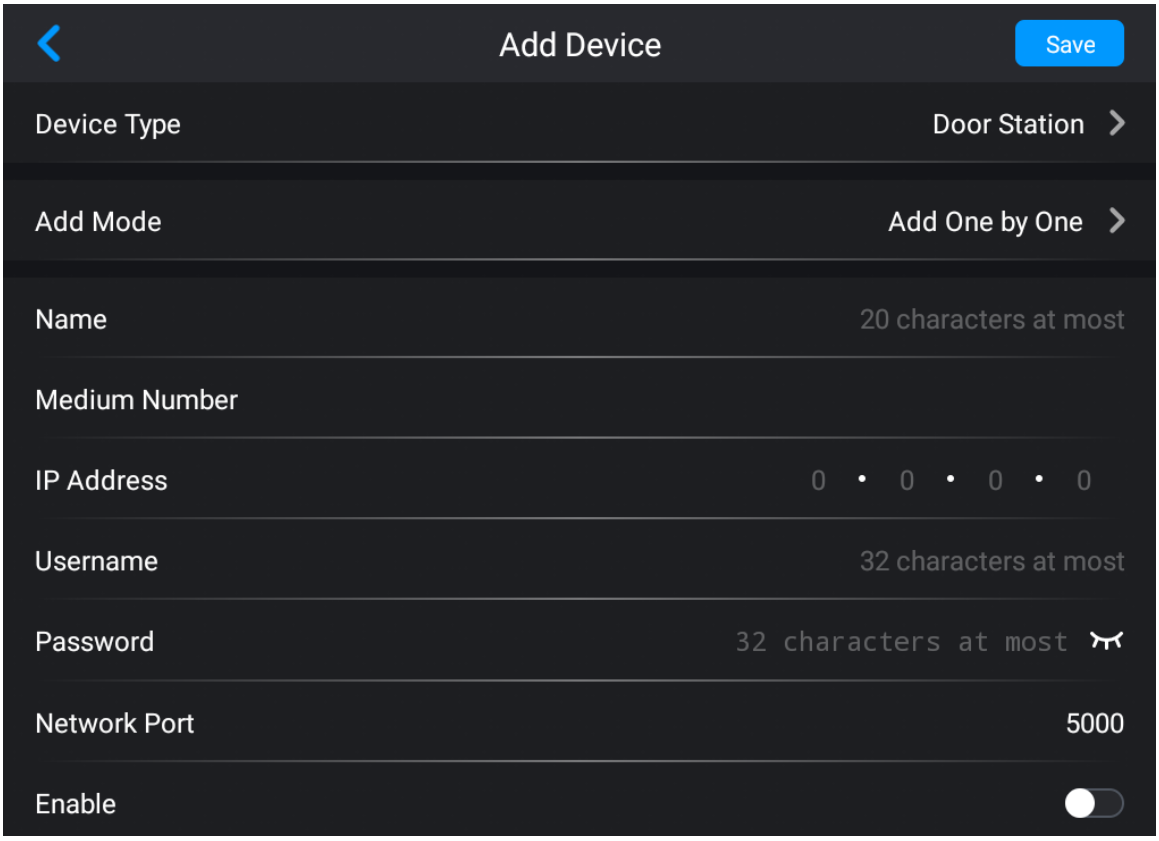
Step 2 Enter the password that you configured during initialization and tap **OK**.

Step 3 Select  > **Add Device**.

Step 4 Add devices.

- Add device one by one.

Figure 3-9 Add device one by one



- Add devices in batches.

Figure 3-10 Add devices in batches

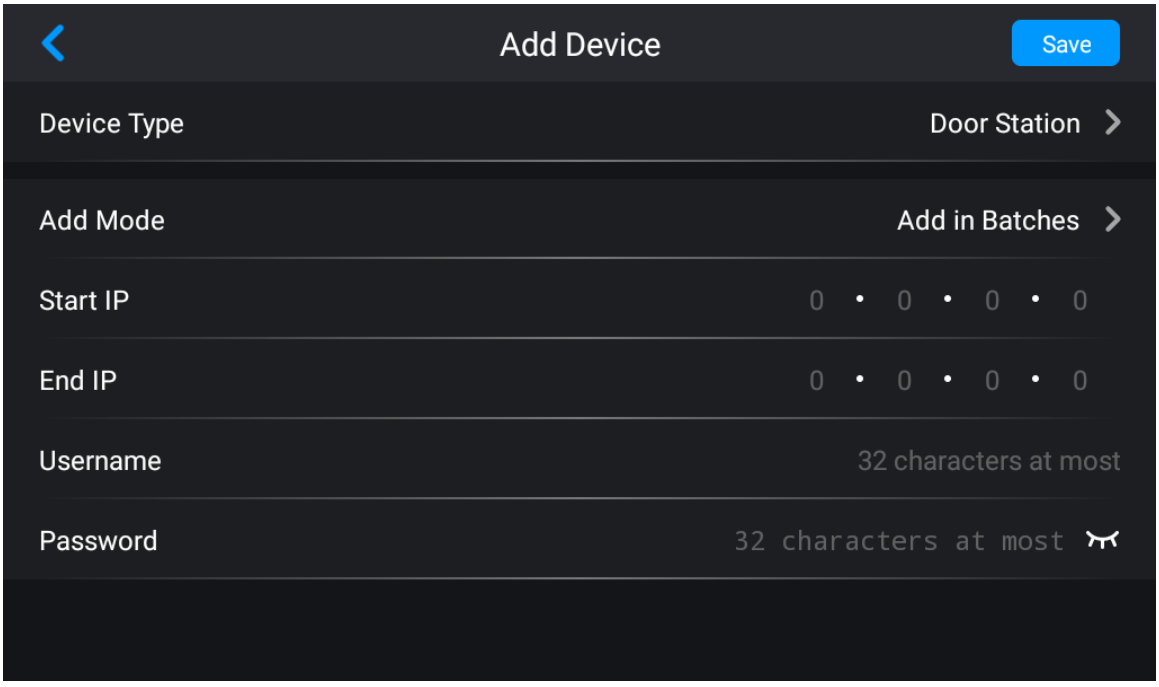


Table 3-6 Parameters description

Device Type	Parameter	Description
Door Station or Fence Station	Add Mode	Supports adding devices one by one or in batches. Only VTO supports adding devices in batches.
	Name	User-defined. You can configure the name that distinguishes the device.
	Medium Number	Cannot be edited.
	IP Address	The IP, username and password of the device that you added.
	Username	
	Password	
	Enable	After turning on, select **Monitor** > **VTO** or **Monitor** > **Fence Station** to monitor the screen.
	Start IP	The start and end IP address of the device if you add devices in batches.
	End IP	
IPC	Name	User-defined. You can configure the name that distinguishes the device.
	No.	User-defined.
	IP Address	The IP, username and password of the device that you added.
	Username	
	Password	
	Stream Type	Select main stream or sub stream. • Main stream: Large stream has high definition, and occupies a large bandwidth. Used for local storage. • Sub stream: Smooth image occupies a small bandwidth. Used for low-bandwidth network transmission.
	Protocol Type	Select the local protocol or ONVIF protocol depending on the IPC that you added.
	Encryption	The video is transferred in encryption when this function is turned on.
	Linkage	VTH supports displaying the image of connected IPC when VTS calls VTH if you turn on this function.

Step 5 Tap **Save**.

3.1.7.2.2 Resetting Information

Turn on the resetting function here, otherwise you cannot reset password if you forget it.

Procedure

Step 1 On the home screen, select **Setting** >  > **Project Settings**.

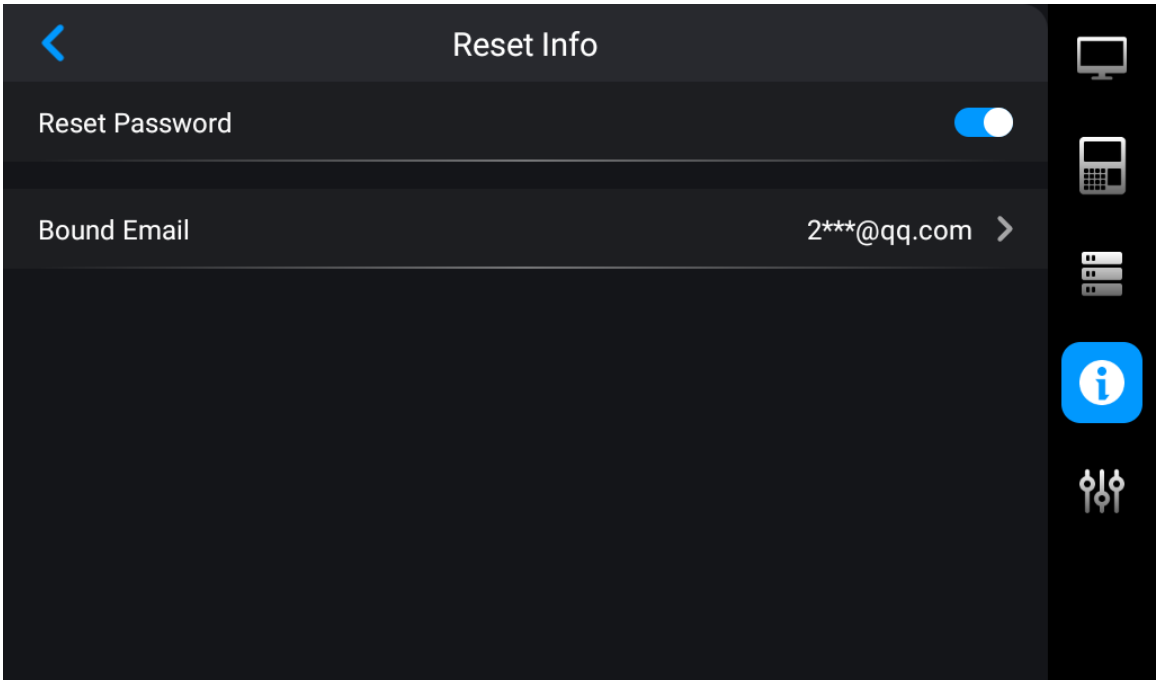
Step 2 Enter the password that you configured during initialization, and then tap **OK**.

Step 3 Tap  .

Step 4 Turn on **Reset Password**.

Step 5 Tap **Bound Email** to enter the e-mail address.

Figure 3-11 Reset information



Step 6 Click **OK**.

3.1.7.2.3 Debugging and Factory Defaults

Procedure

Step 1 On the home screen, select **Setting** >  > **Project Settings**.

Step 2 Enter the password, and then tap **OK**.

Step 3 Tap  , and then configure the functions.

Figure 3-12 Debug and factory defaults

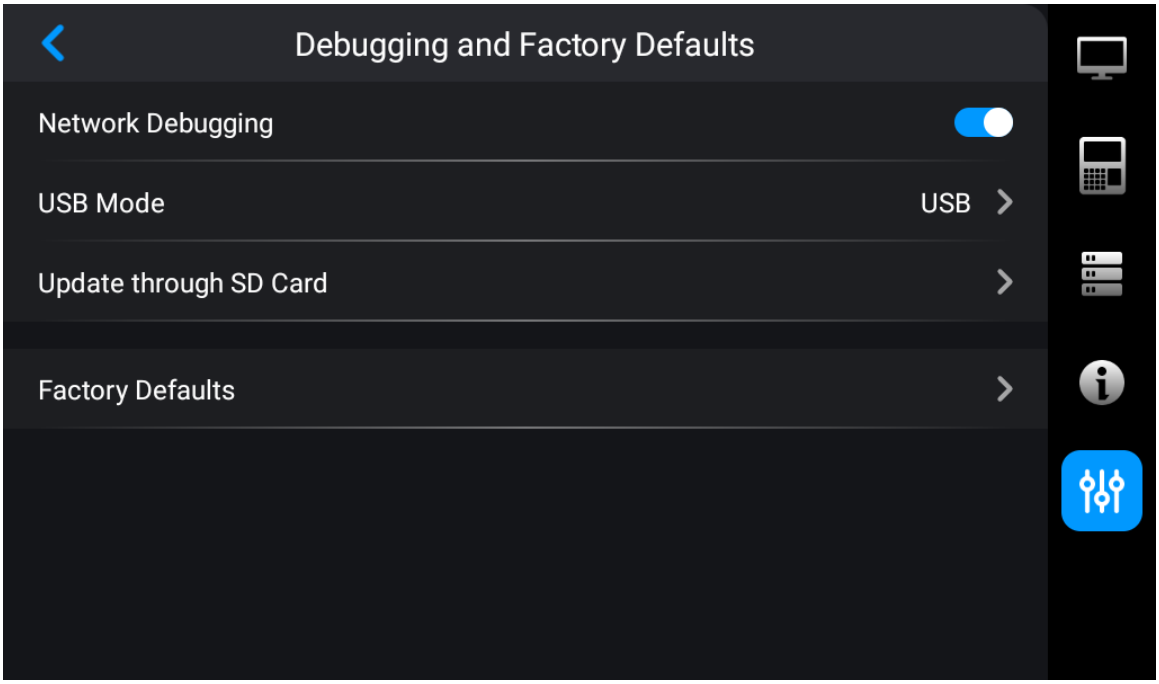


Table 3-7 Parameters description

Parameter	Description
Network Debugging	Only debugged and used by administrators.
USB Mode	• USB: Administrators debug VTS through the USB port. • OTG: Administrators transmit the data with VTS through the OTG port. This mode is only avaiable to the blue USB port.
Update through SD Card	Put the update files into the SD card. Update through the SD card that you plugged into VTS. The update file name must be **update.zip**.
Factory Defaults	VTS clears all information except the IP address, and then it restarts after factory defaults.

3.1.7.3 Setting as SIP Server

Configure the parameters of VTS to work as a SIP server.

Procedure

Step 1 Select **Setting** >  > **Project Setting** on the home screen.

Step 2 Enter the password and tap **OK**.

Step 3 Tap  , and then enable the function.

Figure 3-13 Configure the parameters

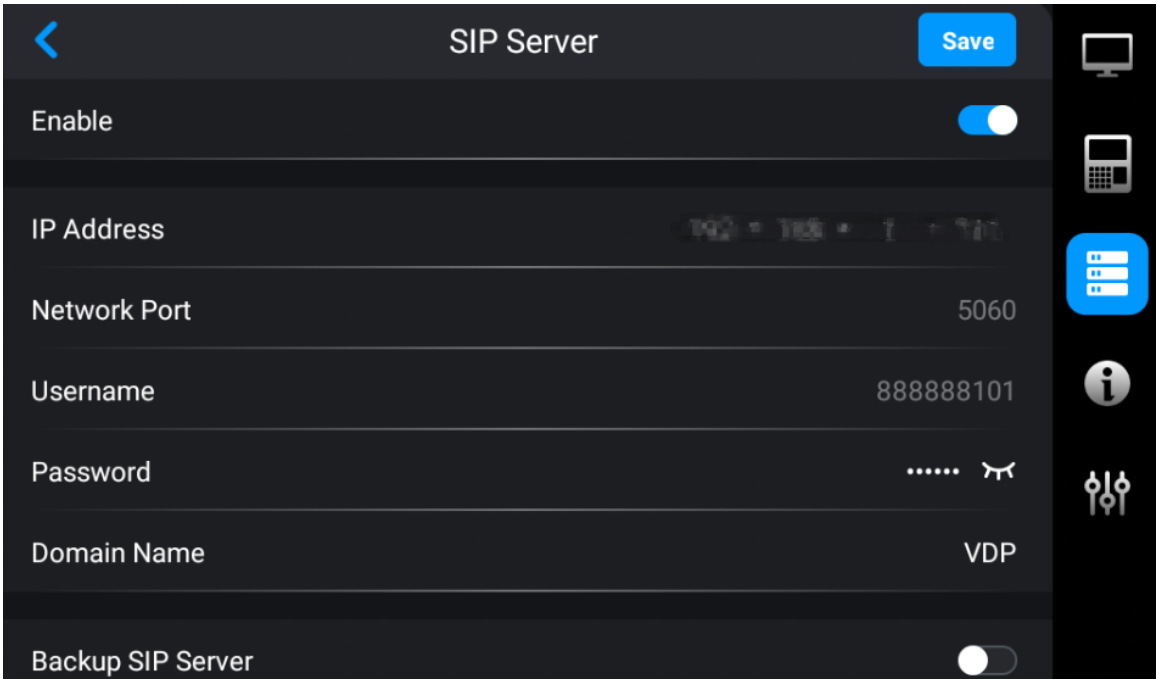


Table 3-8 Parameters description

Parameter	Description
IP Address	IP address of SIP server.
Network Port	Network port number of SIP server. ● VTO as the SIP server: 5060. ● The platform as the SIP server: 5080.
Username	Default.
Password	Default.
Domain Name	Keep consistent with the SIP server. Domain name is VDP by default.
Backup SIP Server	Enable the backup SIP server. Backup SIP server works when the main server goes offline unexpectedly. ● You can enter the room number directly behind the **Room Number of Backup Server**. ● You can also click **Select Online Device** to select online device. ● When the VTO and the VTS crash at the same time, only upper–level calling to lower level is supported, and dual -calling is not supported.
Room Number of Backup Server	

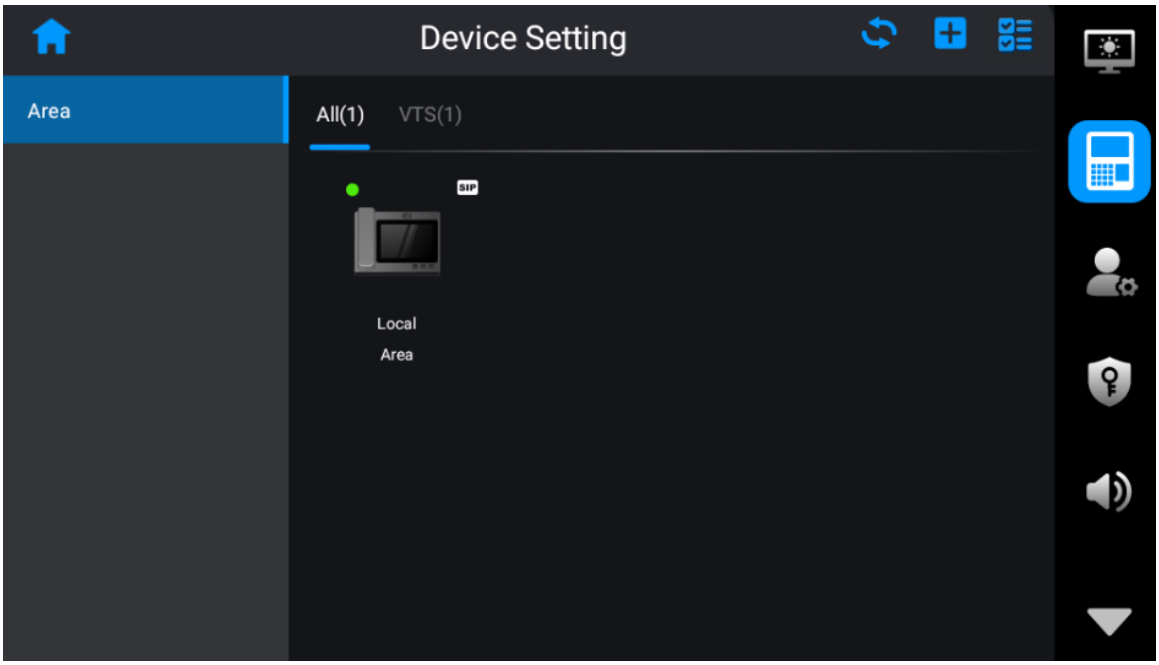
Step 4 Tap **Save**.

3.1.7.3.1 Device Setting

Procedure

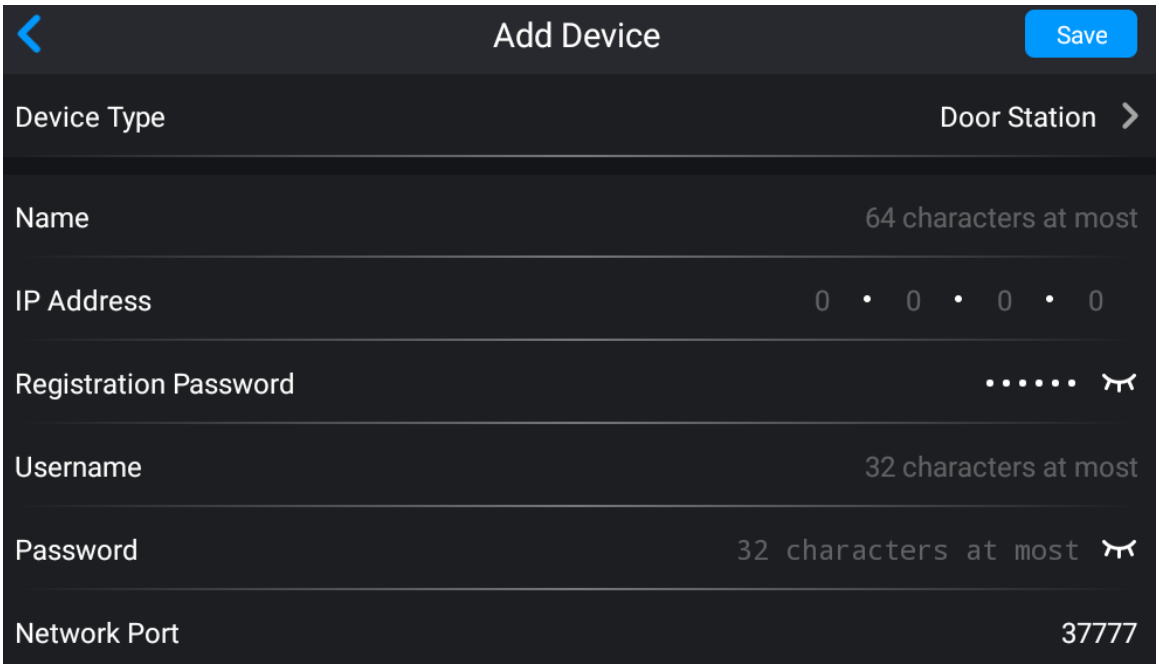
Step 1 Select **Settings** > , you can see all devices.

Figure 3-14 Device setting



Step 2 Tap to add devices.

Figure 3-15 Configure the device parameters



Step 3 Tap the device to enter the device details page, you can modify the information of the device.

Related Operations

- Tap to edit the devices, such as clearing or deleting the devices.
- Tap to refresh the device list.

3.1.7.3.2 Person Management

Procedure

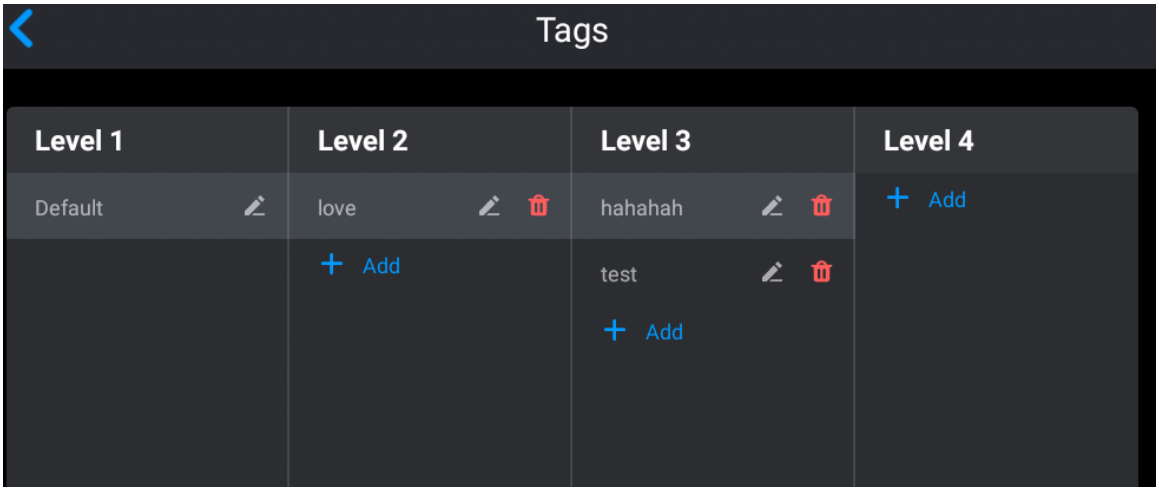
Step 1 Select **Settings** > on the home screen.

Step 2 Click to add persons.

Step 3 Configure the tags.

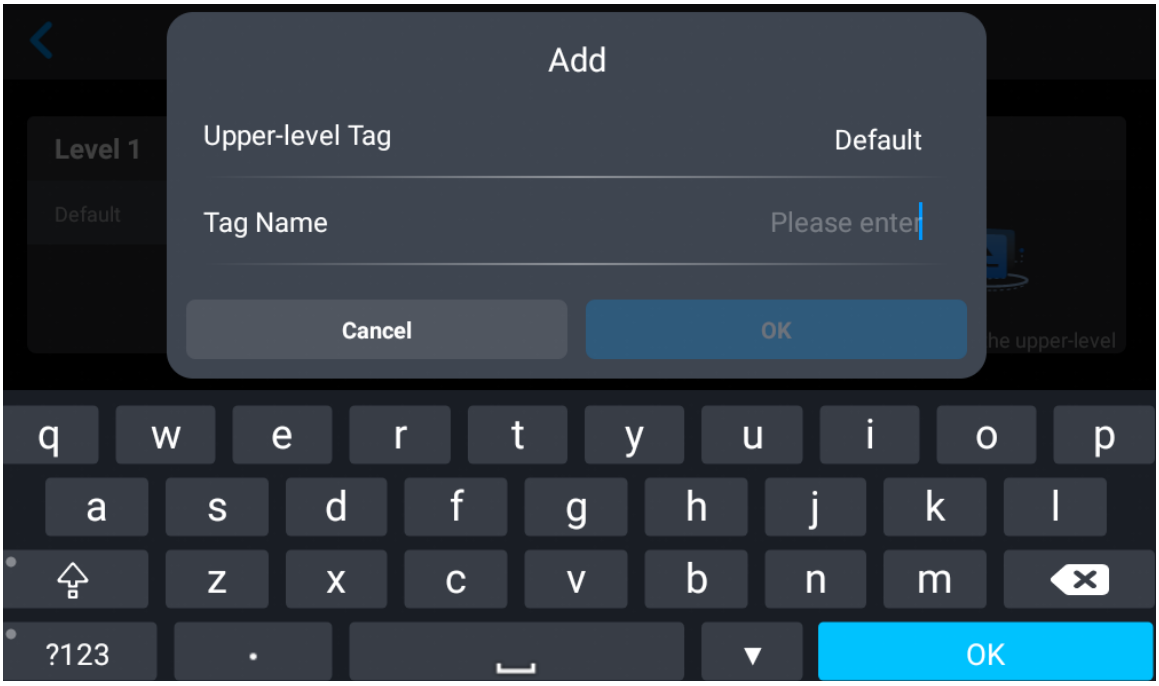
1. Click to see the tags.

Figure 3-16 Tags list



2. Click **Add** to add tags.

Figure 3-17 Add tags



Step 4 Click to edit persons.

3.1.7.3.3 Adding Person

Procedure

Step 1 Select **Settings** > on the home screen.

Step 2 Tap **Add Person** to add person.

