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.
🔑	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.	December 2022

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF

format) cannot be opened.

- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.

Installation Requirements

⚠ WARNING

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

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Table of Contents

1 Initializing VTS

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

1.1 Initialization through Local Device

Procedure

Step 1 Power on the VTS.

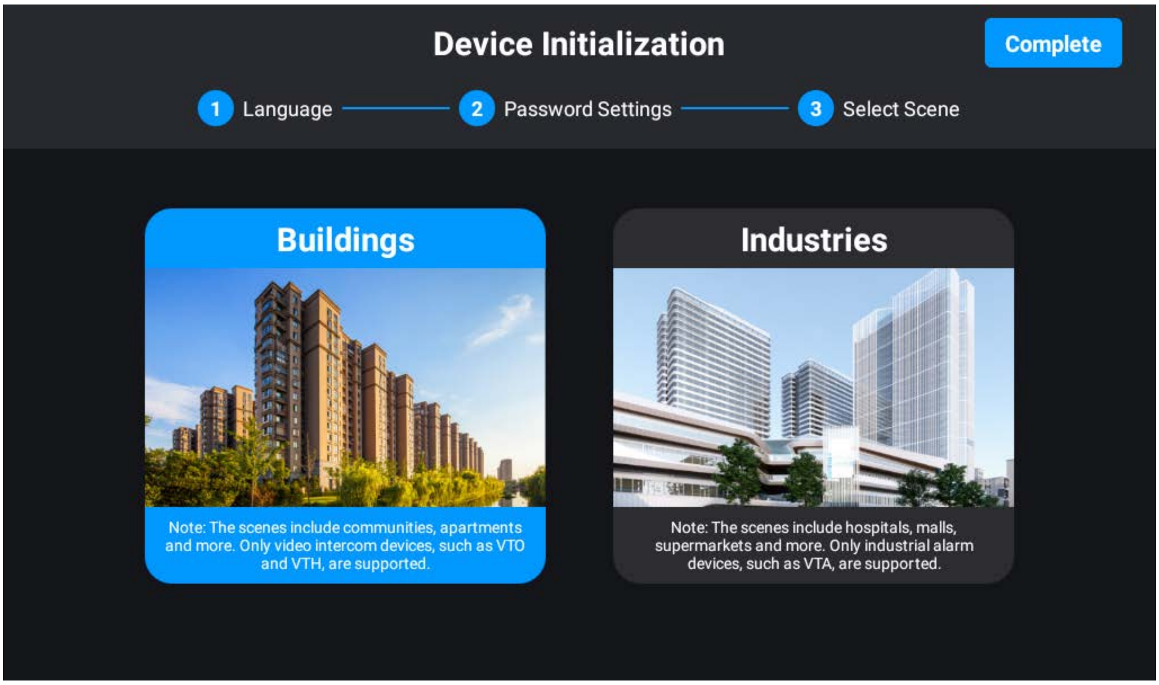
Step 2 Select the language.

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 1-1 Initialization through local device



Note: The scenes include communities, apartments and more. Only video intercom devices, such as VTO and VTH, are supported.

Note: The scenes include hospitals, malls, supermarkets and more. Only industrial alarm devices, such as VTA, are supported.

Step 6 Tap **Complete**.

1.2 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 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 **Done**.

Step 5 Enter the username and password, and then click **Log in**.

Step 6 Select the scene, and then click **OK**.

2 Building Scenes

2.1 Operations on Local Device

2.1.1 Local Screen

Figure 2-1 Local screen

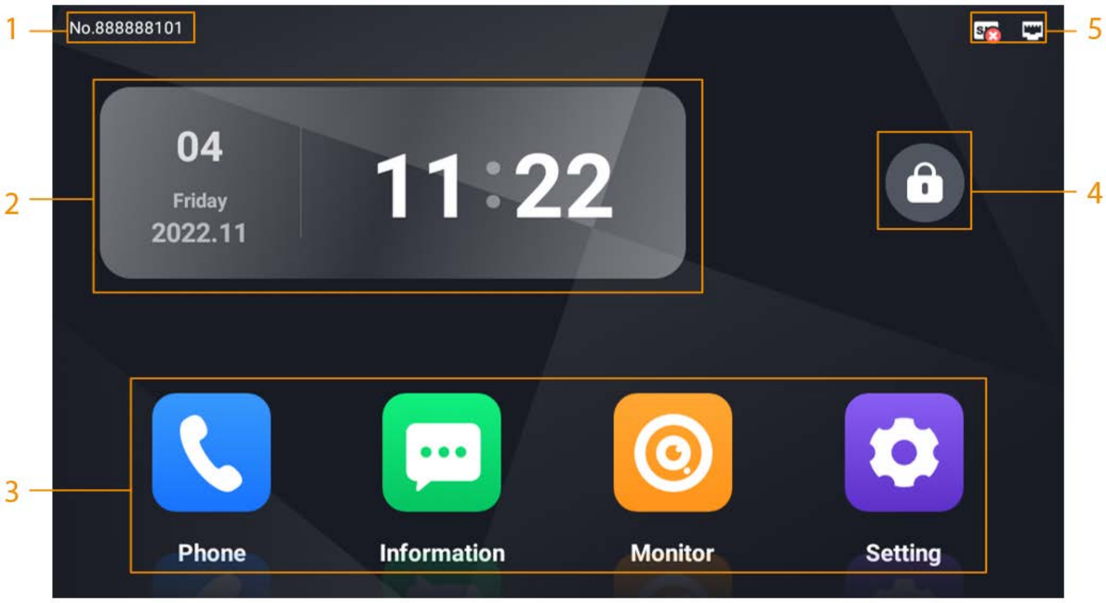


Table 2-1 Home screen introduction

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 "2.1.8.1 Call". ● Information: Check the alarm information, video playback and screenshots. For details, see "2.1.8.2 Checking the Information". ● Monitor: Monitor VTH, VTO and IPC. For details, see "2.1.8.3 Monitoring". ● Setting: Enter the setting screen of VTS.
4	Tap 🔒 to lock the screen. If you have selected **Setting** > **Display Settings**, and enabled **Lock Screen**, you need to enter the default password **123456** when you lock the screen.
5	The connection status of the network, the SIP server, and the SD card.

2.1.2 Configuring the Display Parameters

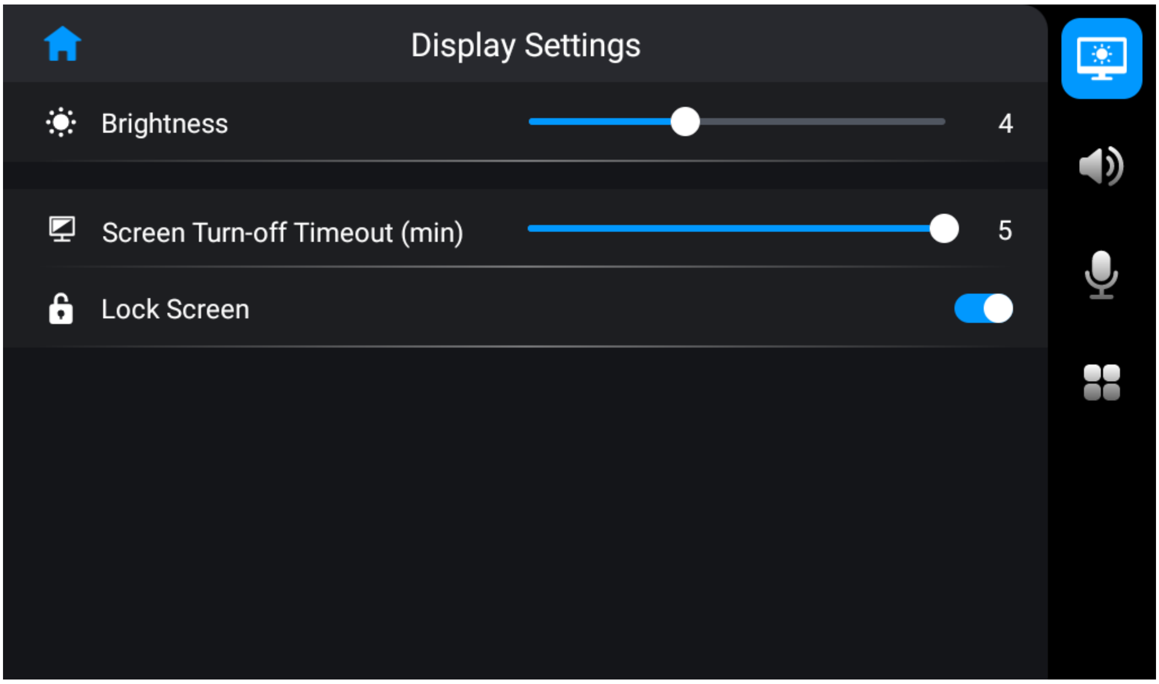
Configure the brightness and screen turn-off time. Turn on or turn off **Lock Screen**.

Procedure

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

Step 2 Configure the parameters.

Figure 2-2 Display settings



Display Settings

Brightness 4

Screen Turn-off Timeout (min) 5

Lock Screen ●

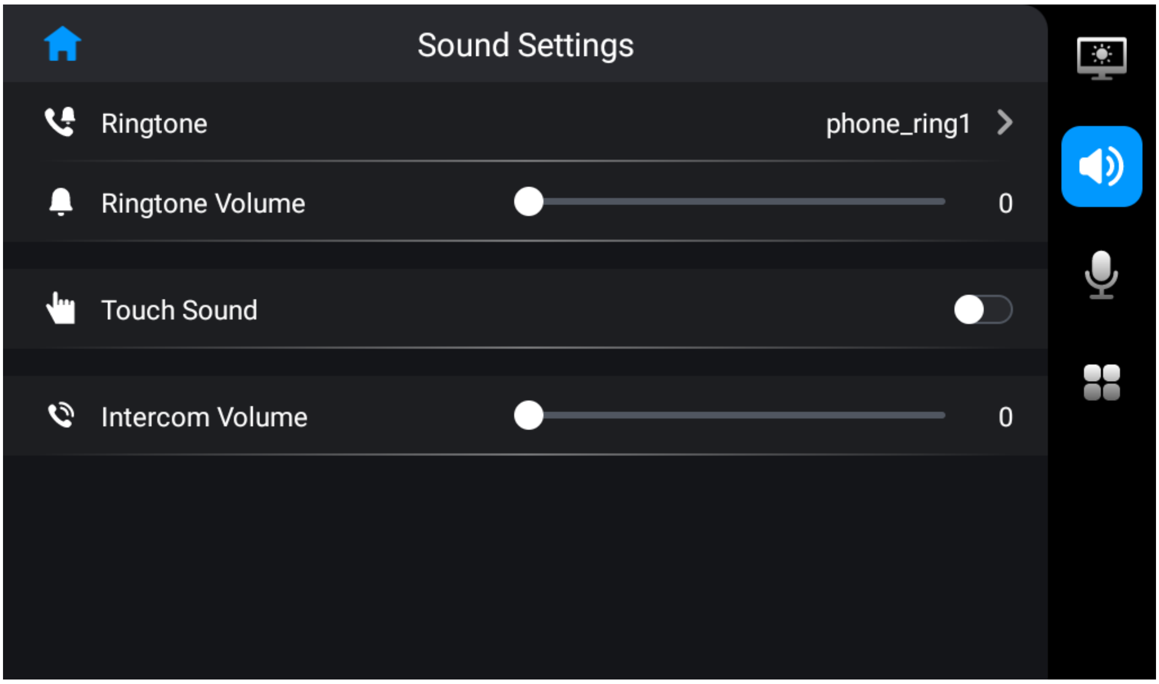
2.1.3 Configuring the Sound Parameters

Procedure

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

Step 2 Configure the parameters.

Figure 2-3 Sound settings



Sound Settings

Ringtone phone_ring1 >

Ringtone Volume 0

Touch Sound

Intercom Volume 0

2.1.4 Configuring the Intercom Parameters

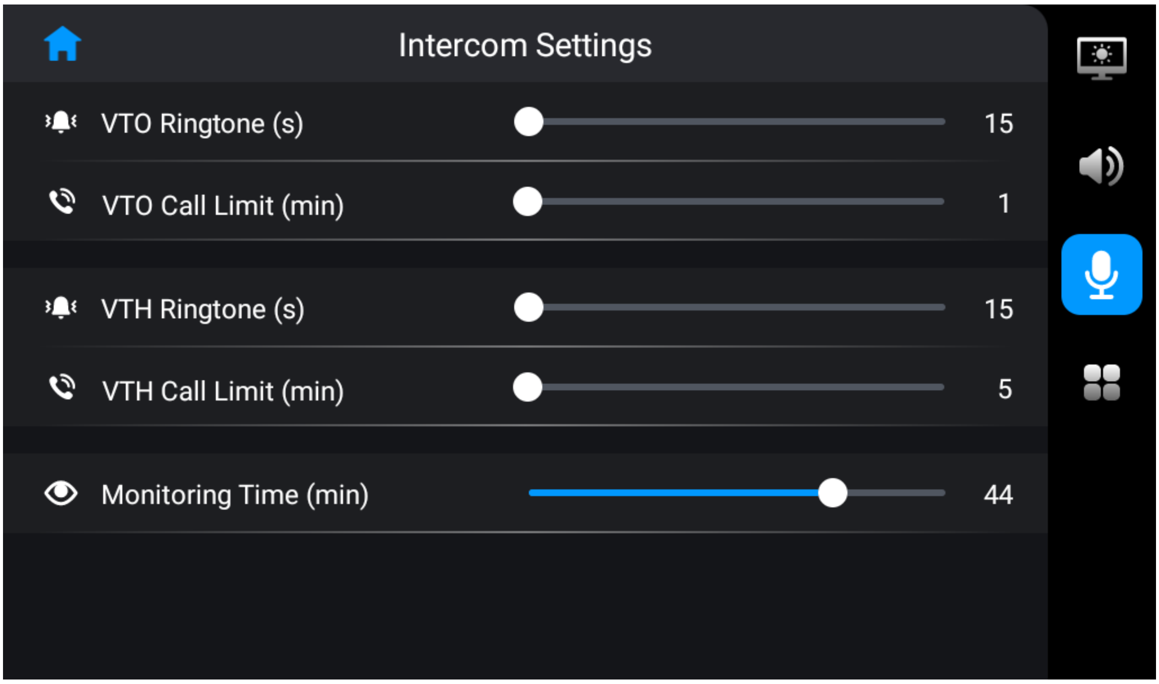
Configure the ringtone and call limit of VTO and VTH, and the monitoring time.

Procedure

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

Step 2 Configure the parameters.

Figure 2-4 Intercom settings



Intercom Settings

VTO Ringtone (s) 15

VTO Call Limit (min) 1

VTH Ringtone (s) 15

VTH Call Limit (min) 5

Monitoring Time (min) 44

Table 2-2 Description of intercom parameters

Parameter	**Description**
VTO Ringtone (s)	The call from VTO stops ringing after the time you set.

Parameter	Description
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 monitors VTO and other devices.

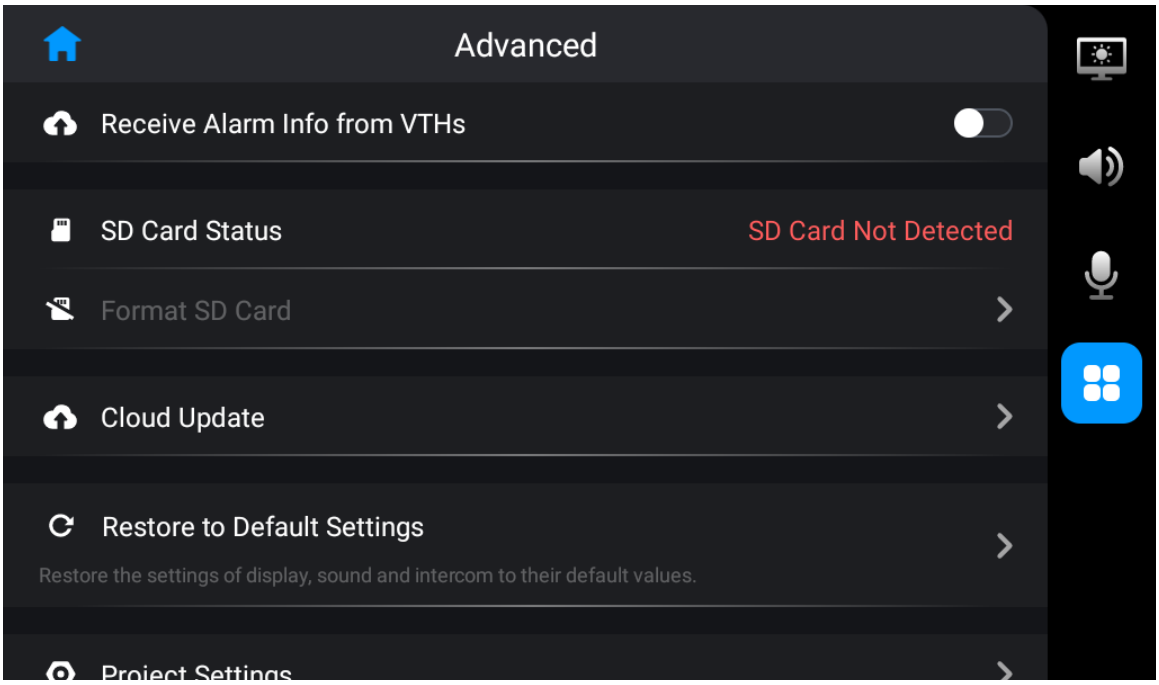
2.1.5 Configuring the Advanced Parameters

Procedure

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

Step 2 Configure the parameters.

Figure 2-5 Advanced settings



Advanced

Receive Alarm Info from VTHs

SD Card Status SD Card Not Detected

Format SD Card

Cloud Update

Restore to Default Settings

Restore the settings of display, sound and intercom to their default values.

Project Settings

Table 2-3 Advanced settings description

Parameter	Description
Receive Alarm Info from VTHs	Enable the function to upload the alarm information from VTH to VTS. Select **Information** > **Alarm Info**, and then check the alarm information.
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. 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.

Parameter	Description
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 "2.1.7 Project Settings".
Device Info	View the legal information, version and security baseline version of VTS.

2.1.6 Resetting Password

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

Prerequisites

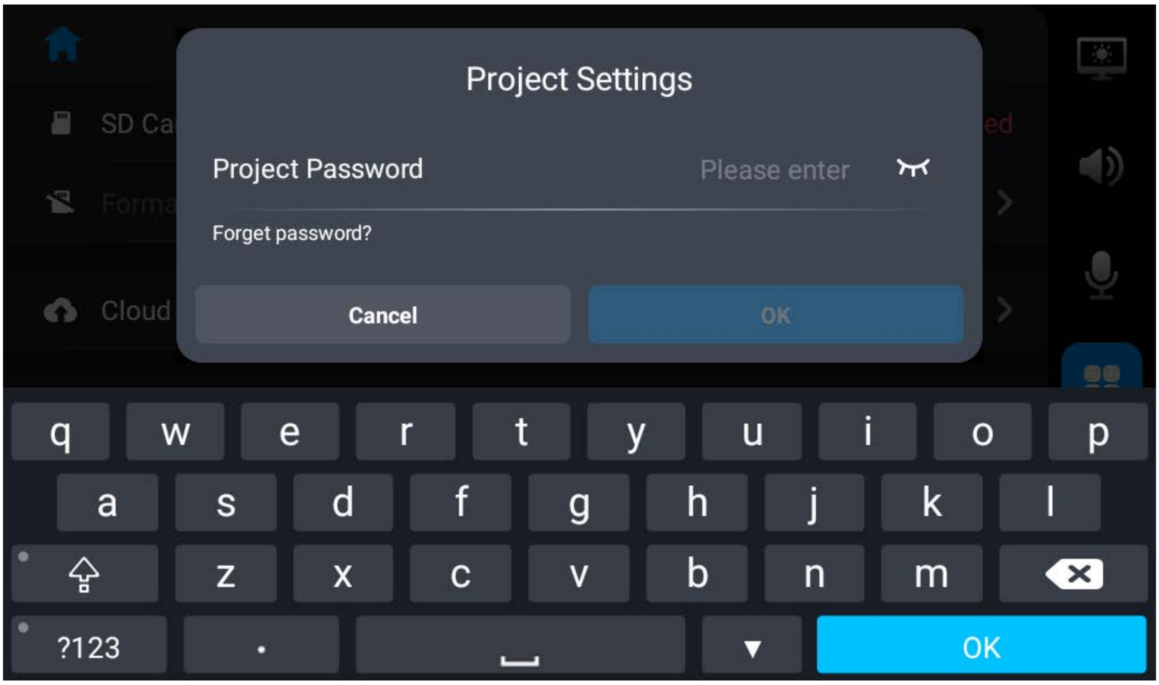
Make sure that you have turned on **Reset Info** in **Project Settings**. For details, see "2.1.7.4 Resetting Information".

