Master Station (VTS8340B)

User's Manual

V1.0.0

Foreword

General

This manual introduces the installation and basic operation of the master station (VTS8340B-CG).

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
🕮 **NOTE**	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision content	Release Date
V1.0.0	First release.	March 2020

About the Manual

- The Manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

This chapter introduces the contents covering proper handling of the VTS, hazard prevention, and prevention of property damage. Read these contents carefully before using the VTS, comply with them when using, and keep the manual well for future reference.

Operating Requirement

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- The device shall be used with screened network cables.

Power Requirement

- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.
- Do not cut off power supply during device upgrade. Power supply can be cut off only after the device has completed upgrade and has rebooted.

⚠

- Risk of explosion if the battery is replaced by an incorrect type.
- Do not throw or immerse into water, heat to more than 100 ºC (212 ºF), repair or disassemble, leave in an extremely low air pressure environment or extremely high-temperature environment, crush, puncture, cut or incinerate.
- Dispose of the battery as required by local ordinances or regulations.

Table of Contents

1 Overview

1.1 Introduction

1.1.1 Product Introduction

As the contact center and service center of the system, VTS can be used:

- As the client of the platform.
- As the device administrator without the platform, which can manage 120 terminal system at most.
- To do business such as the video intercom, monitoring, listening, calling, and broadcast

1.1.2 Features

- Easy operation; no need to install; the bracket can be adjusted within 0–45°.
- Manage 120 Terminal at most.
- The video intercom between VTSs.
- Multi-channel monitoring, and supports 4-channel 720p at most.
- Capacitive touch screen, 10 inch HD LCD
- Two modes: Handsfree and handset.
- SD Card
- 1-channel HDMI output, and resolution is 1024 × 600 at most.

1.2 Device Structure

Put the VTS on a table place such as desk, and adjust the angle within 0°–45° through the bracket on the rear panel.

1.2.1 Front panel

Figure 1-1 Front panel

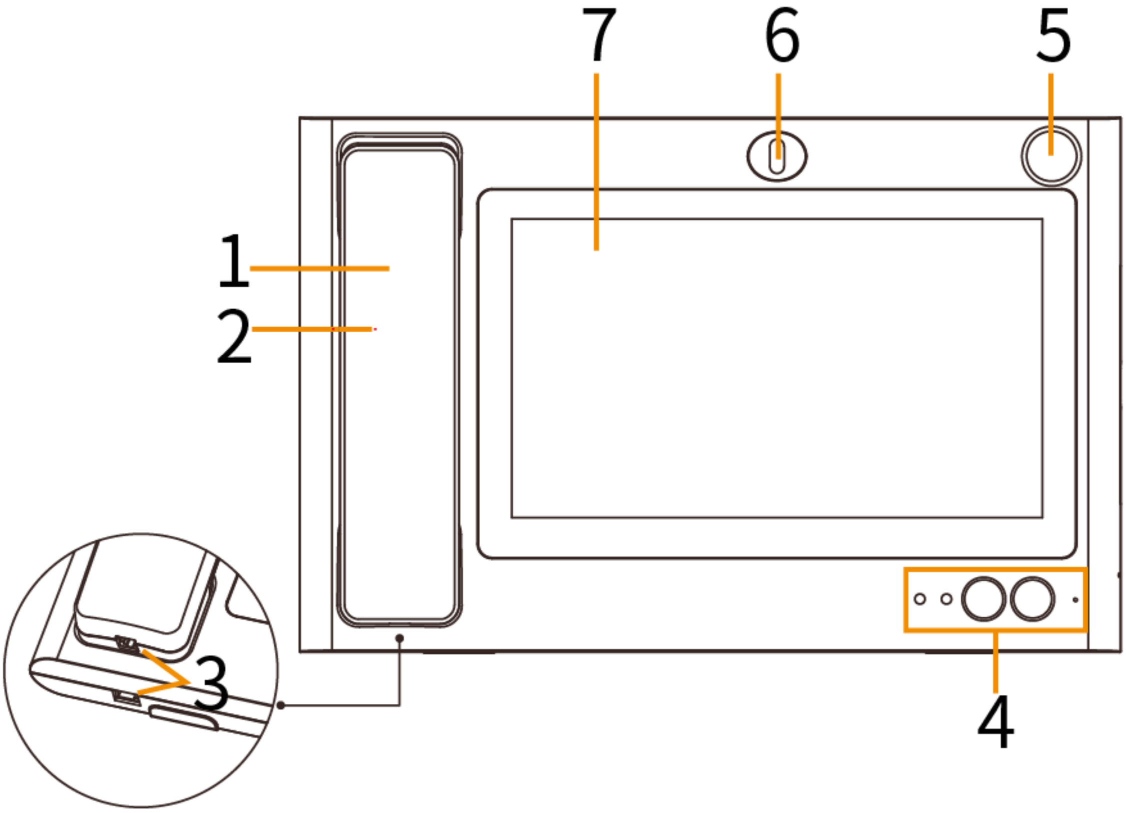


Table 1-1 Front panel description

No.	Parameter	Description
1	Handset	Pick up the handset, the VTS enters handset mode.
2	Speaker	Outputs audio.
3	Telephone line port	Connects the VTS and the receiver.
4	Indicator lights and buttons	From left to right: ● Power indicator light On: Power on; Off: Power off. ● Message indicator light On: There are missed calls; Off: There is no missed call or missed calls have been processed. ● Unlock button (Optional) When the VTS is being called, monitoring or talking, press the button to open some front devices which support unlock function. ● Handfree button Answers calls, and switch between handsfree mode and handset mode. ● Built-in MIC Inputs audio.
5	Speaker port	(Optional) Connects to a microphone. 🕮

No.	Parameter	Description
		This function is only available on the models with built-in camera.
6	Camera	(Optional) You can adjust the camera angle manually.
7	Display and touch screen	LCD display and touch screen.

1.2.2 Rear panel

Figure 1-2 Rear panel

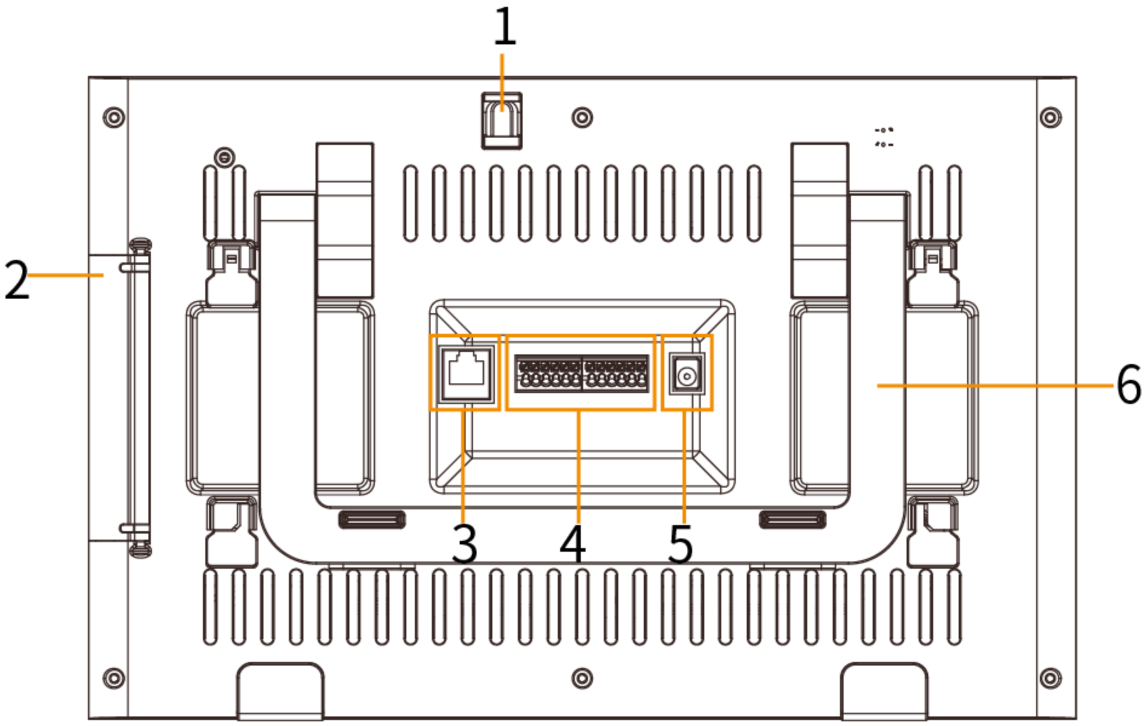


Table 1-2 Rear panel description

No.	Parameter	Description
1	Camera	You can adjust the camera angle manually.
2	Port	Open the cover, ports from top to bottom: ● HDMI video transmission port, which is used for video transmission. ● USB port. ● USB port. ● SD slot.
3	Network port	Connects to RJ-45 cable.
4	12-Core port	From left to right: ● Power output port. ● Ground. ● Alarm input port 1. ● Alarm input port 2. ● Alarm input port 3.