Figure 3-18 Person management (1)

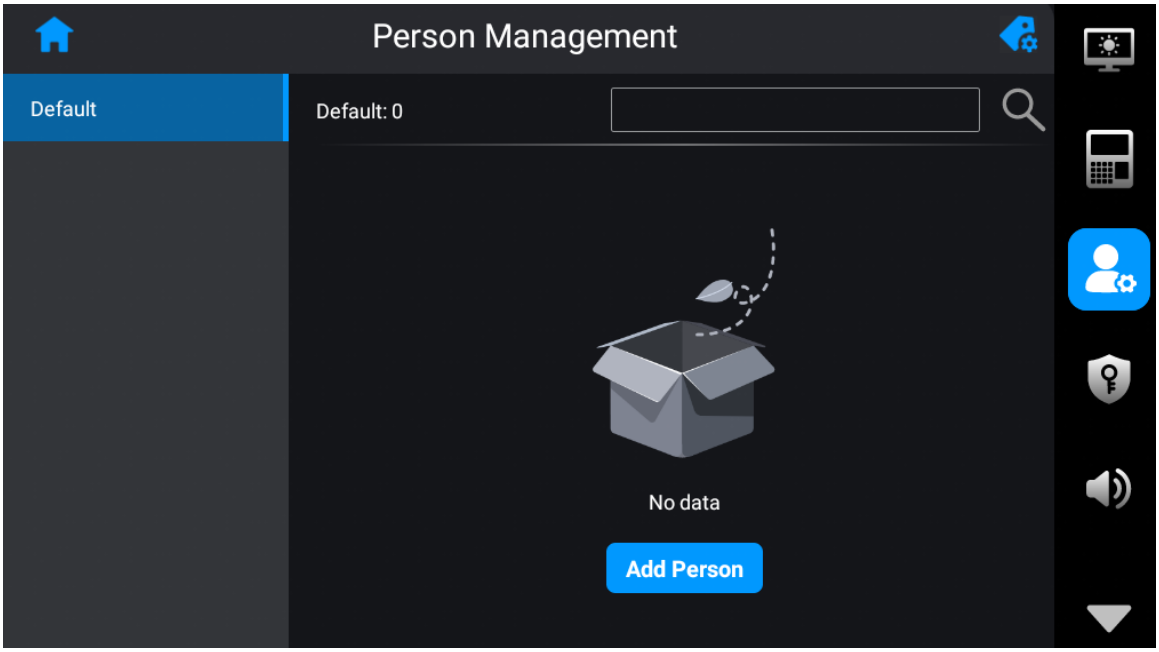
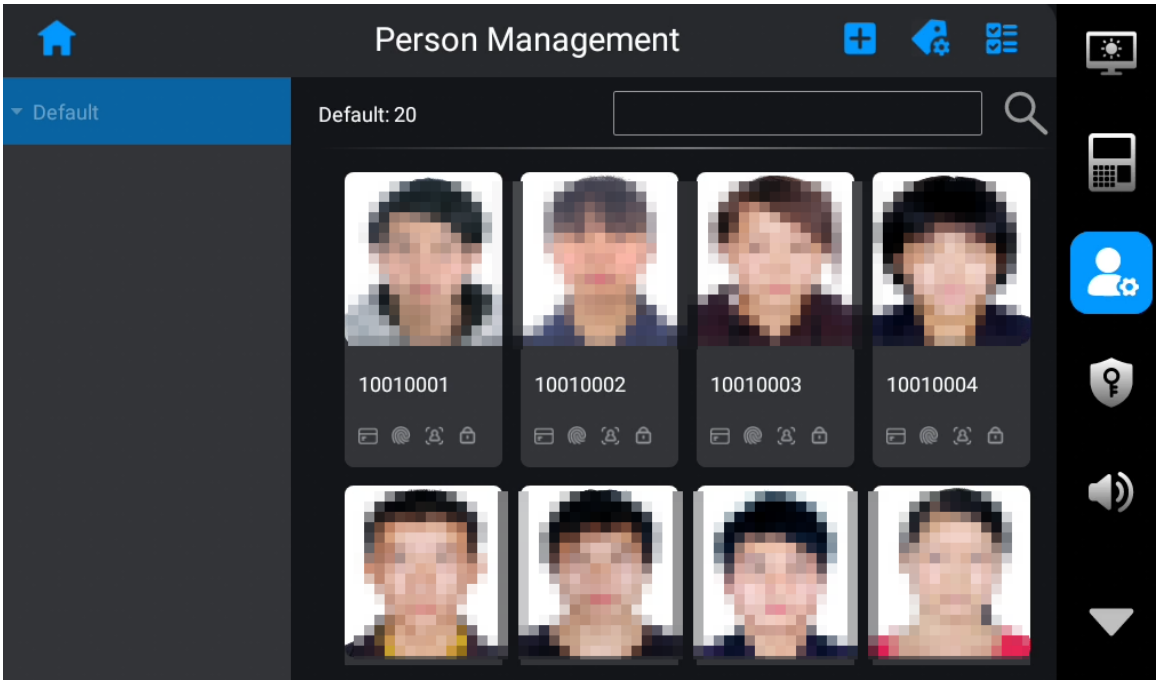


Figure 3-19 Person management (2)

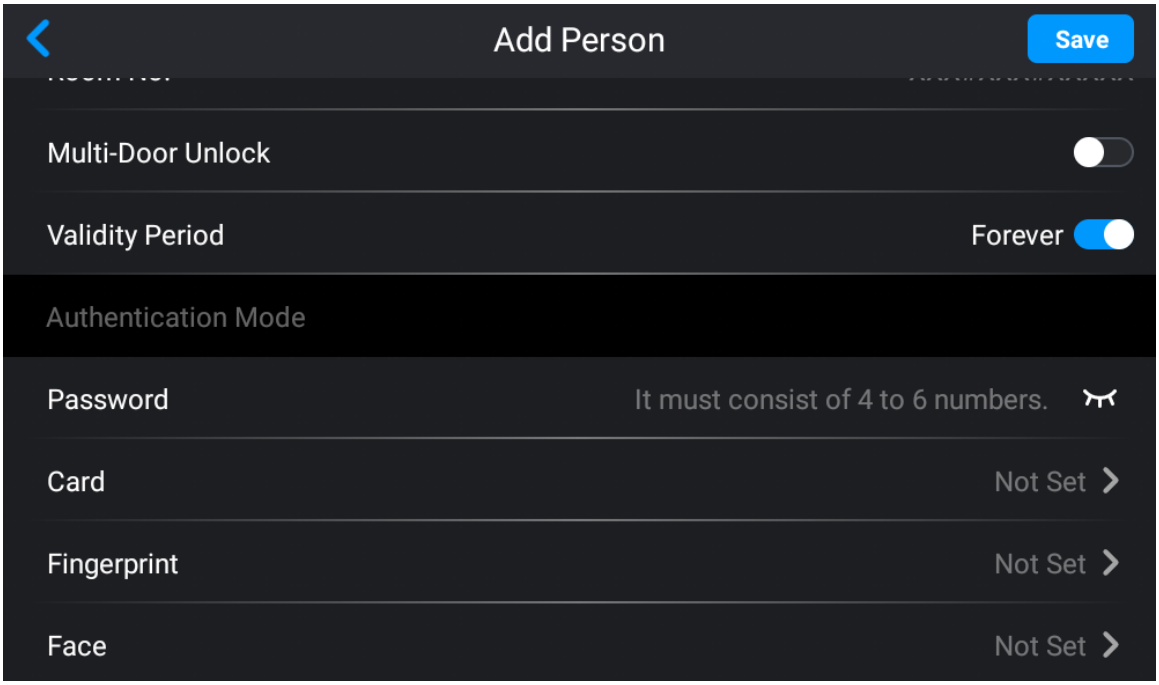


Tap the person image, the page goes to the person information, and then you can configure the details about person such as anthentication mode.

Step 3 Configure the person information, and then tap **Save**.

Figure 3-20 Add persons (1)

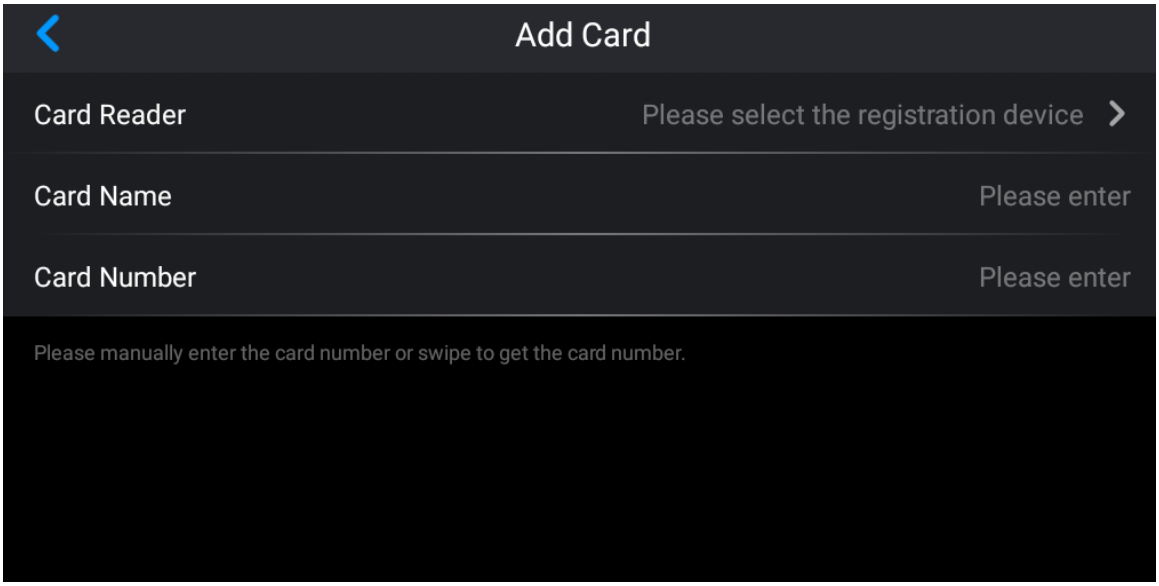
Figure 3-21 Add persons (2)



Step 4 Configure the card.

1. Select **Card** > **Add Card**.
2. Select the registration device and enter the card name and card number.

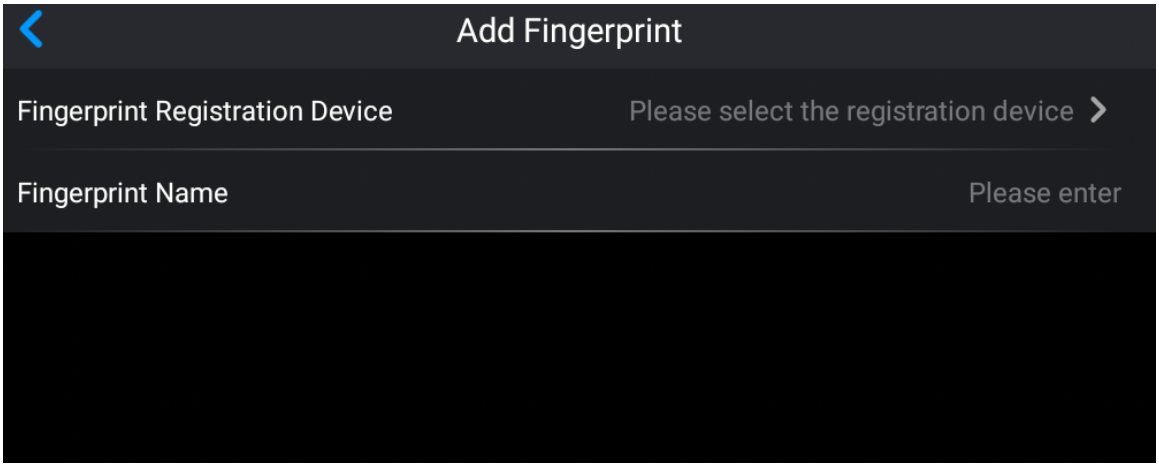
Figure 3-22 Add cards



Step 5 Configure the fingerprint.

1. Select **Fingerprint** > **Add Fingerprint**.
2. Select the registration device and enter the fingerprint name.

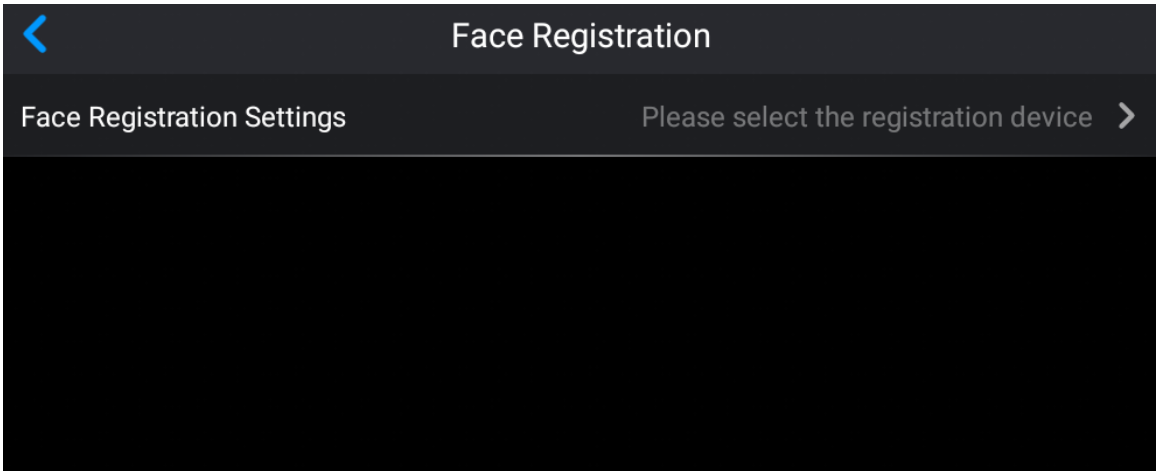
Figure 3-23 Add fingerprint



Step 6 Configure the face registration.

1. Select **Face** > **Face Registration**.
2. Select the registration device, and then scan the face on the device.

Figure 3-24 Add face registration



Related Operations

- Tap to add more persons.
- Tap to see the label list.
- Tap to edit person information

3.1.7.3.4 Authorization Management

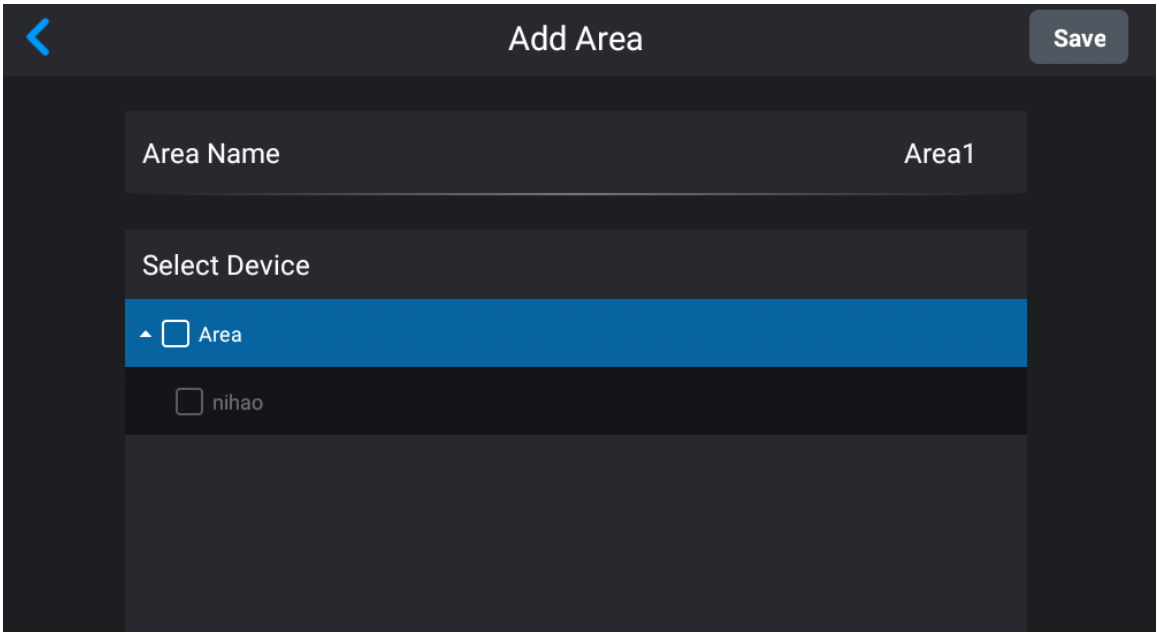
Configuring Area

Procedure

Step 1 Select **Settings** > > **Area Settings** to configure the area.

Step 2 Tap **+** to set the name of area and select the device.

Figure 3-25 Configure the parameters



Step 3 Tap **Save**.

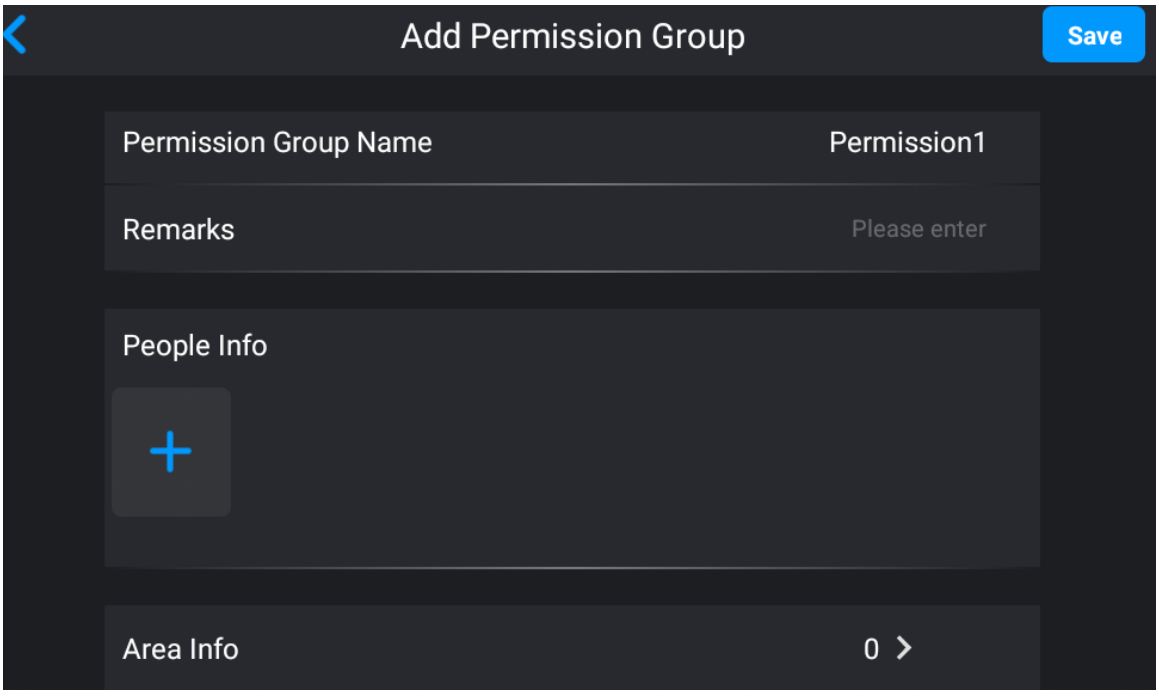
Configuring Permission

Procedure

Step 1 Select **Settings** > > **Permission Settings** configure the permission.

Step 2 Tap **+** to set the permissions.

Figure 3-26 Configure the permissions



Step 3 Tap **+** to add people information.

Step 4 Tap **Area Info** , select area to bind, and then tap **OK**.

Step 5 Tap **Save**.

Viewing Authorization Progress

Select **Settings** > > **Authorization Progress** to view the authorization progress.

3.1.8 Commissioning

3.1.8.1 Call

Call VTH

On the home screen of VTS, tap **Phone**, enter the number of VTH, and then tap .

If you use the gooseneck to talk, the recommended distance is between 5 cm to 10 cm.

Figure 3-27 Dial

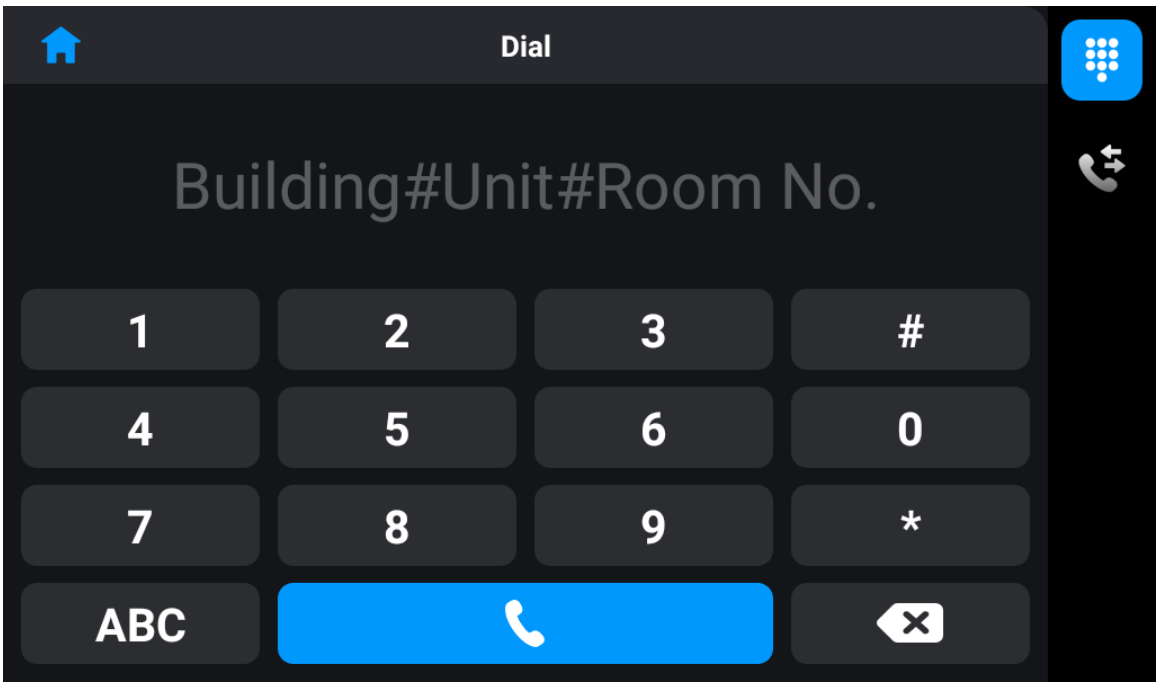


Figure 3-28 Call VTH

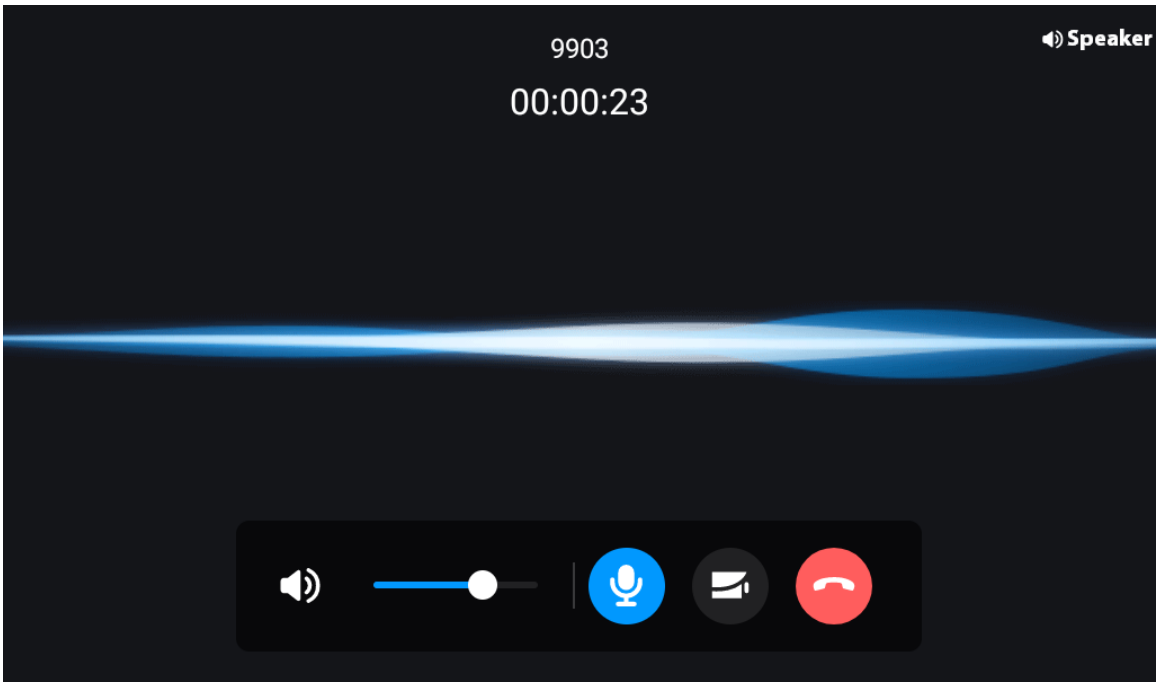


Table 3-9 Icons description

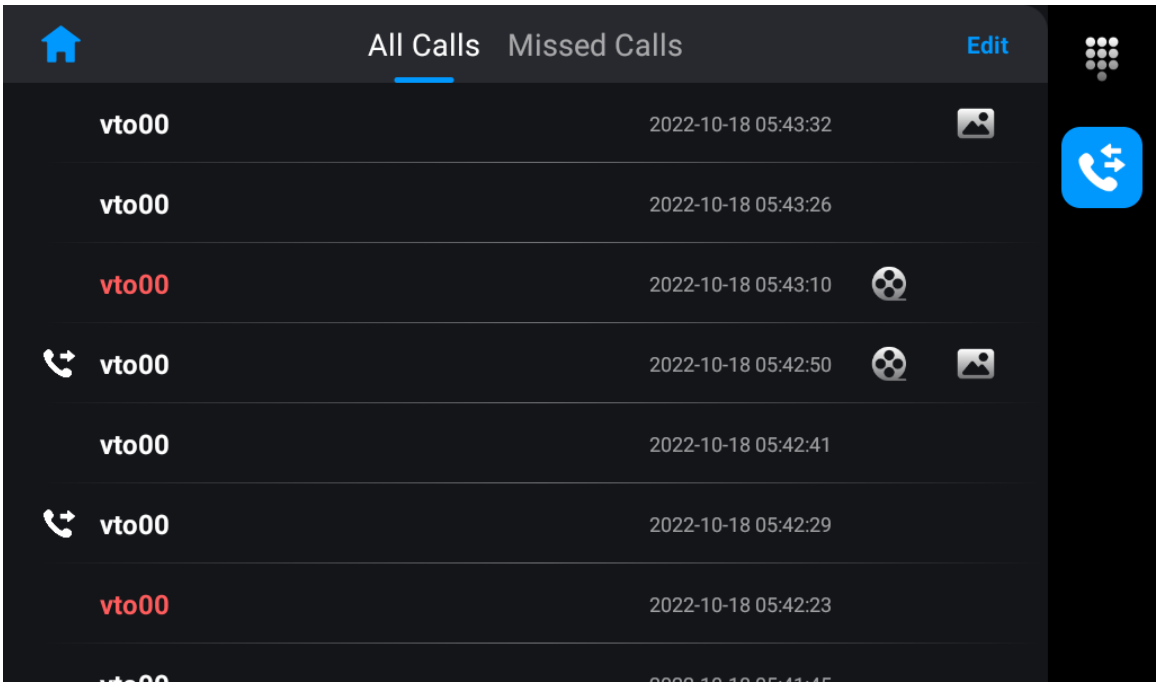
Icon	Description
	Adjust the volume of the speaker during the call.
	Turn on or turn off speech input during the call.
	Tap it to convert to IPC video image during the call.
	Tap it to hang up the call.

Call history

On the home screen of VTS, tap **Phone**, and then tap  to check all calls and missed calls.

- Tap the call on call history list to call back.
-  : Check the snapshot files of the call.
-  : Check the video files of the call.

Figure 3-29 Call history

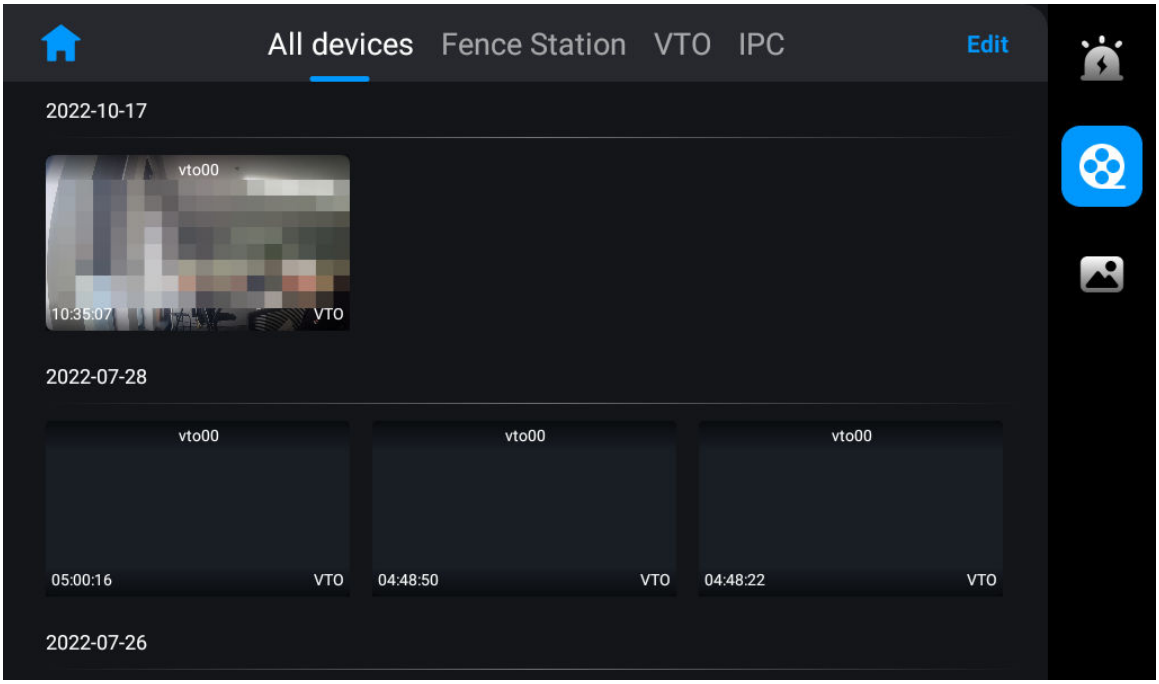


3.1.8.2 Checking the Information

Video files

Check or delete the video files that VTS recorded in monitoring or in the call.

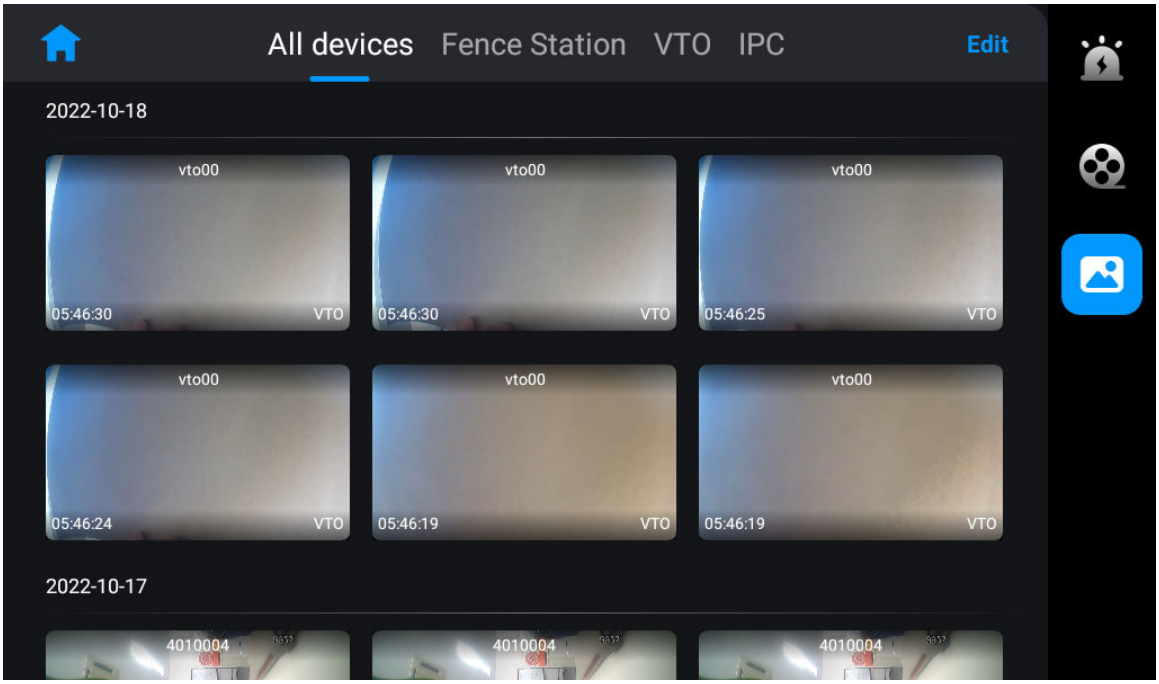
Figure 3-30 Video files



Snapshot files

Check or delete the snapshot files that VTS recorded in monitoring or in the call.