Procedure

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

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

Figure 2-6 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**.

2.1.7 Project Settings

2.1.7.1 Configuring VTS

Configure the number and network parameters of VTS.

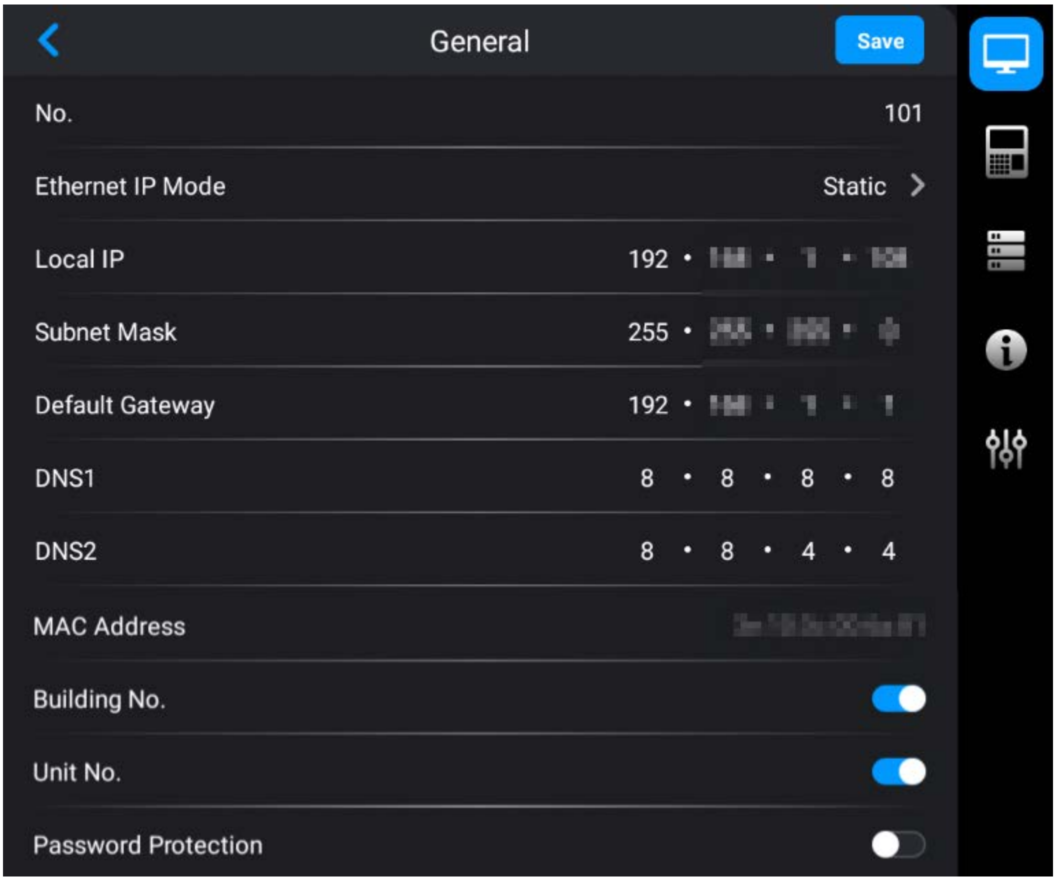
Procedure

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 2-7 Configure the parameters



No. 101

Ethernet IP Mode Static >

Local IP 192 • [redacted]

Subnet Mask 255 • [redacted]

Default Gateway 192 • [redacted]

DNS1 8 • 8 • 8 • 8

DNS2 8 • 8 • 4 • 4

MAC Address [redacted]

Building No. ●

Unit No. ●

Password Protection ○

Table 2-4 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.

Parameter	Description
DNS 2	Standby IP address of DNS server.
Building No.	- If the platform 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.

2.1.7.2 Configuring SIP Server

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

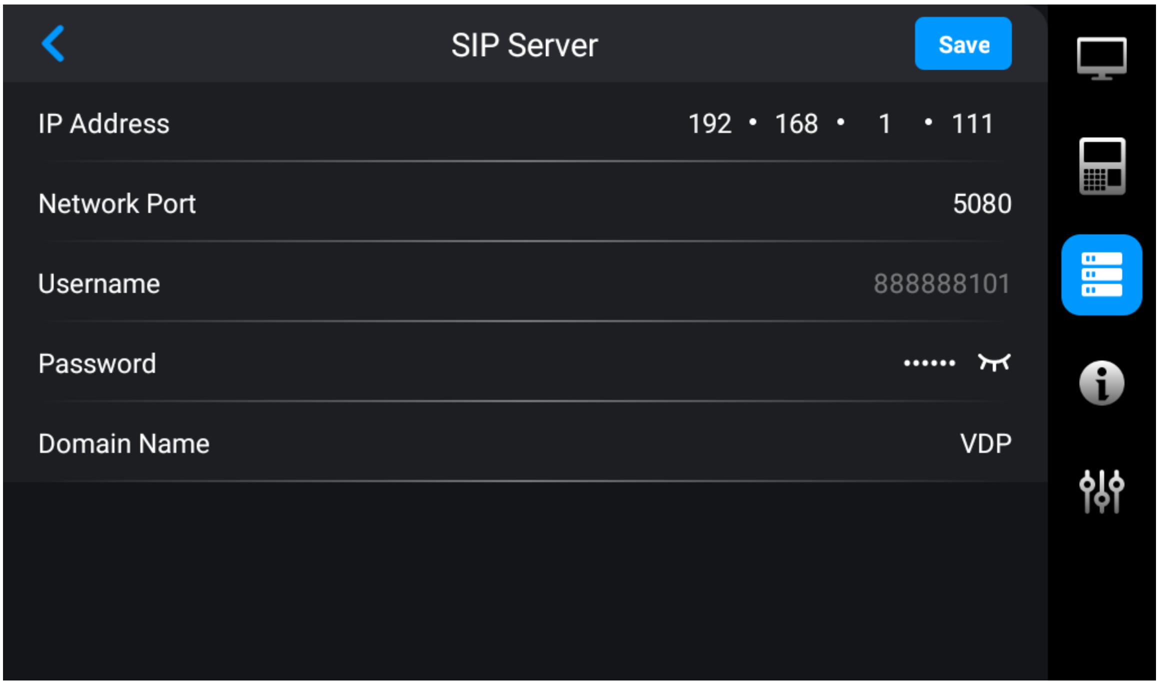
Procedure

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.

Figure 2-8 Configure the parameters



SIP Server

IP Address: 192 • 168 • 1 • 111

Network Port: 5080

Username: 888888101

Password: ••••••

Domain Name: VDP

Table 2-5 Parameters description

Parameter	Description
IP Address	IP address of SIP server.

Parameter	Description
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.

Step 4 Tap **Save**.

2.1.7.3 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.

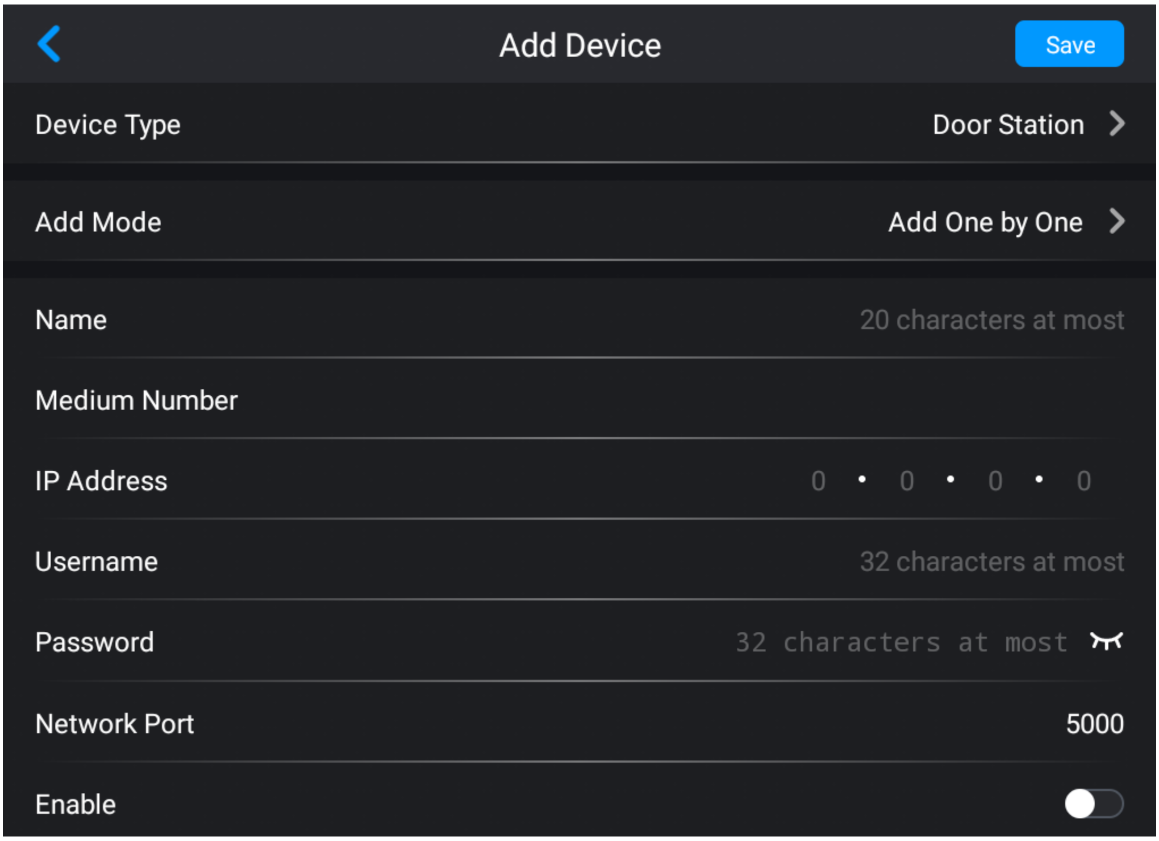
Step 2 Enter the password that you configured during initialization and tap **OK**.

Step 3 Select ▤ > **Add device**.

Step 4 Add devices.

- Add device one by one.

Figure 2-9 Add device one by one



Add Device

Save

Device Type: Door Station

Add Mode: Add One by One

Name: 20 characters at most

Medium Number

IP Address: 0 . 0 . 0 . 0

Username: 32 characters at most

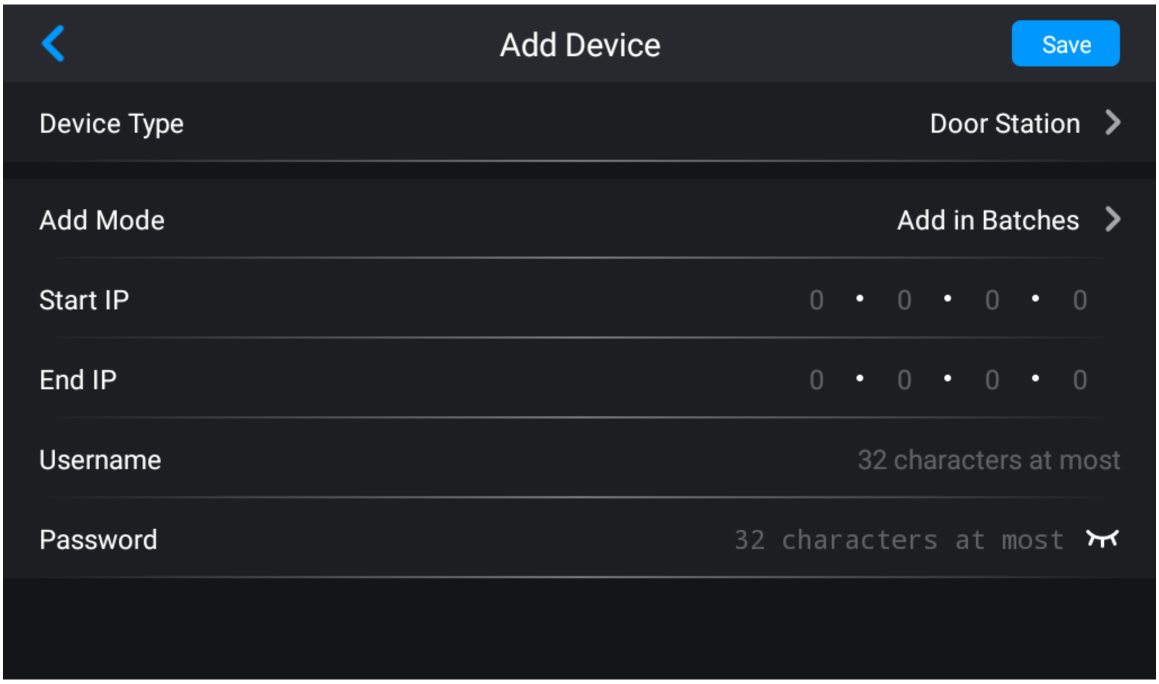
Password: 32 characters at most

Network Port: 5000

Enable

- Add devices in batches.

Figure 2-10 Add devices in batches



Device Type: Door Station

Add Mode: Add in Batches

Start IP: 0 • 0 • 0 • 0

End IP: 0 • 0 • 0 • 0

Username: 32 characters at most

Password: 32 characters at most

Table 2-6 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	

Device Type	Parameter	Description
	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**.

2.1.7.4 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**.

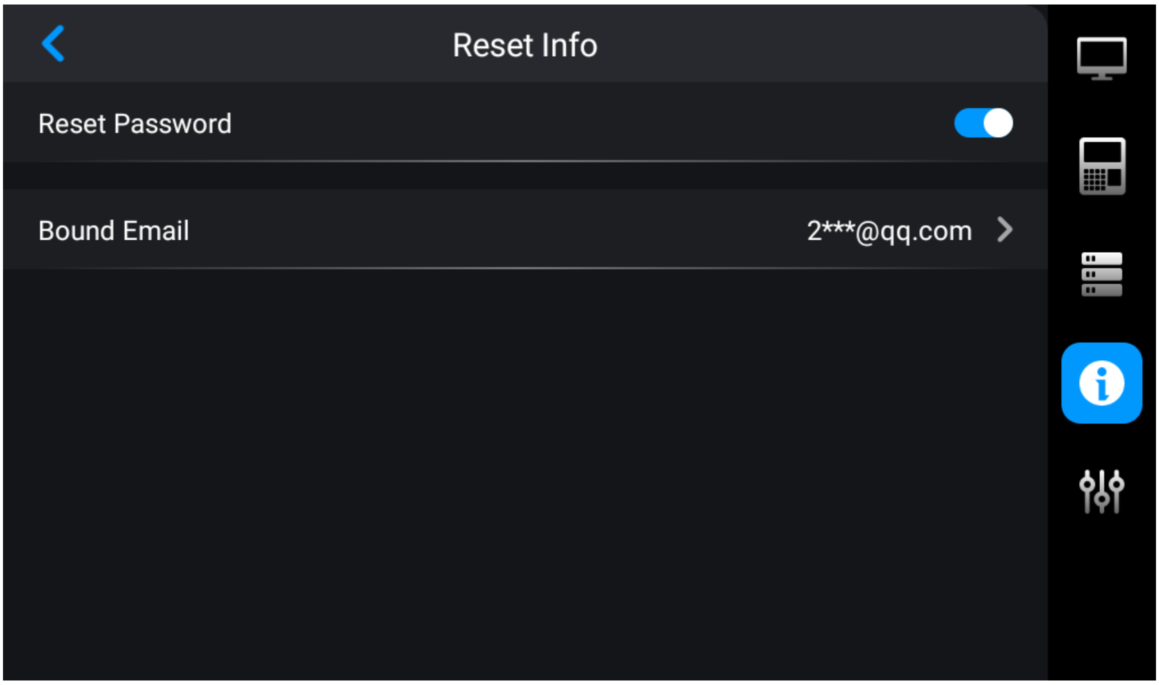
Step 2 Enter the password that you configured during initialization, and then tap **OK**.

Step 3 Tap ⓘ.

Step 4 Turn on **Reset Password**.

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

Figure 2-11 Reset information



Reset Info

Reset Password ●

Bound Email 2***@qq.com >

Step 6 Click **OK**.

2.1.7.5 Debugging and Factory Defaults

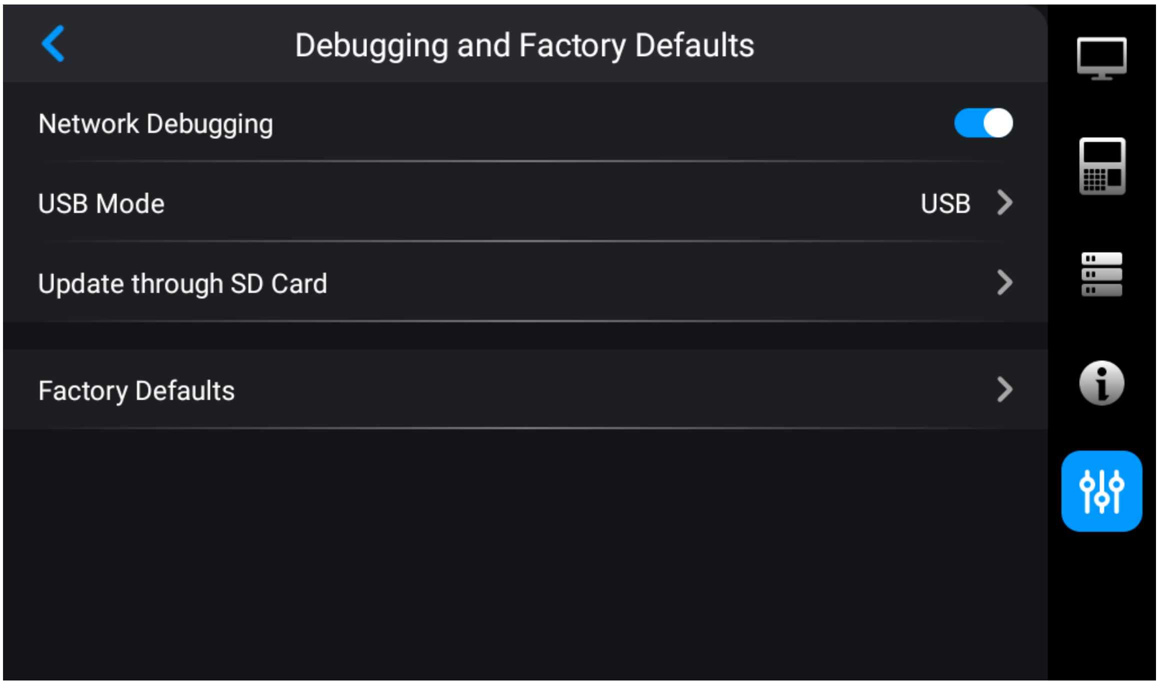
Procedure

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 2-12 Debug and factory defaults



Debugging and Factory Defaults

Network Debugging

USB Mode USB

Update through SD Card

Factory Defaults

Table 2-7 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.
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.