No.	Parameter	Description
		● Alarm input port 4. ● Power input port. ● Ground port. ● RS-485A port. ● RS-485B port. ● Alarm Output No. ● Alarm Output COM.
5	Power	DC 12V power input.
6	Bracket	Adjust the angle within 0°–45° through the bracket on the rear panel.

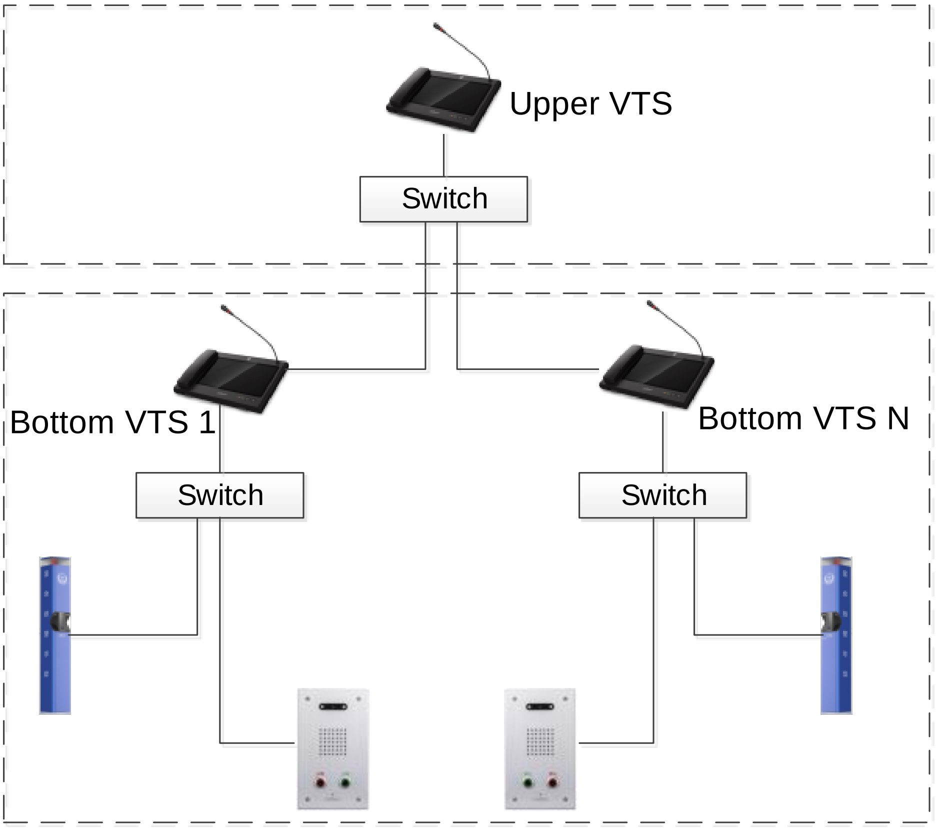
2 Cable Connection

2.1 Important Note

- Use the standard power adapter. Do not supply power with the adapter of other models.
- Before connecting cables, read "1.2 Device Structure" to learn the device structure.
- Before connecting the power source, make sure that all the cables are connected correctly. After power on, the power indicator light is on.

2.2 Network Diagram

Figure 2-1 Network diagram



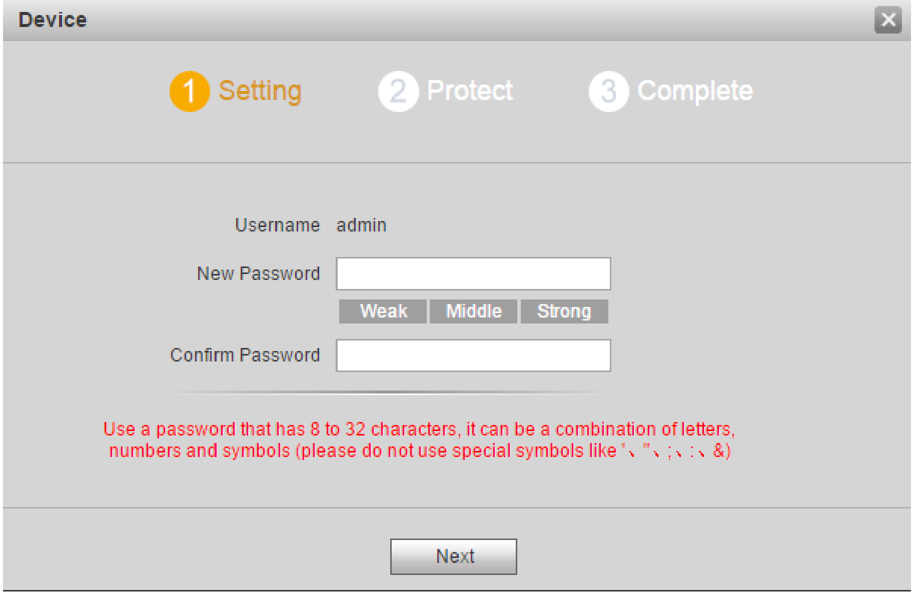
3 Web Operations

3.1 Device Initialization

For first time login, or after default setting, you need to initialize the VTS; otherwise the VTS cannot be used normally.

Step 1 Enter the IP address of the VTS in the address bar.

Figure 3-1 Password setting

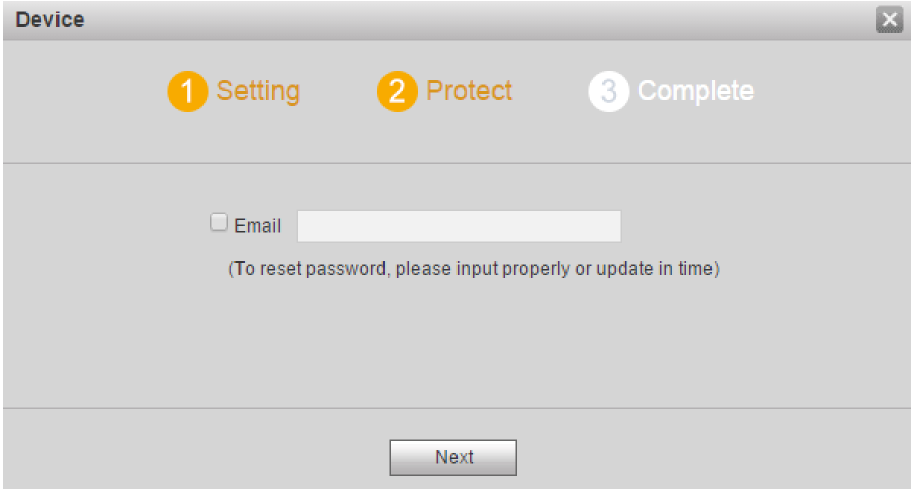


Username admin

Use a password that has 8 to 32 characters, it can be a combination of letters, numbers and symbols (please do not use special symbols like '、"、;、:、&)

Step 2 Follow the screen instruction, enter the new password, confirm the password, and then click **Next**.