Figure 3-31 Snapshot files



3.1.8.3 Monitoring

Monitor VTO, fence station or IPC on VTS. The operations of monitoring IPC or fence stations are the same with the operations of monitoring VTO. This section uses monitoring VTO as an example.

Prerequisites

Make sure that you have added VTO, fence station or IPC before you monitor them.

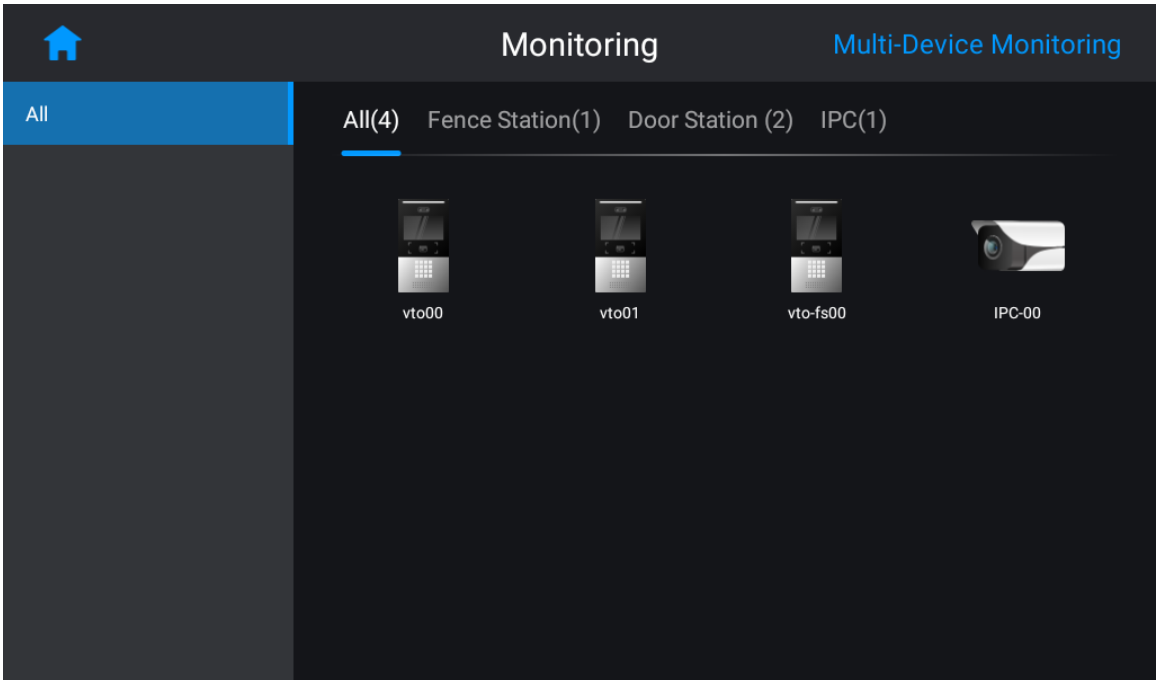
- If VTS works as a SIP server, see "3.1.7.3.1 Device Setting" for details.
- If VTS does not work as a SIP server, see "3.1.7.2.1 Adding Devices" for details.

Procedure

Step 1 On the home screen of VTS, tap **Monitor**.

Step 2 Tap the icon of VTO to monitor.

Figure 3-32 Select VTO



Step 3 Check the monitoring image.

Figure 3-33 Monitoring image

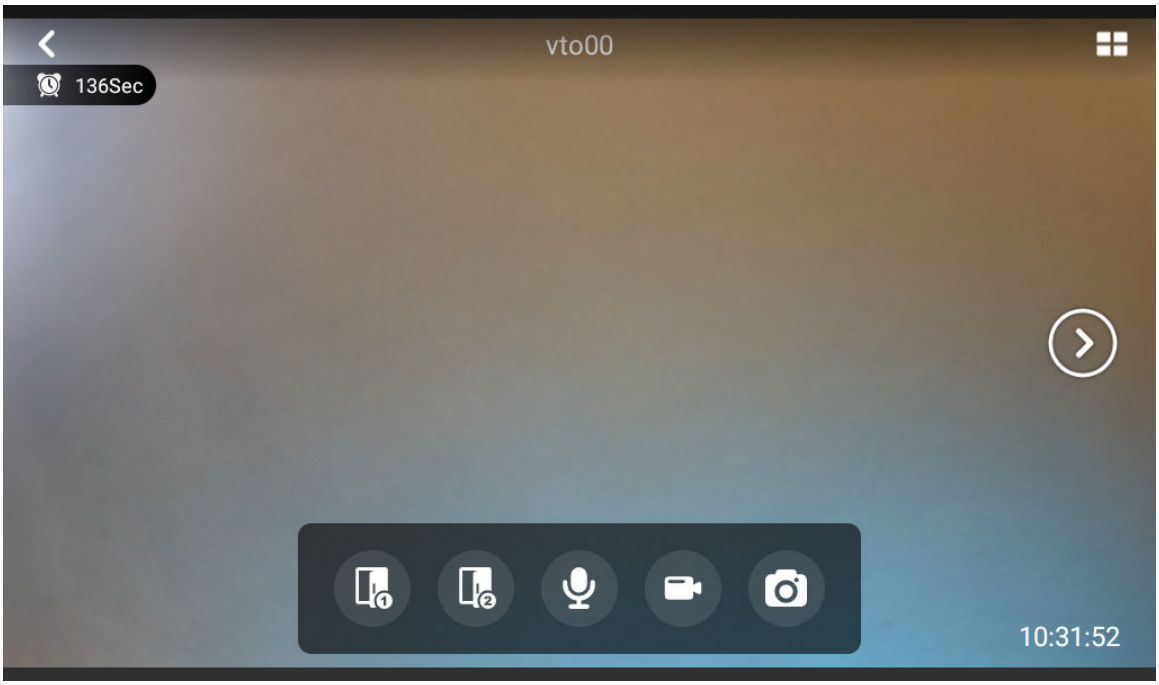


Table 3-10 Monitoring image description

Icon	Description
	Tap to view the monitoring image in 4 windows.
	Tap to convert to monitor other VTOs if VTS connects more than one VTO.

Icon	Description
 	Remotely unlock VTO.
	Call VTO and VTO directly receive the call without taping any icon.
	Tap to start manual recording.
	Tap to manually take snapshots.

3.2 Operations on Webpage

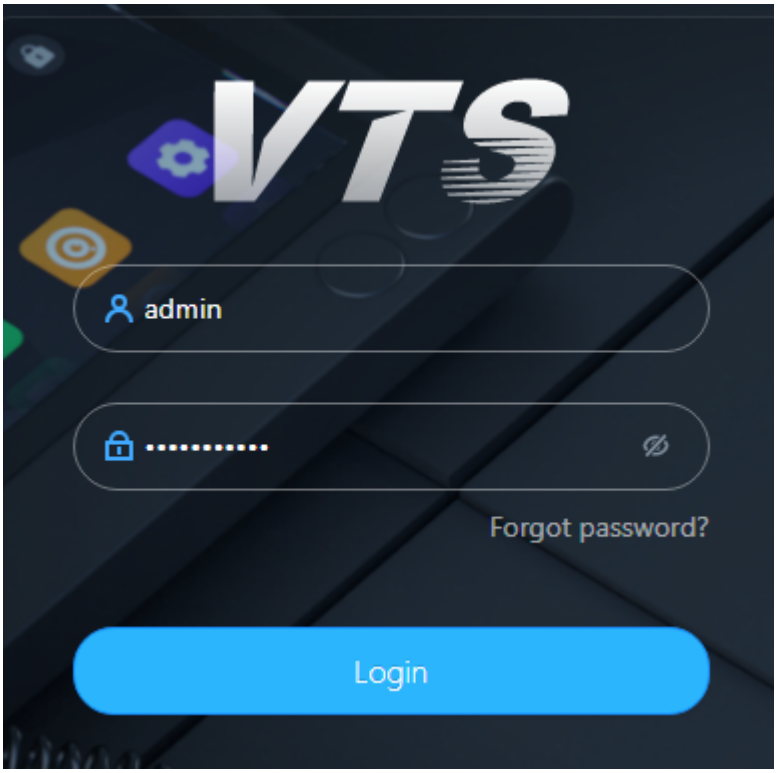
3.2.1 Logging in to the Webpage

Procedure

Step 1 Enter the IP address of VTS in a browser, and then press the Enter key.

Step 2 Enter the username and password.

Figure 3-34 Log in to the webpage



- The default username of administrator is **admin**. The default password is the password that you configured during initialization. We recommend you change the password on a regular basis.
- If you forget the password, click **Forgot password?** to reset the password. For details, see "3.2.2 Resetting Password".

Step 3 Click **Login**.

3.2.2 Resetting Password

Reset password through the e-mail address that you bound if you forget the password.

Procedure

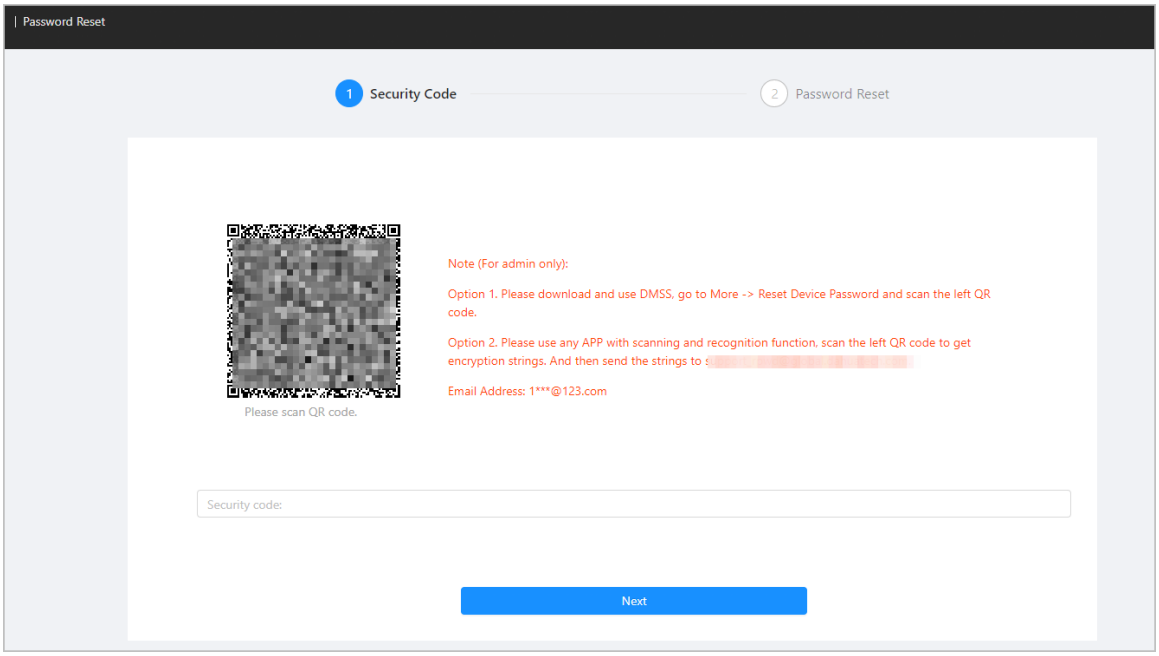
Step 1 On the login page, click **Forgot Password?**

Step 2 Click **OK** on the pop-up window.

Step 3 Scan the QR code on the page, and then get the security code.

- Scan the same QR code, you can get at most 2 security codes. If you need to get the security code again, refresh the QR code page.
- Receive the security code in e-mail. Use the security code in 24 hours to reset the password, otherwise the security code is invalid.
- The account will be locked for 5 minutes if you enter the wrong security code 5 times in a row.

Figure 3-35 Get the security code



Step 4 Enter the security code you received in the **Security code** text box.

Step 5 Click **Next**.

Step 6 Reset new password and confirm the new password.

The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among number, letter and common character (excluding space, ', ", ;, :, &).

Step 7 Click **OK** to reset password.

3.2.3 Home Page Introduction

The system automatically goes to the home page after you log in.

Figure 3-36 Home page

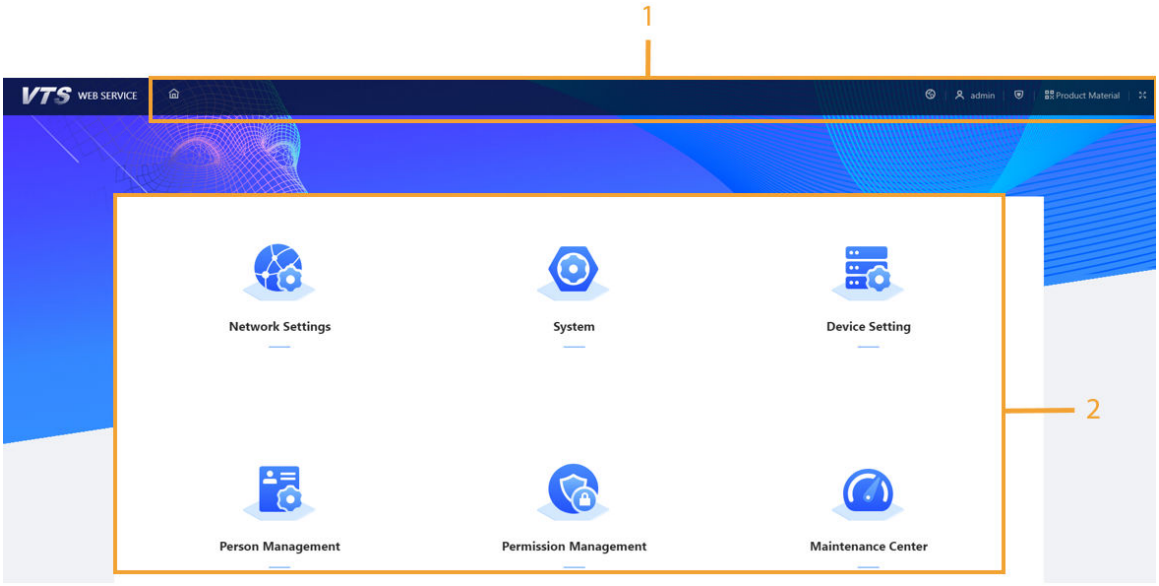


Table 3-11 Home page description

No.	Parameter		Description
1	Navigation Bar		Go to the home page.
		admin	• Click the icon. Select **Restart** to restart VTS. • Click the icon. Select **Logout** to log out the account.
			Open the window in a full screen mode.
2	Function Menu		Functions configuration menu of VTS.

3.2.4 Configuring Network

3.2.4.1 Configuring TCP/IP

Procedure

Step 1 Log in to the webpage of the device.

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

Step 3 Configure the parameters.

Figure 3-37 Configure the parameters

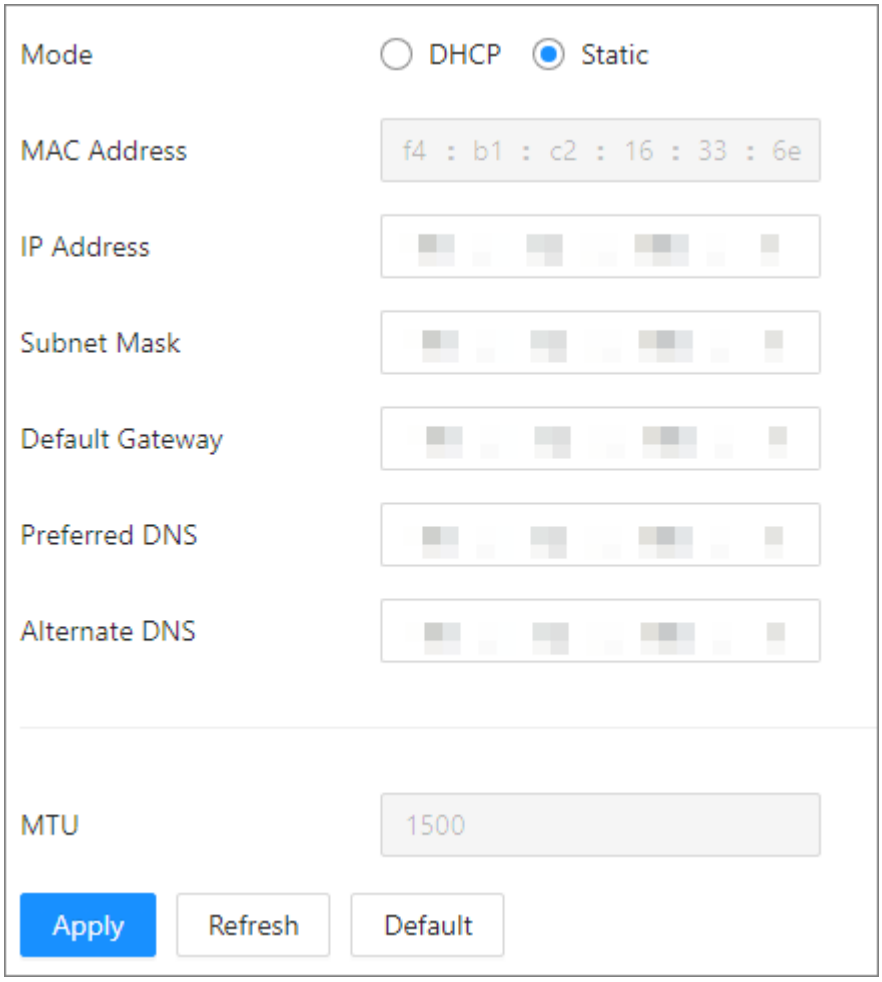


Table 3-12 Parameters description

Parameter	Description
Mode	• Static: Manually configure **IP** , **Subnet Mask** and **Default Gateway**. Click **Apply** and the webpage automatically goes to the login page of the IP that you configured. • DHCP (Dynamic Host Configuration Protocol): Select **DHCP** if there is a DHCP server. The device automatically gets a dynamic IP address.
MAC Address	MAC (Media Access Control) address of the device.
IP Address	If you select **Static** in **Mode**, enter the IP address, subnet mask and default gateway according to the network planning. • There is no subnet mask in IPv6 version. • IP address and default gateway should be on the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of DNS server.
Alternate DNS	Alternate IP address of DNS server.

Step 4 Click **Apply**.

3.2.4.2 Configuring SIP Server

Configure the parameters of SIP server. Connect to VTO through SIP agreement to achieve video intercom.

Procedure

Step 1 Log in to the webpage of VTS.

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

Step 3 Configure the parameters.

Figure 3-38 SIP server parameters

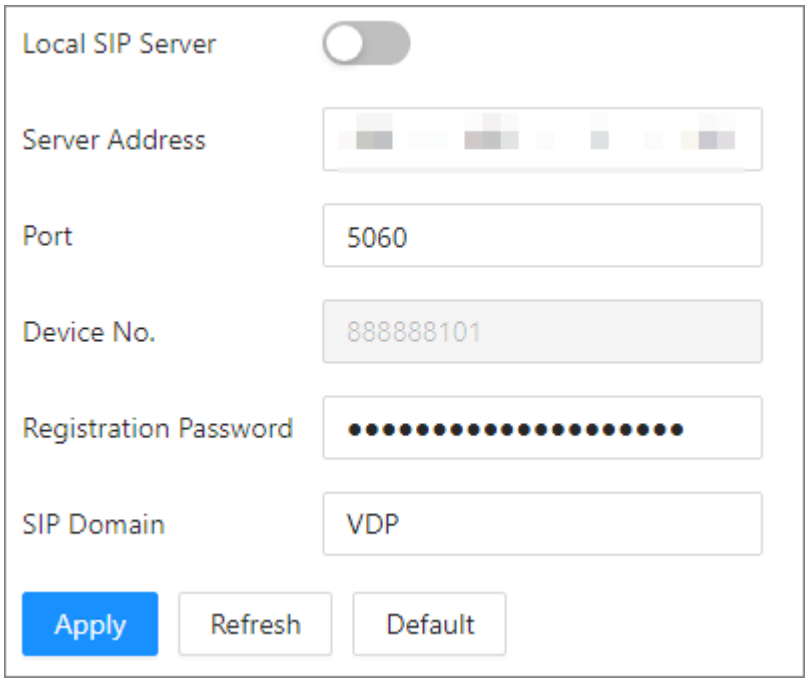


Table 3-13 Parameters description

Parameter	Description
Server Address	IP address of SIP server.
Port	Network port number of SIP server. • VTO as the SIP server: 5060. • VTS as the SIP server: 5060. • The platform as the SIP server: 5080.
Device No.	Default.
Registration Password	Default.
SIP Domain	Keep consistent with the SIP server. Domain name is VDP by default.

Step 4 Click **Apply**.

3.2.4.3 Configuring VTS as SIP Server

Configure VTS as a SIP server.

Procedure

Step 1 Log in to the webpage of VTS.

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

Step 3 Enable **Local SIP Server**.

Step 4 Configure the parameters.

Figure 3-39 VTS as SIP server parameters

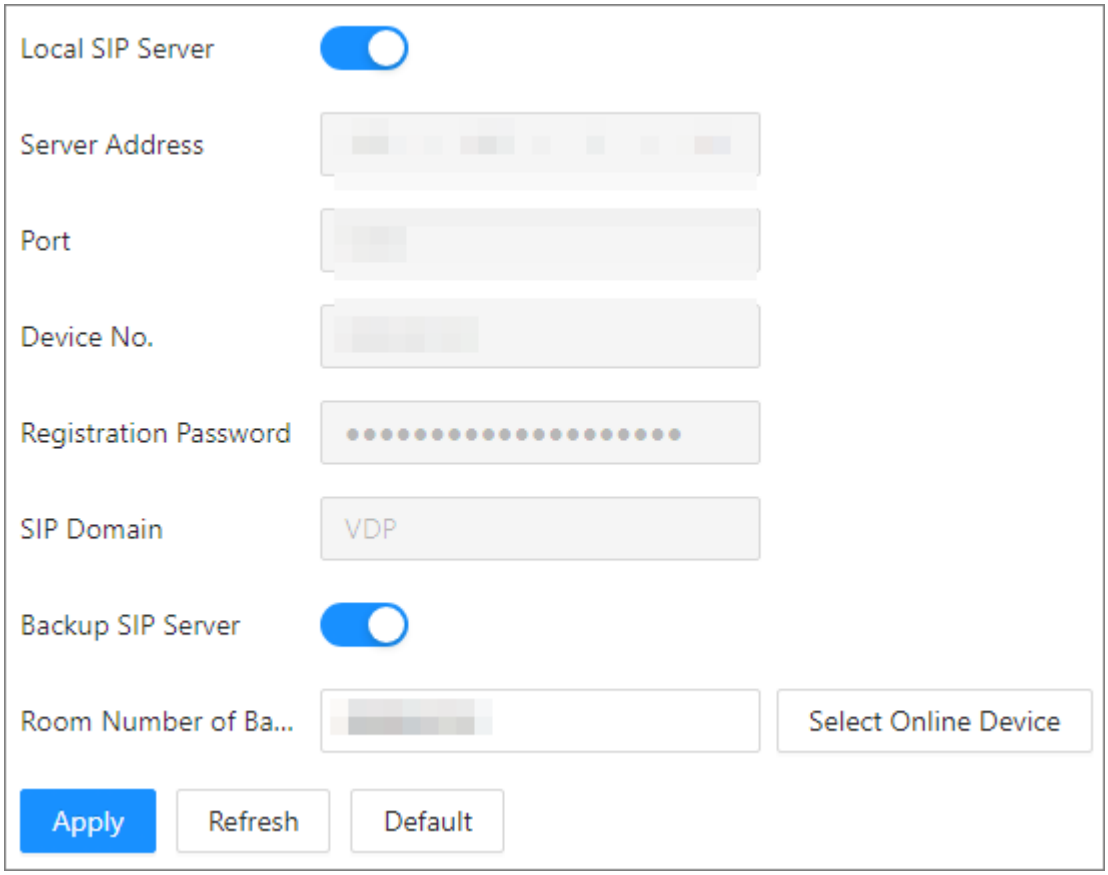


Table 3-14 Parameters description

Parameter	Description
Server Address	IP address of SIP server.
Port	Network port number of SIP server. • VTO as the SIP server: 5060. • The platform as the SIP server: 5080.
Device No.	Default.
Registration Password	Default.
SIP Domain	Keep consistent with the SIP server. Domain name is VDP by default.

Parameter	Description
Backup SIP Server	Enable the backup SIP server. Backup SIP server works when the main server goes offline unexpectedly.
Room Number of Backup Server	• You can enter the room number directly behind the **Room Number of Backup Server**. • You can also click **Select Online Device** to select online device. • When the VTO and the VTS crash at the same time, only upper–level calling to lower level is supported, and dual -calling is not supported.

Step 5 Click **Apply**.

3.2.4.4 Configuring Basic Services

Turn on the protocol as needed when connected VTS with the third-party platform.

Log in to the webpage of VTS, and then select **Network Settings** > **Basic Services**.

Figure 3-40 Basic services

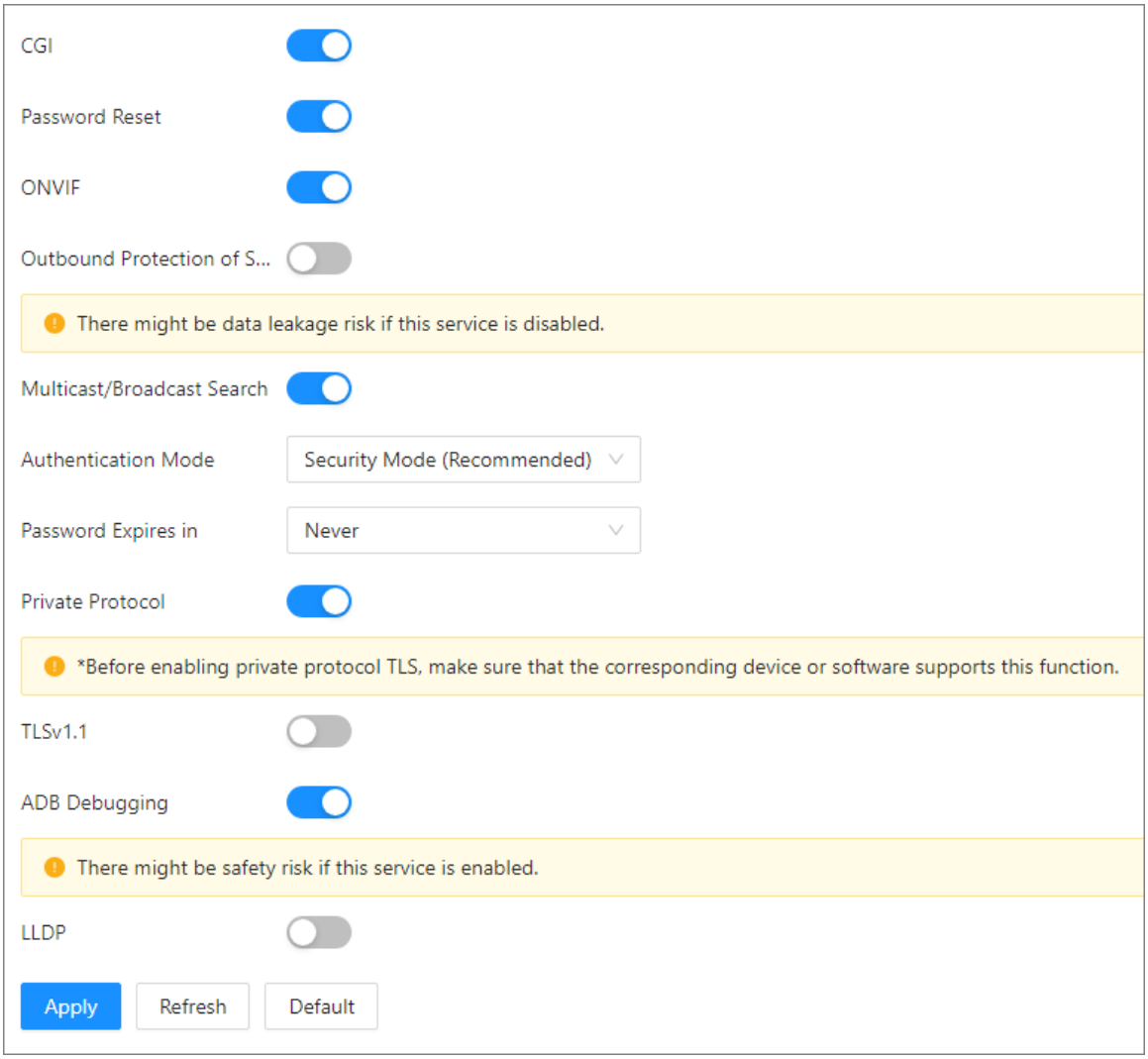


Table 3-15 Description of basic services

Service	Description
CGI	Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similarly to console applications running on a server that dynamically generates web pages. If enabled, CGI commands can be used. The CGI is enabled by default.
Password Reset	Enabled by default. Enable the function, and then configure the email address. After configuration, you can click **Forget Password?** on the login page to reset the password.
ONVIF	Enable other devices to pull video stream of the device through the ONVIF protocol.
Outbound Protection of Service Password	If enabled, the device password cannot be got through the third protocol tool.
Multicast/Broadcast Search	Enable this function, and then when multiple users are previewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
Authentication Mode	• **Security Mode (Recommended)** : The mode does not support logging in with Digest, DES and plain text authentication. • **Compatibility Mode** : The mode supports logging in with Digest, DES and plain text authentication.
Password Expires in	Set the validity period of the password.
ADB Debugging	This function is only available for debugging personnel.
Private Protocol	If enabled, the platform can access to the device with private protocol.
TLSv1.1	⚠ There is security risk if you enable **TLSv1.1**.
LLDP	Improves the efficiency of information exchange among network devices.