2.1.8 Commissioning

2.1.8.1 Call

Call VTH

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

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

Figure 2-13 Dial

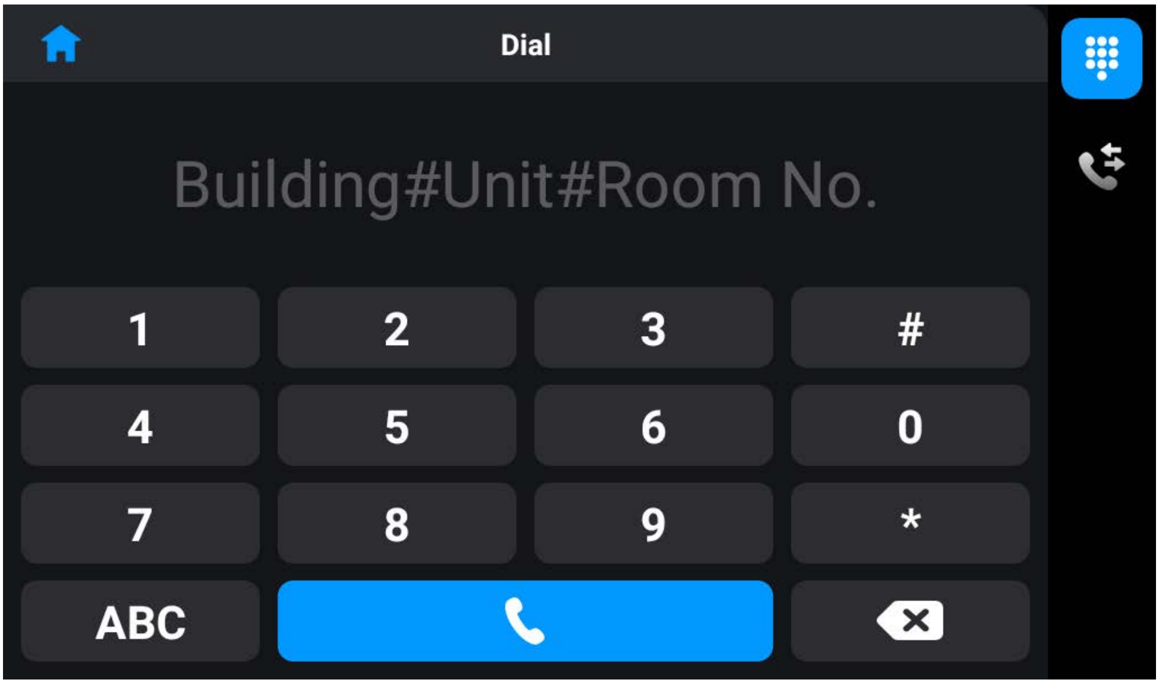


Figure 2-14 Call VTH

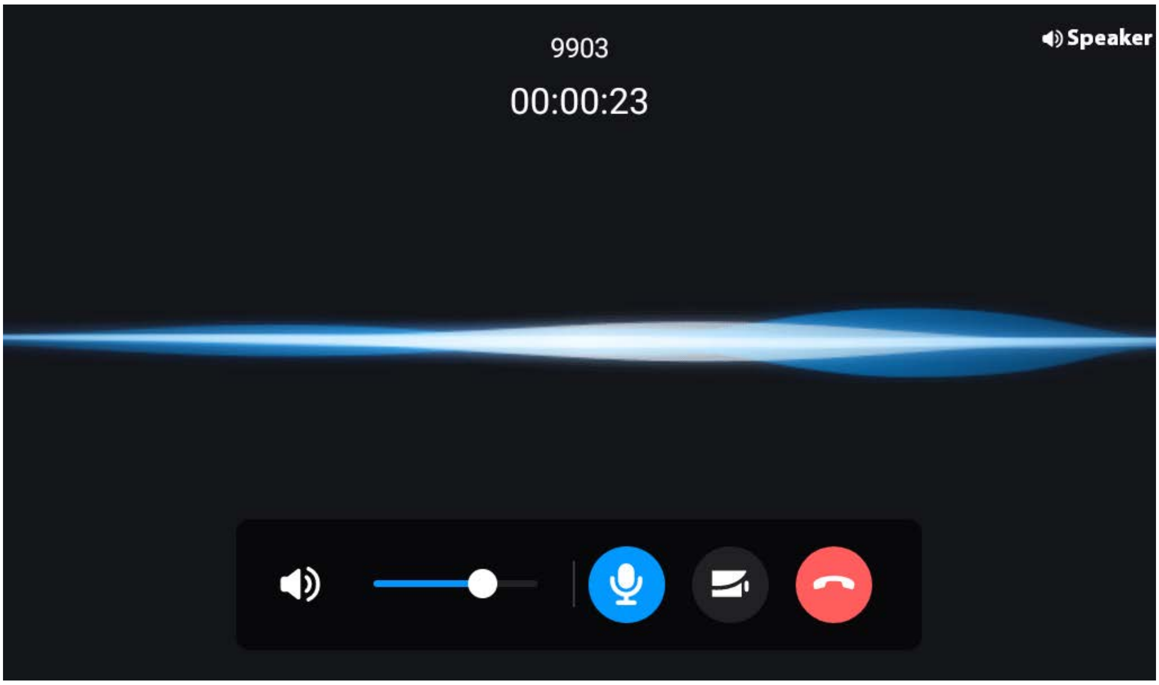


Table 2-8 Icons description

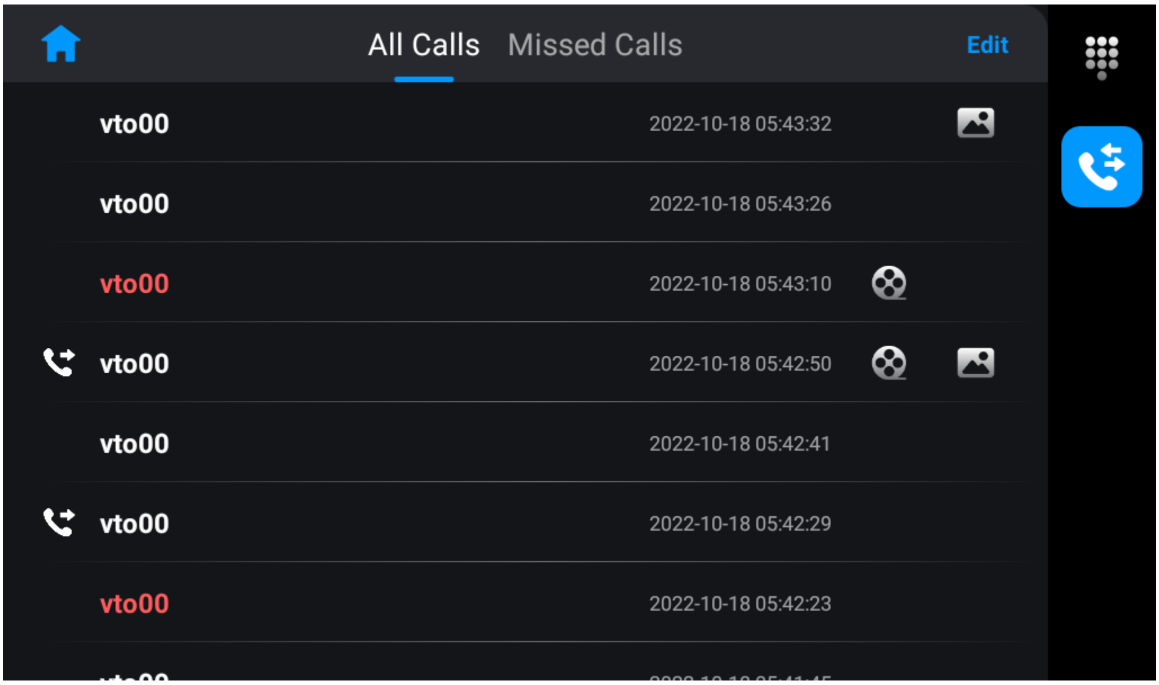
Icon	Description
🔊	Adjust the volume of the speaker during the call.
🎤	Turn on or turn off speech input during the call.
📹	Tap it to convert to IPC video image during the call.
☎	Tap it to hang up the call.

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 2-15 Call history



All Calls Missed Calls Edit

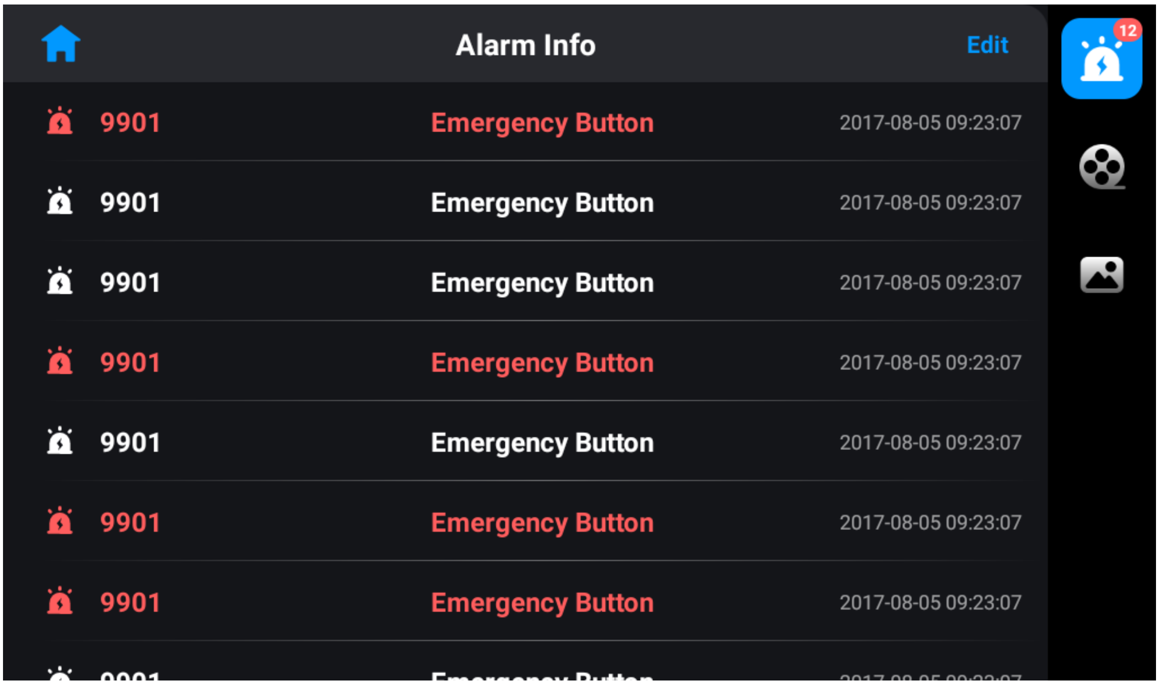
vto00	2022-10-18 05:43:32	🖼
vto00	2022-10-18 05:43:26	
vto00	2022-10-18 05:43:10	🎞
vto00	2022-10-18 05:42:50	🎞 🖼
vto00	2022-10-18 05:42:41	
vto00	2022-10-18 05:42:29	
vto00	2022-10-18 05:42:23	

2.1.8.2 Checking the Information

Alarm information

Check or delete the alarm information that VTH uploaded.

Figure 2-16 Alarm information



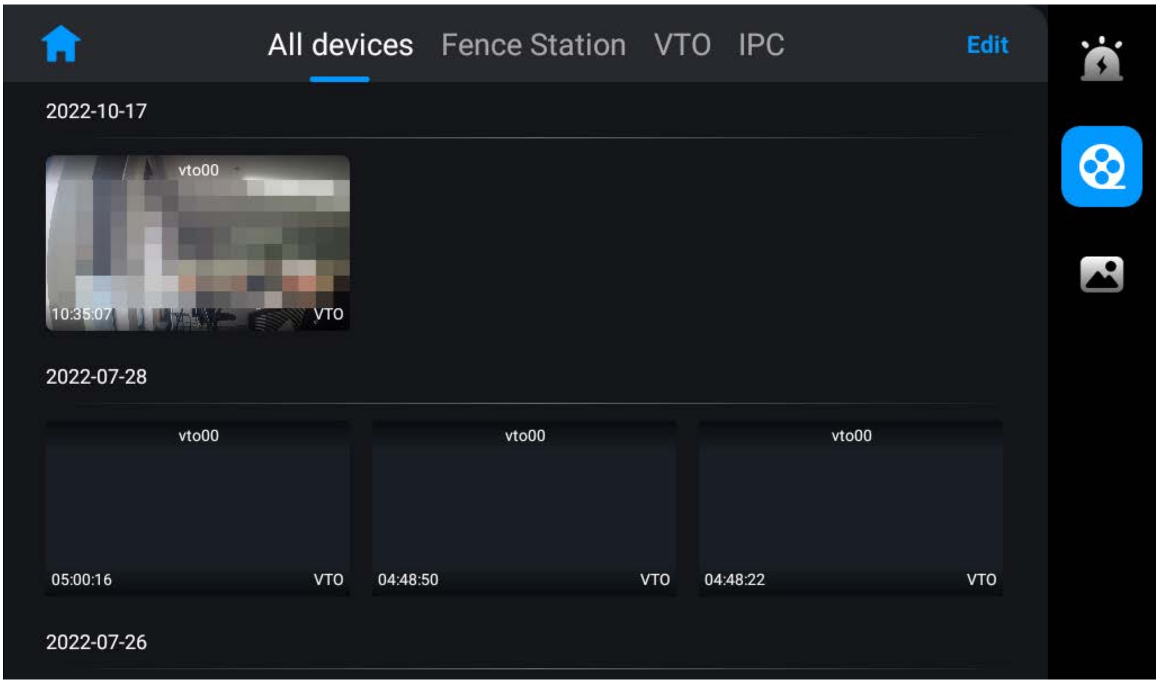
Alarm Info Edit

9901	Emergency Button	2017-08-05 09:23:07
9901	Emergency Button	2017-08-05 09:23:07
9901	Emergency Button	2017-08-05 09:23:07
9901	Emergency Button	2017-08-05 09:23:07
9901	Emergency Button	2017-08-05 09:23:07
9901	Emergency Button	2017-08-05 09:23:07
9901	Emergency Button	2017-08-05 09:23:07

Video files

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

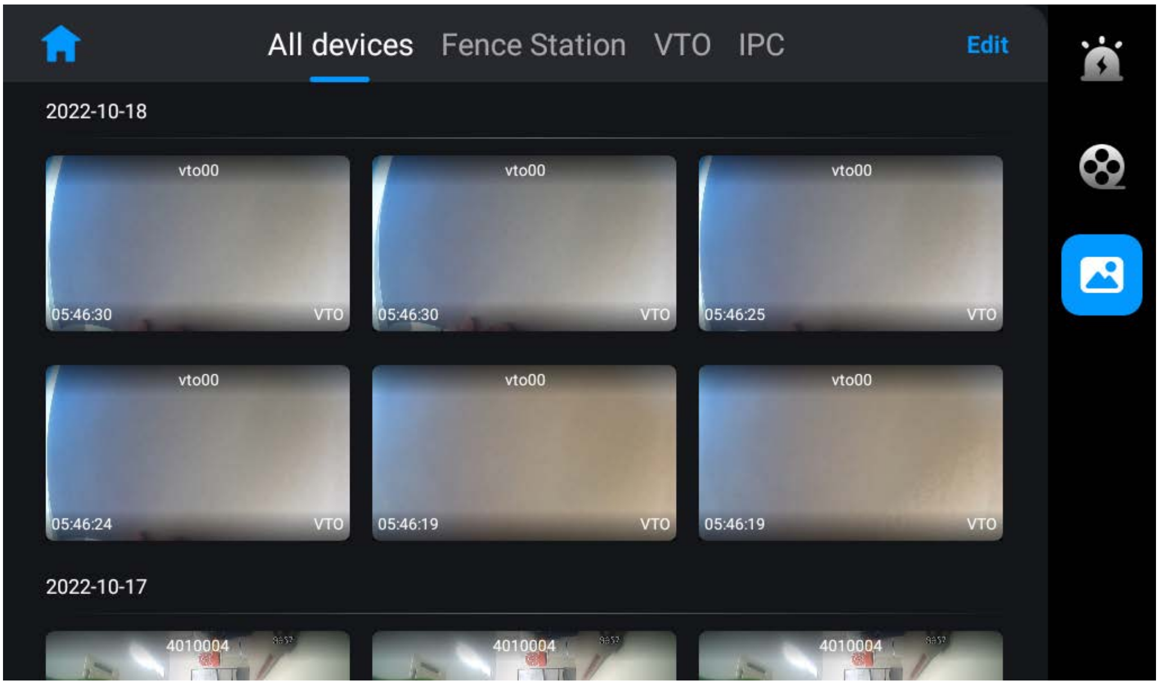
Figure 2-17 Video files



Snapshot files

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

Figure 2-18 Snapshot files



2.1.8.3 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

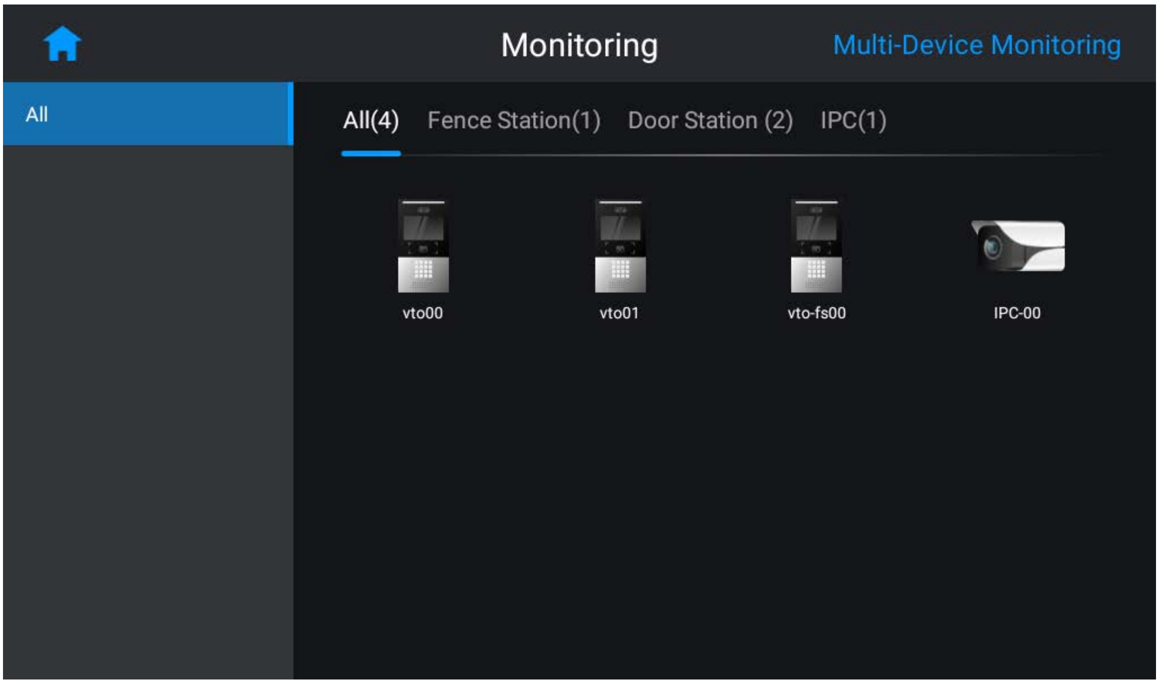
Make sure that you have added VTO, fence station or IPC before you monitor them. For details, see "2.1.7.3 Adding Devices".

Procedure

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

Step 2 Tap the icon of VTO to monitor.

Figure 2-19 Select VTO



Step 3 Check the monitoring image.

Figure 2-20 Monitoring image

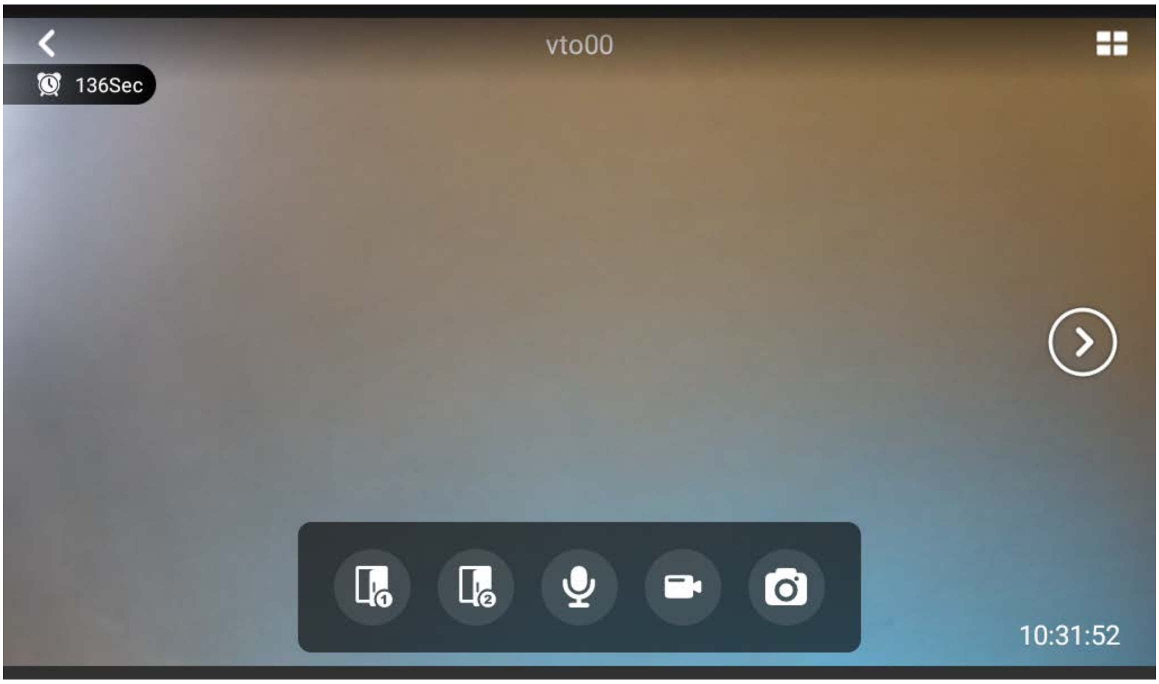


Table 2-9 Monitoring image description

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.
🔓	Remotely unlock VTO.

Icon	Description
🚪	
🎤	Call VTO and VTO directly receive the call without taping any icon.
📹	Tap to start manual recording.
📷	Tap to manually take snapshots.