Figure 3-2 Password Protection

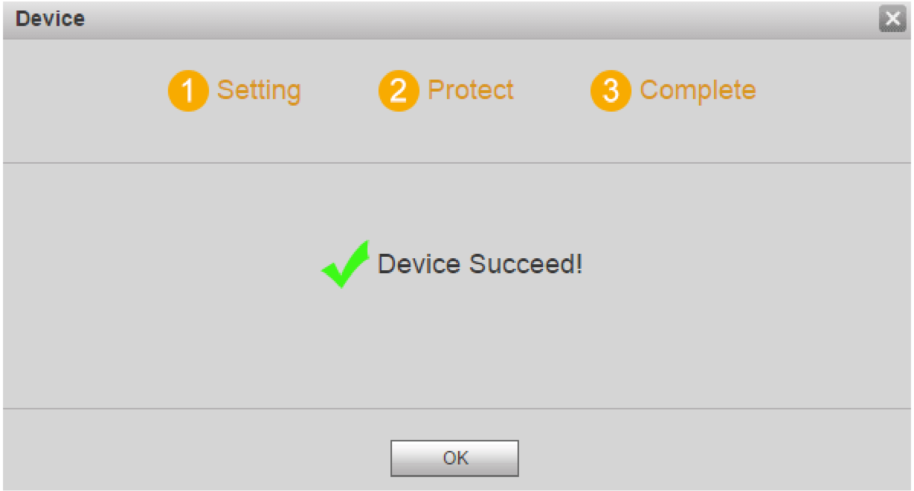


□ Email

(To reset password, please input properly or update in time)

Step 3 Select the **Email** check box, and then enter your email address, Click **Next**.

Figure 3-3 Completed



Device Succeed!

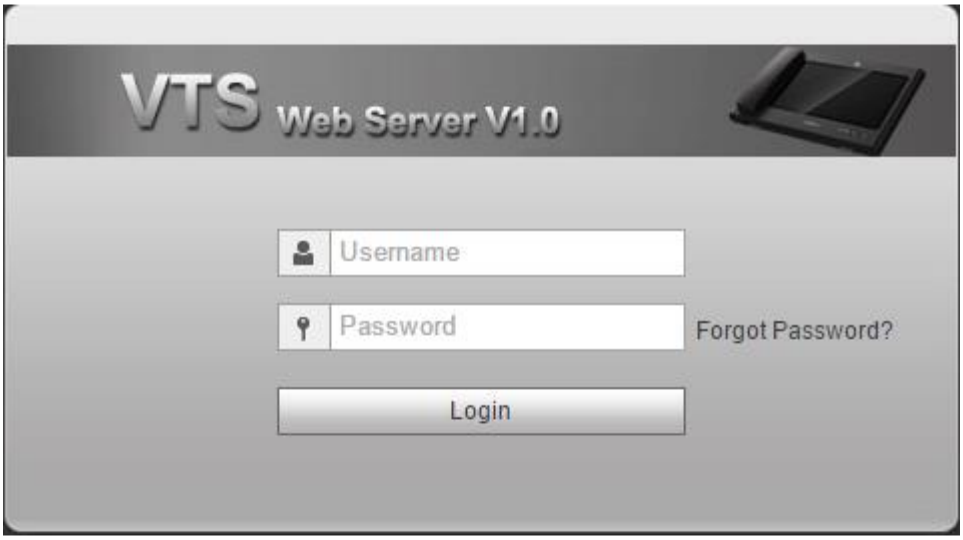
Step 4 Click **Save**. The login interface is displayed.

3.2 Login

Step 1 Enter the IP address of the VTS in the address bar.

Make sure that the PC IP address is in the same network segment device with that of the VTS. The IP of the VTS is 192.168.1.108 by default.

Figure 3-4 Login



Step 2 Enter the username and password

Step 3 Click **Login**.

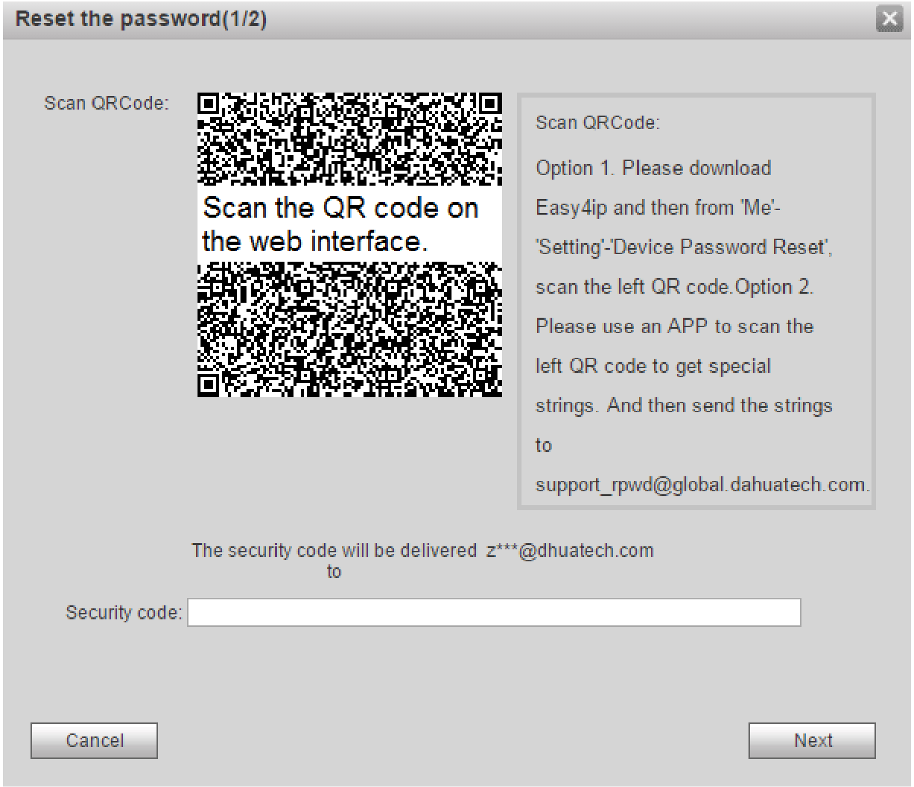
3.3 Password Reset

If you forgot the password, you can reset the password through this function.

Step 1 Click **Forgot password ?** on the login interface.

If you use IE browser, the system might prompt **Stop running the script**, click **No** and continue to run the script.

Figure 3-5 Reset password (1)



Reset the password(1/2)

Scan QRCode:

Scan the QR code on the web interface.

Scan QRCode:

Option 1. Please download Easy4ip and then from 'Me'-'Setting'-'Device Password Reset', scan the left QR code.Option 2. Please use an APP to scan the left QR code to get special strings. And then send the strings to support_rpwd@global.dahuatech.com.

The security code will be delivered to z***@dhuatech.com

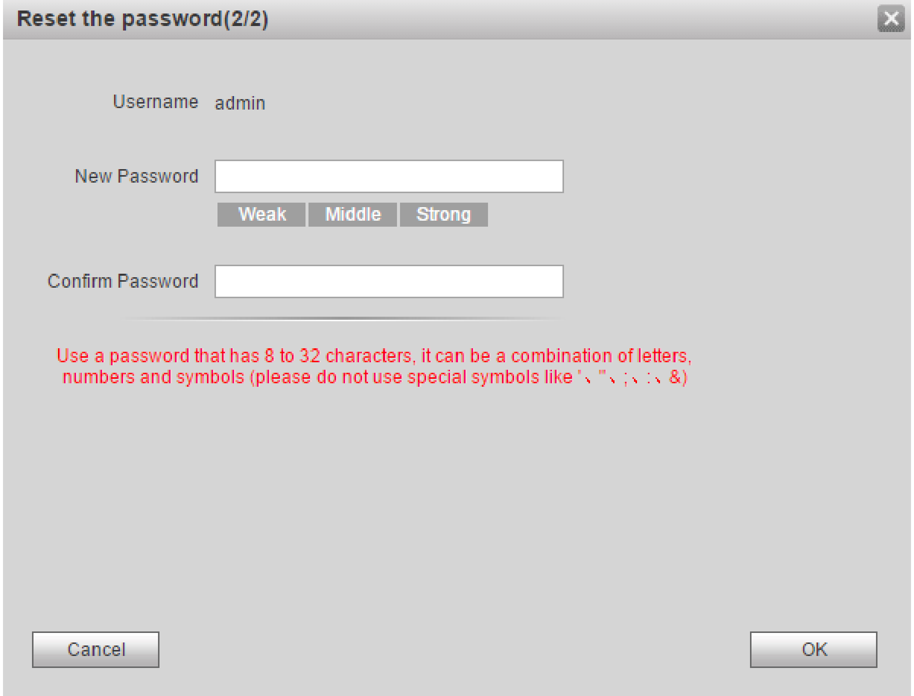
Security code:

Step 2 Scan the QR code, and you will get the security code.