3.2.4.5 Configuring Auto Registration

VTS automatically register on the server, and report its IP address to designated server

Procedure

Step 1 Log in to the webpage of VTS.

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

Step 3 Turn on **Enable**. Enter the server address, port number and sub-device ID.

Figure 3-41 Auto registration

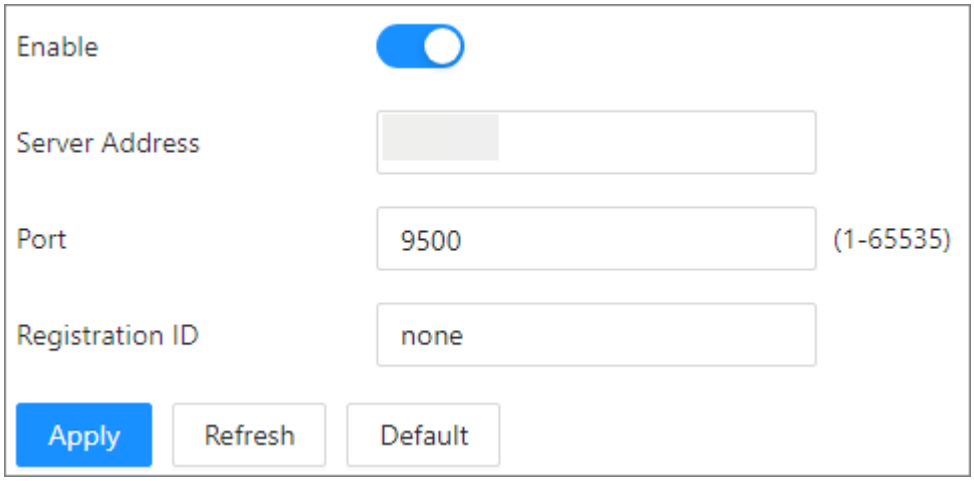


Table 3-16 Parameters description

Parameter	Description
Server Address	IP address or domain name of the server that is needed in registration.
Port	Port number that the server automatically registers.
Registration ID	The server distributes an ID for the device. Keep consistent with the ID registered on the server.

Step 4 Click **Apply**.

3.2.5 System Management

3.2.5.1 Configuring Basic Parameters of VTS

Configure the number and other functions of VTS.

Procedure

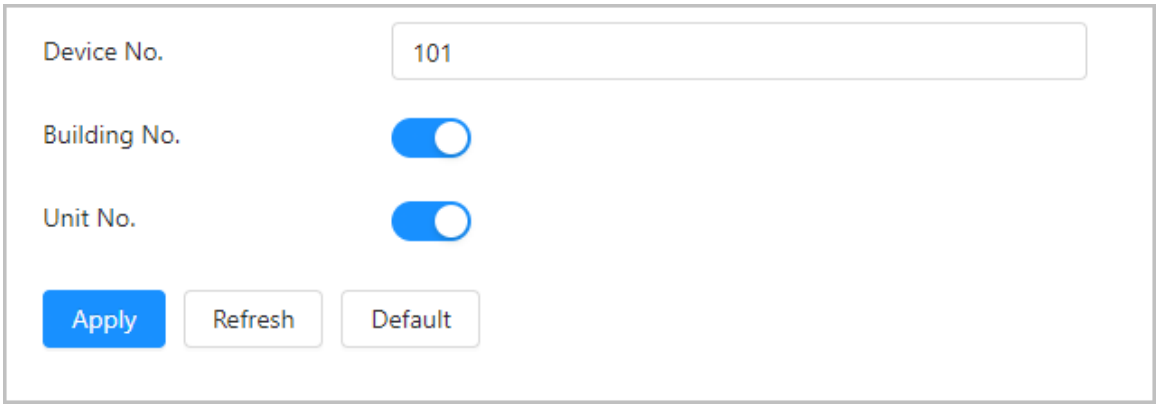
Step 1 Log in to the webpage of VTS.

Step 2 Select **System** > **General**.

Step 3 Configure the parameters.

- You can configure the number from 101 to 999.
- Turn on the **Building No.** and **Unit No.** as needed.

Figure 3-42 Configure basic parameters



Step 4 Click **Apply**.

3.2.5.2 Configuring Video Parameters

Video is available on select models.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **System** > **Video**.

Step 3 Configure the parameters.

Figure 3-43 Video parameters

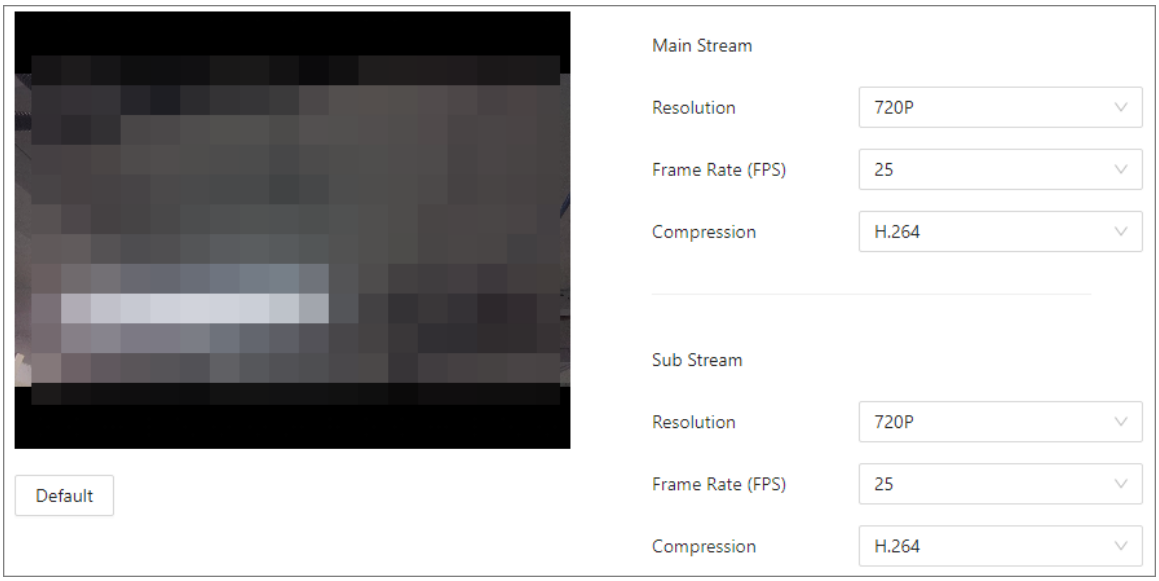


Table 3-17 Parameters description

Parameter		Description
Main Stream	Compression	Select the compression mode depending on the actual bandwidth. • H.264: Main profile compression. • H.265: Main profile compression occupies smaller bandwidth than H.264 in the same image quality.
	Resolution	Select the resolution as needed.
	Frame Rate (FPS)	The number of frames that appears within a second. Higher FPS refers to more vivid and smoother image.
Sub Stream	Compression	Select the compression mode depending on the actual bandwidth. • H.264: Main profile compression. • H.265: Main profile compression occupies smaller bandwidth than H.264 in the same image quality.
	Resolution	Select the resolution as needed.
	Frame Rate (FPS)	The number of frames that appears within a second. Higher FPS refers to more vivid and smoother image.

3.2.5.3 Configuring Audio

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **System** > **Audio**.

Step 3 Click to enable the audio collection.

Step 4 Click **Apply**.

3.2.5.4 Configuring Event

This function is only available to server VTS.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **System** > **Event**.

Step 3 Enable the function, and then click **Apply**.

- **System Event** : System events include tamper alarms, heat alarms and unlock timeout alarms.
- **Zone Events** : Zone events include local alarm inputs of VTOs and local zone alarms of VTHs.

3.2.5.5 Account Management

Add user and edit user information depending on different protocols.

3.2.5.5.1 Adding User

You are admin user by default. You can add users. Newly added users can only log in to the webpage of VTS.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **System** > **Account**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 3-44 Add users

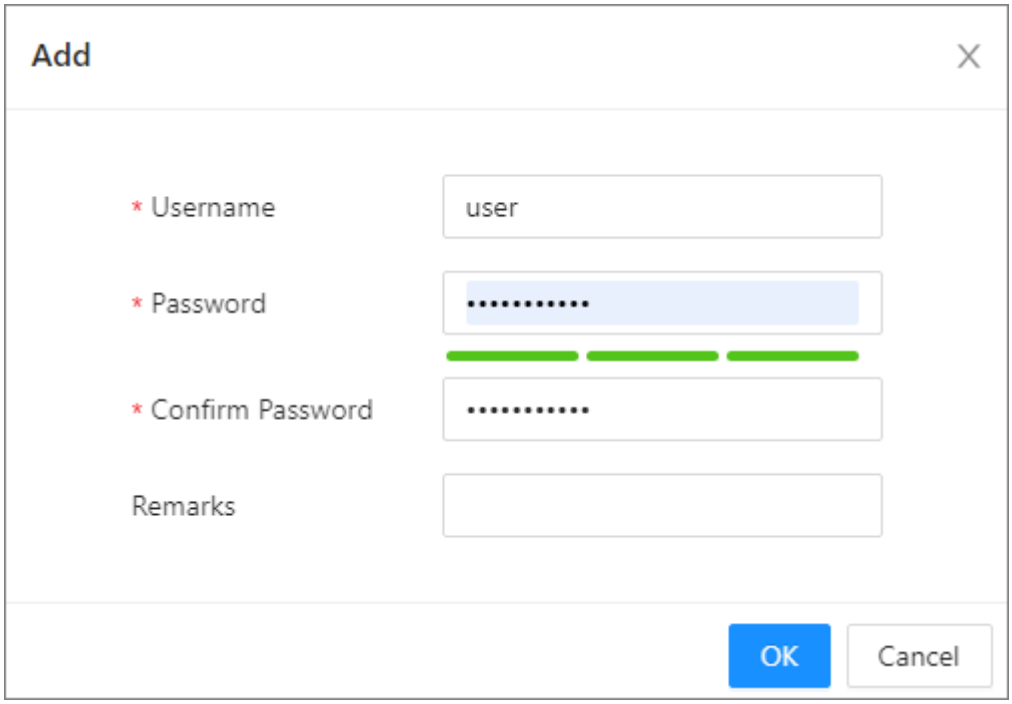


Table 3-18 Description of user parameters

Parameter	Description
Username	User's unique identification. You cannot use existing user name. The max. length of the username is 31 characters which consist of number, letter, underline, dash, dot and @.
Password	The password must consist of 8–32 non-blank characters and contain at least two types of number, letter, and special characters (excluding ' " ; : &).
Confirm Password	
Remarks	User-defined.

Step 5 Click **OK**.

The newly added user is displayed in the user list.

Related Operations

- Modify user information. Click to edit password, group of the added user.

For admin account, you can only edit the password.

- Delete user. Click to delete the added user.

The admin account cannot be deleted.

3.2.5.5.2 Resetting Password

Reset password through the e-mail address that you bound if you forget the password.

Procedure

Step 1 Log in to the webpage of VTS.

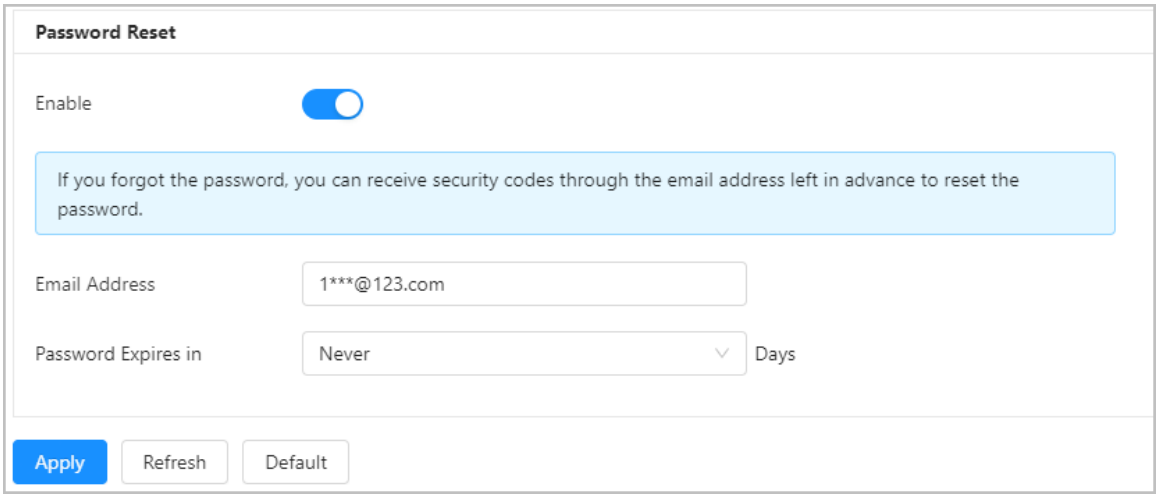
Step 2 Select **System** > **Account**.

Step 3 Click to enable **Password Reset**.

Step 4 Enter the email address and configure the password expiry period.

Password expires in x days: User-defined. If you select **Never**, the system does not remind you to change the password.

Figure 3-45 Reset password



Step 5 Click **Apply**.

3.2.5.5.3 Adding ONVIF User

You can add, delete ONVIF user, and change their passwords. The default ONVIF user is admin.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **System** > **Account** > **ONVIF User**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 3-46 Add ONVIF user

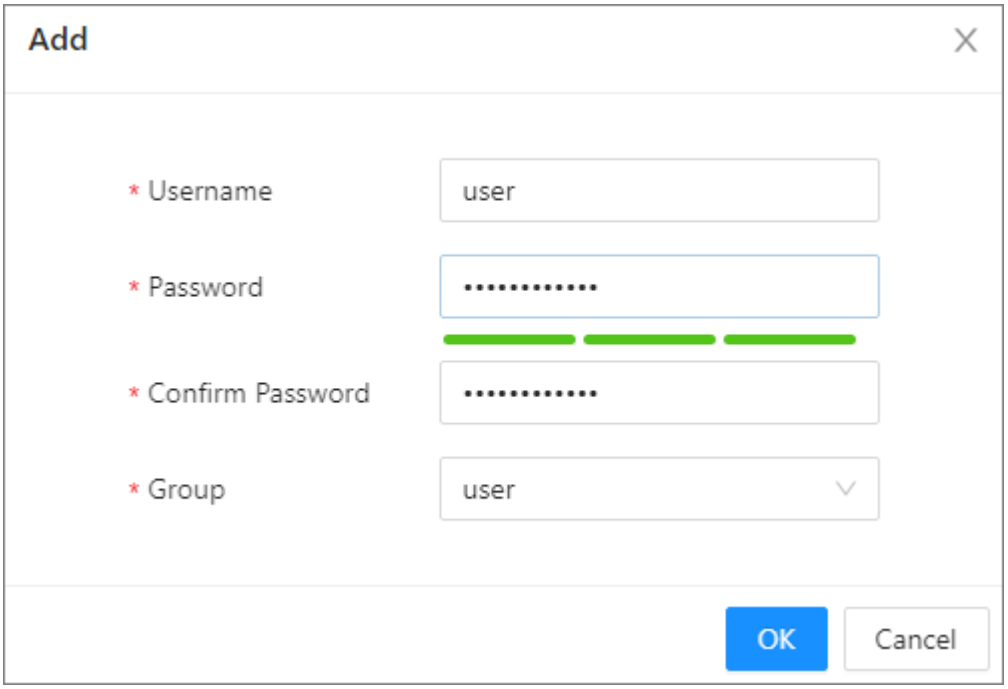


Table 3-19 Description of ONVIF user parameters

parameter	Description
Username	User's unique identification. You cannot use existed username. The max length of the user or group name is 31 characters which consist of number, letter, underline, dash, dot and @.
Password	The password must consist of 8–32 non-blank characters and contain at least two types of number, letter, and special characters (excluding ' " ; : &).
Confirm Password	
Group	The group that users belong to. Each group has different authorities.

Step 5 Click **OK**.

The newly added user displays in the username list.

Related Operations

- Modify user information. Click to edit password, group of the added user.

  For admin account, you can only edit the password.

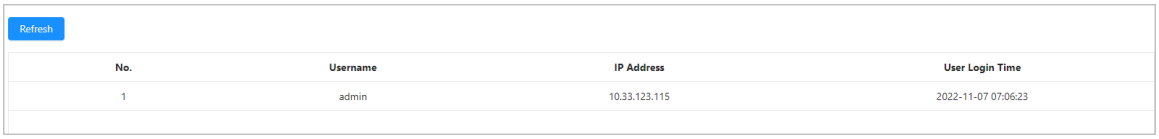
- Delete user. Click to delete the added user.

  The admin account cannot be deleted.

3.2.5.6 Viewing Online User

Log in to the webpage of VTS. Select **System** > **Online User** to view the current users logging into the web. You can view username, IP address and login time.

Figure 3-47 Online user



3.2.5.7 Configuring Time

You can configure date, time zone, and NTP (Network Time Protocol) server.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **System** > **Time**.

Step 3 Configure the parameters.

Figure 3-48 Configure time

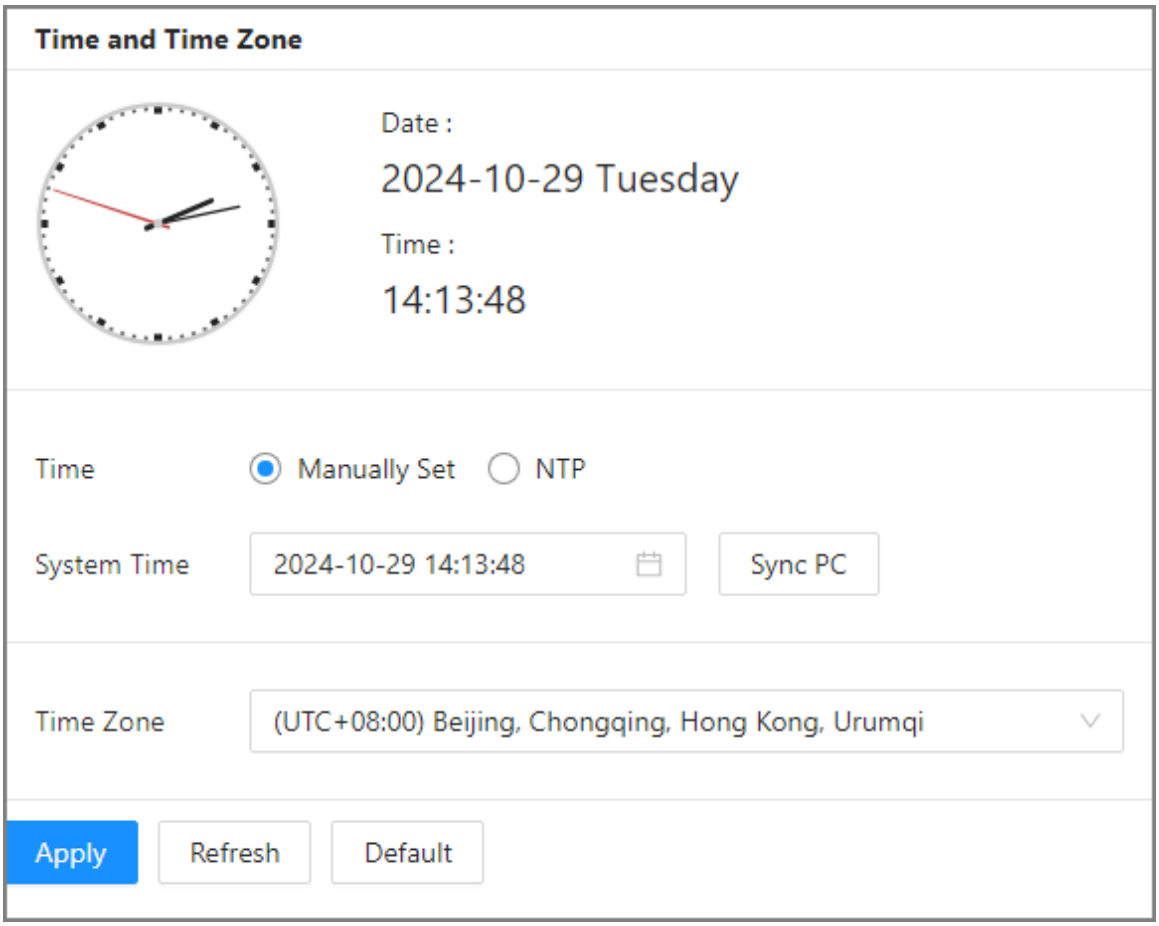


Table 3-20 Description of date and time parameters

Parameter		Description
Time and Time Zone	Time	Select **Manual Settings** or **NTP**.

Parameter		Description
	System Time	If you select **Manual Settings**, configure the system time manually. Click **Sync PC**, and the system time changes to the PC time.
	Server	If you select **NTP**, the system then syncs time with the internet server in real time. You can also enter the IP address, port, and interval of a PC running NTP server to use NTP.
	Port	
	Interval	
	Time Zone	Configure the time zone that VTS is at.

Step 4 Click **Apply**.

3.2.6 Device Management

3.2.6.1 Configuring IPC

Supports connecting with no more than 32 IPC. VTS monitors the devices in an integrated way.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **Device Setting** > **IPC Info**.

Step 3 Click ✎ to configure the parameters of IPC.

Figure 3-49 Configure IPC

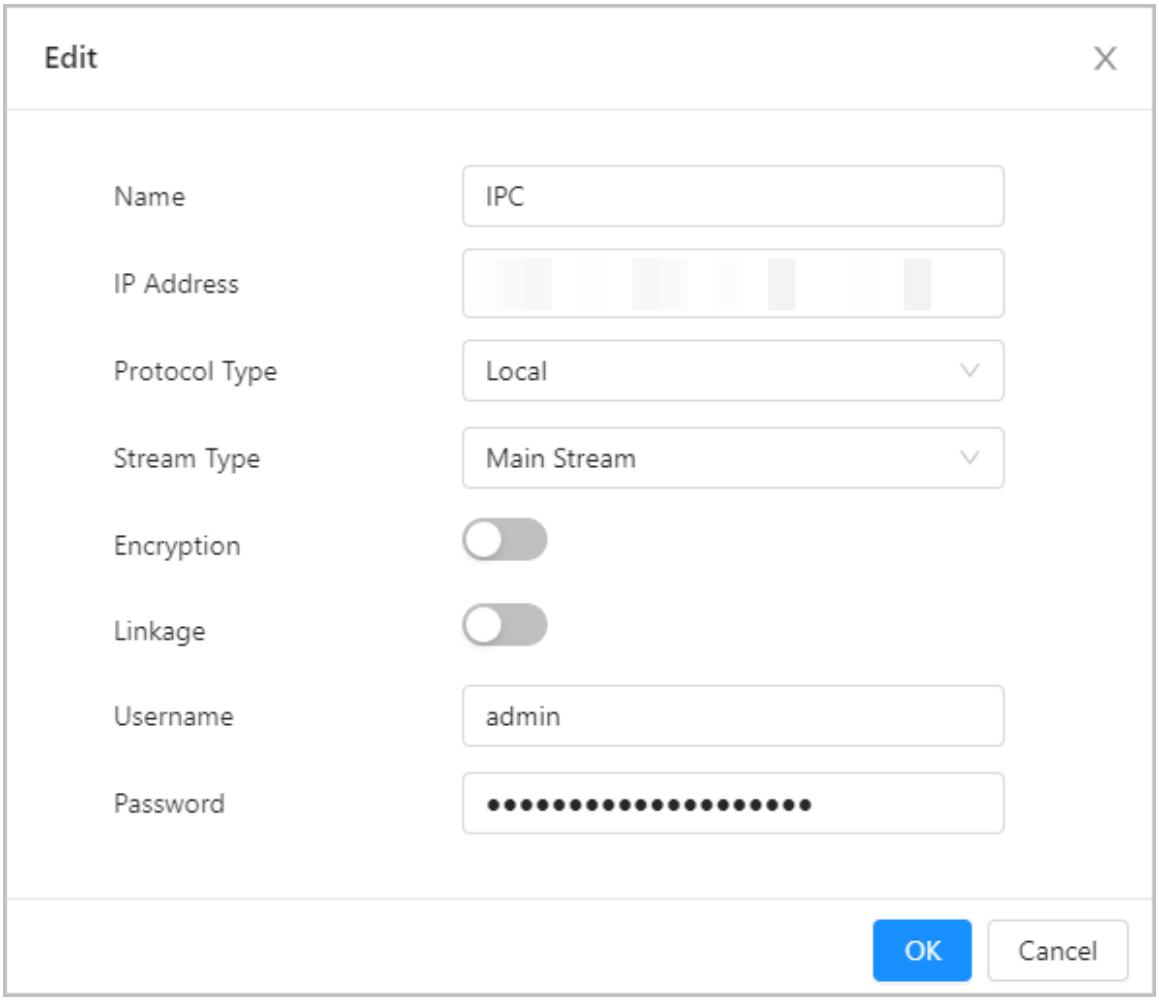


Table 3-21 Description of IPC parameters

Parameter	Description
Name	User-defined. You can configure the name that distinguishes the device.
IP Address	IP address of the added IPC.
Protocol Type	Select local protocol or ONVIF protocol depending on the IPC that you added.
Stream Type	Select main stream or sub stream. • Main stream: Large stream has high definition, occupying a large bandwidth. Used for local storage. • Sub stream: Smooth image occupies a small bandwidth. Used for low-bandwidth network transmission.
Encryption	Turn on encryption. The video is transferred in encryption.
Linkage	VTH supports displaying the image of connected IPC when VTS calls VTH if you turn on this function.
Username	The username and password of the IPC that you added.
Password	

3.2.6.2 Adding VTO or VTS (VTS as Server)

Procedure

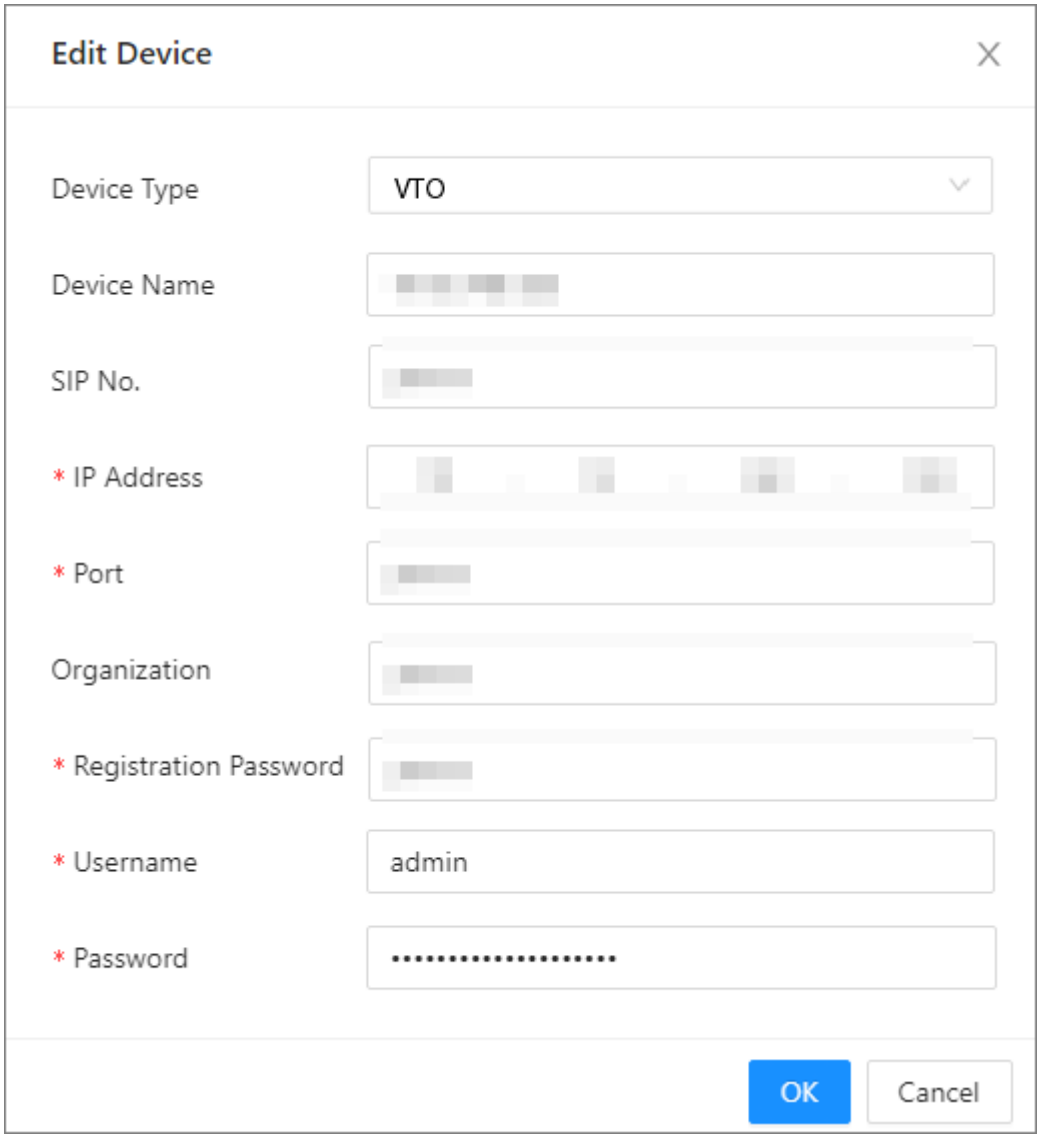
Step 1 Log in to the webpage of VTS.