2.2 Operations on Webpage

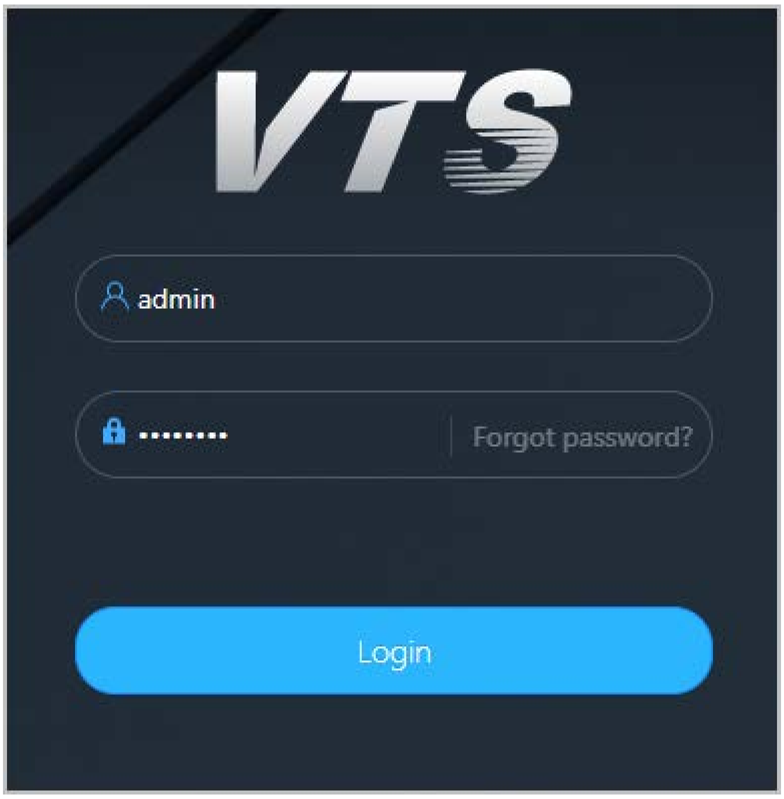
2.2.1 Logging in to the Webpage

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 2-21 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 "2.2.2 Resetting Password".

Step 3 Click **Login**.

2.2.2 Resetting Password

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

Procedure

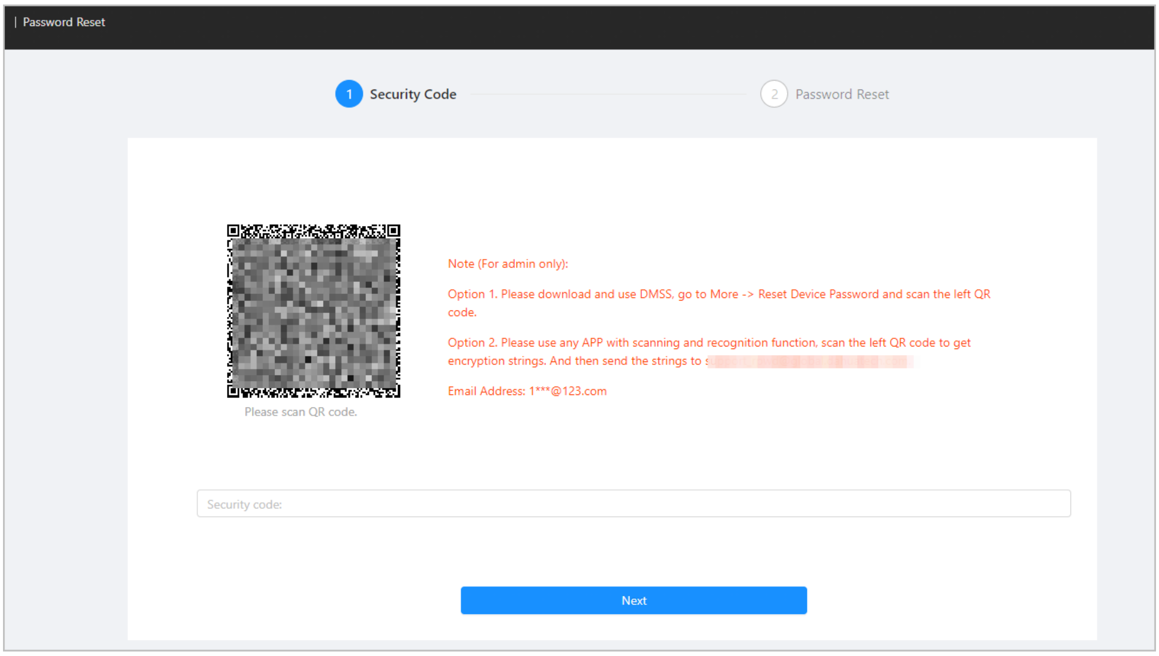
Step 1 On the login page, click **Forgot Password?**

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 two 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 2-22 Get the security code



Password Reset

Note (For admin only):

Option 1. Please download and use DMSS, go to More -> Reset Device Password and scan the left QR code.

Option 2. Please use any APP with scanning and recognition function, scan the left QR code to get encryption strings. And then send the strings to s[redacted]

Email Address: 1***@123.com

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.

2.2.3 Home Page Introduction

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

Figure 2-23 Home page

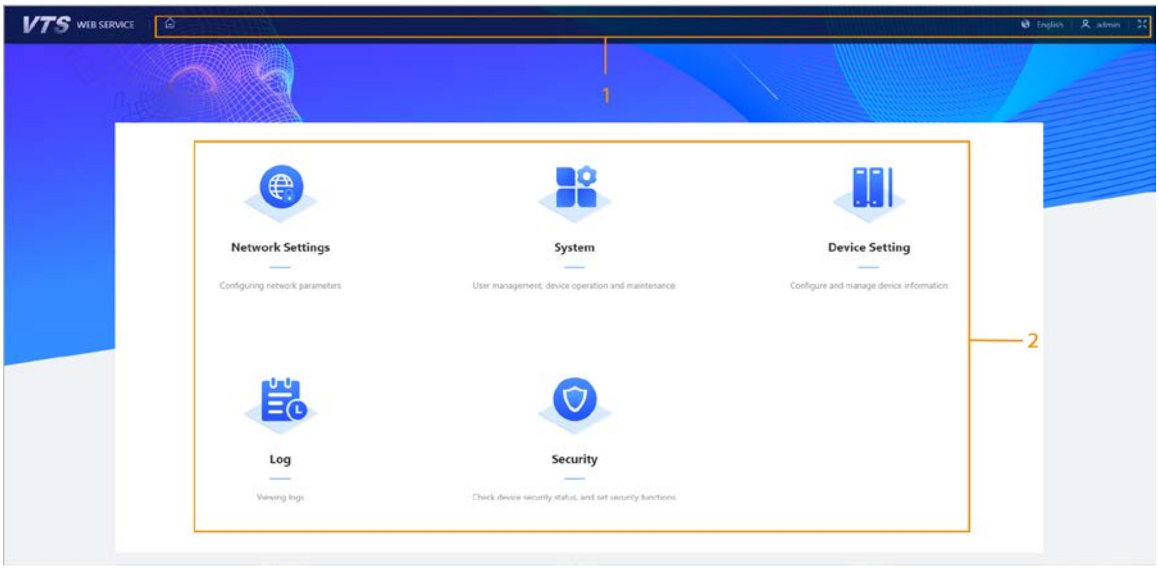

VTS WEB SERVICE
English
admin
1
Network Settings
Configuring network parameters
System
User management, device operation and maintenance
Device Setting
Configure and manage device information
2
Log
Viewing logs
Security
Check device security status, and set security functions

Table 2-10 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.

2.2.4 Configuring Network

2.2.4.1 Configuring TCP/IP

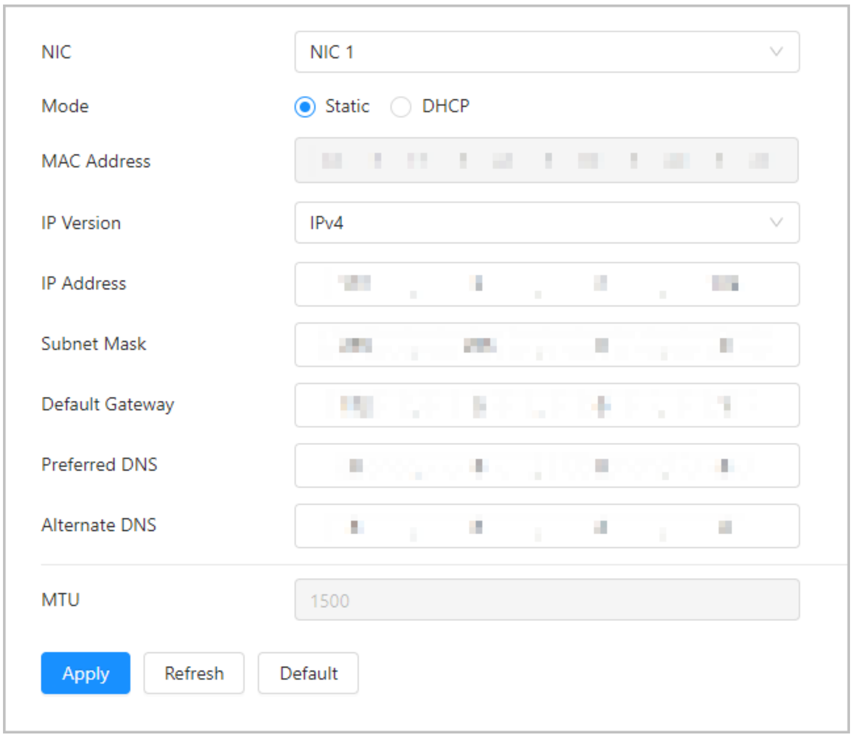
Procedure

Step 1 Log in to the webpage of the device.

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

Step 3 Configure the parameters.

Figure 2-24 Configure the parameters



NIC: NIC 1

Mode: ● Static ○ DHCP

MAC Address: [redacted]

IP Version: IPv4

IP Address: [redacted]

Subnet Mask: [redacted]

Default Gateway: [redacted]

Preferred DNS: [redacted]

Alternate DNS: [redacted]

MTU: 1500

Table 2-11 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 Version	Select **IPv4**.
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**.

2.2.4.2 Configuring SIP Server

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

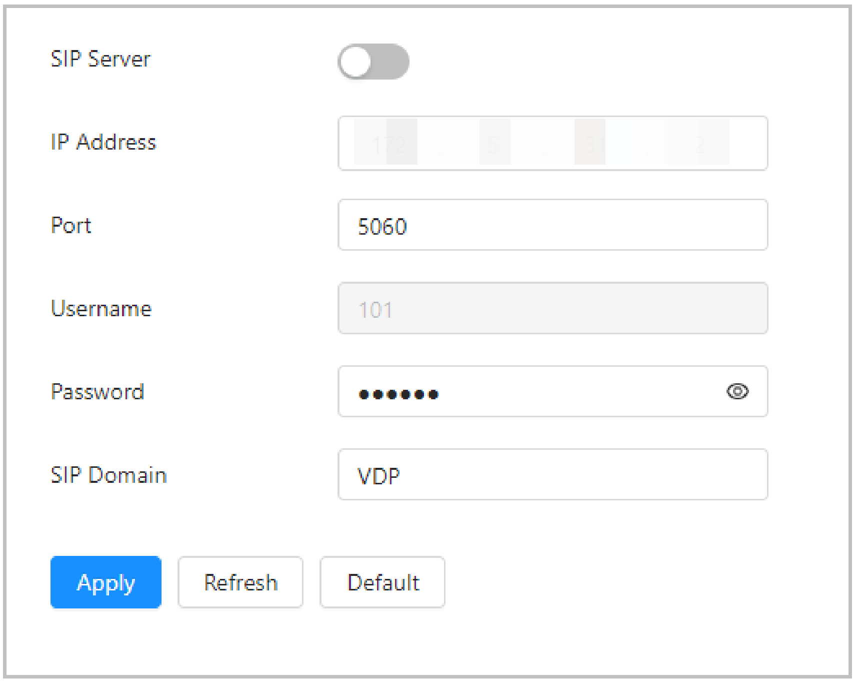
Procedure

Step 1 Log in to the webpage of VTS.

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

Step 3 Configure the parameters.

Figure 2-25 SIP server parameters



SIP Server

IP Address [redacted]

Port 5060

Username 101

Password ••••••

SIP Domain VDP

Table 2-12 Parameters description

Parameter	Description
IP 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.
Username	Default.
Password	Default.
SIP Domain	Keep consistent with the SIP server. Domain name is VDP by default.

Step 4 Tap **Save**.

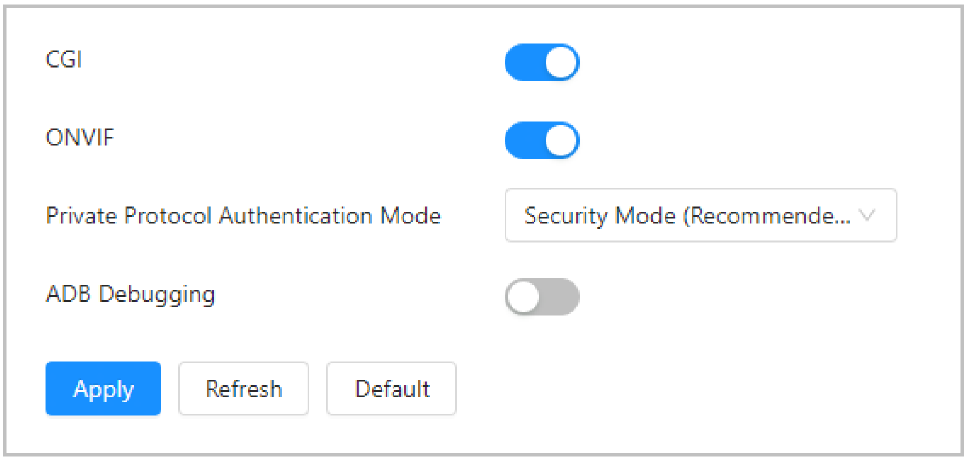
2.2.4.3 Configuring Basic Services

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**.

- CGI: Used to transmit data between external applications and web servers. Turn on CGI to use CGI commands.
- ONVIF: Turn on or turn off ONVIF protocol.
- Private Protocol Authentication Mode: Select **Security Mode (Recommended)** or **Compatibility Mode**.
- ADB Debugging: Only used by testers.

Figure 2-26 Basic services



CGI ●

ONVIF ●

Private Protocol Authentication Mode: Security Mode (Recommende...

ADB Debugging ○

2.2.4.4 Configuring Auto Registration

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

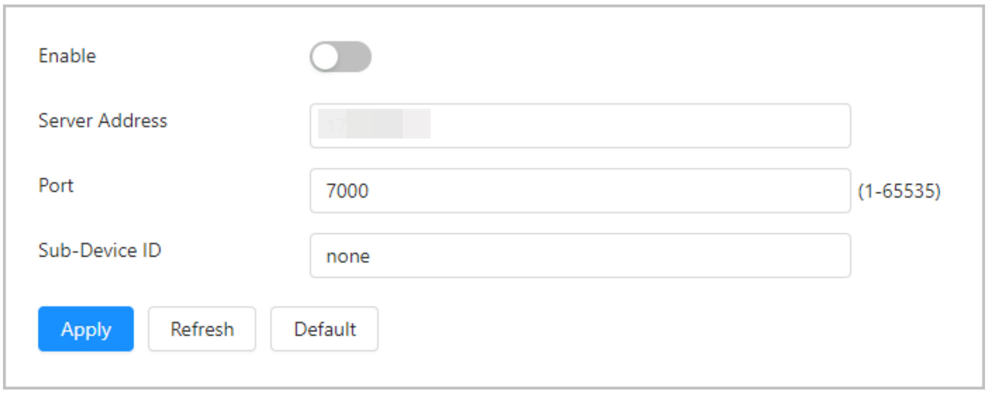
Procedure

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 2-27 Auto registration



Enable ○

Server Address: [redacted]

Port: 7000 (1-65535)

Sub-Device ID: none

Table 2-13 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.
Sub-Device ID	The server distributes an ID for the device. Keep consistent with the ID registered on the server.

2.2.5 System Management

2.2.5.1 Configuring Basic Parameters of VTS

Configure the number and other functions of VTS.

Procedure

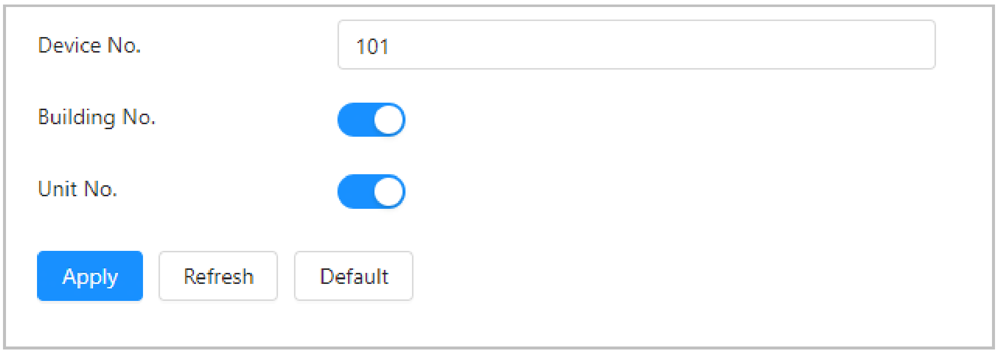
Step 1 Log in to the webpage of VTS.

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 2-28 Configure basic parameters



Device No. 101

Building No. ●

Unit No. ●

Step 4 Click **Apply**.

2.2.5.2 Configuring Video Parameters

Background Information

Video is available on select models.

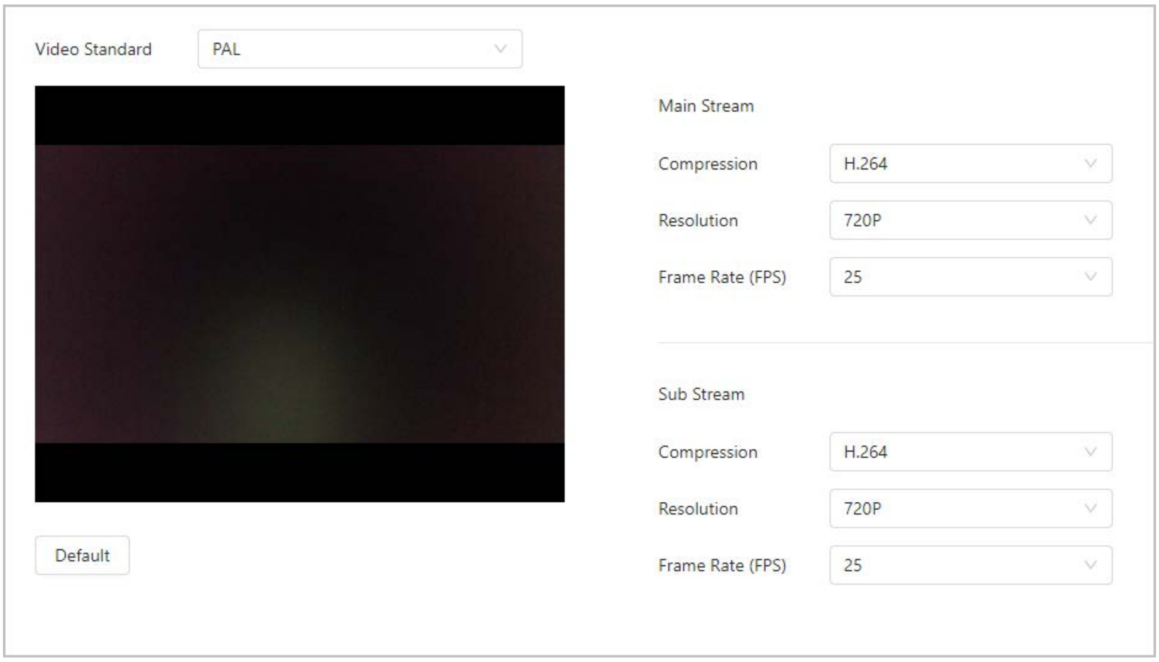
Procedure

Step 1 Log in to the webpage of VTS.

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

Step 3 Configure the parameters.

Figure 2-29 Video parameters



Video Standard PAL

Main Stream

Compression H.264

Resolution 720P

Frame Rate (FPS) 25

Sub Stream

Compression H.264

Resolution 720P

Frame Rate (FPS) 25

Table 2-14 Parameters description

Parameter		Description
Video Standard		● PAL: The default stream frame rate is 25 fps. ● NTSC: The default stream frame rate is 30 fps.
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.

2.2.5.3 Account Management

Add user and edit user information depending on different protocols.