Step 3 Enter the security code that you have received.

Step 4 Click **Next**.

Figure 3-6 Reset the password (2)



Reset the password(2/2)

Username admin

New Password

Confirm Password

Use a password that has 8 to 32 characters, it can be a combination of letters, numbers and symbols (please do not use special symbols like '、"、;、:、&)

Step 5 Enter the new password and confirm it.

The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). **Password** and **Confirm Password** shall be the same. Enter a strong password according to the password strength indication.

Step 6 Click **OK** and password reset is completed.

3.4 System Setup

3.4.1 Local Setup

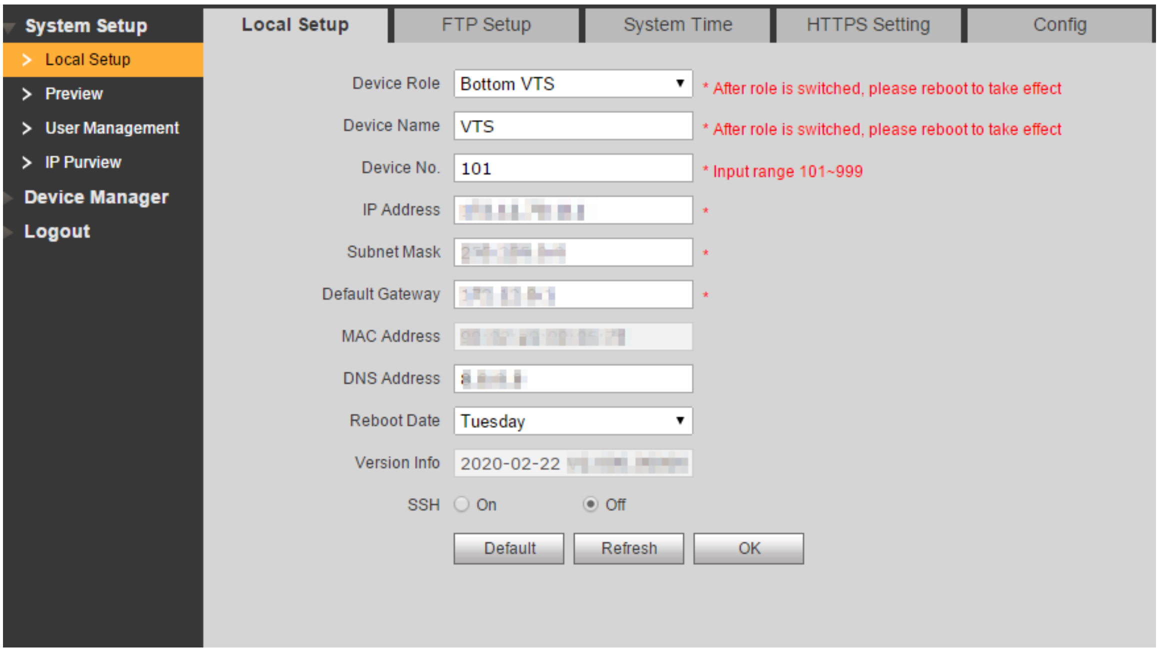
You can configure local information, FTP, system time, and HTTPS, and export, import and default the configuration.

3.4.1.1 Local Setup

Set the information such as device role, device name and IP address.

Step 1 Select **System Setup > Local Setup**, Click the **Local Setup** Tab.

Figure 3-7 Local setup



Device Role: Bottom VTS ▼ * After role is switched, please reboot to take effect

Device Name: VTS * After role is switched, please reboot to take effect

Device No.: 101 * Input range 101~999

IP Address: [redacted] *

Subnet Mask: [redacted] *

Default Gateway: [redacted] *

MAC Address: [redacted]

DNS Address: [redacted]

Reboot Date: Tuesday ▼

Version Info: 2020-02-22 [redacted]

SSH ○ On ● Off

Step 2 Configure parameters.

Table 3-1 Local setup parameter description

Parameter	Description
Device Role	Includes 3 role types, and the default one is **Bottom VTS**. ● Bottom VTS: When used without platform, VTS can be used as bottom VTS, which has management permission. ● Upper VTS: When used without platform, VTS can be used as upper VTS, which has the permission to add the VTS of lower level, but does not have the permission to manage the organization structure. ● Platform client: When used with platform, VTS can be used as platform client, which does not have the permission to manage device.

Parameter	Description
Device Name	Customize the name for the device.
Device No.	Customize the number for the device. Do not modify it arbitrarily. If you modify the number of the VTS of lower level, you need to add the device to the upper VTS.
IP Address	Enter the IP address, subnet mask, and gateway If you modify the IP address of the VTS of lower level, you need to add the device to the upper VTS.
Subnet Mask	
Default Gateway	
MAC Address	Displays the MAC address of the Device.
DNS address	The DNS address of the device, and it is 8.8. 8.8 by default.
Reboot Date	Set the time at which the VTS auto reboots. The time is 2:00, Tuesday by default.
Version Info	Display the current Version.
SSH	Enable or disable the SSH debug function. ● If you have enabled the SSH function the **Advanced Config** on the device, the function is enabled on the web interface. See "4.2.6.2 Local Setup." ● You can modify VTS number, local IP address, subnet mask, and gateway; and view the MAC address and version information. See Figure 4-14. ● You can modify VTS number, local IP address, subnet mask, and gateway; and view the MAC address and version information. See Figure 4-14.

Step 3 Press **OK**.

- Click **Default** to restore all the configuration of this tab to the default value.
- Click **Refresh** to display the current system configuration.

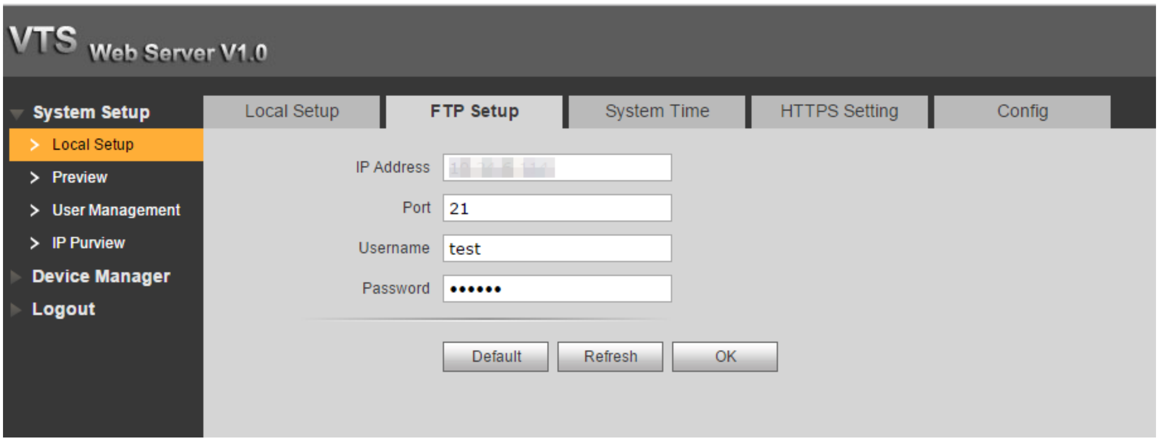
- The parameter with * indicates necessary.
- After Device Role is modified, the system will go to the login interface, and you need to log in again.
- After IP Address is modified, the system will go to the login interface, and you need to log in again.

3.4.1.2 FTP Setup

Get audio files from FTP and play them.