Step 2 Select **Device Setting** > **Device Setting**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 3-50 Add VTO



Step 5 Click **OK**.

Related Operations

- Export: Export the device information.
- Import: Import the file to the current device to add devices in batches. The file must be exported from the device in the same model.
- Edit: Click to edit the device information.
- Go to device webpage: Click to go to the device webpage.
- Delete: Click to delete the device.

3.2.6.3 Adding VTO or Fence Station (VTS not as Server)

Procedure

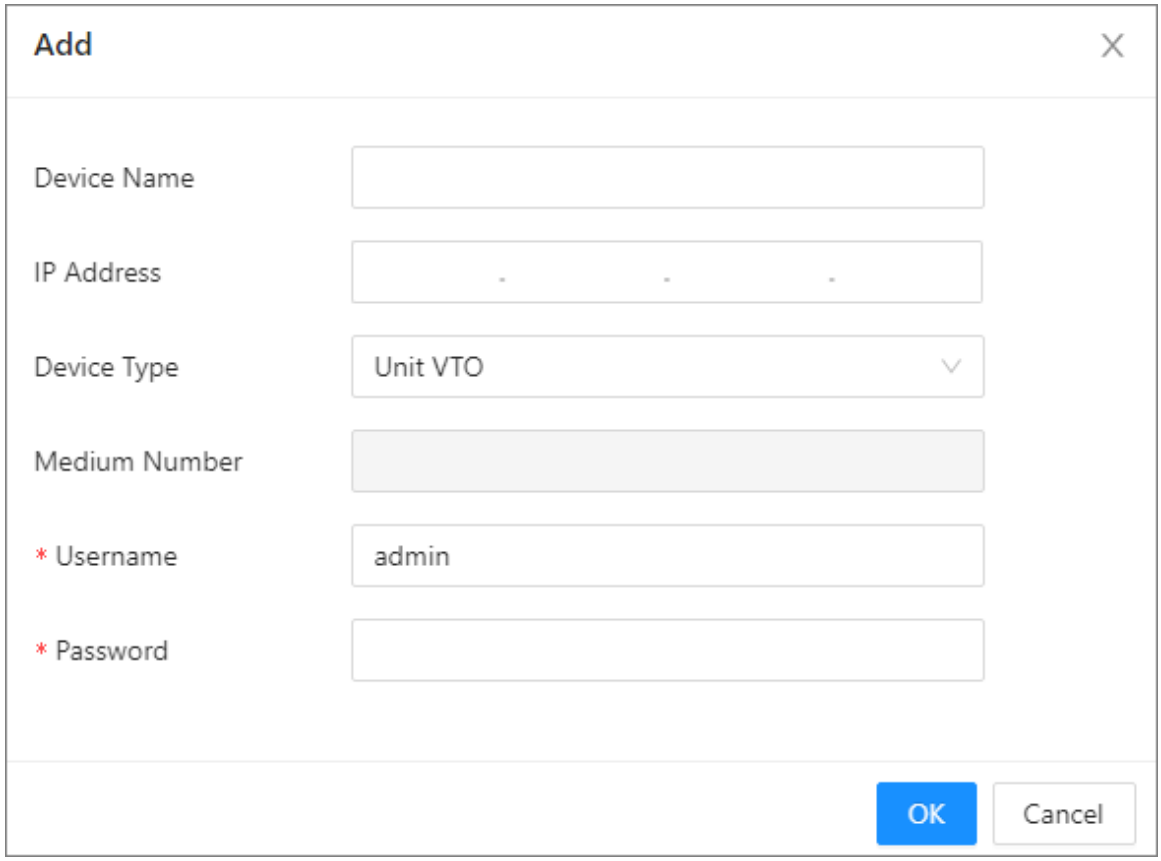
Step 1 Log in to the webpage of VTS.

Step 2 Select **Device Setting** > **Device Setting**.

Step 3 Click **Unit VTO** to add unit VTOs.

1. Click **Add**.
2. Configure the parameters.

Figure 3-51 Add VTOs

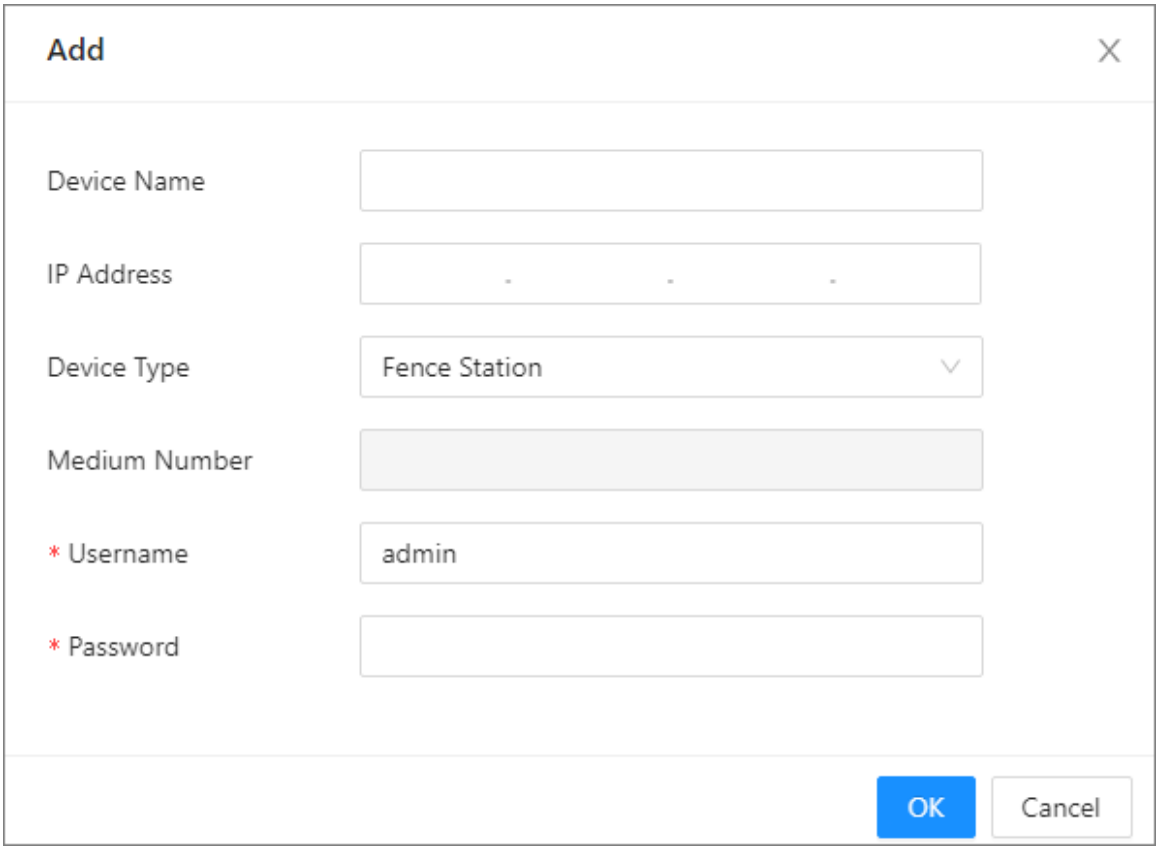


3. Click **OK**.

Step 4 Click **Fence Station** to add fence stations.

1. Click **Add**.
2. Configure the parameters.

Figure 3-52 Add VTO



3. Click **OK**.

Related Operations

- Export: Export the device information.
- Import: Import the file to the current device to add devices in batches. The file must be exported from the device in the same model.
- Edit: Click to edit the device information.
- Go to device webpage: Click to go to the device webpage.
- Delete: Click to delete the device.

3.2.6.4 Call Management

3.2.6.4.1 Call Group Configuration

Procedure

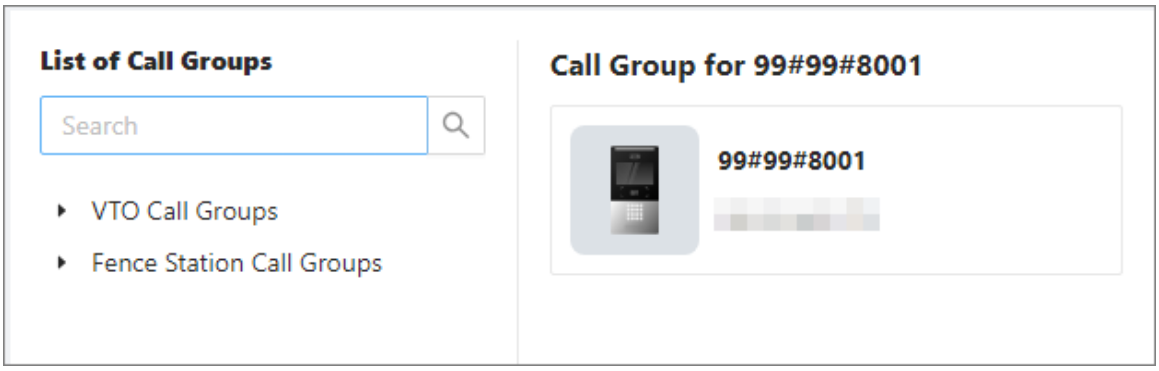
Step 1 Log in to the webpage of VTS.

Step 2 Select **Device Setting** > **Call Management** > **Call Group Config**.

Results

You can see the list of call groups.

Figure 3-53 Call group



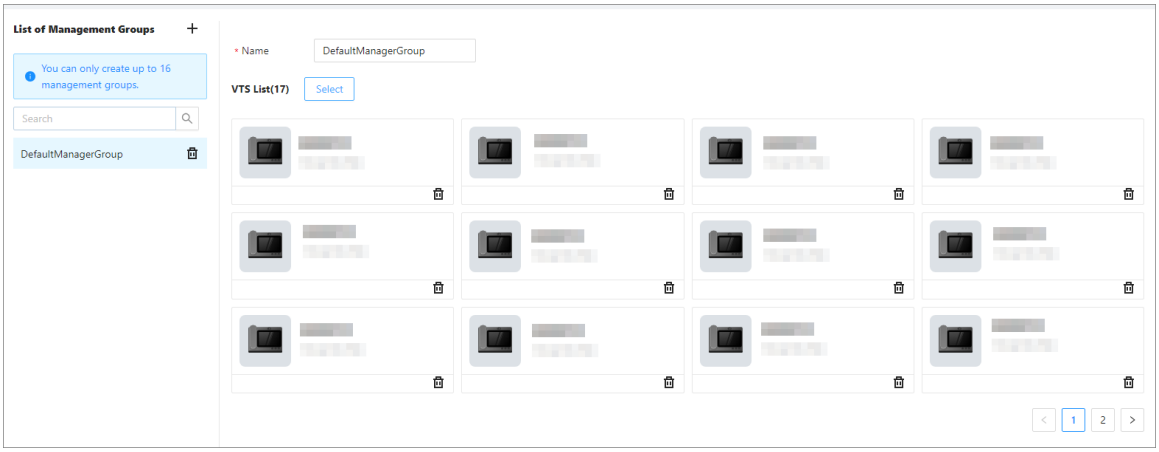
3.2.6.4.2 Management Group Configuration

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **Device Setting** > **Call Management** > **Management Group Config**.

Figure 3-54 Configure management group



Step 3 Click + to add new groups.

1. Enter a name for the group.
2. Click **Select** to select devices into the group, and then click **OK**.

You can only create up to 16 management groups.

Step 4 Click **Apply**.

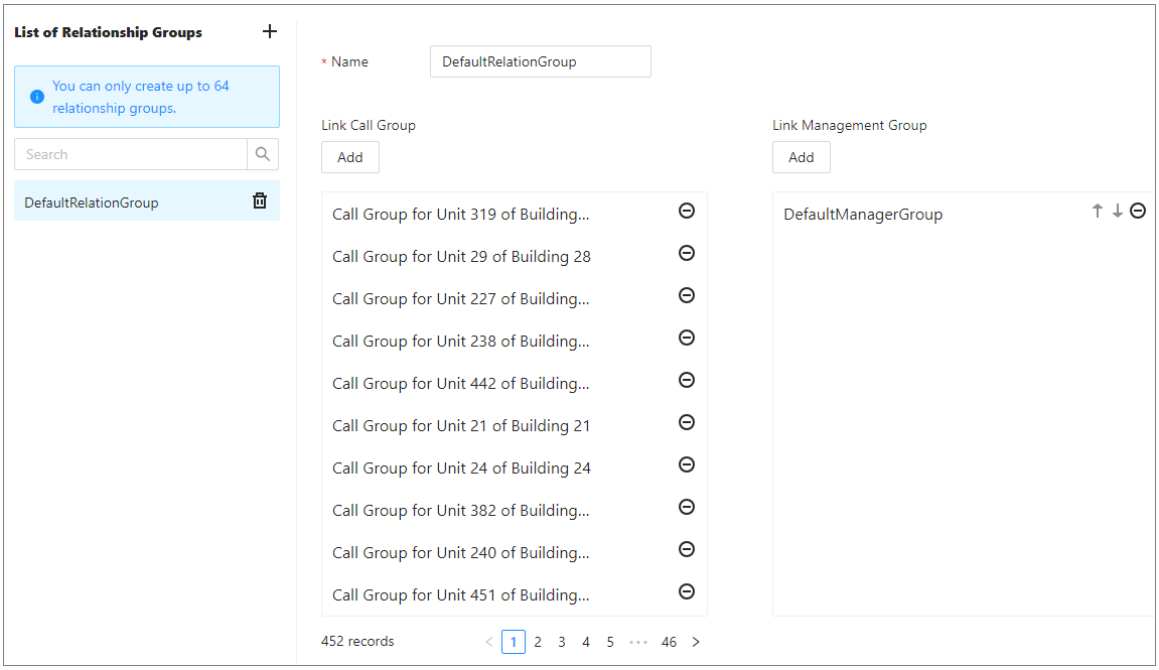
3.2.6.4.3 Relationship Group Configuration

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **Device Setting** > **Call Management** > **Relationship Group Config**.

Figure 3-55 Configure relationship group



Step 3 Click + to add a relationship group.

1. Enter a name for relationship group.
2. Click **Add** near the **Link Call Group** to add the call group.
3. Click **Add** near the **Link Management Group** to add the management group.

Step 4 Click **Apply**.

3.2.7 Person Management

Manage and view the information of the people such as password, cards, face and fingerprints.

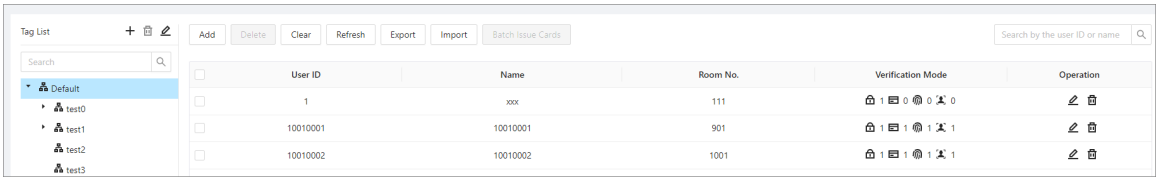
The card and fingerprint information that registered on the VTS will be uploaded to the personnel management in real time.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Person Management**.

Figure 3-56 Person management



Step 3 Click **Add**.

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

Figure 3-57 Add the person

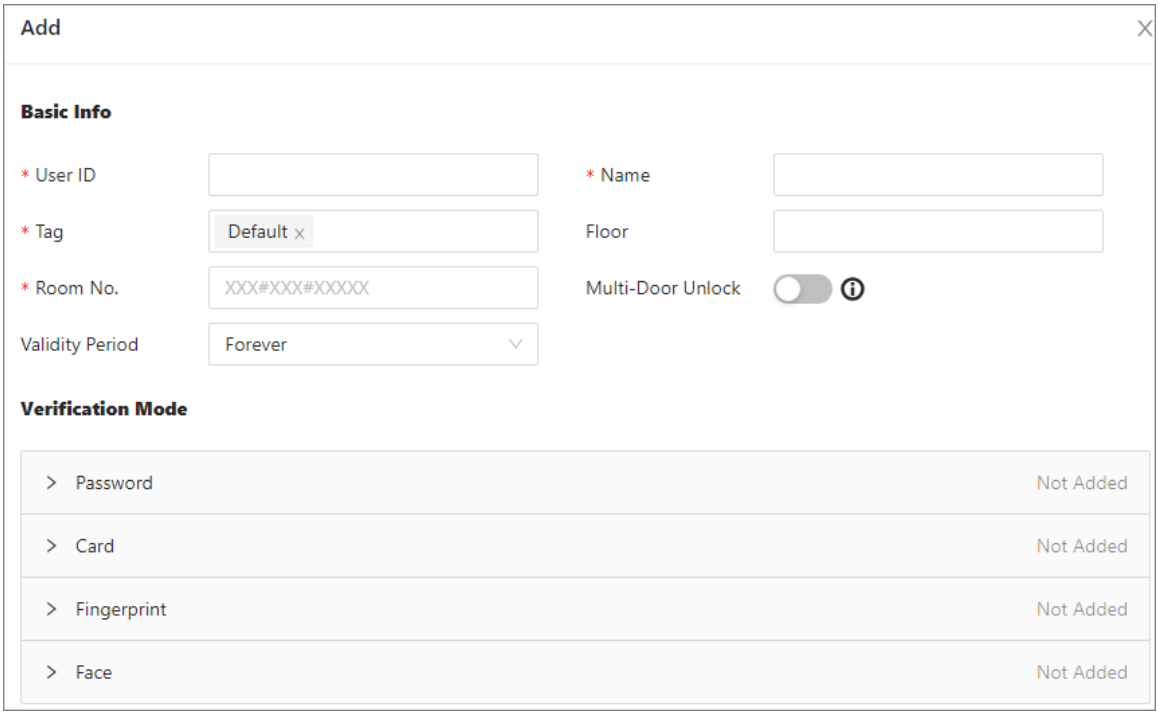


Table 3-22 Person parameters description

Parameter	Description
User ID	Customize the number.
Name	Enter the user name.
Tag	Set the tag for user.
Floor	Choose the floor which can be given the permission.
Room No.	Enter the corresponding room number of the VTH.
Multi-Door Unlock	When verification is successful, the local lock and external lock will open at the same time.
Validity Period	Configure the validity period during which people have access permissions.
Password	1. Select **Password** > **Add**. 2. Enter the password, and then confirm it again. The password must consist of 4-6 digits. 3. Click **OK**.

Parameter	Description
Card	You can add up to 5 cards by entering the card number or adding cards on the device. The card also can be issued by the USB card reader plugged onto the computer. 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. ● : Change the card number. ● : If you lost your card, click to report the loss. The icon becomes . ● : Delete the card.
Fingerprint	1. Select **Fingerprint** > **Add**. 2. Record your fingerprint according to the prompts. 3. Click **OK**.
Face	● **Upload** : Click **Upload** to upload the face image from the local computer. ● **Local Collection** : Click **Local Collection**, and then click **Start Snapshot** to snap through the device or the USB camera plugged onto the computer. ● The face image is only used for the device to unlock the door and does not involve other purposes. ● With no face algorithm, the quality of face cannot be guaranteed, so failure or unrecognition may occur when the image is sent to VTO. ● To ensure the quality of face collection, take the following requirement. ◇ The image format should be .jpg, .jpeg or .png. ◇ Do not cover your eyebrows, eyes, nose and mouth. ◇ Make sure that the face takes up more than 1/3 but no more than 2/3 of the whole image area. ◇ The horizontal rotation angle of the face, the pitch angle and the inclination angle should be within ±10°. ◇ Make sure the regular image brightness, moderate contrast, no shadow on the face, no overexposure and no underexposure. ◇ Make sure face integrity, clear outline and features, no heavy makeup, and image face area should be without editing modification processing.

Related Operations

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

- Click **Import**, and then select the file to import the person information.

3.2.8 Permission Management

3.2.8.1 Configuring Area

Procedure

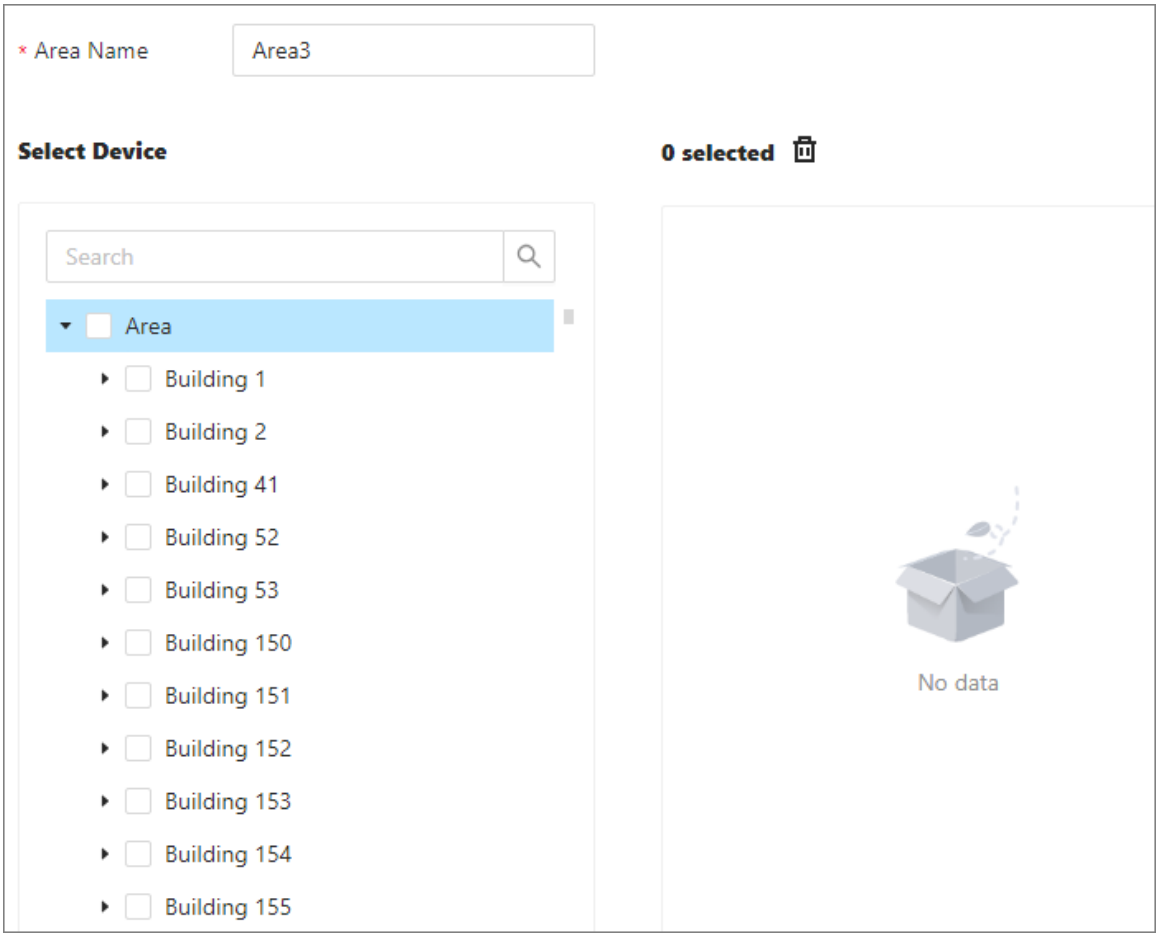
Step 1 Log in to the webpage.

Step 2 Select **Permission Management** > **Area Setting**.

Step 3 Click + to add new areas.

You can only create up to 40 areas.

Figure 3-58 Add new area



1. Enter an area name.
2. Select the device from the area list, and then add it to the selected list.

Step 4 Click **Apply**.

3.2.8.2 Permission Settings

Procedure

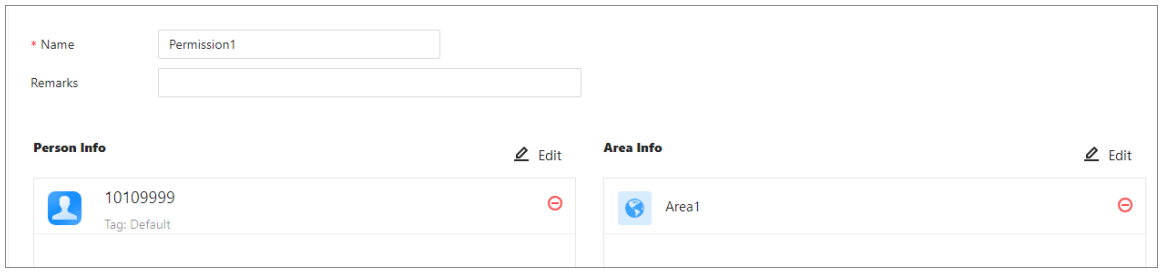
Step 1 Log in to the webpage.

Step 2 Select **Permission Management** > **Permission Settings**.

Step 3 Click + to add permission rules.

You can only create up to 128 rules.

Figure 3-59 Add new rules



Step 4 Click **Add** /**Edit** to add persons who need to follow the permission, and then click **OK**.

- Select by Tag: You can choose persons with the same tag.
- Select by Person: You can choose persons by user ID

Step 5 Click **Add** /**Edit** to add areas where need to follow the permission, and then click **OK**.

Step 6 Click **Apply**.

Related Operations

Click to delete added permissions.

3.2.8.3 Authorization Progress

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Permission Management** > **Authorization Progress**.

Figure 3-60 Progress

Device Name	Type	Progress	Results	Time	Operation
C6-151	Sync Person Info to VTO	84%	Succeed: 887, Failed: 168875	2024-10-31 14:09:29	
Local	Sync Person Info to Local Device		Succeed: 500, Failed: 0	2024-10-31 09:07:14	
C6-157	Sync Person Info to VTO		Succeed: 2000, Failed: 198000	2024-10-30 14:36:39	
C6-156	Sync Person Info to VTO		Succeed: 2000, Failed: 198000	2024-10-30 14:36:39	
C6-154	Sync Person Info to VTO		Succeed: 2000, Failed: 198000	2024-10-30 14:36:35	
C6-155	Sync Person Info to VTO		Succeed: 2000, Failed: 198000	2024-10-30 14:37:00	
C6-153	Sync Person Info to VTO		Succeed: 2000, Failed: 198000	2024-10-30 14:36:40	
C6-152	Sync Person Info to VTO		Succeed: 2000, Failed: 198000	2024-10-30 14:37:00	
95ttttdev	Sync Person Info to VTO		Succeed: 200000, Failed: 0	2024-10-30 19:28:22	
C6-151	Sync Person Info to VTO		Succeed: 2000, Failed: 198000	2024-10-30 14:37:02	

Related Operations

- Click to view the details of authorization.
- Click to retry the authorization.

3.2.9 Maintenance Center

3.2.9.1 One-Click Diagnosis

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

Procedure

Step 1 Log in to the webpage.

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

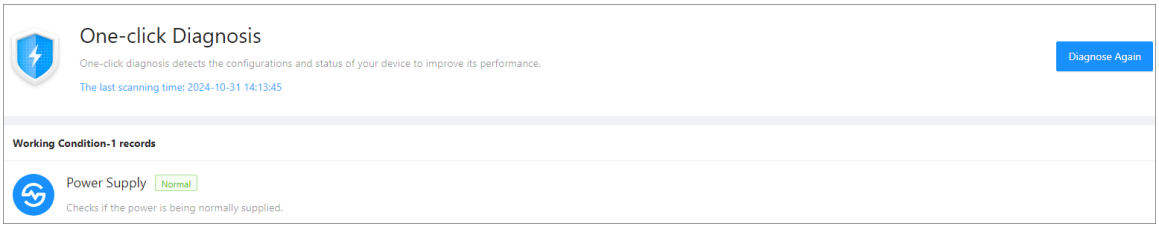
Step 3 Click **Diagnose**.

The system automatically diagnoses the configurations and the status of the device and display diagnosis results after it completes.

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

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

Figure 3-61 One-click diagnosis



3.2.9.2 System Information

3.2.9.2.1 Viewing Version Information

On the webpage, select **Maintenance Center** > **System Info** > **Version**, and you can view version information of the Device.

3.2.9.2.2 Viewing Legal Information

On the home page, select **Maintenance Center** > **System Info** > **Legal Info**, and then you can view the software license agreement, privacy policy and open source software notice.

3.2.9.3 Data Capacity

You can see how many users, cards and face images that the VTS can store.

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

Figure 3-62 Data capacity

3.2.9.4 Viewing Logs

View logs such as system logs, alarm logs, and unlock records.

3.2.9.4.1 System Logs

View and search for system logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **Log**.

Step 3 Select the time range and the log type, and then click **Search**.

Related Operations

- Click **Export** to export the searched logs to your local computer.
- Click **Encrypt Log Backup**, and then enter a password. The exported file can be opened only after entering the password.
- Click to view details of a log.

3.2.9.4.2 Call History

View call logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **Call History**.

3.2.9.4.3 Alarm Logs

View alarm logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **Alarm Logs**.

3.2.9.5 Maintenance Management

When more than one Device need the same configurations, you can configure parameters for them by importing or exporting configuration files.