2.2.5.3.1 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

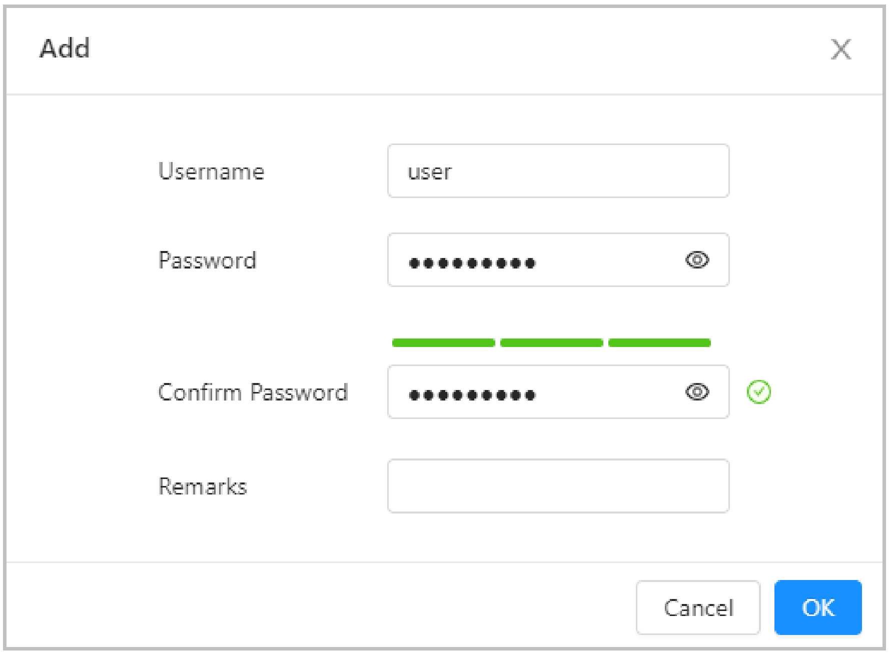
Step 1 Log in to the webpage of VTS.

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

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 2-30 Add users



Add

Username: user

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●● ✓

Remarks:

Table 2-15 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.

2.2.5.3.2 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.

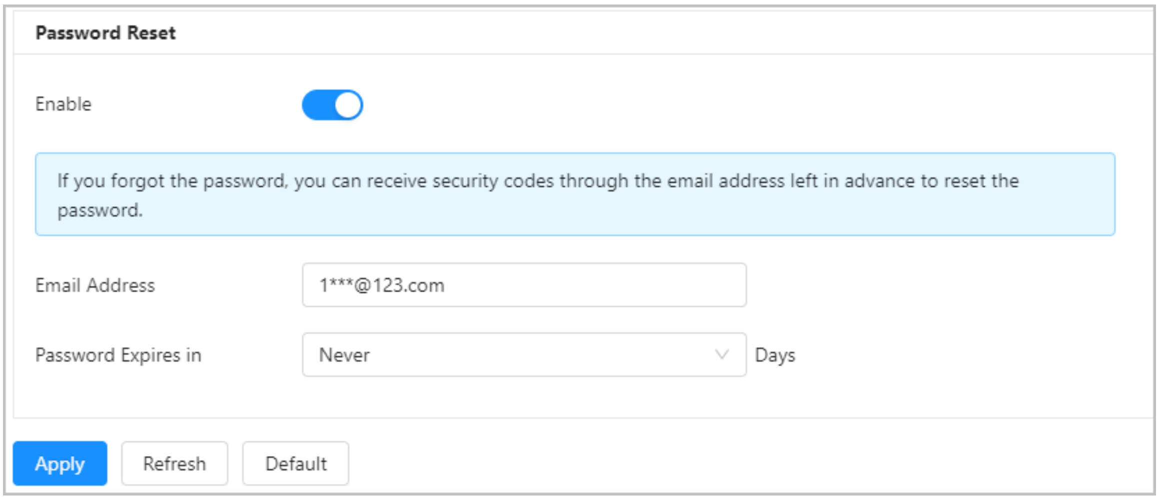
Step 2 Select **System** > **Account**.

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 2-31 Reset password



Password Reset

Enable

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Email Address: 1***@123.com

Password Expires in: Never Days

Step 5 Click **Apply**.

2.2.5.3.3 Adding ONVIF User

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

Procedure

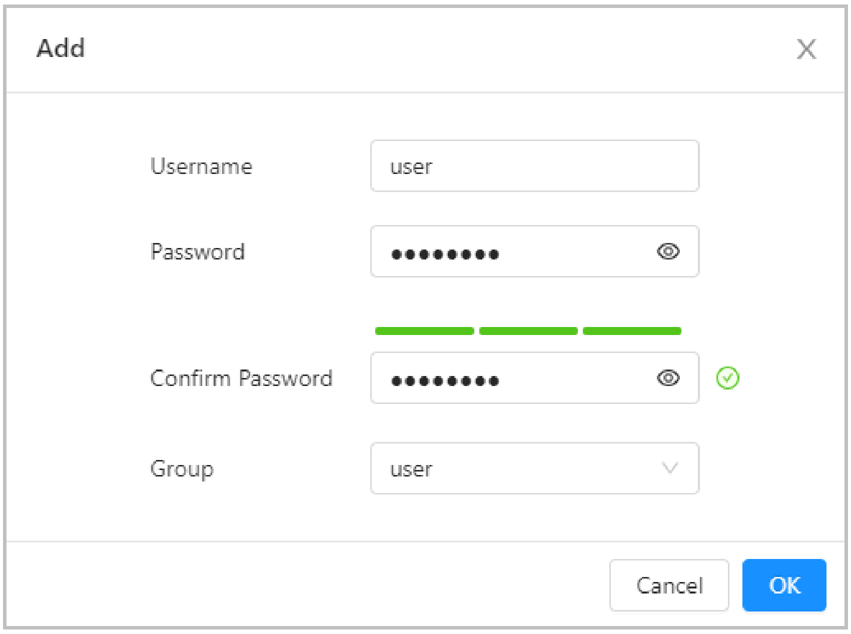
Step 1 Log in to the webpage of VTS.

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

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 2-32 Add ONVIF user



Add

Username: user

Password: ●●●●●●●●

Confirm Password: ●●●●●●●● ✓

Group: user

Table 2-16 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.

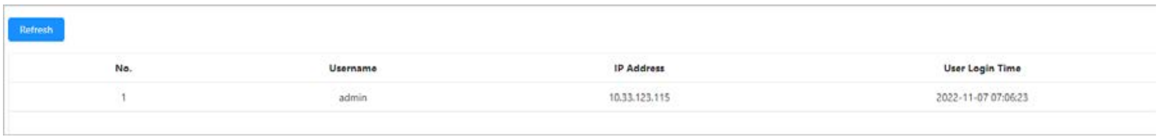
- Delete user. Click to delete the added user.

  The admin account cannot be deleted.

2.2.5.4 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 2-33 Online user



No.	Username	IP Address	User Login Time
1	admin	10.33.123.115	2022-11-07 07:06:23

2.2.5.5 Configuring Time

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

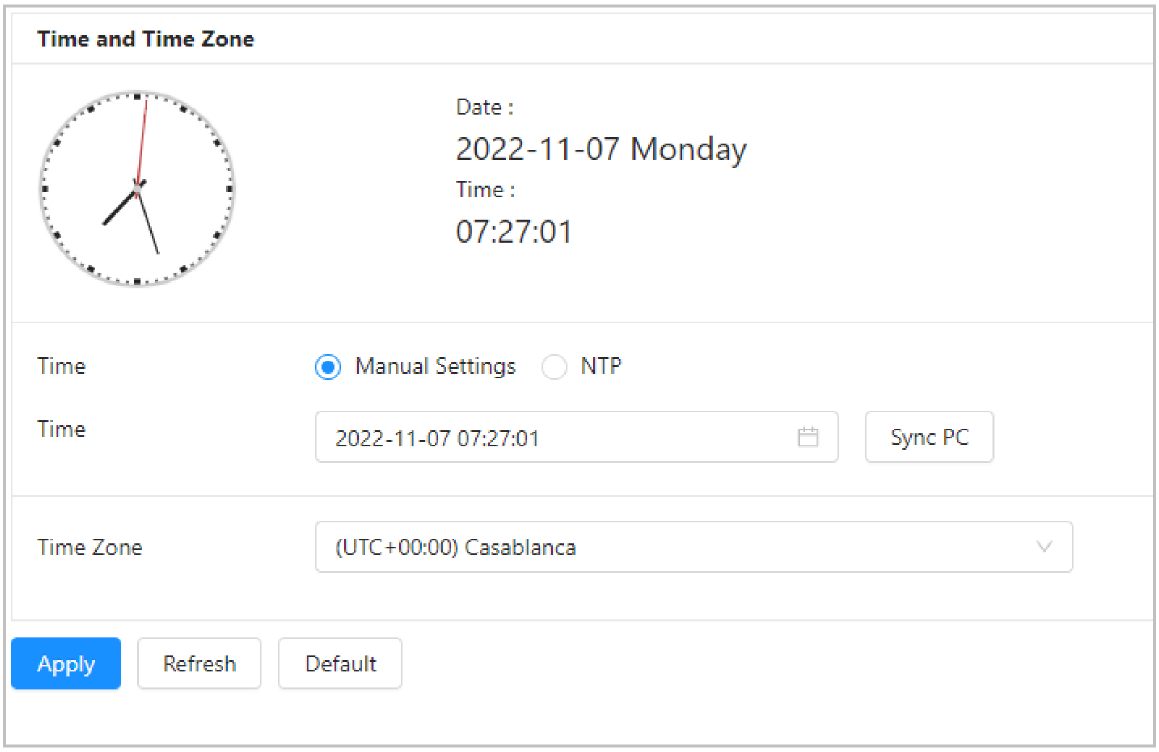
Procedure

Step 1 Log in to the webpage of VTS.

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

Step 3 Configure the parameters.

Figure 2-34 Configure time



Time and Time Zone

Date :
2022-11-07 Monday
Time :
07:27:01

Time ● Manual Settings ○ NTP

Time 2022-11-07 07:27:01 Sync PC

Time Zone (UTC+00:00) Casablanca

Apply Refresh Default

Table 2-17 Description of date and time parameters

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

2.2.5.6 Configuring Maintenance

Configure the auto restarting time so that the VTS can restart automatically to improve the running speed.

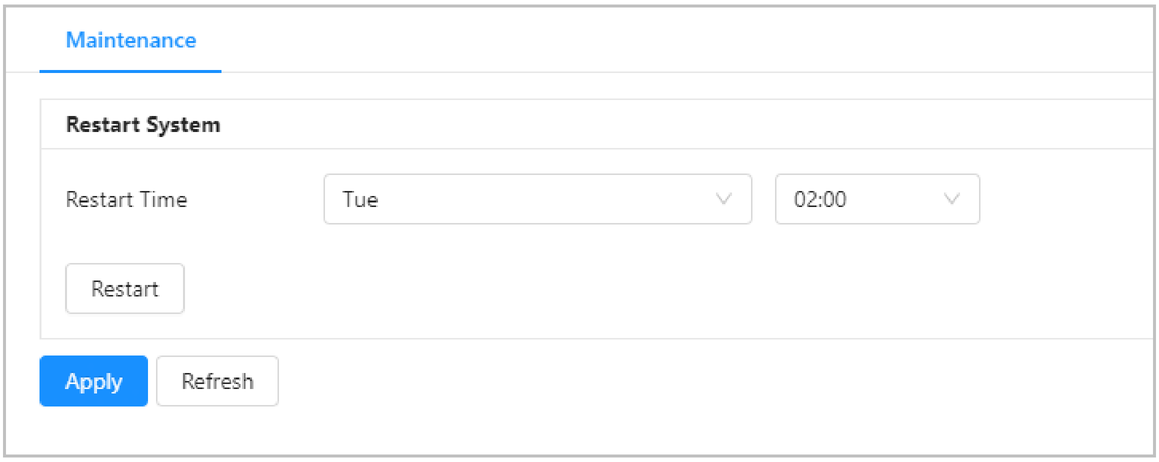
Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **System** > **Maintenance**.

Step 3 Configure **Restart Time**.

Figure 2-35 Maintenance



Restart Time: Tue 02:00

The default restart time is 2 o'clock every Tuesday.

Step 4 Click **Apply**.

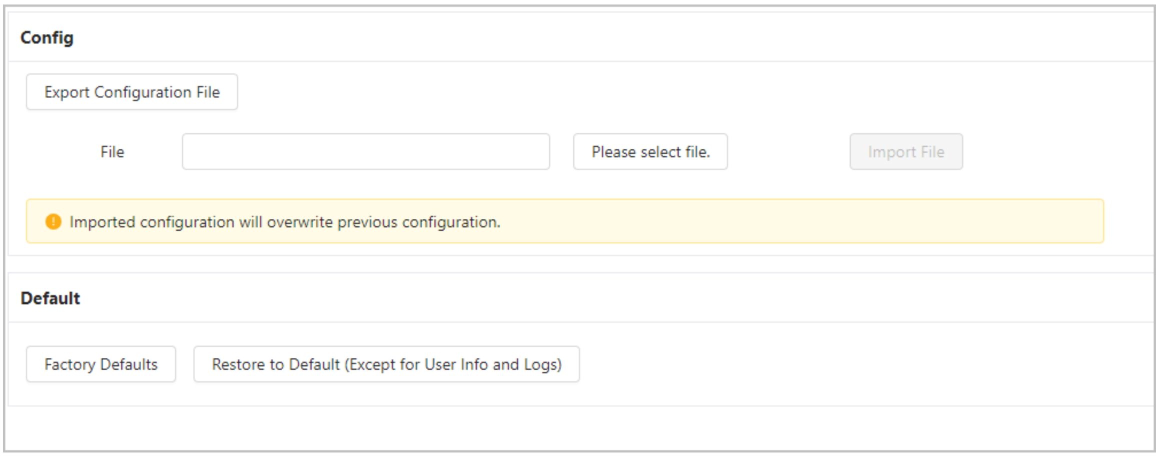
Related Operations

Click **Restart** to restart VTS.

2.2.5.7 Configuration Management

Log in to the webpage of VTS. Select **System** > **Config**.

Figure 2-36 Configuration management


Config
Export Configuration File
File
Please select file.
Import File
Default
Factory Defaults
Restore to Default (Except for User Info and Logs)

Imported configuration will overwrite previous configuration.

2.2.5.7.1 Import/Export Configuration File

Import or export the system configuration file. Use configuration backup file when many devices need the same parameters configuration.

Export configuration file

Click **Export Configuration File** to export the system configuration file to local storage.

The export file excludes IP information.

Import configuration file

1. Click **Please select file.** to select local configuration file.

2. Click **Import File**.

Supports importing the configuration file to devices of the same mode.

2.2.5.7.2 Factory Default

This function will restore the device to default configuration or factory settings. The data will be lost. Operate it carefully.

- **Factory Defaults**: All the configurations are restored to factory settings. Device information and user information will be cleared.
- **Restore to Default (Except for User Info and Logs)**: All the configurations except user information and logs are recovered to default.

2.2.5.8 Updating

Background Information

- Do not power off the device or the network, restart of turn off the device.
- If wrong upgrade file has been used, restart the device; otherwise some functions might not work properly.
- Degrade has potential security risks. Operate it carefully.

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **System** > **Update**.

Step 3 Select the updating mode as needed.

- File update
  1. Click **Browse**, and then upload updating file. The updating file should be a .bin file.
  2. Click **Update**.
- Online update

  Get the new version through auto check or manual check. Click **Update Now**.
  - ◇ Auto check: Click **Auto Check**. The system automatically checks the new version once everyday, and remind you if there is a new version.

    We will collect IP address, device name, hardware version, device serial number and other device information to inform you update in time. The information collected are only used for verification of the device legitimacy and for notification of the updating.
  - ◇ Manual check: Click **Manual Check** to manually check the new version of the system.

2.2.5.9 Viewing Version

Log in to the webpage. Select **System** > **Version** to view the model, serial number of the device, system version and hardware version and other version information.

2.2.5.10 Viewing Legal Information

Log in to the webpage. Select **System** > **Legal Info** to view the open source software notice and other legal information.

2.2.6 Device Management

2.2.6.1 Configuring IPC

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

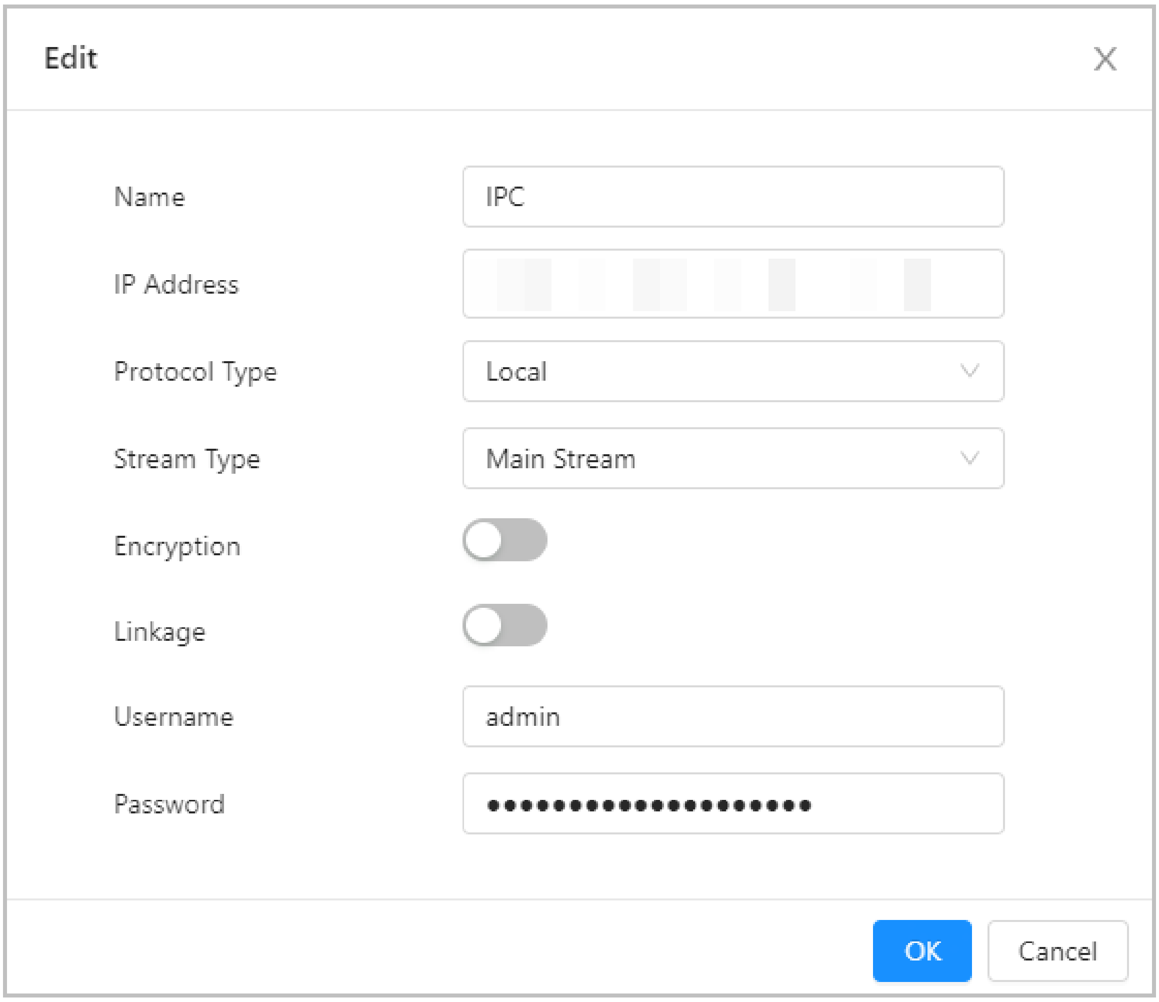
Procedure

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 2-37 Configure IPC



Edit

Name: IPC

IP Address: [redacted]

Protocol Type: Local

Stream Type: Main Stream

Encryption: ○

Linkage: ○

Username: admin

Password: ••••••••••••••••••••

Table 2-18 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.

Parameter	Description
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	

2.2.6.2 Adding VTO or Fence Station

Procedure

Step 1 Log in to the webpage of VTS.

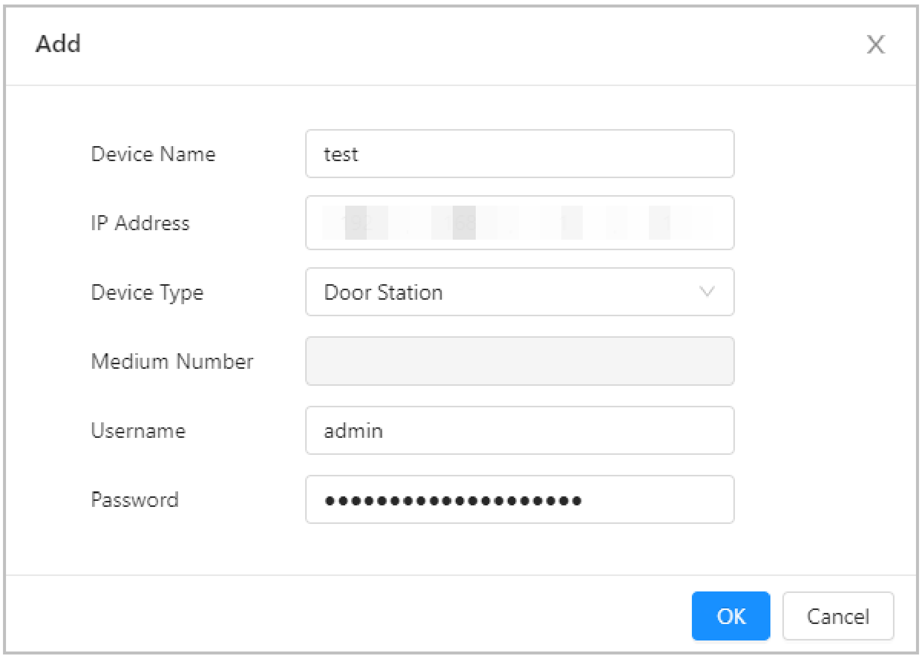
Step 2 Select **Device Setting** > **Device Setting** > **All**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

You can select door station or fence station.