Step 1 Select **System Setup > Local Setup**, Click the **FTP Setup** Tab.

Figure 3-8 FTP Setup



IP Address [redacted]

Port 21

Username test

Password ••••••

Step 2 Enter the IP address, port, username and password of the FTP.

Step 3 Press **OK**.

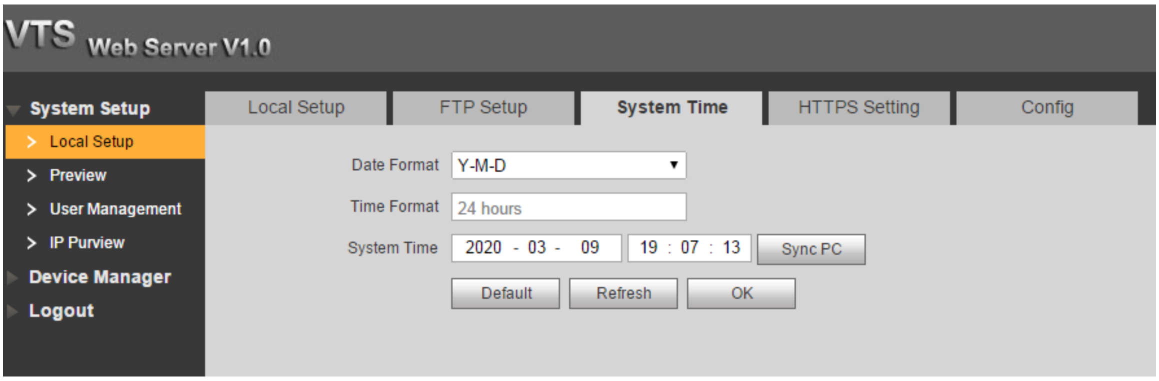
- Click **Default** to restore all the configuration of this tab to the default value.
- Click **Refresh** to display the current system configuration.

3.4.1.3 System Time

Set the system time.

Step 1 Select **System Setup > Local Setup**, Click the **System Time** tab.

Figure 3-9 System time



Date Format Y-M-D

Time Format 24 hours

System Time 2020 - 03 - 09 19 : 07 : 13

Step 2 Configure parameters. See Table 3-2.

Table 3-2 Local setup

Parameter	Description
Date Format	Set the data format. You can select from **Year-Month-Day**, **Month-Day-Year**, and **Day-Month-Year**.
Time Format	Configure the time format, you can select from **12-Hour** and **24-Hour**.
System Time	Set the system time.
Sync PC	Click **Sync PC** to sync the VTO system time and the PC system time.

Step 3 Press **OK**.

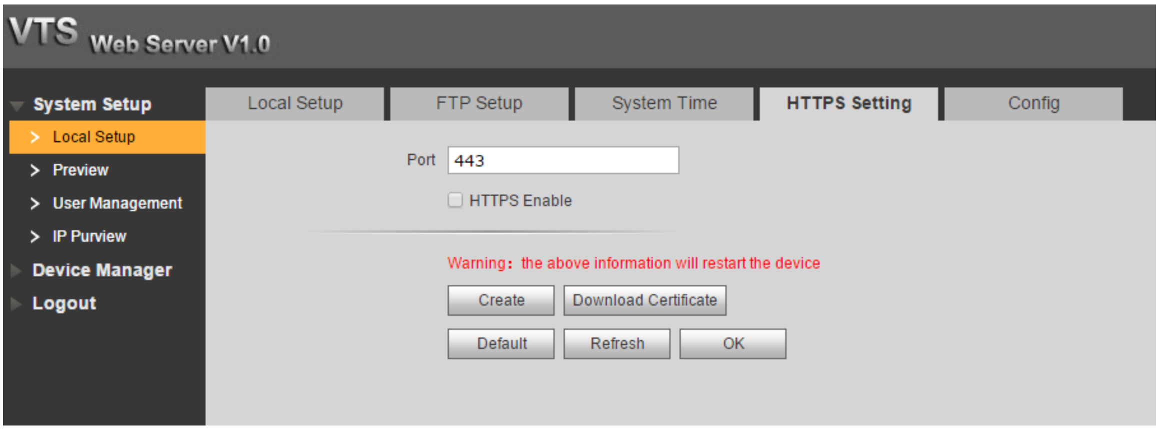
- Click **Default** to restore all the configuration of this tab to the default value.
- Click **Refresh** to display the current system configuration.

3.4.1.4 HTTPS Setting

Through creating server certificate or downloading root certificate, and setting port number, the PC can log in to the device by HTTPS to ensure the security of communication data and guard the users information and device security with stable technology measure.

Select **System Setup > Local Setup > HTTPS Setting**. See Figure 3-10.

Figure 3-10 HTTPS setting



Port 443

□ HTTPS Enable

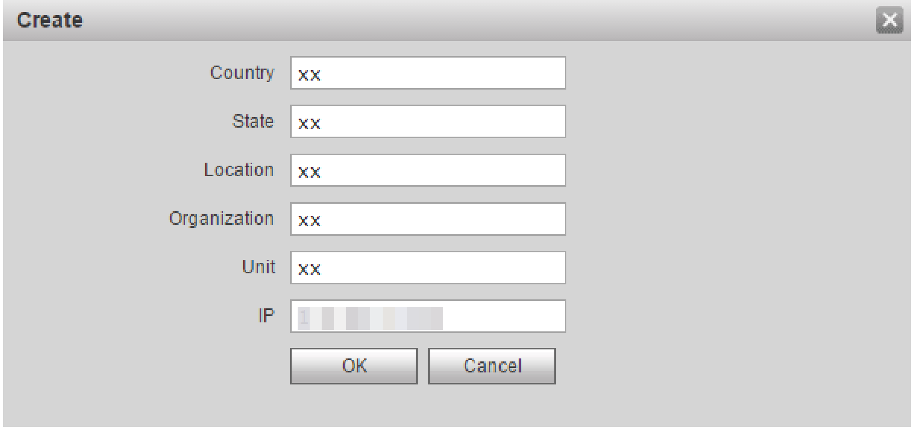
Warning：the above information will restart the device

- For the first time to use this function or after changing IP address of the device, you need to create server certificate again.
- For the first time to use HTTPS after changing the PC, you need to download root certificate again.

3.4.1.4.2 Create Server Certificate

Step 1 Click **Create Server Certificate**.

Figure 3-11 Create server certificate



Country xx

State xx

Location xx

Organization xx

Unit xx

IP

Step 2 Enter the required information and then click **OK**.

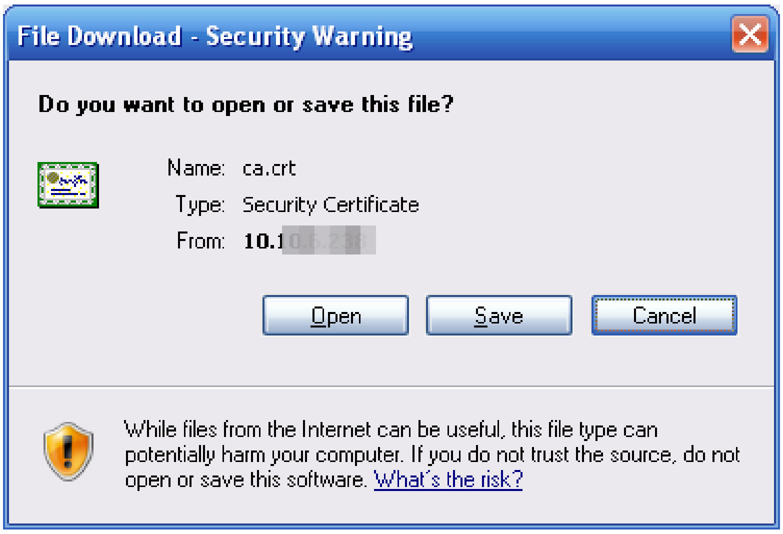
If the operation is correct, then the **Create successful** prompt is displayed.

The entered **IP or Domain name** must be the same as the IP or domain name of the device.