3.2.9.5.1 Exporting and Importing Configuration Files

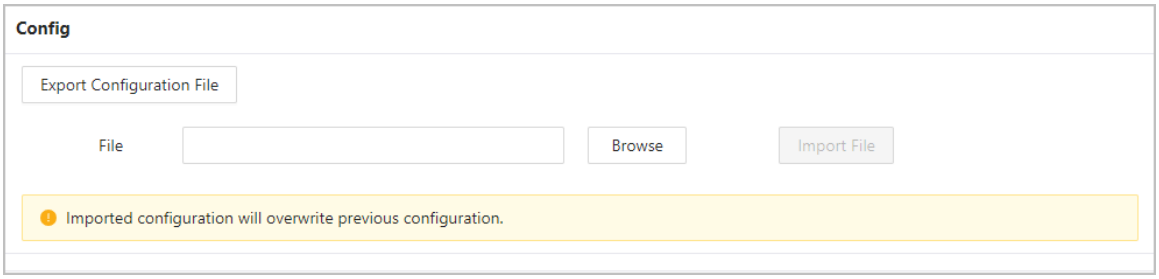
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Maintenance Management** > **Config**.

Figure 3-63 Configuration management



Step 3 Export or import configuration files.

- Export the configuration file.

  Click **Export Configuration File** to download the file to the local computer.

  The IP will not be exported.

- Import the configuration file.

  1. Click **Browse** to select the configuration file.
  2. Click **Import configuration**.

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

Step 4 (Optional) Click **Factory Defaults** to restore the device to the factory settings.

3.2.9.5.2 Maintenance

Regularly restart the VTO during its idle time to improve its performance.

Procedure

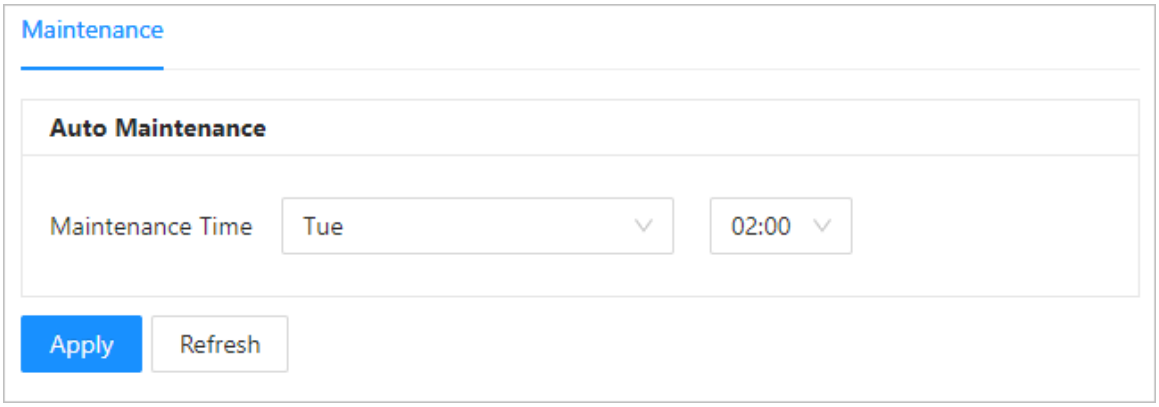
Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Maintenance Management** > **Maintenance**.

Step 3 Set the maintenance time, and then click **Apply**.

The Device will restart at the scheduled time, or you can click **Restart** to restart it immediately.

Figure 3-64 Maintenance time



3.2.9.6 Updating the System

- Use the correct update file. Make sure that you get the correct update file from technical support.
- Do not disconnect the power supply or network, and do not restart or shutdown the Device during the update.

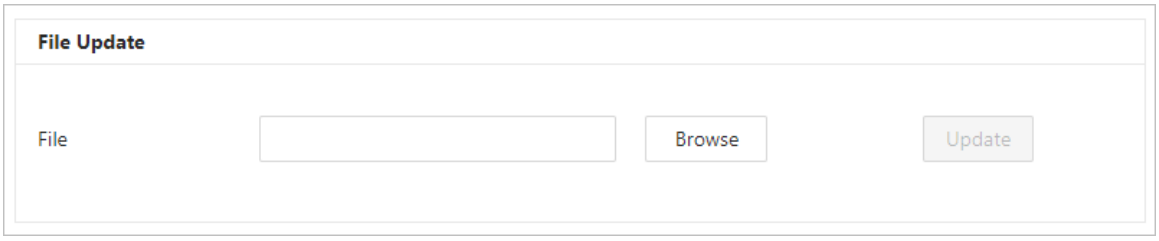
File Update

1. Log in to the webpage.
2. Select **Maintenance Center** > **Update**.
3. In the **File Update** area, click **Browse**, and then upload the update file.

   The update file should be a .bin file.
4. Click **Update**.

   The VTS will restart after the update finishes.

Figure 3-65 File update



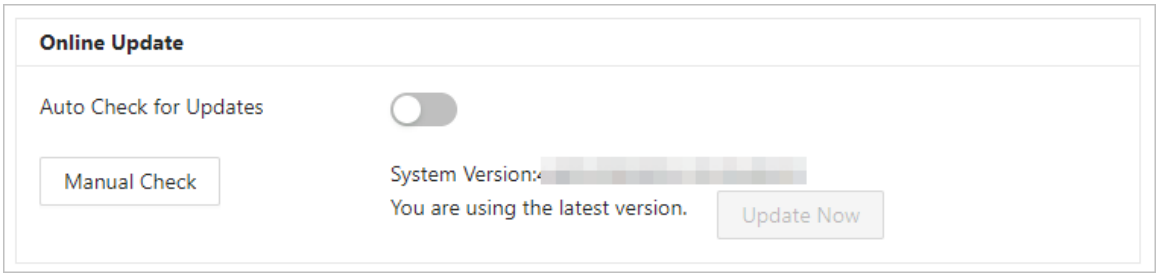
Online Update

1. Log in to the webpage.
2. Select **Maintenance Center** > **Update**.
3. In the **Online Update** area, select an update method.
   - Enable **Auto Check for Updates**, and then VTS will automatically check for the latest version update.

- Click **Manual Check**, and then you can immediately check whether the latest version is available.

4. (Optional) Click **Update Now** to update the VTS immediately.

Figure 3-66 Online update



3.2.9.7 Advanced Maintenance

Acquire device information and capture packet to make easier for maintenance personnel to perform troubleshooting.

3.2.9.7.1 Exporting

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Advanced Maintenance** > **Export**.

Step 3 Click **Export** to export the serial number, firmware version, device operation logs and configuration information.

3.2.9.7.2 Packet Capture

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Figure 3-67 Packet Capture

Step 3 Enter the IP address, click .

changes to .

Step 4 After you acquired enough data, click .

Captured packets are automatically downloaded to your local computer.

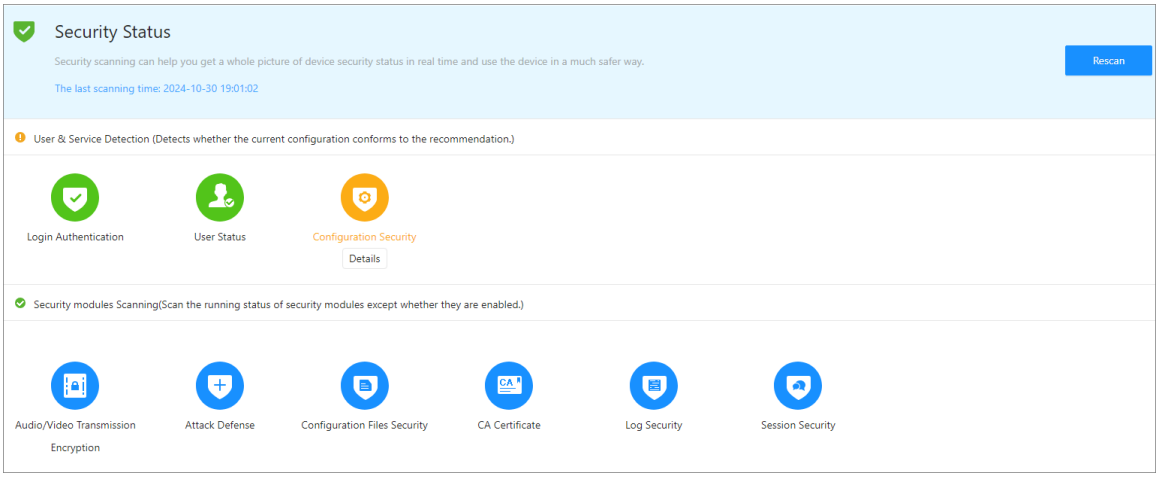
3.2.10 Security

3.2.10.1 Security Status

Detect and check the security status of the device.

Log in to the webpage of VTS. Select > **Security Status**. Click **Rescan** to scan the security status of the device.

Figure 3-68 Security status



User & Service Detection

- If the configuration of the detection item conforms to the recommendation, the icon is green.
- If the detection item needs to be optimized, the icon is yellow. Click **Details** to view the details of the scanning result. Click **Ignore** to ignore the exception, and it will not be scanned in next scanning.
- If the detection item will not be scanned, the icon is grey. Click **Start Detection** to include the detection item in next scanning.

Hover over the detection item to view the configuration of the current detection.

Security Modules Scanning

Hover over the security module icon to view the operating status.

3.2.10.2 Configuring System Service

Background Information

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your PC. The HTTPS can protect page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing private.

We recommend you enable the HTTPS. Otherwise, the device data may be leaked.

Procedure

Step 1 Log in to the webpage of VTS.

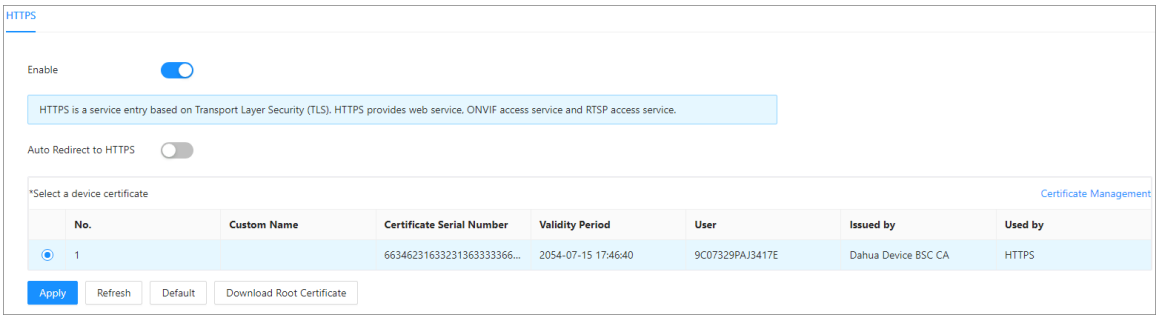
Step 2 Select > **System Service**.

Step 3 Click to enable HTTPS.

Step 4 Select the certificate.

If there is no certificate in the list, click **Certificate Management** at the left navigation bar. For details, see "3.2.10.4 Installing Device Certificate".

Figure 3-69 HTTPS



Step 5 Click **Apply**.

Results

Enter https://*IPaddress: https port* in the browser.

- If you have already installed the certificate, the normal login page will be displayed.
- If you have not installed the certificate, the browser displays a certificate error message.

3.2.10.3 Attack Defense

3.2.10.3.1 Configuring Firewall

Configure firewall to limit access to the device.

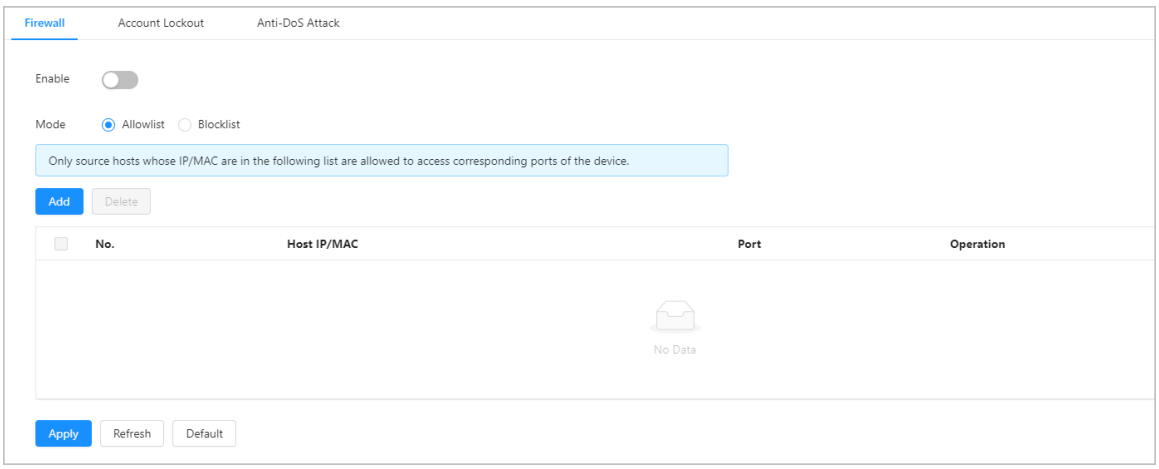
Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select > **Attack Defense** > **Firewall**.

Step 3 Click to enable the firewall function.

Figure 3-70 Firewall

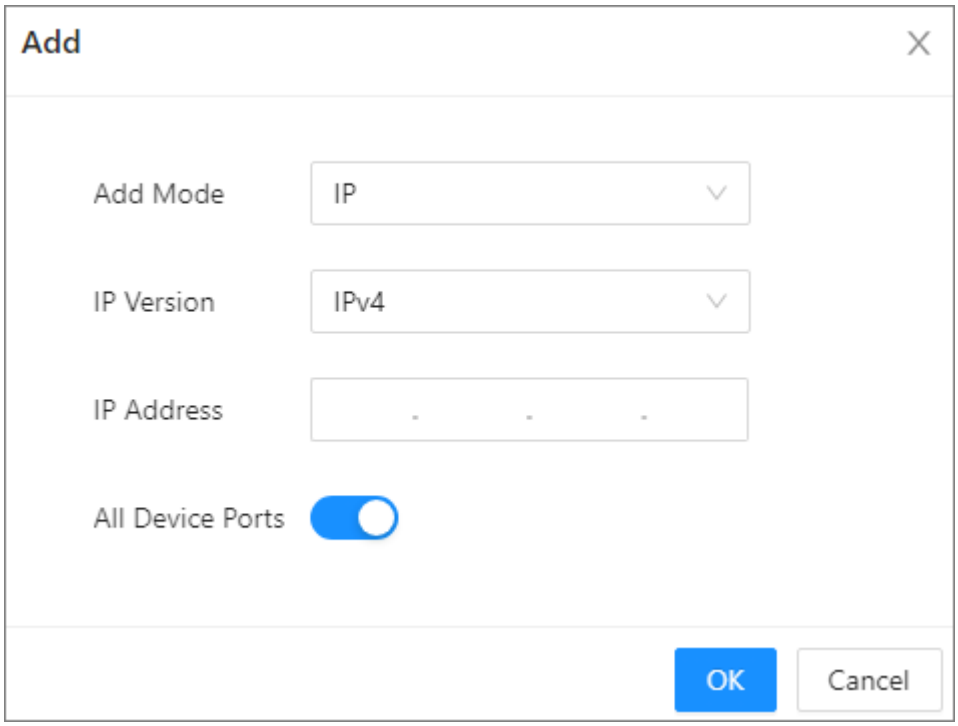


Step 4 Select **Allowlist** or **Blocklist** as the mode.

- Allowlist: Only when the IP/MAC address of your PC is in the allowlist, can you access VTS. Ports are the same.
- Blocklist: When the IP/MAC address of your PC is in the blocklist, you cannot access VTS. Ports are the same.

Step 5 Click **Add** to add the host IP/MAC address to **Allowlist** or **Blocklist**, and then click **OK**.

Figure 3-71 Add the address



Step 6 Click **Apply**.

Related Operations

- Click to edit the host information.
- Click to delete the host information.

3.2.10.3.2 Configuring Account Lockout

If you consecutively enter a wrong password more than the configured value, the account will be locked.

Procedure

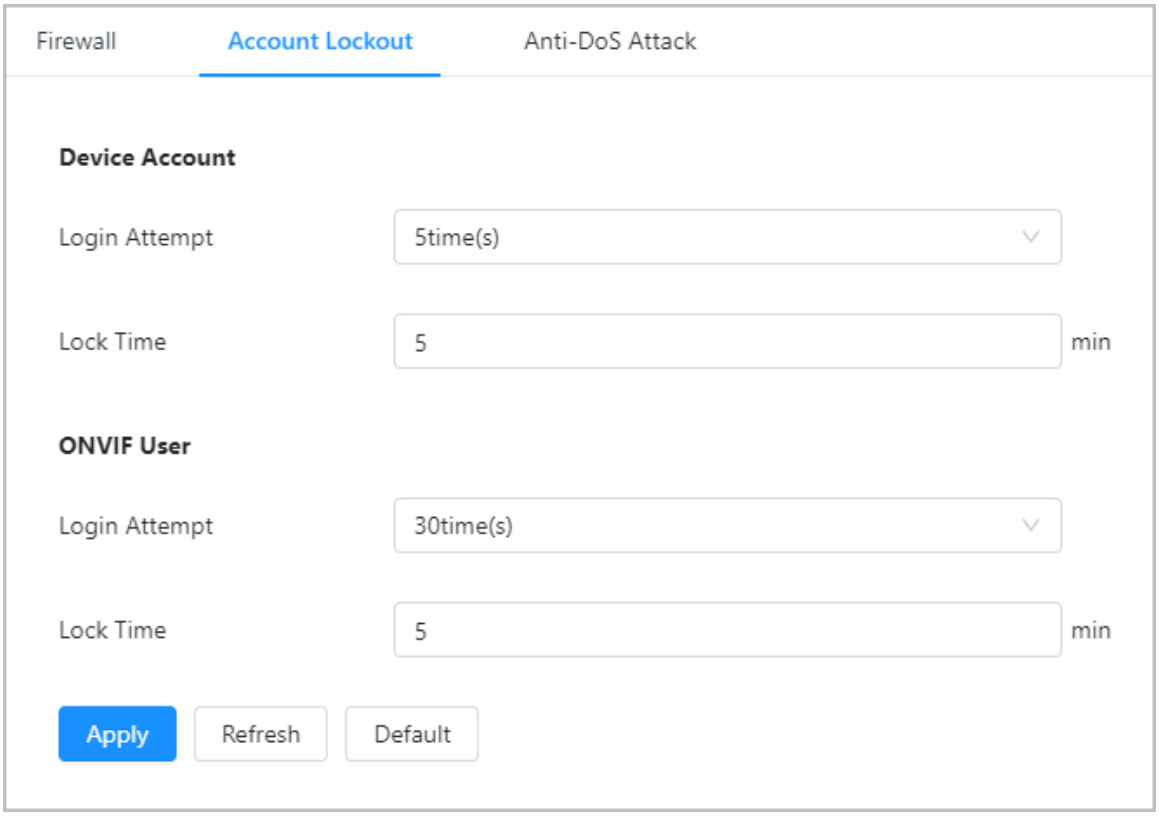
Step 1 Log in to the webpage of VTS.

Step 2 Select > **Attack Defense** > **Account Lockout**.

Step 3 Configure the login attempt and lock time for device account and ONVIF user.

- Login attempt: Upper limit of login attempts. If you consecutively enter a wrong password more than the defined value, the account will be locked.
- Lock time: The period during which you cannot log in after the login attempts reaches upper limit.

Figure 3-72 Account lockout



Step 4 Click **Apply**.

3.2.10.3.3 Configuring Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the device against DoS (Denial of Service) attack.

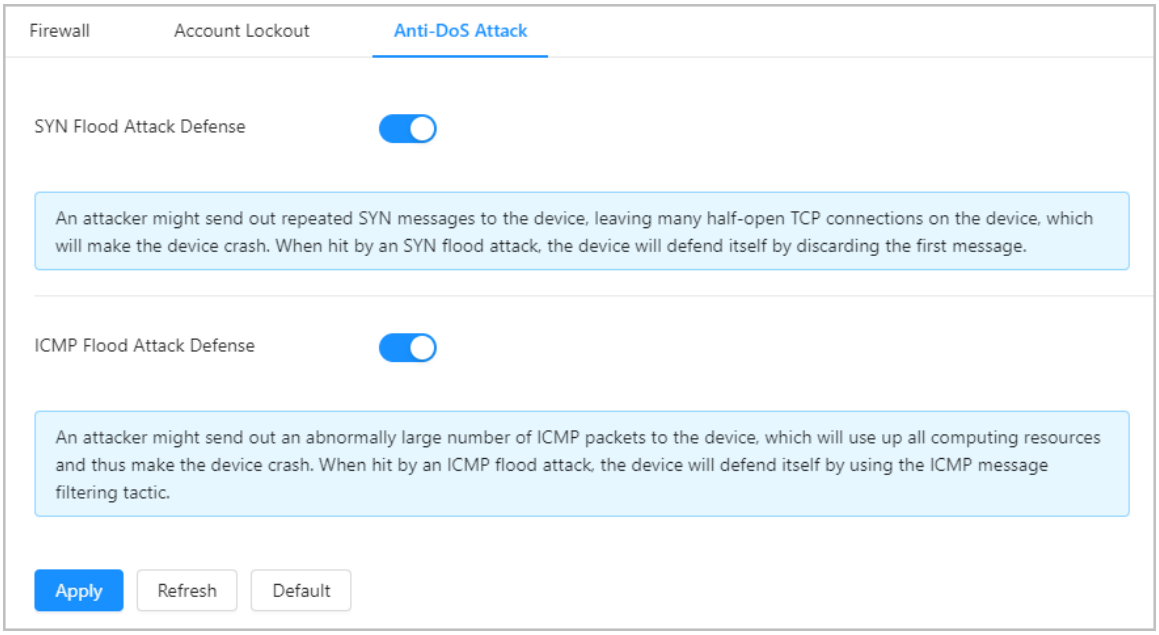
Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select > **Attack Defense** > **Anti-DoS Attack**.

Step 3 Select **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to defend the device against DoS (Denial of Service) attack.

Figure 3-73 Anti-DoS Attack



Step 4 Click **Apply**.

3.2.10.4 Installing Device Certificate

Create a certificate or upload an authenticated certificate, for example when you log in through HTTPS with your PC, you need to verify device certificate.

3.2.10.4.1 Creating Certificate

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select > **CA Certificate** > **Device Certificate**.

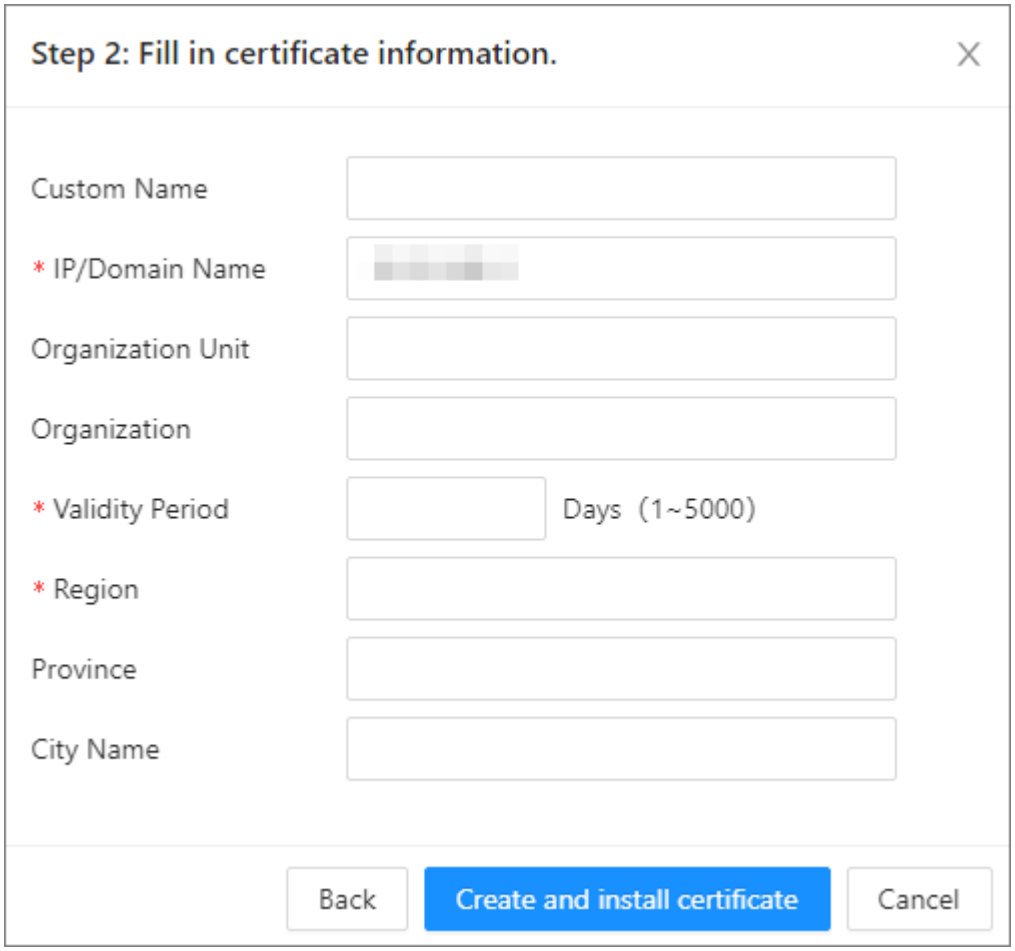
Step 3 Click **Install Device Certificate**.

Step 4 Select **Create Certificate** , and then click **Next**.

Step 5 Enter the certificate information.

IP or domain name of the device is automatically entered in **IP/Domain Name**.

Figure 3-74 Certificate Information (1)



Step 6 Click **Create and install certificate**.

After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

3.2.10.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the device.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select > **CA Certificate** > **Device Certificate**.

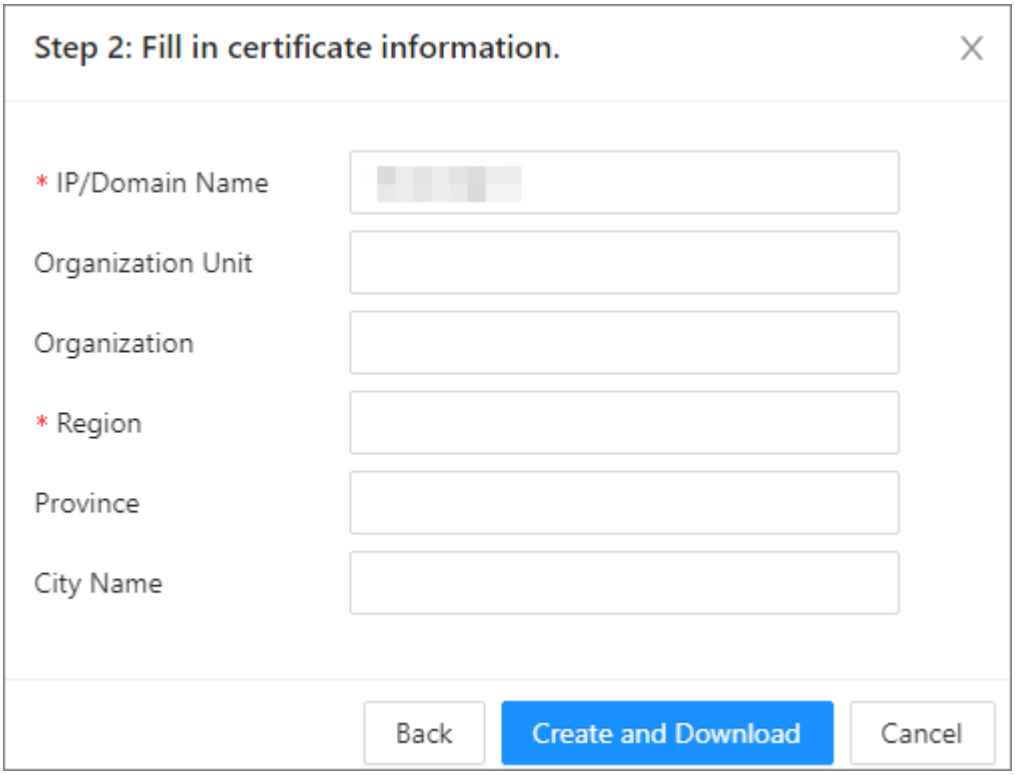
Step 3 Click **Install Device Certificate**.

Step 4 Select **Apply for CA Certificate and Import (Recommended)** , and then click **Next**.

Step 5 Enter the certificate information.

IP or domain name of the device is automatically entered in **IP/Domain Name**.

Figure 3-75 Certificate information (2)



Step 6 Click **Create and Download**.

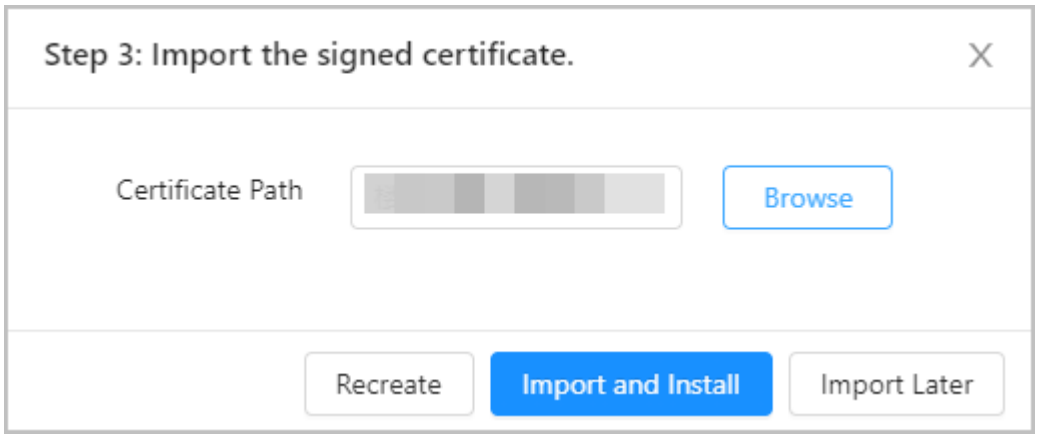
Save the request file to your PC.

Step 7 Apply for the CA certificate from the third-party certificate authority.

Step 8 Import the signed CA certificate.