Figure 2-38 Add door station of fence station



Add

Device Name: test

IP Address: [redacted]

Device Type: Door Station

Medium Number:

Username: admin

Password: ••••••••••••••••••••

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.

2.2.7 Log

2.2.7.1 Viewing System Log

Procedure

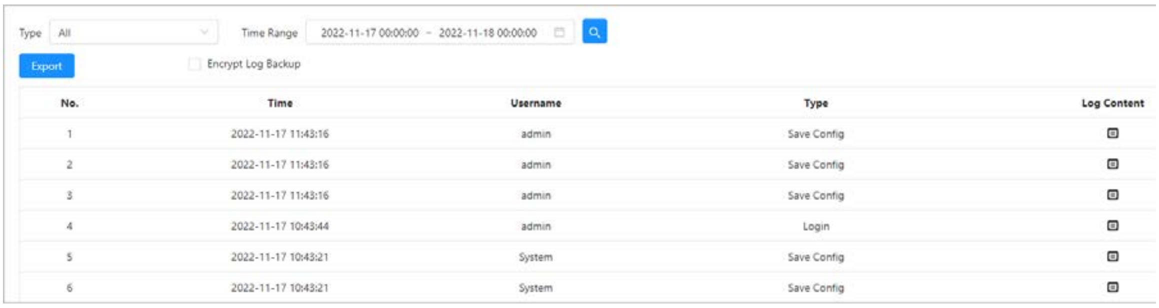
Step 1 Log in to the webpage of VTS.

Step 2 Select **Log** > **Log**.

Step 3 Select the log type, configure the time range, and then click 🔍.

- Click **Export** to export the log to the local computer. If you select **Encrypt Log Backup**, enter the encryption password, and then export the log.
- Click ▤ to view the log information.

Figure 2-39 System log



Type All

Time Range 2022-11-17 00:00:00 - 2022-11-18 00:00:00

Export

□ Encrypt Log Backup

No.	Time	Username	Type	Log Content
1	2022-11-17 11:43:16	admin	Save Config	▤
2	2022-11-17 11:43:16	admin	Save Config	▤
3	2022-11-17 11:43:16	admin	Save Config	▤
4	2022-11-17 10:43:44	admin	Login	▤
5	2022-11-17 10:43:21	System	Save Config	▤
6	2022-11-17 10:43:21	System	Save Config	▤

2.2.7.2 Viewing Call History

Procedure

Step 1 Log in to the webpage of VTS.

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

Step 3 (Optional) Click **Export** to export the call history to local computer.

2.2.7.3 Viewing Alarm Log

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **Log** > **Log**.

Step 3 Select the log type, configure the time range, and then click 🔍.

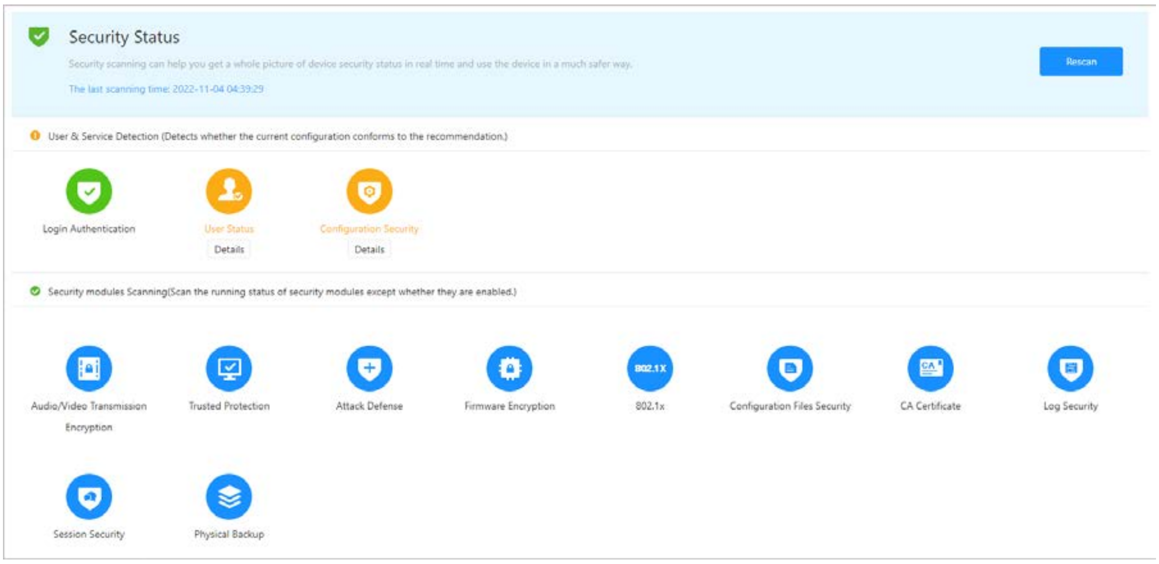
2.2.8 Security

2.2.8.1 Security Status

Detect and check the security status of the device.

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

Figure 2-40 Security status



Security Status

Security scanning can help you get a whole picture of device security status in real time and use the device in a much safer way.

The last scanning time: 2022-11-04 04:39:29

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

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

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.

2.2.8.2 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 **Security** > **System Service**.

Step 3 Click ○ to enable HTTPS.

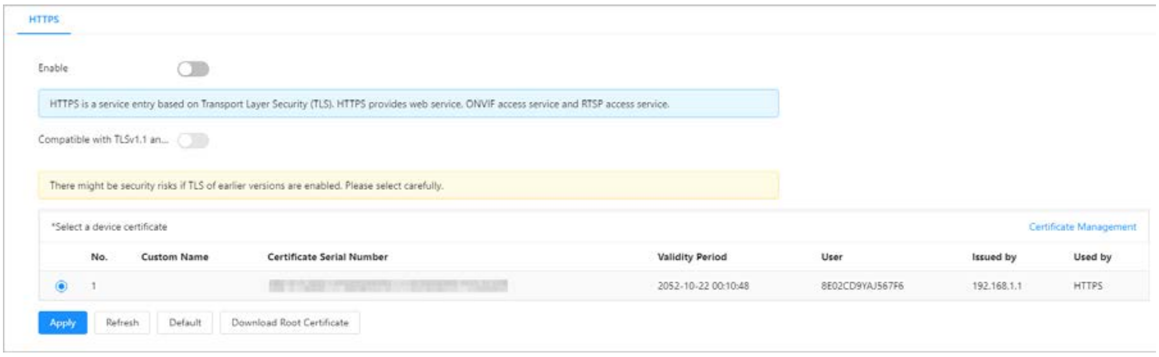
If you turn on **Compatible with TLSv1.1 and earlier versions**, there might be security risks. Please select carefully.

Step 4 Select the certificate.

If there is no certificate in the list, click **Certificate Management** at the left navigation bar.

For details, see "2.2.8.4 Installing Device Certificate".

Figure 2-41 HTTPS



Enable ○

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

Compatible with TLSv1.1 an... ○

There might be security risks if TLS of earlier versions are enabled. Please select carefully.

*Select a device certificate

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
●	1		[redacted]	2052-10-22 00:10:48	8E02CD9YAJ567F6	192.168.1.1	HTTPS

Step 5 Click **Apply**.

Result

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.

2.2.8.3 Attack Defense

2.2.8.3.1 Configuring Firewall

Configure firewall to limit access to the device.

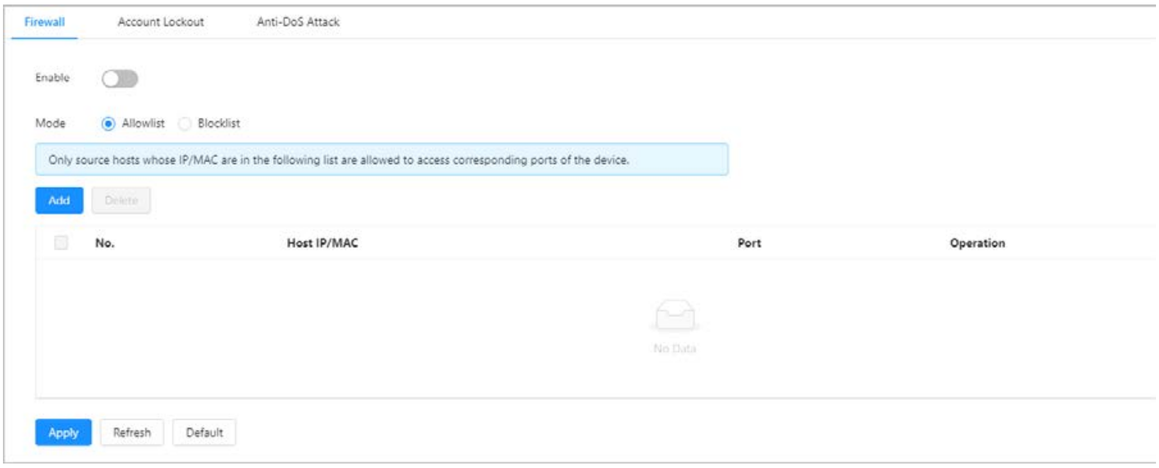
Procedure

Step 1 Log in to the webpage of VTS.

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

Step 3 Click ○ to enable the firewall function.

Figure 2-42 Firewall



Enable ○

Mode ● Allowlist ○ Blocklist

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

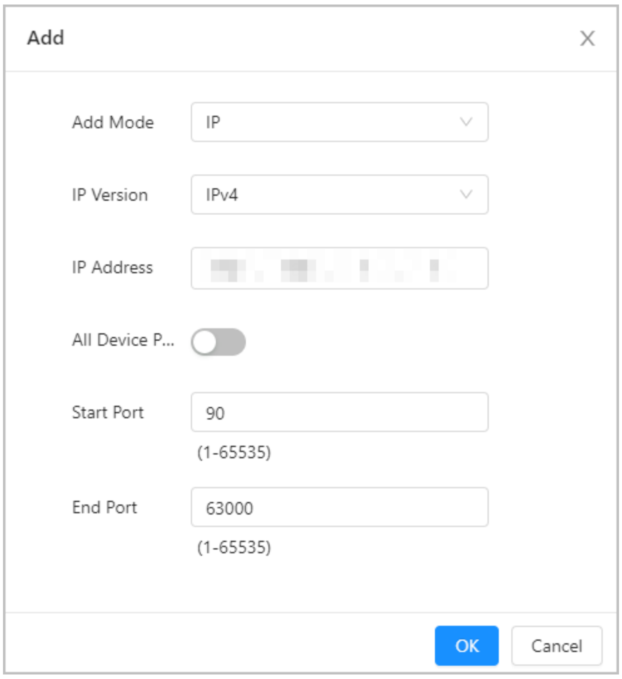
□	No.	Host IP/MAC	Port	Operation

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 2-43 Add the address



Add

Add Mode: IP

IP Version: IPv4

IP Address: [redacted]

All Device P...: ○

Start Port: 90 (1-65535)

End Port: 63000 (1-65535)

Step 6 Click **Apply**.

Related Operations

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

2.2.8.3.2 Configuring Account Lockout

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

Procedure

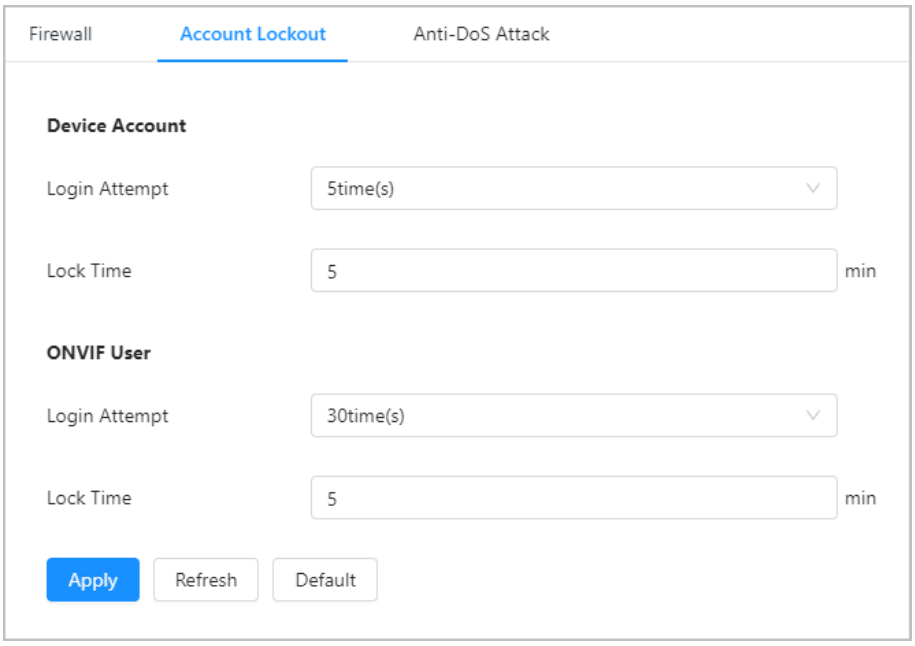
Step 1 Log in to the webpage of VTS.

Step 2 Select **Security** > **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 2-44 Account lockout



Device Account

Login Attempt: 5time(s)

Lock Time: 5 min

ONVIF User

Login Attempt: 30time(s)

Lock Time: 5 min

Step 4 Click **Apply**.

2.2.8.3.3 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.

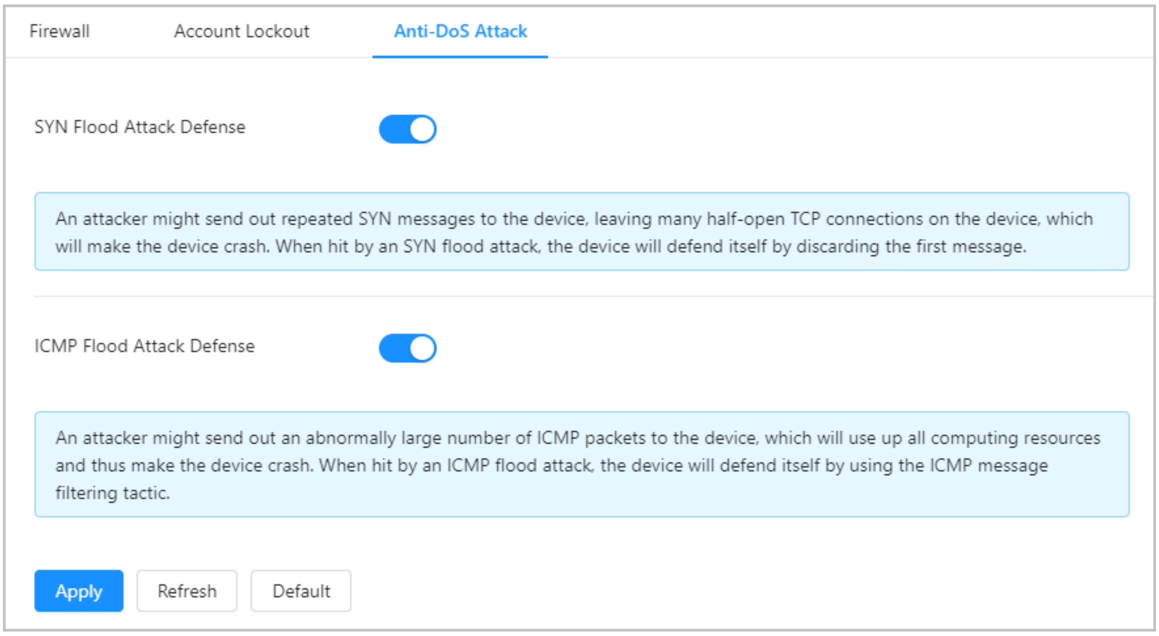
Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **Security** > **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 2-45 Anti-DoS Attack



SYN Flood Attack Defense: on

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

ICMP Flood Attack Defense: on

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

Step 4 Click **Apply**.

2.2.8.4 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.

2.2.8.4.1 Creating Certificate

Procedure

Step 1 Log in to the webpage of VTS.

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

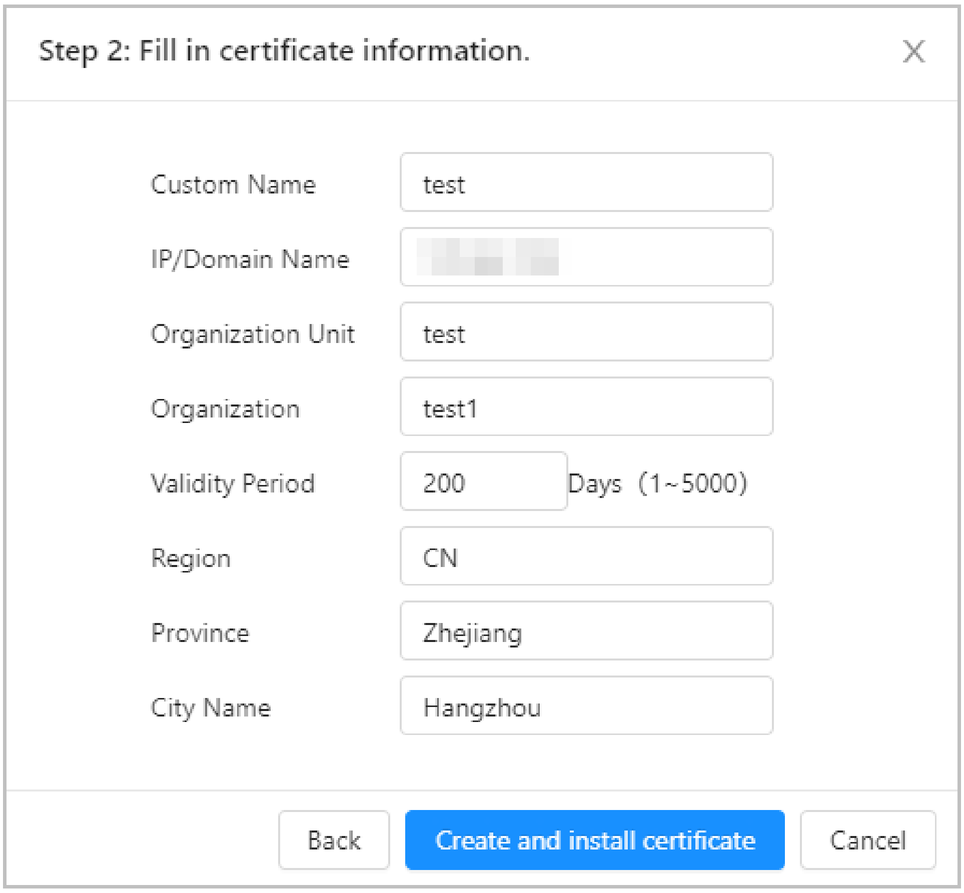
Step 3 Click **Install Device Certificate**.

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 2-46 Certificate Information (1)



Step 2: Fill in certificate information.

Custom Name	test
IP/Domain Name	[redacted]
Organization Unit	test
Organization	test1
Validity Period	200 Days (1~5000)
Region	CN
Province	Zhejiang
City Name	Hangzhou

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.

2.2.8.4.2 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 **Security** > **CA Certificate** > **Device Certificate**.