3.4.1.4.3 Download Root Certificate

Step 1 Click **Download Certificate**.

Figure 3-12 Download certificate file



Do you want to open or save this file?

Name: ca.crt

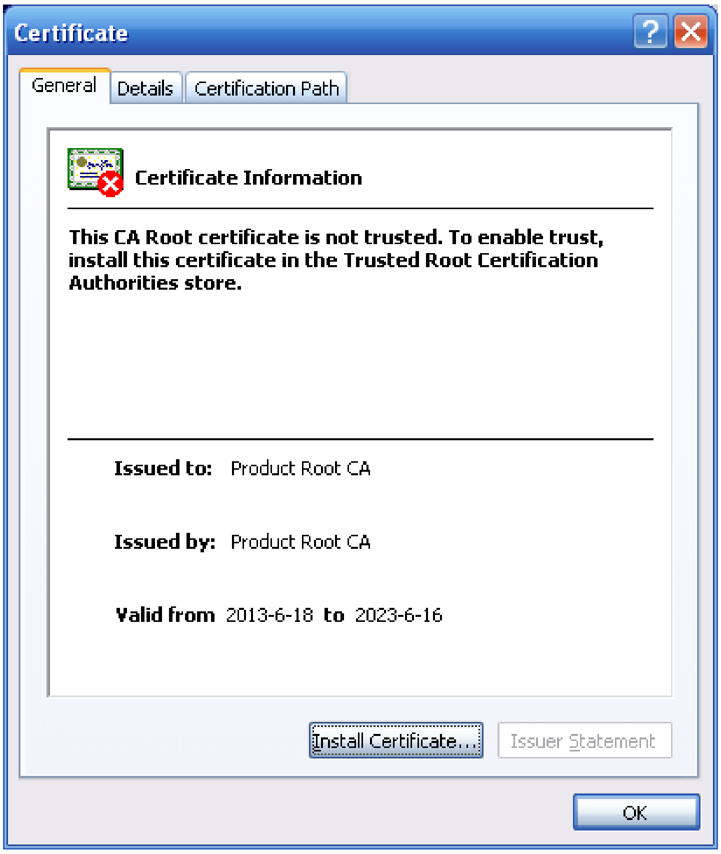
Type: Security Certificate

From: 10.1[redacted]

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Step 2 Click **Open**.

Figure 3-13 Certificate



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

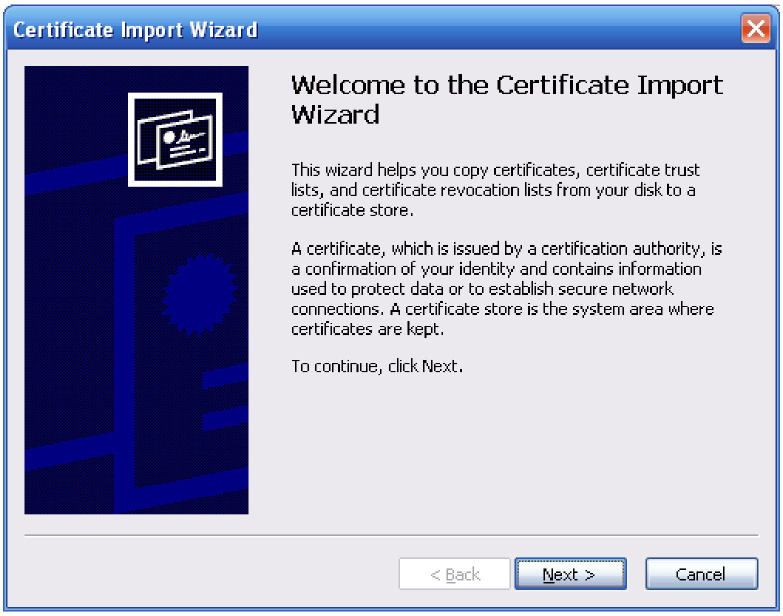
Issued to: Product Root CA

Issued by: Product Root CA

Valid from 2013-6-18 to 2023-6-16

Step 3 Click **Install certificate**.

Figure 3-14 Certificate import wizard



Certificate Import Wizard

Welcome to the Certificate Import Wizard

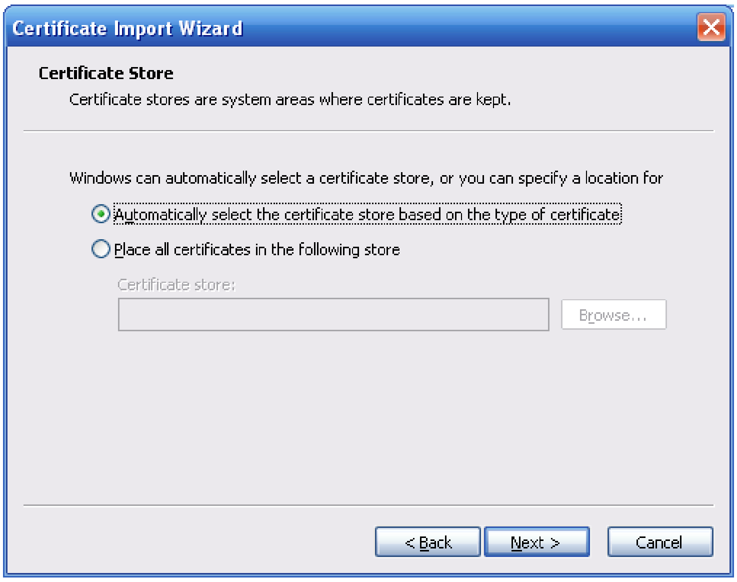
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Step 4 Click **Next**.

Figure 3-15 Certificate store



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

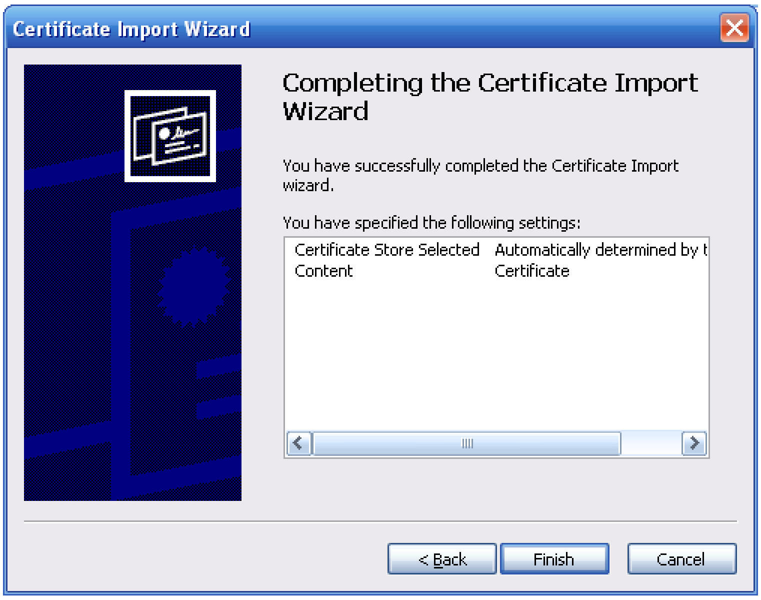
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Step 5 Select **Place all certificates in the following store**, and click **Next**.

Figure 3-16 Completing certificate import wizard



Completing the Certificate Import Wizard

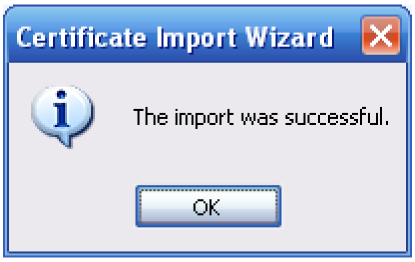
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

Step 6 Click **Finish** and a dialog box showing **The import was successful** pops up

Figure 3-17 Imported successfully.



The import was successful.

3.4.1.4.4 Set HTTPS Port

Enter the port number (the default one is 44, and select the **HTTPS Enable** check box, click OK to enable the HTTPS function.

3.4.1.4.5 Use HTTPS

Enter https://xx.xx.xx.xx:port in the browser bar, and the login interface the box.