1. Save the CA certificate to the PC.
2. Select **Install Device Certificate** , click **Apply for CA Certificate and Import (Recommended)**, and then click **Next**.
3. Click **Browse** to select the signed CA certificate.

Figure 3-76 Import the signed CA certificate



4. Click **Import and Install**.

   After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.

   - Click **Recreate** to create the request file again.

- Click **Import Later** to import the certificate next time.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

3.2.10.4.3 Installing Existing Certificate

Import the existing third-party certificate to the device. When apply for the third-party certificate, you also need to apply for the private key file and private key password.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select > **CA Certificate** > **Device Certificate**.

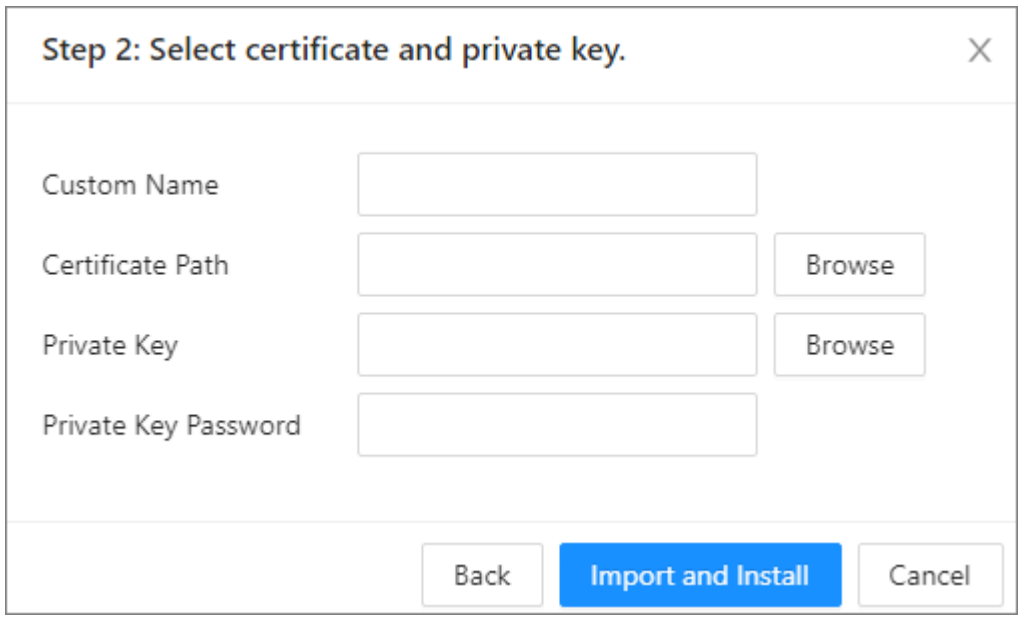
Step 3 Click **Install Device Certificate**.

Step 4 Select **Install Existing Certificate** , and then click **Next**.

Step 5 Click **Browse** to select the certificate and private key file.

Enter the private key password if the private key file is encrypted.

Figure 3-77 Certificate and private key



Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

3.2.10.5 Installing Trusted CA Certificate

CA certificate is a digital certificate for the legal identity of the camera. For example, when the camera accesses the LAN through 802.1x, the CA certificate is required.

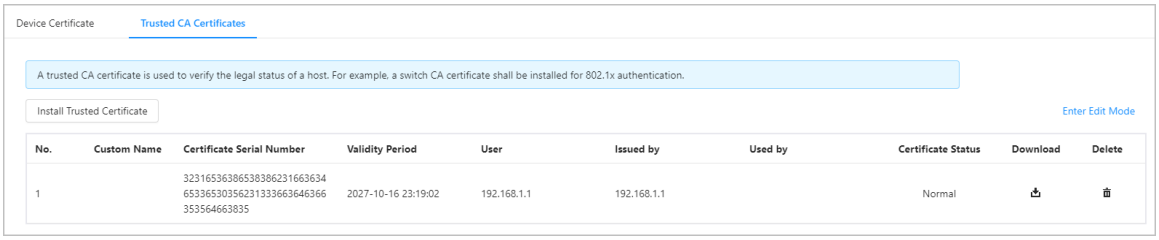
Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select > **CA Certificate** > **Trusted CA Certificate**.

Step 3 Click **Install Trusted Certificate**.

Figure 3-78 Install trusted certificate



Step 4 Click **Browse** in the pop-up window to select the certificate.

Step 5 Click **OK** to import the trusted certificate.

After the certificate is imported successfully, you can view the imported certificate on the **Trusted CA Certificate** page.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

3.2.10.6 Configuring Video Encryption

The device supports audio and video encryption during data transmission.

Background Information

We recommend you enable video encryption function. There might be safety risk if this function is disabled.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select > **Video Encryption**.

Step 3 Configure the parameters.

Figure 3-79 Video encryption

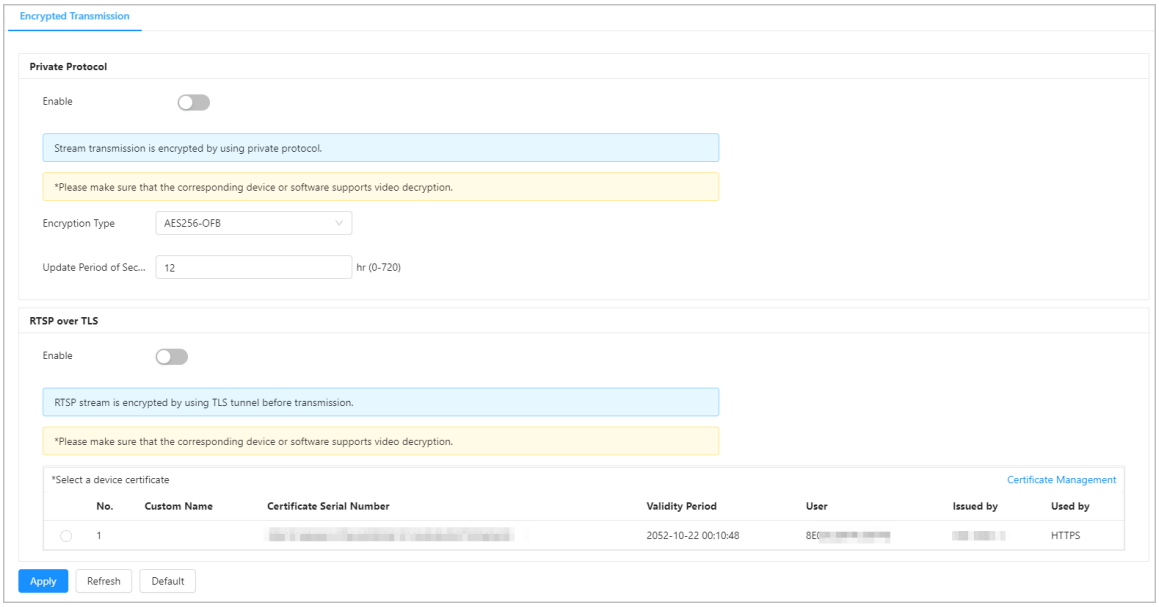


Table 3-23 Description of video encryption parameters

Area	Parameter	Description
Private Protocol	Enable	Enable stream frame encryption by using private protocol. Click to enable audio and video encryption during data transmission. Select the encryption type, and then configure update period of secret key. • **Encryption Type** : Use the default setting. • **Update Period of Secret Key** : Value range is 0–720 hours. 0 means never update the secret key.
	Encryption Type	
	Update Period of Secret Key	
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. Click , and then select a device certificate from certificate list.
	Certificate Management	For details about certificate management, see "3.2.10.4 Installing Device Certificate". Created certificate of imported certificate are displayed in **Select a device certificate** list.

4 Industrial Scenes

4.1 Operations on Local Device

This chapter introduces different configurations in industrial scene. Other configurations are the same with that in buildings scene.

4.1.1 Local Screen

Figure 4-1 Local screen

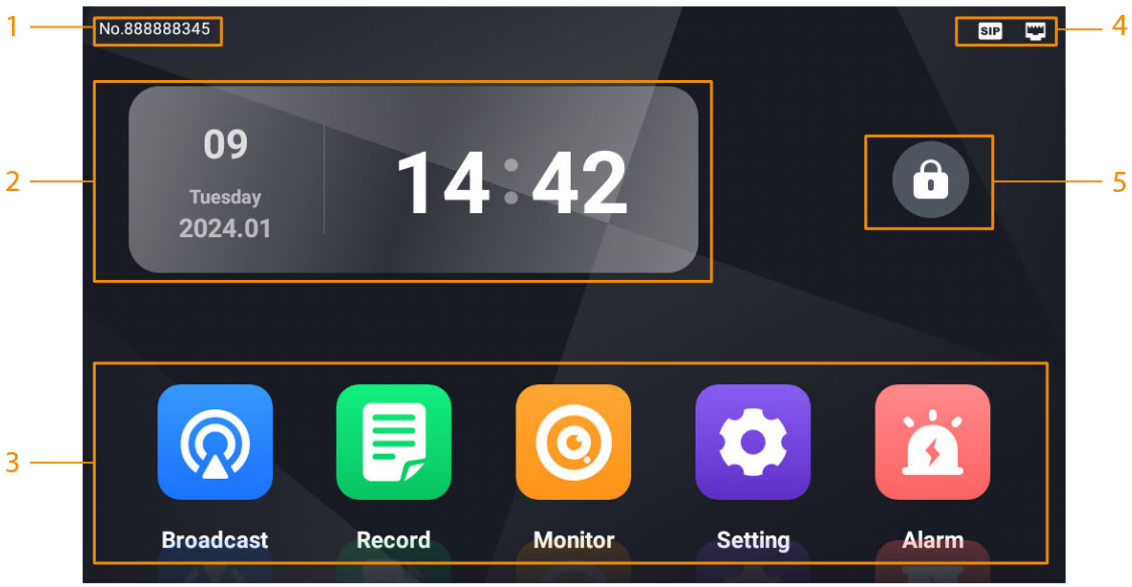


Table 4-1 Home screen introduction

No.	Description
1	The number of VTS.
2	Date and time.
3	Function buttons. • Broadcast: Play the voice or manual broadcasting on part of terminal devices or all terminal devices. For details, see "4.1.5.1 Broadcasting". • Record: Check the call history, video files and snapshot files. For details, see "4.1.5.2 Record". • Monitor: Monitor VTA and IPC. For details, see "4.1.5.3 Monitoring". • Setting: Enter the setting screen of VTS. For details, see "4.1.4 Project Settings". • Alarm: Displays the alarm messages reported by the VTA.

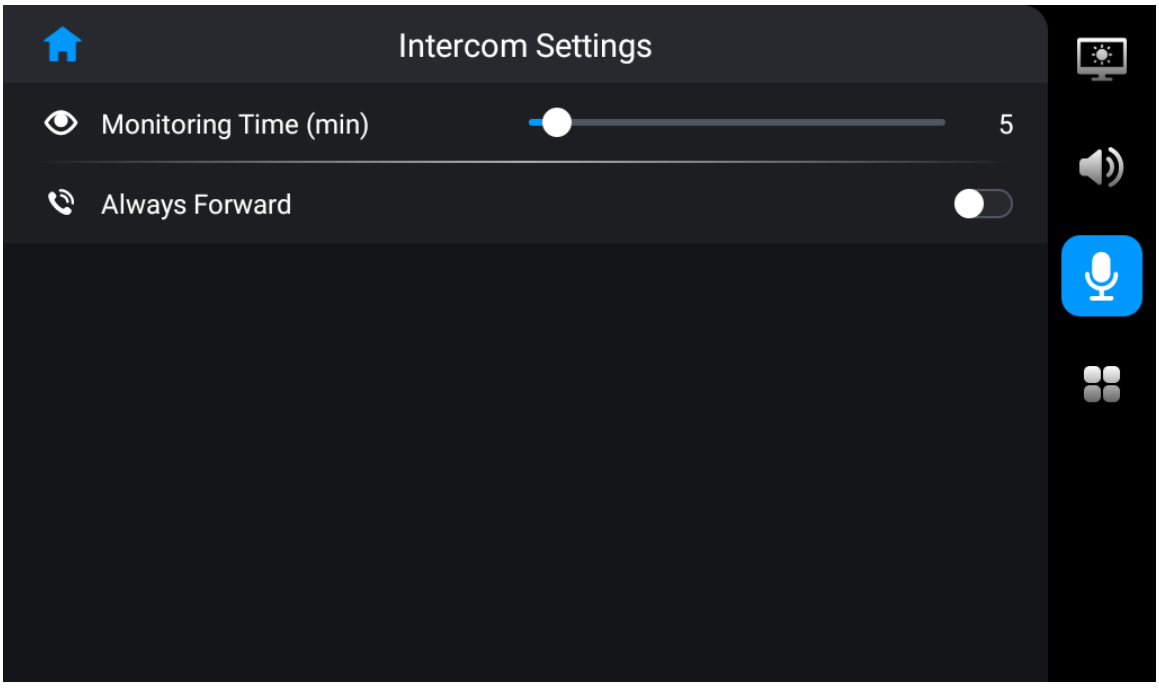
No.	Description
4	Tap  to lock the screen. If you select **Setting** > **Display Settings**, and turn on **Lock Screen** , you need to enter the default password **123456** to unlock the screen when you lock it after the configuration.
5	The connection status of the network, the SIP server, and the SD card.

4.1.2 Configuring Intercom Parameters

On the home screen, select **Setting** >  .

- The SIP server is not enabled: The parameters are the same with the parameters of building scene. For details, see "3.1.4 Configuring the Intercom Parameters".
- The SIP server is enabled: You can enable or disable **Always Forward**. After enabled, the call will be forwarded to other devices that you configured on the platform.

Figure 4-2 Intercom settings



4.1.3 Configuring the Advanced Parameters

The configurations of the advanced settings are the same with that in buildings scene. For details, see "3.1.5 Configuring the Advanced Parameters".

Receive Alarm Info from VTHs is not available under industrial scene.

4.1.4 Project Settings

4.1.4.1 Configuring VTS

Configure the number and network parameters of VTS.

Procedure

Step 1 Select **Settings** >  > **Project Setting** on the home screen.

Step 2 Enter the password, and then tap **OK**.

Step 3 Tap  , and then configure the parameters.

Figure 4-3 Configure the parameters

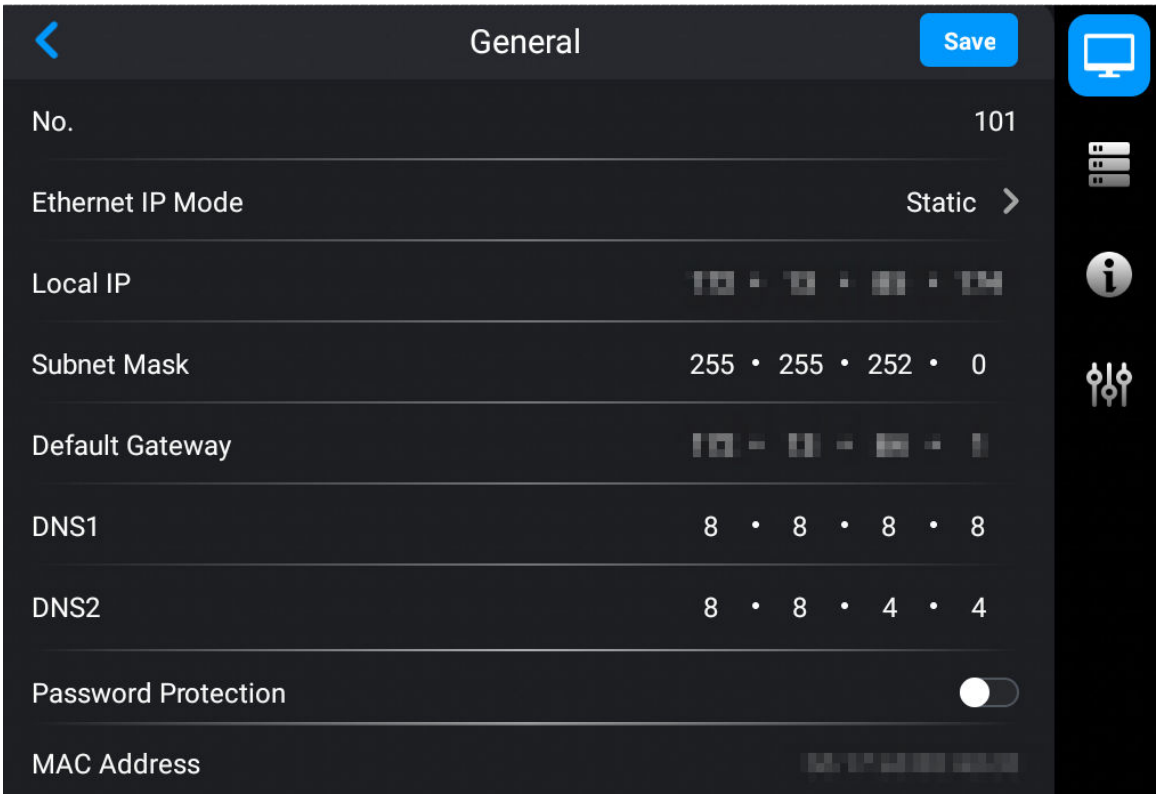


Table 4-2 Description of VTS parameters

Parameter	Description
No.	User-defined. You can configure the number from 101 to 999.
Ethernet IP Mode	Configure the mode to get the IP. • Static: Manually set **Local IP** , **Subnet Mask** and **Default Gateway**. • DHCP (Dynamic Host Configuration Protocol): Select **DHCP** if there is a DHCP server. The device automatically gets a dynamic IP address.
Local IP	If you select **Static** in **Ethernet IP Mode**, configure the IP address, subnet mask and default gateway according to the network planning.
Subnet Mask	

Parameter	Description
Default Gateway	
DNS 1	IP address of DNS server.
DNS 2	Standby IP address of DNS server.
Password Protection	Turn on password protection. The password is transferred in encryption when the device is registered on the platform through SIP.

4.1.4.2 Configuring Protocols

Procedure

Step 1 Select **Settings** >  > **Project Setting** on the home screen.

Step 2 Enter the password, and then tap **OK**.

Step 3 Tap  , and then configure the parameters.

- If VTS does not need the platform to connect, select **Private Protocol**.
- If VTS is connected to the platform through SIP agreement, select **SIP Server**, and then configure the parameters.

Table 4-3 Description of SIP server parameters

Parameter	Description
IP Address	IP address of SIP server.
Network Port	Network port number of SIP server. The platform as the SIP server: 5080.
Username	Default.
Password	Default.
Domain Name	Keep consistent with the SIP server. VDP as default.

Step 4 Tap **Save**.

4.1.5 Commissioning

4.1.5.1 Broadcasting

Play the voice or manual broadcasting on part of terminal devices or all terminal devices.

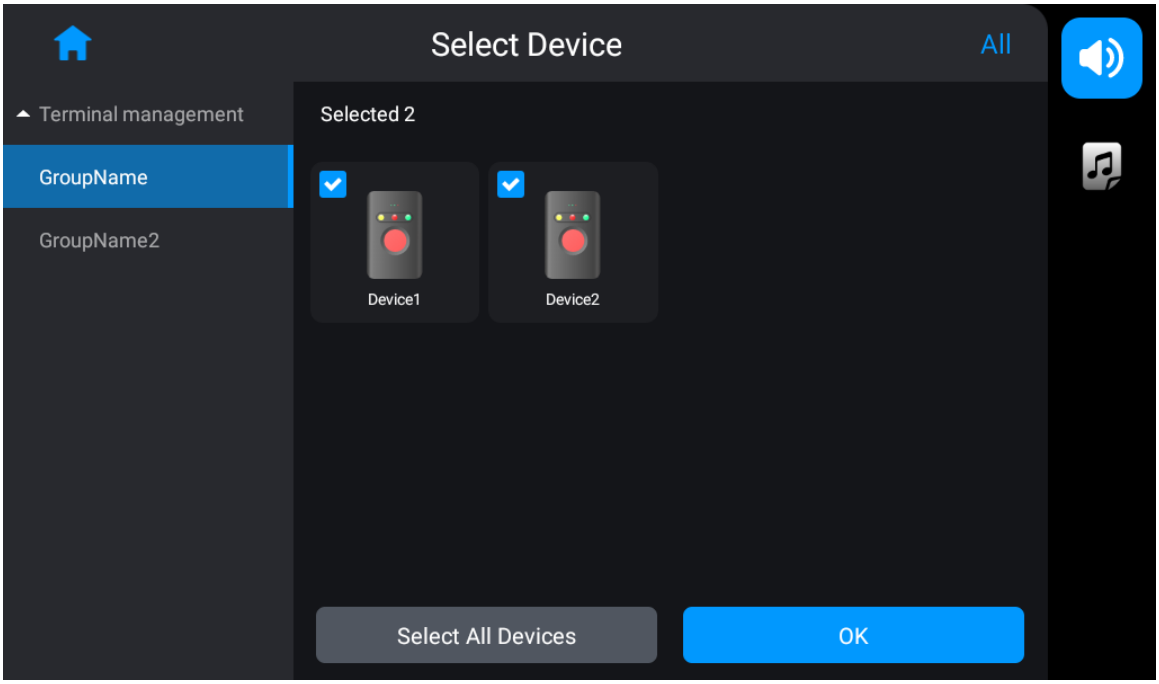
4.1.5.1.1 Broadcasting on Part of the Devices

Procedure

Step 1 Tap **Broadcast** on the home screen of VTS.

Step 2 Select the terminal devices, and then tap **OK**.

Figure 4-4 Select the terminal devices



Step 3 Select **Broadcast Type** , and then tap **Start Broadcast**.

- Audio File: Select the audio in the audio file list, and then tap **Start Broadcast** to play the audio.
- Manual Broadcast: Tap **Start Broadcast**, and then tap to broadcast.

Figure 4-5 Audio broadcasting

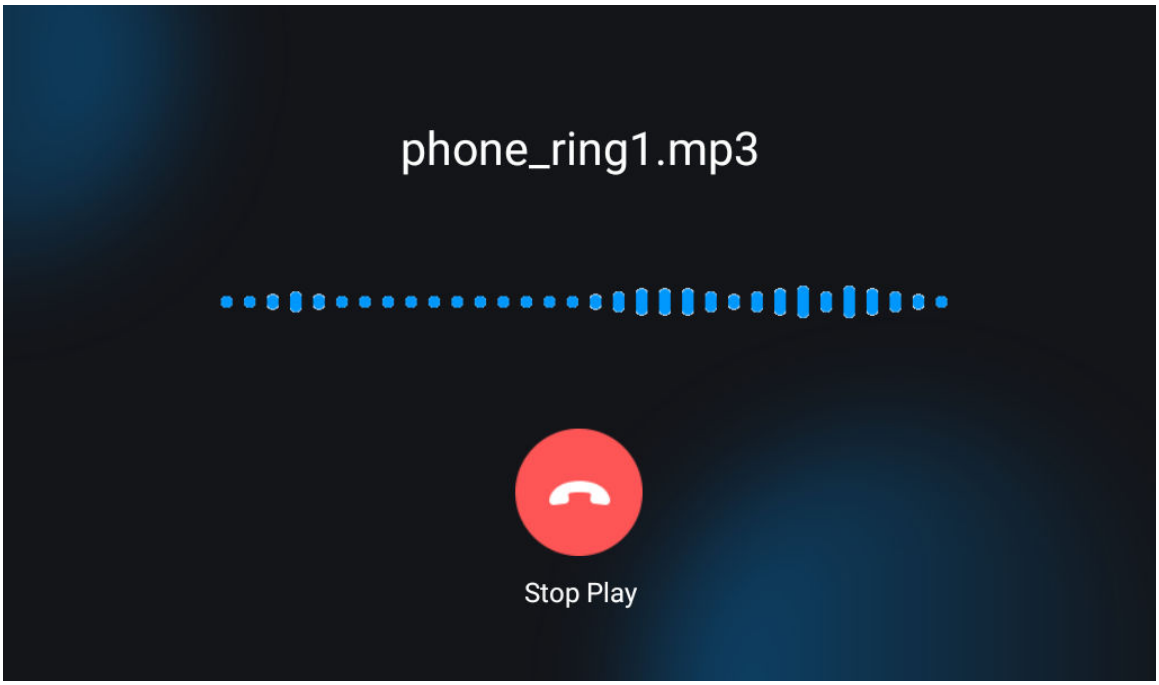
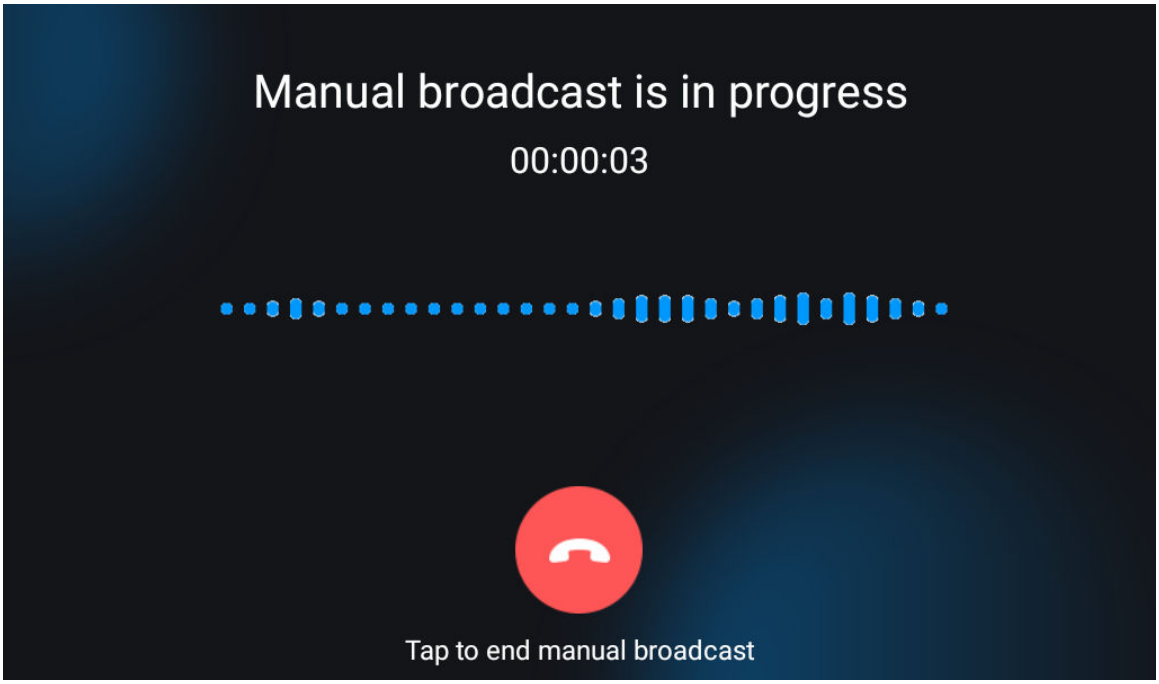


Figure 4-6 Manual broadcasting



4.1.5.1.2 Broadcasting on All Devices

Procedure

Step 1 Tap **Broadcast** on the home screen of VTS.

Step 2 Tap **Select All Devices**.

Step 3 Select **Broadcast Type**, and then start broadcast.

- Audio File: Select the audio in the audio file list, and then tap **Start Broadcast** to play the audio.
- Manual Broadcast: Tap **Start Broadcast**, and then tap  to broadcast.

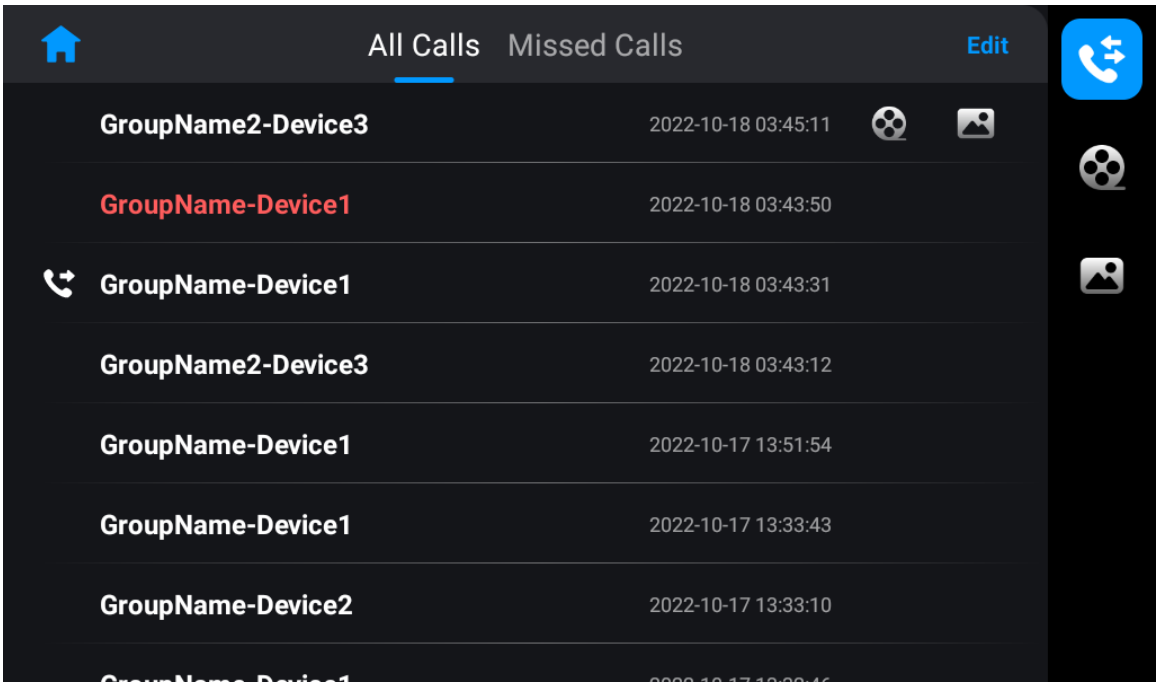
4.1.5.2 Record

Check the call history, the missed call records, video files and snapshot files.