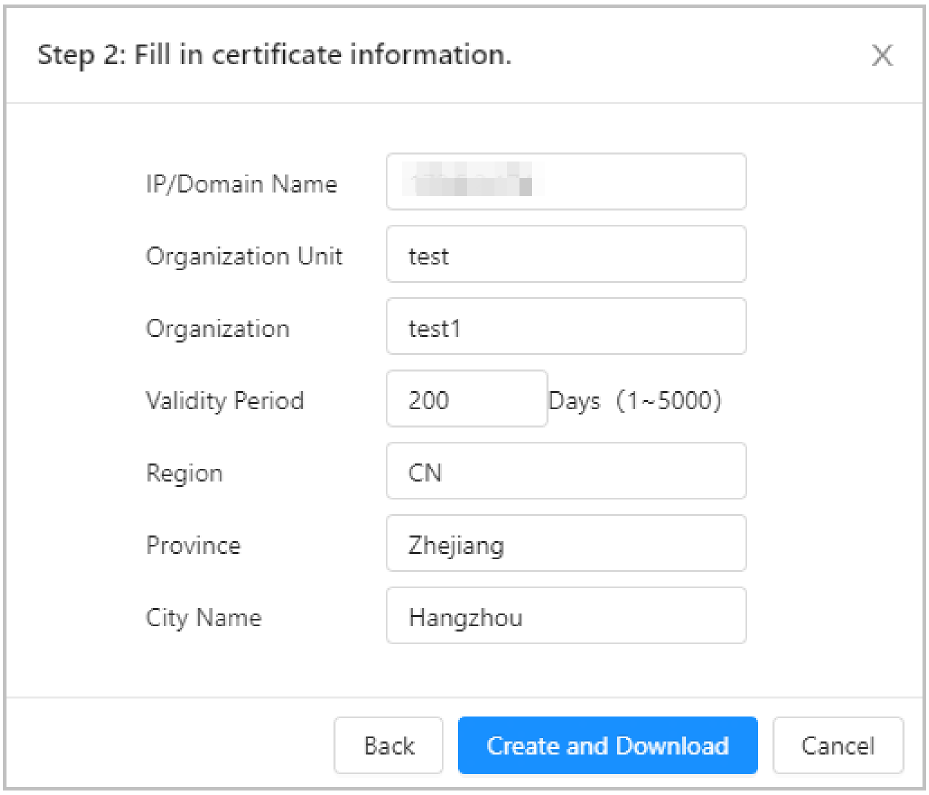
Step 3 Click **Install Device Certificate**.

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 2-47 Certificate information (2)



Step 2: Fill in certificate information.

IP/Domain Name	[redacted]
Organization Unit	test
Organization	test1
Validity Period	200 Days (1~5000)
Region	CN
Province	Zhejiang
City Name	Hangzhou

Step 6 Click **Create and Download**.

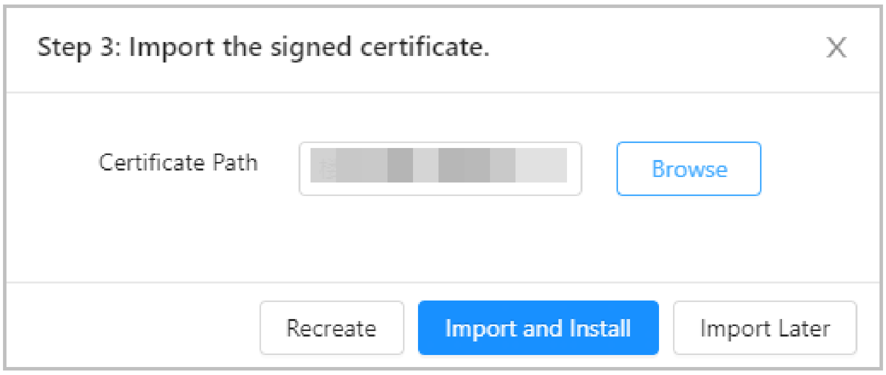
Save the request file to your PC.

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 2-48 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.

2.2.8.4.3 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 **Security** > **CA Certificate** > **Device Certificate**.

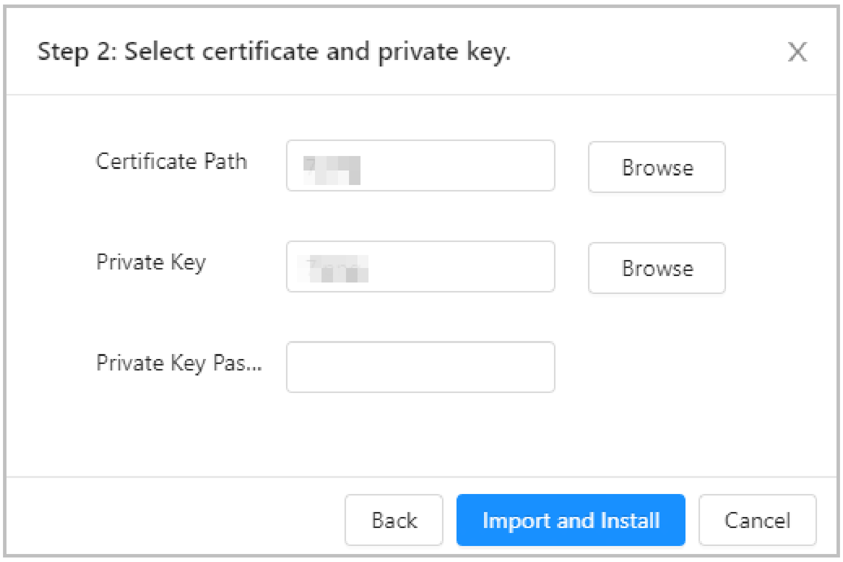
Step 3 Click **Install Device Certificate**.

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 2-49 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.

2.2.8.5 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.

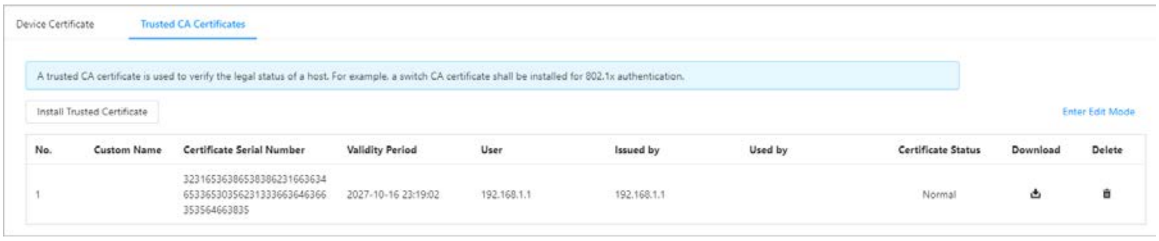
Procedure

Step 1 Log in to the webpage of VTS.

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

Step 3 Click **Install Trusted Certificate**.

Figure 2-50 Install trusted certificate



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

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by	Certificate Status	Download	Delete
1		323165363865383862316636346533653035623133366364636635356466 3835	2027-10-16 23:19:02	192.168.1.1	192.168.1.1		Normal	⬇	🗑

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.

2.2.8.6 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.

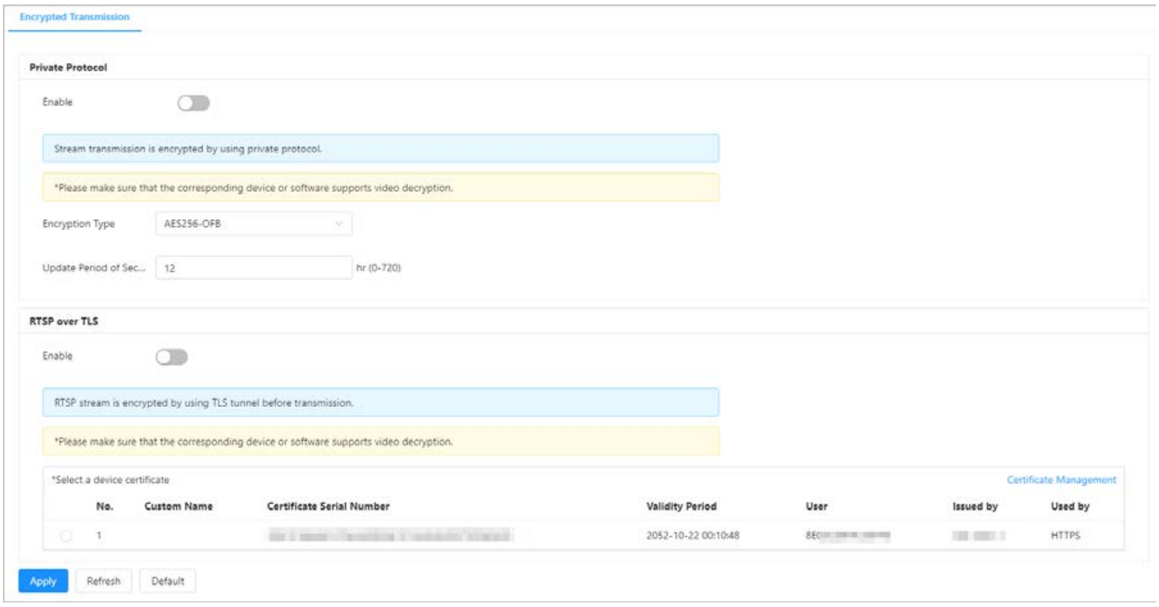
Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **Security** > **Video Encryption**.

Step 3 Configure the parameters.

Figure 2-51 Video encryption



Encrypted Transmission

Private Protocol

Enable ○

Stream transmission is encrypted by using private protocol.

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

Encryption Type: AES256-OFB

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

RTSP over TLS

Enable ○

RTSP stream is encrypted by using TLS tunnel before transmission.

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

*Select a device certificate — Certificate Management

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
○	1		[redacted]	2052-10-22 00:10:48	[redacted]	[redacted]	HTTPS

Apply | Refresh | Default

Table 2-19 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 "2.2.8.4 Installing Device Certificate". Created certificate of imported certificate are displayed in **Select a device certificate** list.

3 Industrial Scenes

3.1 Operations on Local Device

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

3.1.1 Local Screen

Figure 3-1 Local screen

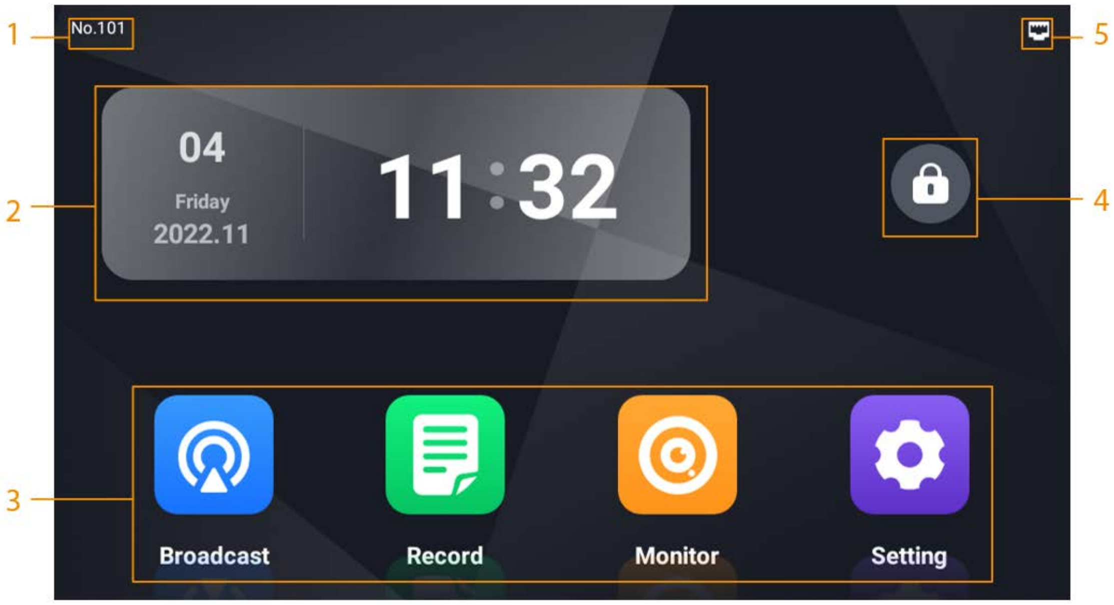


Table 3-1 Home screen introduction

No.	Description
1	The number of VTS.
2	Date and time.
3	Function buttons. ● Broadcast: Play the voice or manual broadcasting on part of terminal devices or all terminal devices. For details, see "3.1.4.1 Broadcasting". ● Record: Check the call history, video files and snapshot files. For details, see "3.1.4.2 Record". ● Monitor: Monitor VTA and IPC. For details, see "3.1.4.3 Monitoring". ● Setting: Enter the setting screen of VTS. For details, see "3.1.3 Project Settings".
4	Tap 🔒 to lock the screen. 📖 If you have selected **Setting** > **Display Settings**, and enabled **Lock Screen**, you need to enter the default password **123456** when you lock the screen.
5	The connection status of the network, the SIP server, and the SD card.

3.1.2 Configuring the Advanced Parameters

The configurations of the advanced settings are the same with that in buildings scene. For details, see "2.1.5 Configuring the Advanced Parameters".

The VTS in the industrial scene does not have **Receive Alarm Info from VTHs** function.

3.1.3 Project Settings

3.1.3.1 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.

Table 3-2 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	
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.

3.1.3.2 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 3-3 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**.

3.1.4 Commissioning

3.1.4.1 Broadcasting

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

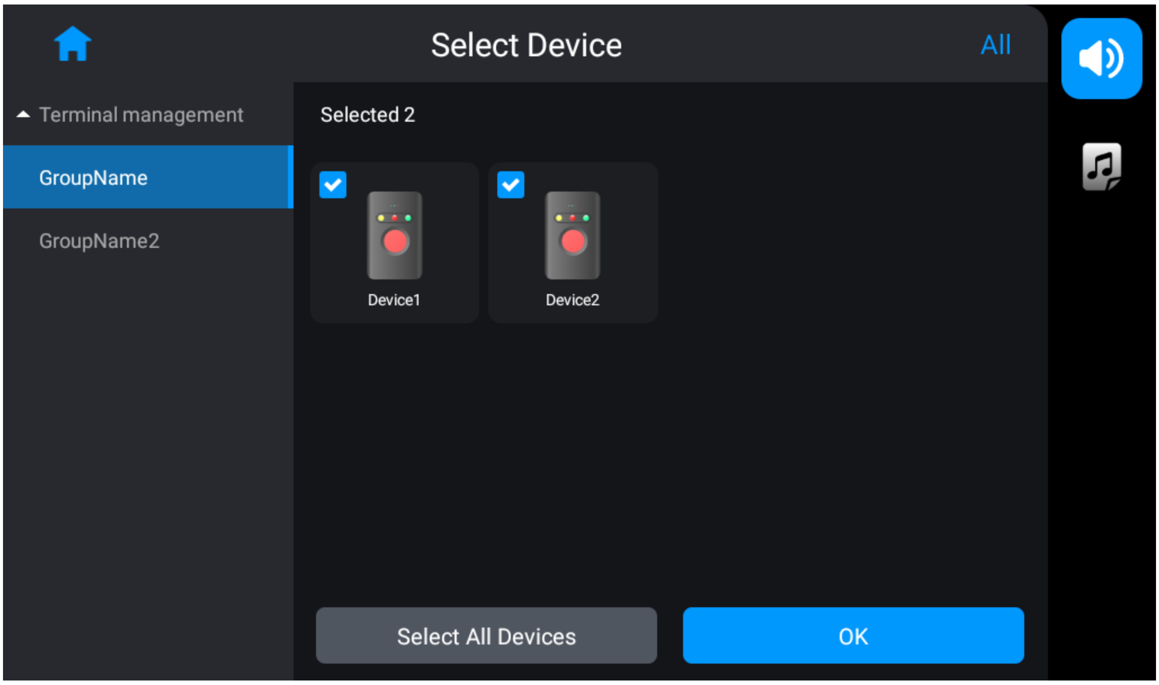
3.1.4.1.1 Broadcasting on Part of the Devices

Procedure

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

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

Figure 3-2 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 3-3 Audio broadcasting

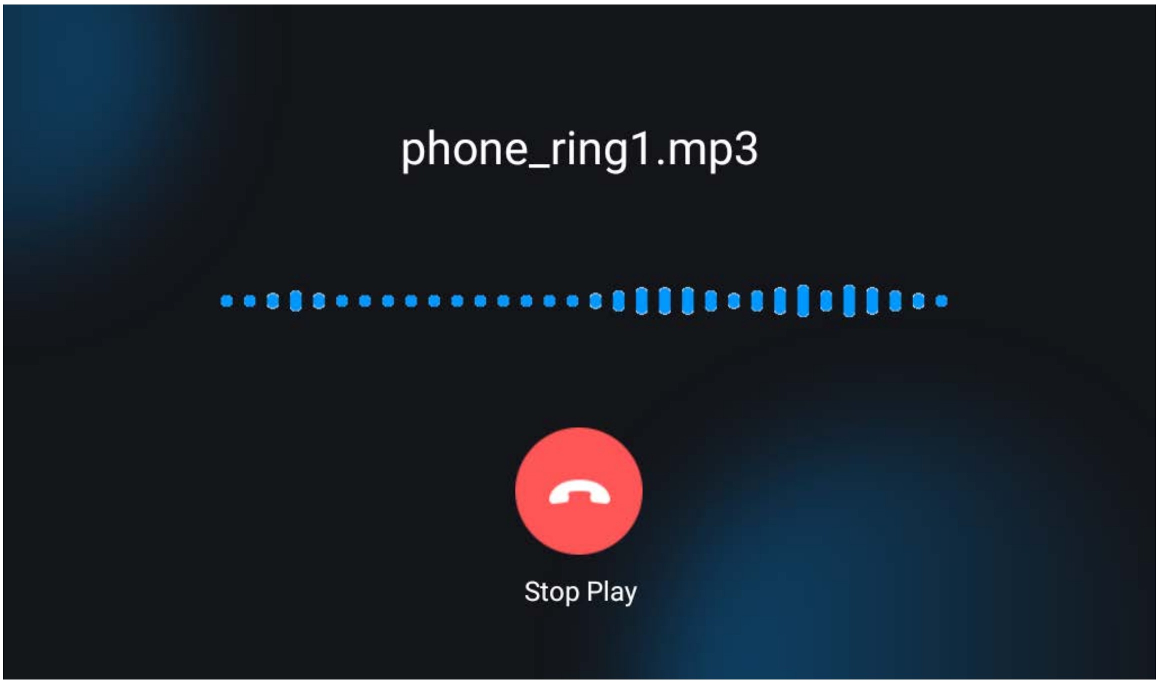
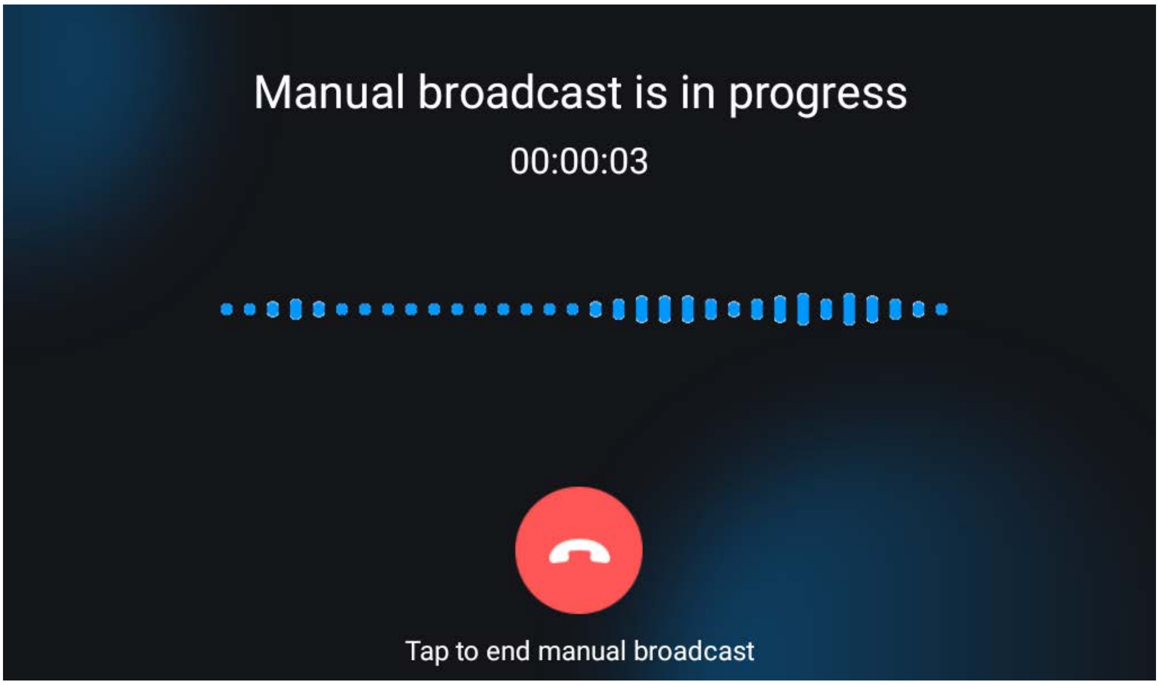

phone_ring1.mp3

Figure 3-4 Manual broadcasting


Manual broadcast is in progress

00:00:03

3.1.4.1.2 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.