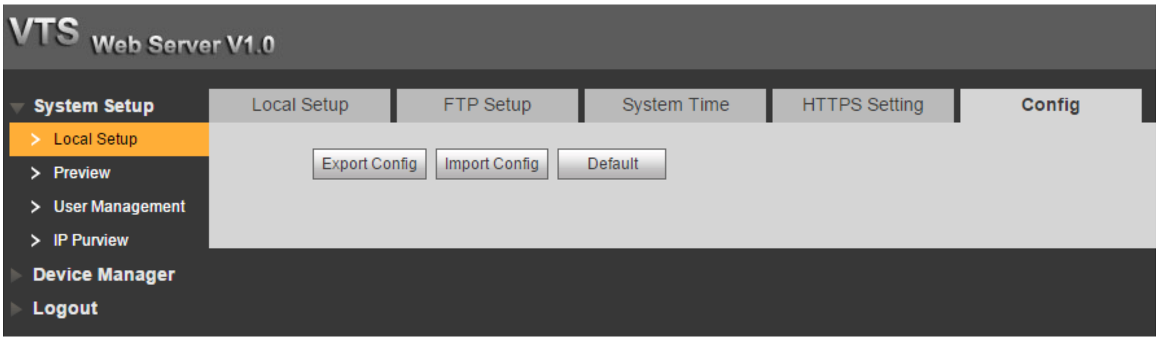
- xx.xx.xx.xx corresponds to your IP address or domain name.
- **Port** corresponds to your HTTPS port. If the default value is 443, you do not need to enter Port, and just enter https://xx.xx.xx.xx.

3.4.1.5 Configuration

Import and export the system configuration, or restore factory default.

Select **System Setup > Local Setup**, Click the **Local Setup** Tab.

Figure 3-18 Configuration



Export Configuration

Click **Export Config** to save the configuration to the PC.

Import Configuration

When you want to set several devices to the some configuration or restore the device to certain configuration, click **Import Config**, select the upload file, and then restart the device.

Default

Click **Default**, and then restart the device. The VTS will restart, and all the configuration except IP address will be to factory default.

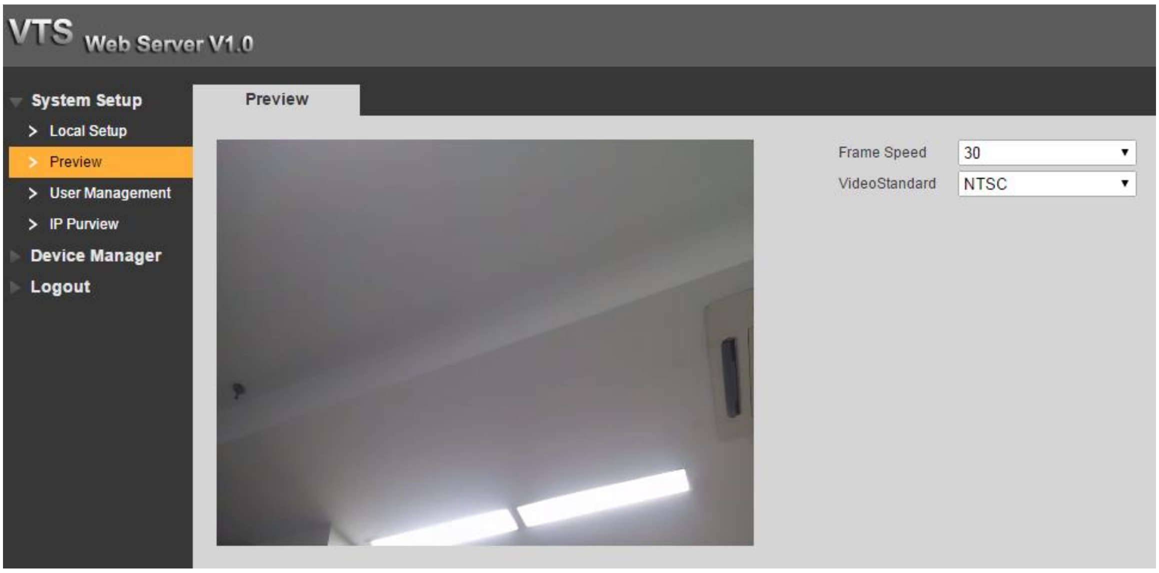
After default, password initialization will be required when you log in to the web interface.

3.4.2 Preview

Select **System Setup > Preview** to view the live video. See Figure 3-19.

Frame Speed indicates the frame number per second, which refers to the updating rate of the video stream. The bigger the value is, the higher the updating rate will be (Unit: fps).

Figure 3-19 Preview



Frame Speed 30

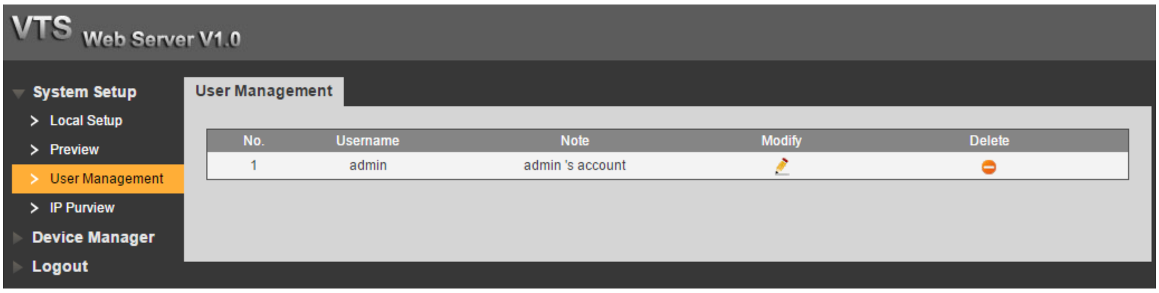
VideoStandard NTSC

3.4.3 User Management

You can delete, or modify web user information.

Select **System Setup > User Config**.

Figure 3-20 User management

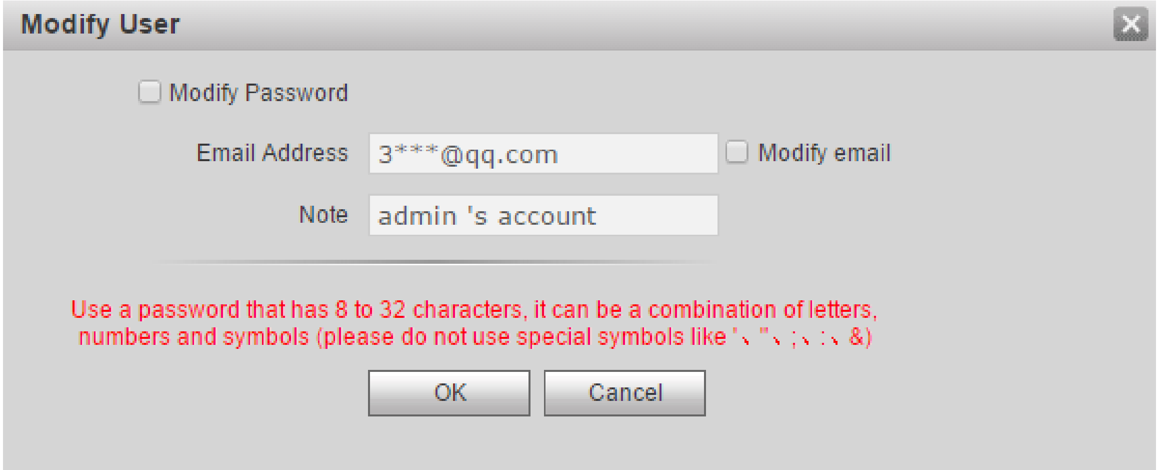


No.	Username	Note	Modify	Delete
1	admin	admin 's account	✎	⊖

3.4.3.1 Modify

Click ✎ in the admin information bar to modify the reserved email address.