Call History

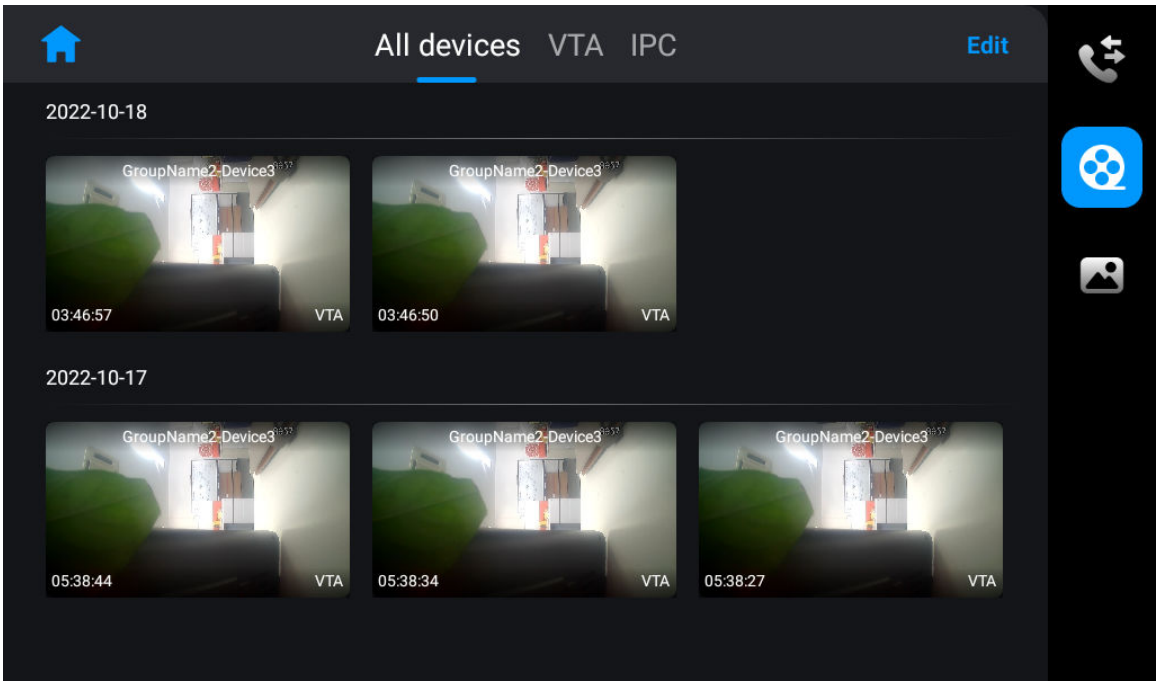
- Tap the call on call history list to call back.
-  : Check the snapshot files of the call.
-  : Check the video files of the call.

Figure 4-7 Call history



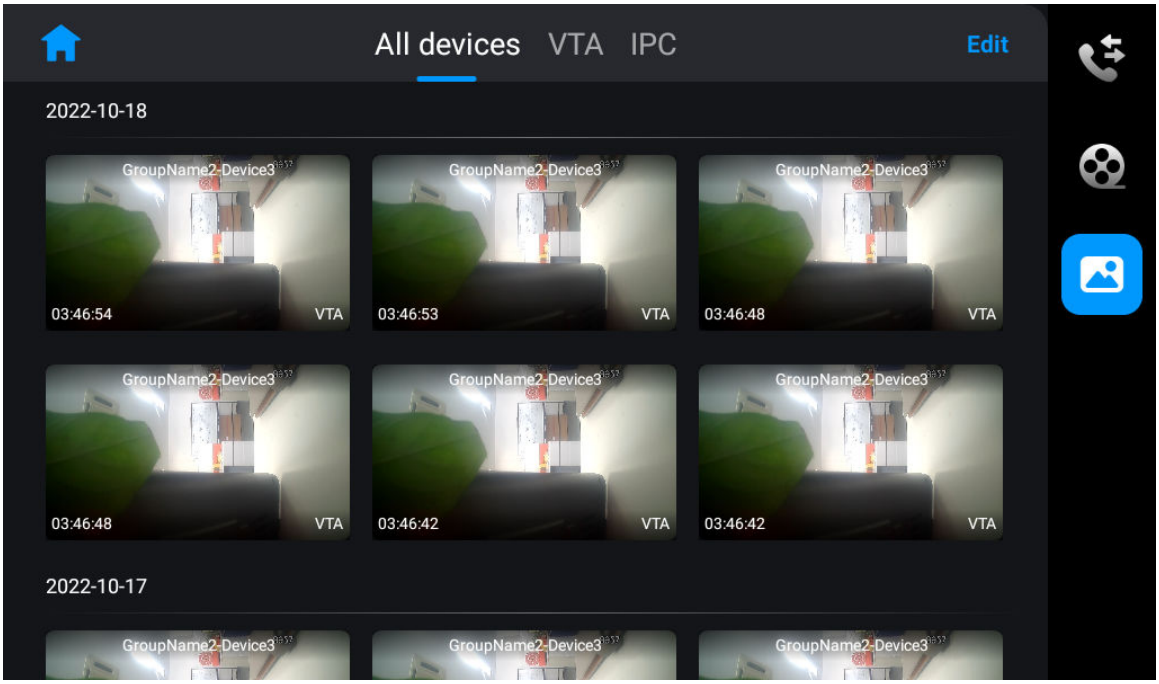
Video

Figure 4-8 Video files



Snapshot

Figure 4-9 Snapshot files



4.1.5.3 Monitoring

- VTS as the lower-level VTS: You can monitor and call VTA. IPC and VTA receive the call.
- VTS as the upper-level VTS: You can monitor and call VTA.

Use monitoring VTA as an example.

Tap **Monitor** on the home screen of VTS, and then tap the icon of VTA.

Figure 4-10 Monitor VTA

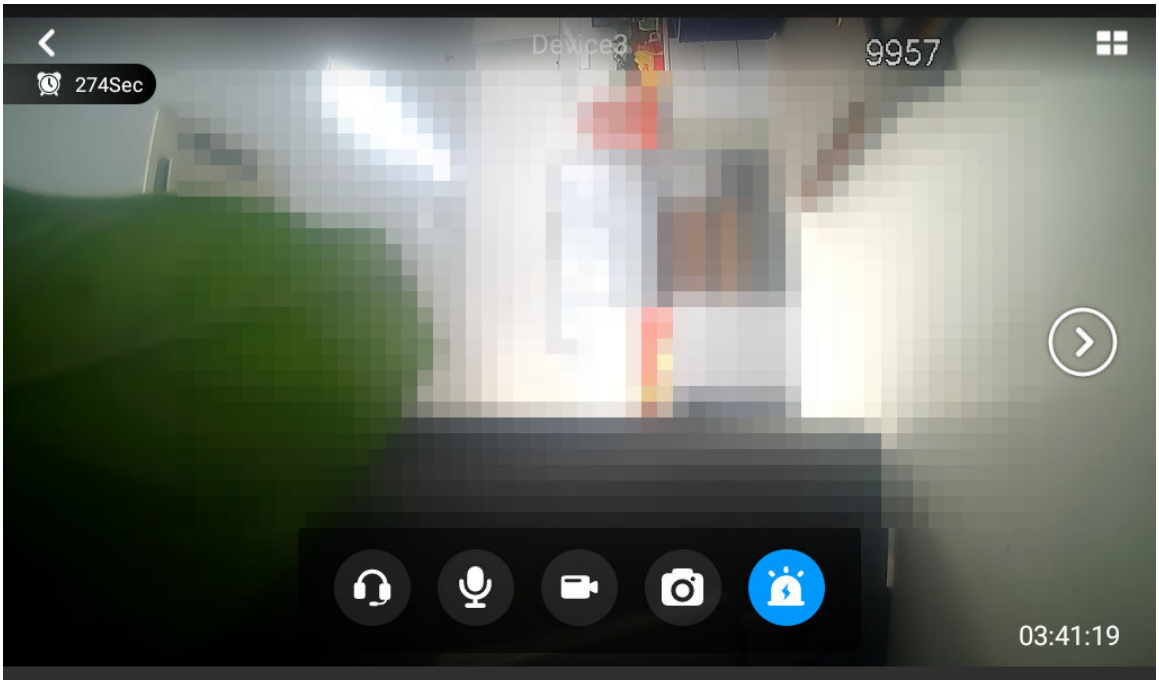


Table 4-4 Monitoring image description

Icon	Description
	Tap to view the monitoring image in 4 windows.
	Tap to convert to monitoring image of other terminal devices if VTS connects more than one terminal devices.
	Tap to receive the audio from VTA.
	Talk with the peer device.
	Tap to start manual recording.
	Tap to manually snapshot.
	Control the alarm indicator of VTA. ●  : The alarm indicator is on. ●  : The alarm indicator is off.

4.2 Operations on Webpage

This section introduces different configurations of VTS in industrial scene. Other configurations are the same with that in buildings scene.

4.2.1 Configuring Device Role

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **System** > **General**.

Step 3 Configure the parameters.

Figure 4-11 Configure the parameters

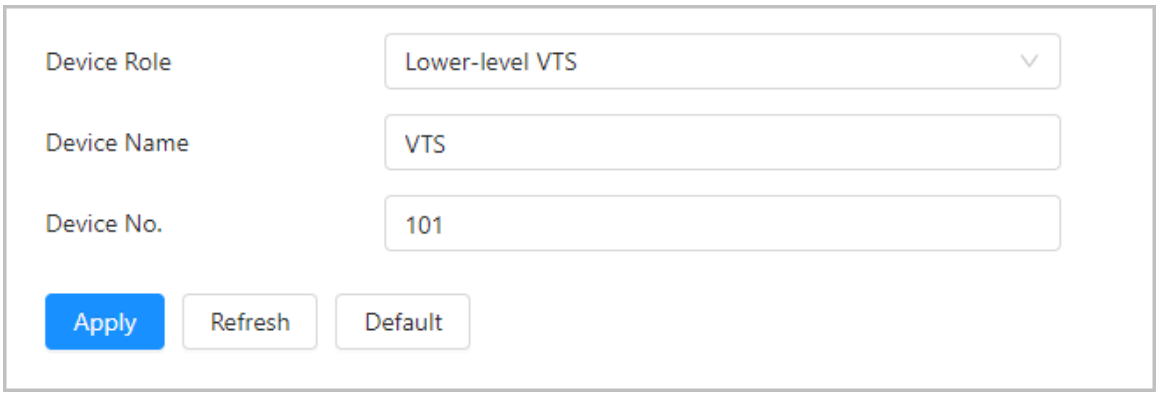


Table 4-5 Description of the device role parameters

Parameter	Description
Device role	Select from lower-level VTS, upper-level VTS and platform client. The information saved on the device will be cleared after you change the device role. • Lower-level VTS: Used as the lower-level VTS if there is no platform. It has the management permission of the device. You can add VTA and IPC. The operations of adding IPC are the same with that in buildings scene. • Upper-level VTS: Used as the upper-level VTS if there is no platform. It has permissions to add lower-level VTS. It does not have permission to manage organizational structure. You can add lower-level VTS. • Platform client: Used as the platform client if there is the platform. It does not have the management permission of the device.
Device name	You can configure the name that distinguishes the device.
Device No.	You can configure the number from 101 to 999.

Step 4 Click **Apply**.

4.2.2 Configuring SIP Server

Configure the parameters of SIP server. Connect to VTA through SIP agreement to achieve video intercom.

Procedure

Step 1 Log in to the webpage of VTS.

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

Step 3 Configure the parameters.

Figure 4-12 SIP server parameters

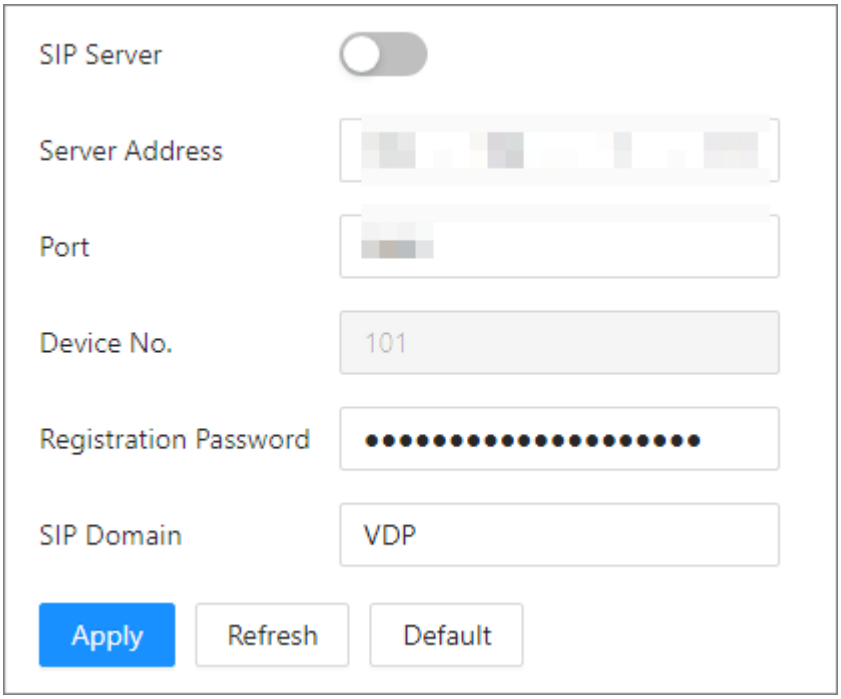


Table 4-6 Parameters description

Parameter	Description
Server Address	IP address of SIP server.
Port	Network port number of SIP server. The platform as the SIP server: 5080.
Device No.	Default.
Registration Password	
SIP Domain	Keep consistent with the SIP server. Domain name is VDP by default.

Step 4 Click **Apply**.

4.2.3 Configuring FTP

Get the audio file from FTP and play it.

If the SIP server is enabled, this function will not be displayed.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Network Settings** > **FTP**.

Step 3 Turn on **Enable**, and then configure the IP address, port, user name and password.

Step 4 Click **Apply**.

4.2.4 Device Setting

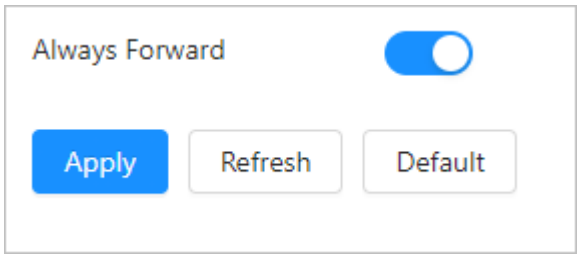
4.2.4.1 Using with the Platform

When using the device with the platform, enable the SIP server, and then configure the parameters.

4.2.4.1.1 Call Forwarding

Log in to the webpage of VTS, and then select **Device Setting** > **Call Forwarding**. Enable **Always Forward** , and then click **Apply**. Configure the device that receives the forwarding call, and the call will be forwarded.

Figure 4-13 Call forwarding



4.2.4.1.2 Device Management

Procedure

Step 1 Log in to the webpage.

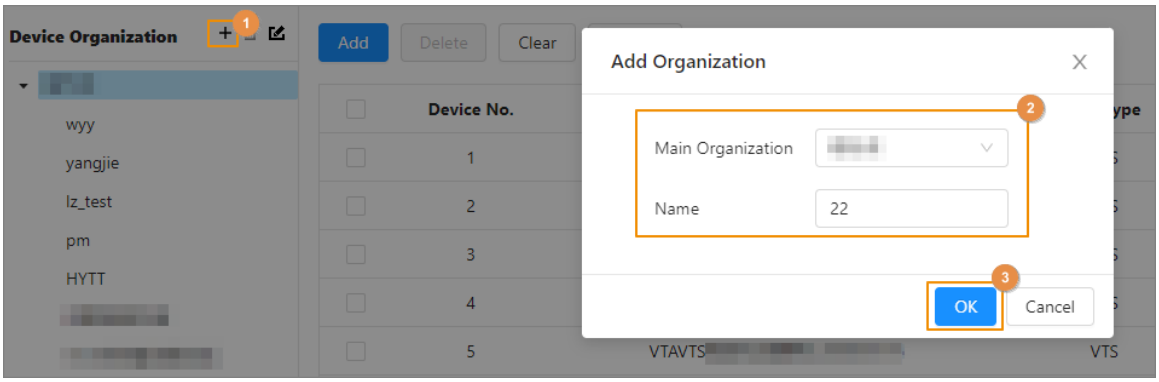
Step 2 Select **Device Setting** > **Device Setting**.

The devices that are sent by the platform are displayed.

Step 3 (Optional) Add the organization.

1. Click **+**.
2. Select main organization, and then enter the name.
3. Click **OK**.

Figure 4-14 Add the organization



Step 4 (Optional) Add the device.

You can add VTS and VTA.

- VTS: Used as contacts.
- VTA: You can call and monitor VTA on the VTS.

1. Click **Add**.
2. Configure the parameters, and then click **OK**.

4.2.4.2 Using without the Platform

When using the device without the platform, configure the device role as lower-level VTS or upper-level VTS.

4.2.4.2.1 Call Forwarding

Manage the forwarding and receiving of the call between the VTS devices.

When the call of device A is forwarded to device B, configure **Forwarding** on device A, and then configure **Receiving** on device B. If you only configure one side, that call fails to be forwarded.

Forwarding

Configure the forwarding, and the call of the current VTS will be entrusted or forwarded to the VTS that you configured.

1. Log in to the webpage.
2. Select **Device Setting** > **Call Forwarding** > **Forwarding**.
3. Click **Add**.
4. Configure the parameters.

Figure 4-15 Add the VTS for forwarding the call

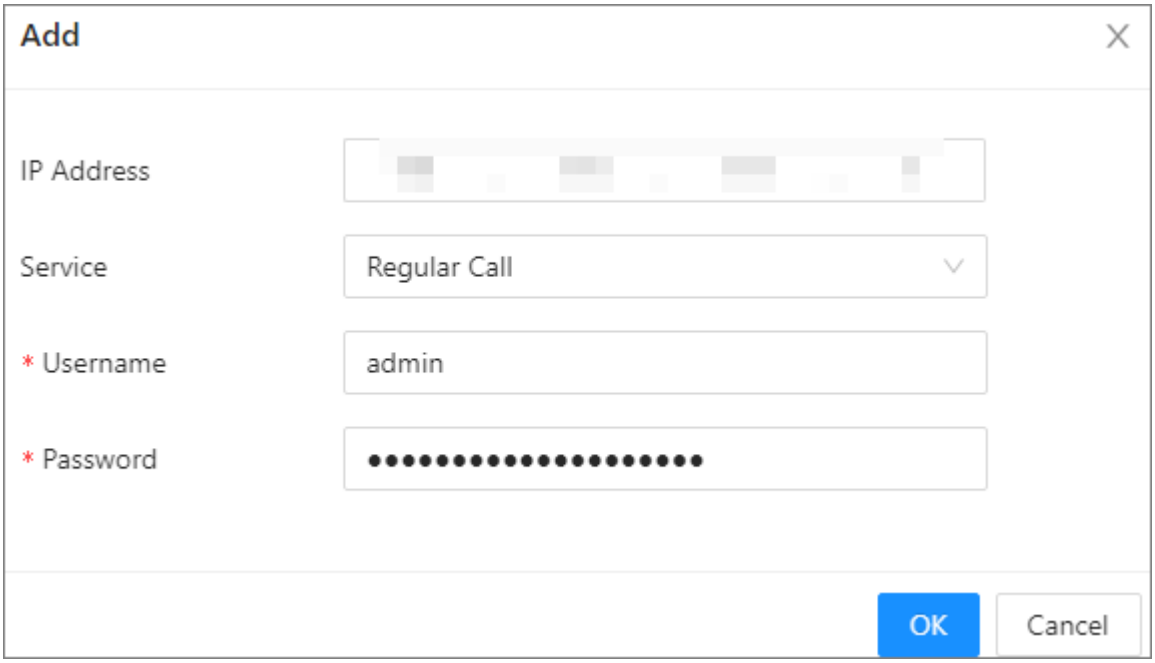


Table 4-7 Description of forwarding parameters

Parameter	Description
IP Address	The IP address of the VTS that receives the forwarding call.

Parameter	Description
Service	• Regular call: Intercom between VTS and other VTS. • Entrusting: All calls of the current VTS will be forwarded to other VTS. • Call Forwarding: If the current VTS missed the call, the call will be forwarded to other VTS.
Username	The username and the password of the VTS that receives the forwarding call.
Password	

5. Click **OK**.

Receiving

Configure the receiving, and the current VTS will receive the call that peer VTS entrusted or forwarded.

1. Log in to the webpage.
2. Select **Device Setting** > **Call Forwarding** > **Receiving**.
3. Click **Add**.
4. Enter the IP address, username and password of other VTS.
5. Click **OK**.

4.2.4.2.2 Adding VTA

When the device is configured as lower-level VTS, you can add VTA and IPC. The operations of adding IPC are the same with the operations in building scene. This section introduces the operations of adding VTA.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **Device Setting** > **Terminal Management**.

Step 3 Click **Add**, and then configure the parameters.

Figure 4-16 Add VTA

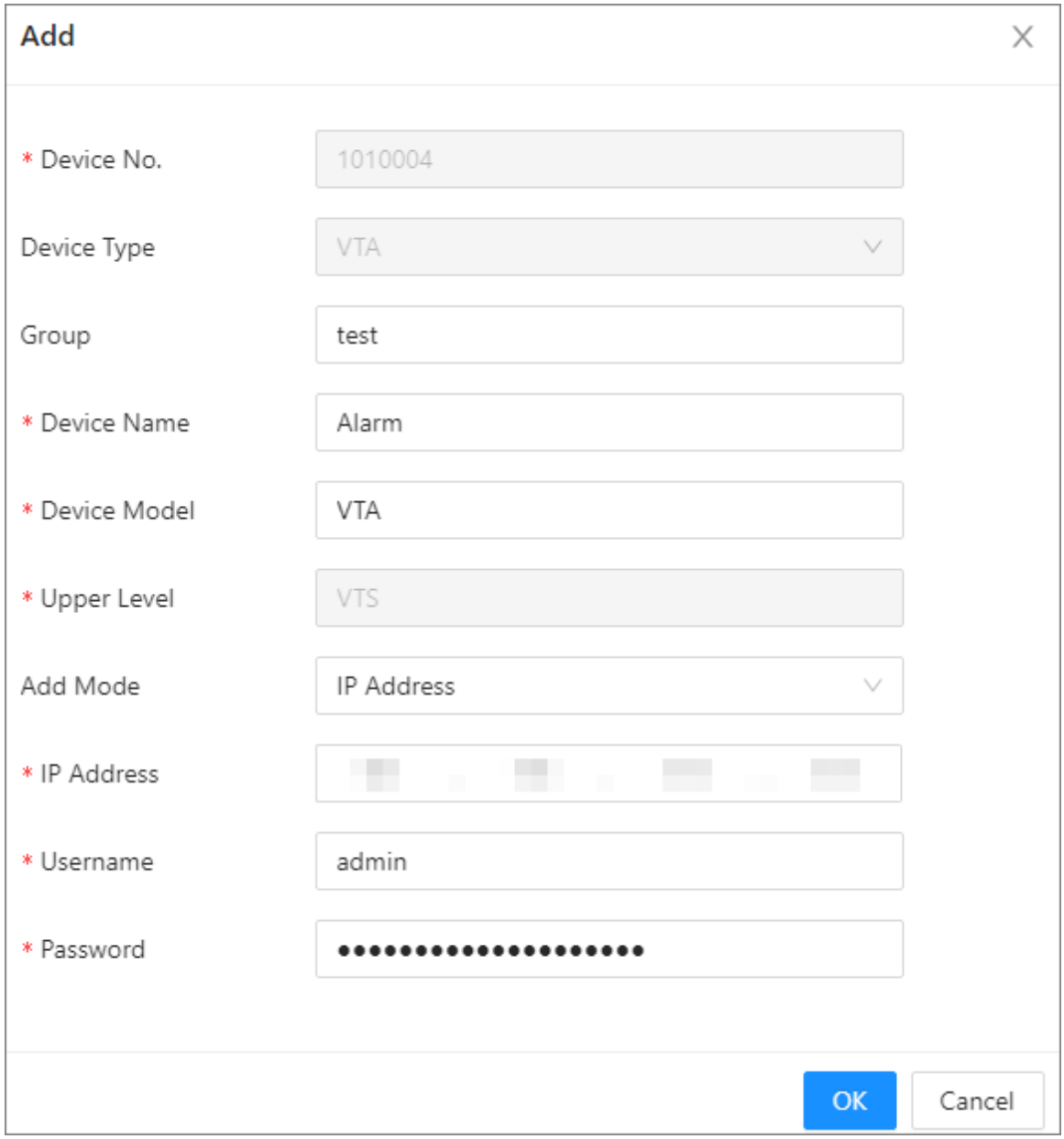


Table 4-8 Parameters description

Parameter	Description
Group	Select **Monitor** > **Terminal Management** on the VTS, and then you can view the devices of the group that you configured.
Device Name	User-defined.
Device Model	Enter the complete device model that you can get from the device label.
Add Mode	You can add VTA in the following 2 ways. ● IP address: Enter the IP address of the VTA. ● Register: Configure the parameters for registering on the VTS.
Username	Enter the username and password of the device that you added.

Parameter	Description
Password	

Step 4 Click **OK**.

4.2.4.2.3 Adding Lower-level VTS

When the device is configured as upper-level VTS, you can add the lower-level VTS.

Procedure

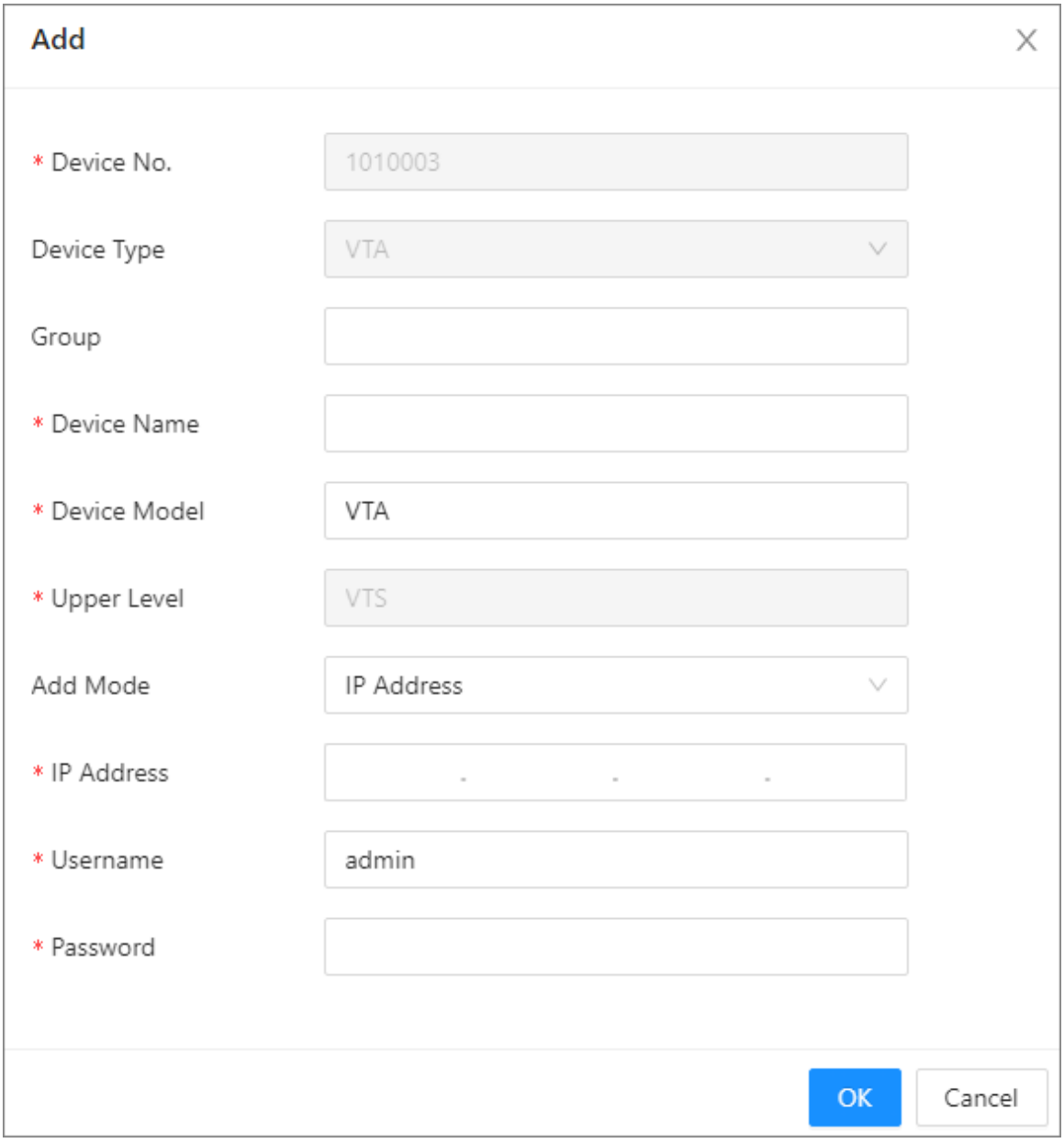
Step 1 Log in to the webpage of the device.

Step 2 Select **Device Setting** > **Terminal Management**.

Step 3 Click **Add**.

Step 4 Enter IP address, username and password of the VTS.

Figure 4-17 Add lower-level VTS



Step 5 Click **OK**.

Appendix 1 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**

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

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

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

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

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

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

Network Configuration

1. **Enable Allow list**

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

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

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

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

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

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

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

Software Security

1. **Update firmware in time**

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

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

Physical Protection

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

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