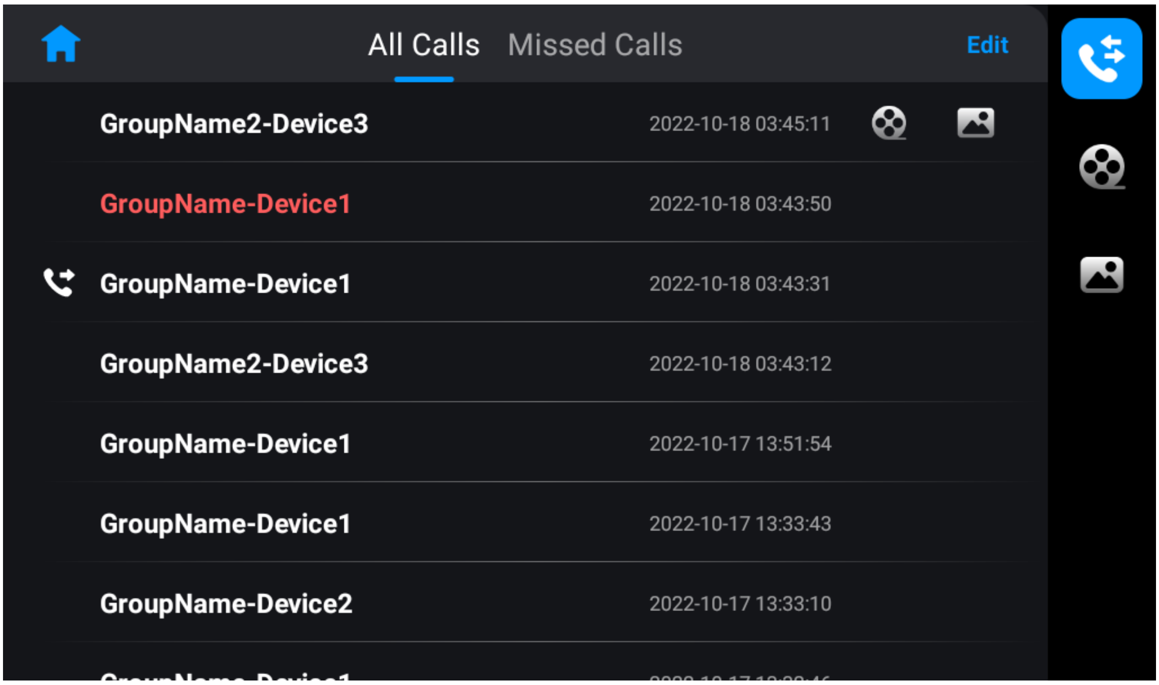
3.1.4.2 Record

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 3-5 Call history



All Calls   Missed Calls   Edit

GroupName2-Device3   2022-10-18 03:45:11

GroupName-Device1   2022-10-18 03:43:50

GroupName-Device1   2022-10-18 03:43:31

GroupName2-Device3   2022-10-18 03:43:12

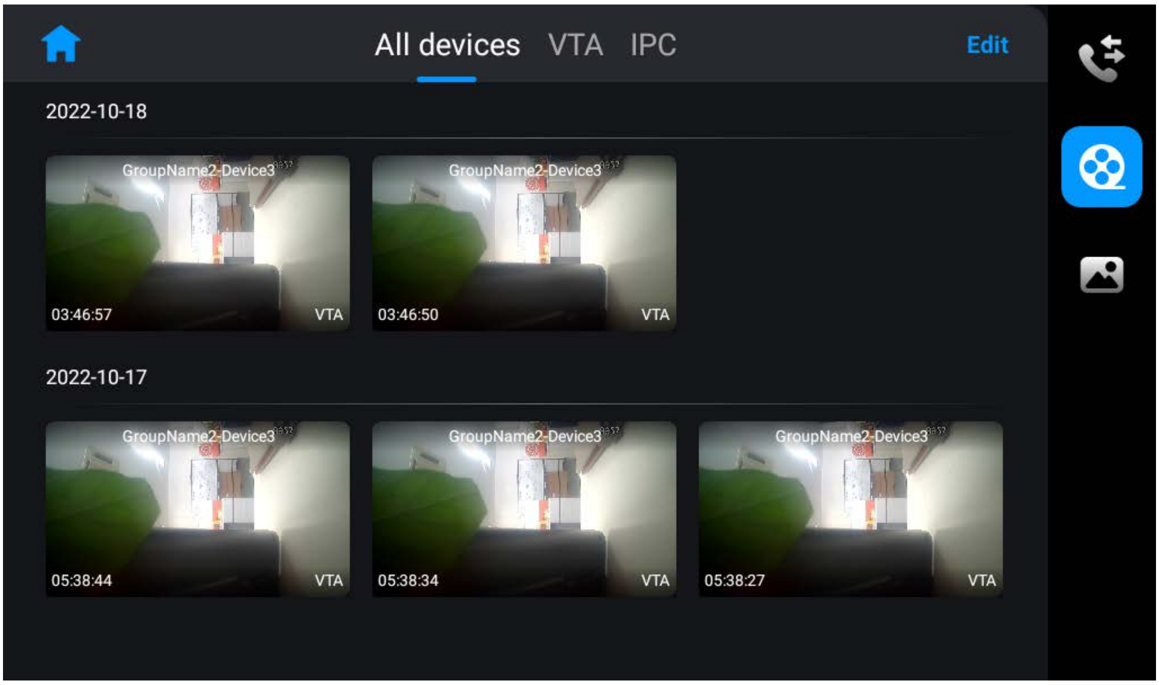
GroupName-Device1   2022-10-17 13:51:54

GroupName-Device1   2022-10-17 13:33:43

GroupName-Device2   2022-10-17 13:33:10

Video

Figure 3-6 Video files



All devices   VTA   IPC   Edit

2022-10-18

GroupName2-Device3   03:46:57   VTA

GroupName2-Device3   03:46:50   VTA

2022-10-17

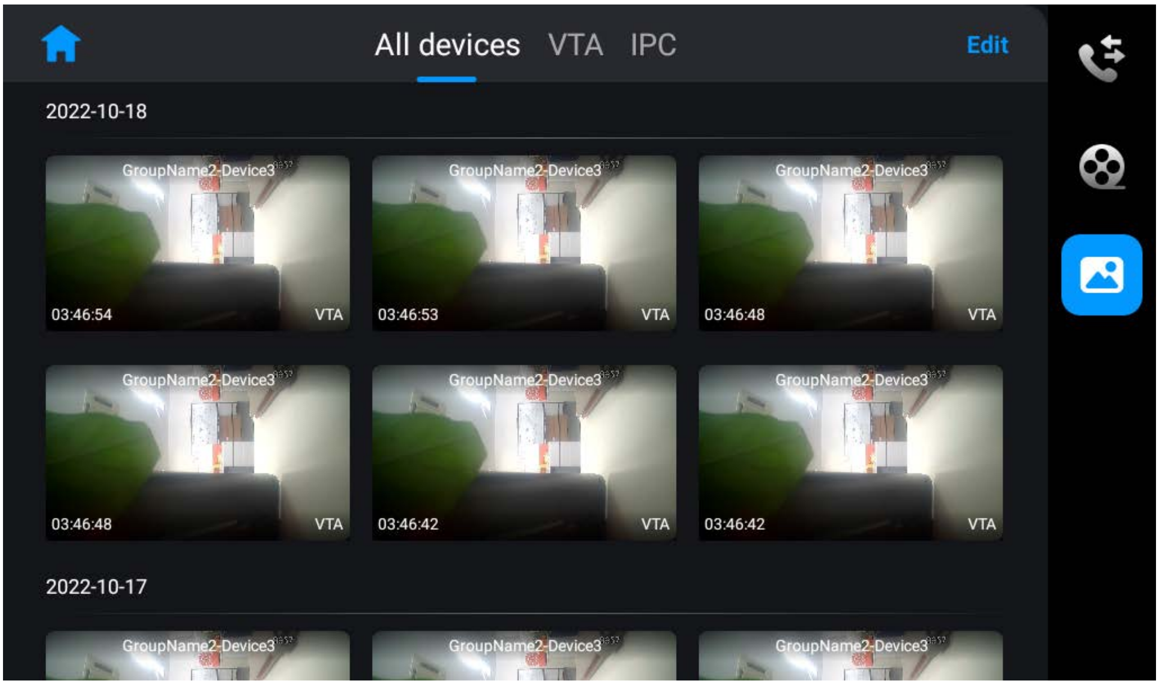
GroupName2-Device3   05:38:44   VTA

GroupName2-Device3   05:38:34   VTA

GroupName2-Device3   05:38:27   VTA

Snapshot

Figure 3-7 Snapshot files



3.1.4.3 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 3-8 Monitor VTA

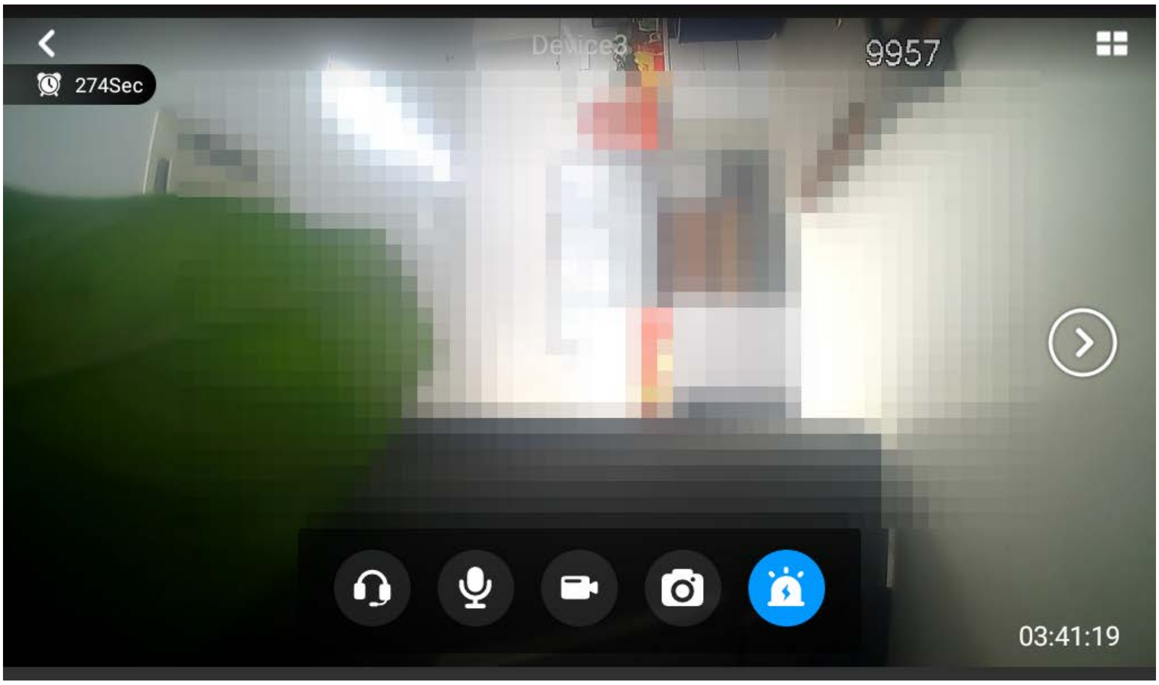


Table 3-4 Monitoring image description

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.

3.2 Operations on Webpage

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

3.2.1 Configuring Device Role

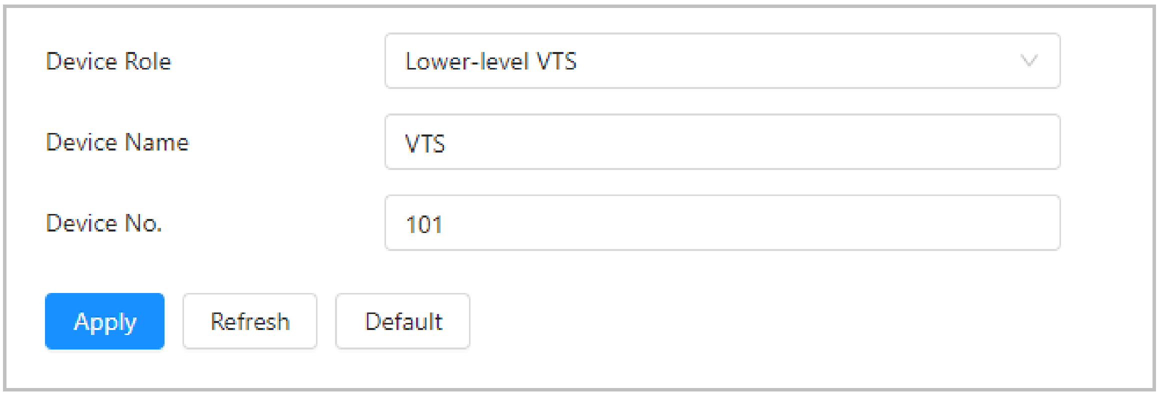
Procedure

Step 1 Log in to the webpage of the device.

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

Step 3 Configure the parameters.

Figure 3-9 Configure the parameters



Device Role	Lower-level VTS
Device Name	VTS
Device No.	101

Table 3-5 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. ● 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. ● 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**.

3.2.2 Configuring FTP

Get the audio file from FTP and play it.

Procedure

Step 1 Log in to the webpage.

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

Step 3 Turn on **Enable**, and then configure the parameters.

Step 4 Click **Apply**.

3.2.3 Adding Devices

- VTS as lower-level VTS: You can add VTA and IPC. The operations of adding IPC are the same with that in buildings scene.
- VTS as upper-level VTS: You can add lower-level VTS.

3.2.3.1 Adding VTA

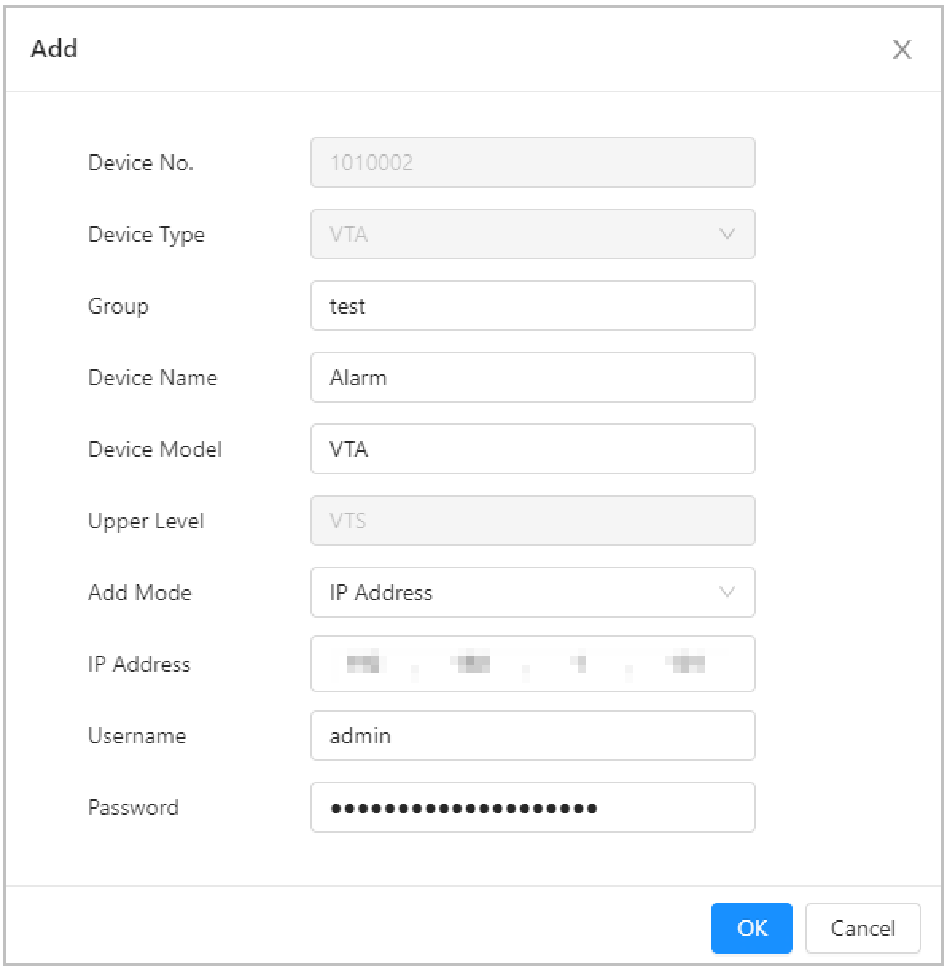
Procedure

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 3-10 Add VTA



Add

Device No.	1010002
Device Type	VTA
Group	test
Device Name	Alarm
Device Model	VTA
Upper Level	VTS
Add Mode	IP Address
IP Address	[redacted]
Username	admin
Password	••••••••••••••••••••

Table 3-6 Parameters description

Parameter	**Description**
Group	Select **Monitor** > **Terminal Management** on local 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 VTO in the following 2 ways. ● IP address: Enter the IP address of the device. ● Register: Configure the parameters for registering on the device.
Username	Enter the username and password of the device that you added.
Password	

Step 4 Click **OK**.

3.2.3.2 Adding Lower-level VTS

Procedure

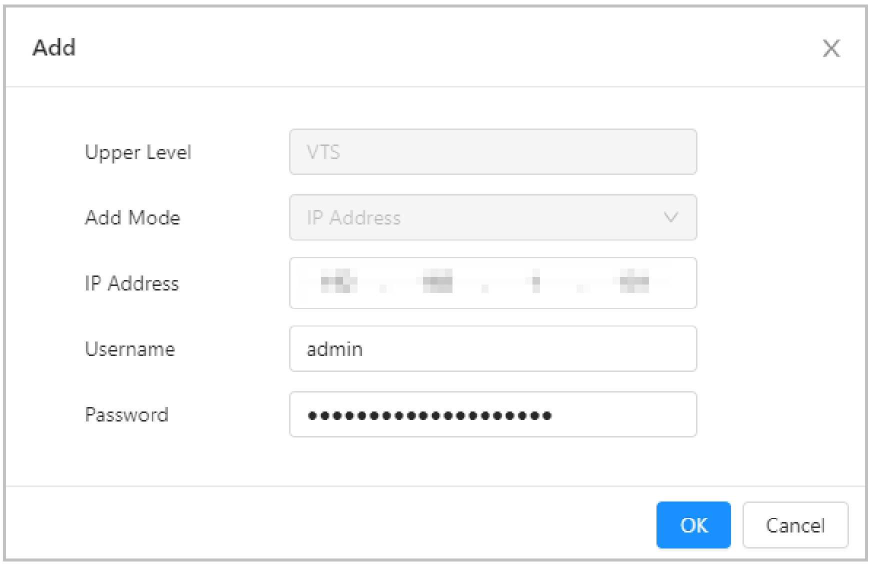
Step 1 Log in to the webpage of the device.

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

Step 3 Click **Add**.

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

Figure 3-11 Add lower-level VTS



Add

Upper Level: VTS

Add Mode: IP Address

IP Address: [redacted]

Username: admin

Password: ●●●●●●●●●●●●●●●●●●●

Step 5 Click **OK**.

3.2.4 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, tha call fails to be forwarded.

3.2.4.1 Configuring Forwarding

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

Procedure

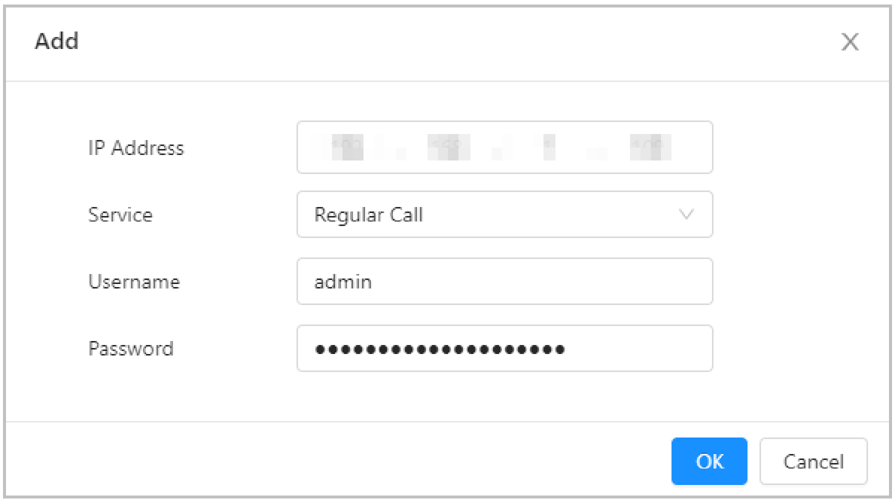
Step 1 Log in to the webpage.

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

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 3-12 Add the VTS for forwarding the call



Add

IP Address: [redacted]

Service: Regular Call

Username: admin

Password: ●●●●●●●●●●●●●●●●●●●●

Table 3-7 Description of forwarding parameters

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

Step 5 Click **OK**.

3.2.4.2 Configuring Receiving

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

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Device Setting** > **Call Forwarding** > **Receiving**.

Step 3 Click **Add**.

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

Step 5 Click **OK**.

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the “auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

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

4. **Enable Account Lock**

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

5. **Change Default HTTP and Other Service Ports**

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

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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