Figure 3-21 Modify the reserved email address



□ Modify Password

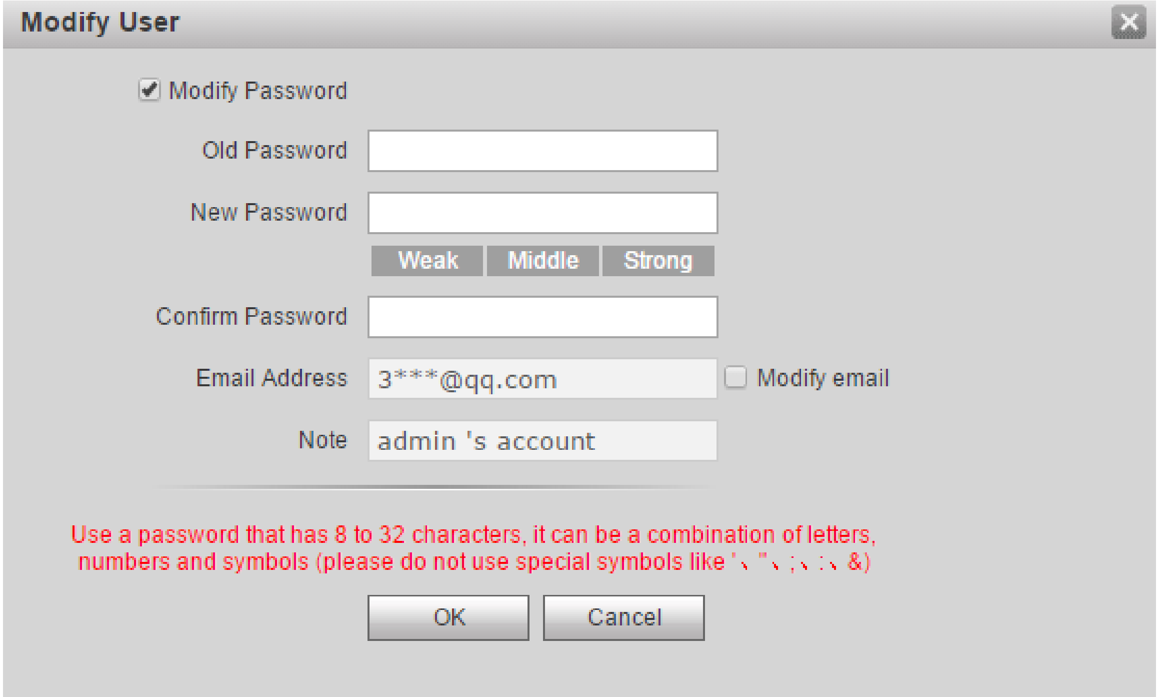
Email Address: 3***@qq.com □ Modify email

Note: admin 's account

Use a password that has 8 to 32 characters, it can be a combination of letters, numbers and symbols (please do not use special symbols like '、"、;、:、&)

If you need to modify the password, select the **Modify Password** check box. Enter old password, new password, confirm password, and then click **OK**.

Figure 3-22 Modify password(1)



Modify User

☑ Modify Password

Old Password

New Password

Confirm Password

Email Address: 3***@qq.com ☐ Modify email

Note: admin 's account

Use a password that has 8 to 32 characters, it can be a combination of letters, numbers and symbols (please do not use special symbols like '、"、;、:、&)

3.4.3.2 Delete User

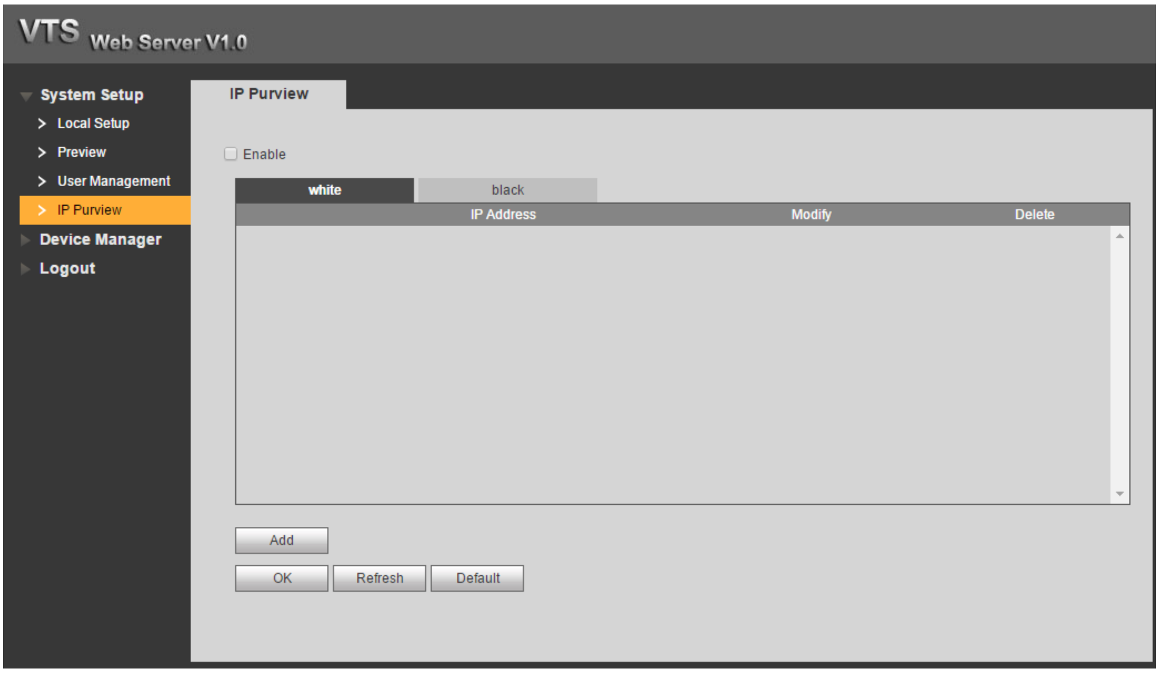
Click ⛔ in the user information bar to delete a certain user.

3.4.4 IP Purview

To enhance network and data security, you need to configure access authority of IP hosts (IP hosts refer to the PCs with IP address or the servers with IP address). When the IP address of the IP host in the white list, you can access the host; when the IP address of the IP host in the black list, you can not access the host.

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

Figure 3-23 IP Purview



Step 2 Select **Enable**.

The system displays **White** check box and **Black** check box.

- Select the **White** check box, and click **White** tab to add devices to the white List.

1) Click **Add,** and then the **Add** dialog box is displayed. Configure the IP address, see Table 3-3.

   The system supports 64 IP addresses at most.

Table 3-3 IP address parameters description

Parameter	Description
IP Address	Enter the IPv4 IP address, such as 192.168.1.120.
IP Segment	Input the start IP and end IP of the target IP segment.

2) Click **OK**.

   Log in the web interface with the IP hosts in the white list. Login to the device successfully.

- Select the **Black** check box, and click **Black** tab to add devices to the **black** List.

1) Configure the IP address, see Table 3-3.
2) Click **OK**.

   Log in the web interface with the IP hosts in the black list. System prompts login failed.

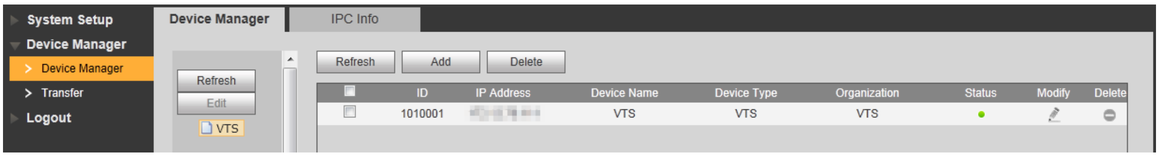
3.5 Device Management

3.5.1 Device Manager

3.5.1.1 Device Manager

- When the device role is bottom VTS, it can add VTT (Video Intercom terminal) and VTA (Emergency phone terminal)
- When the device role is bottom VTS, it can add bottom VTS.

Select **Device Manager > Device Manager**, and click the **Device Manager** tab. Device manager



□	ID	IP Address	Device Name	Device Type	Organization	Status	Modify	Delete
□	1010001	[redacted]	VTS	VTS	VTS	●	✎	⊖

3.5.1.1.1 Adding Device

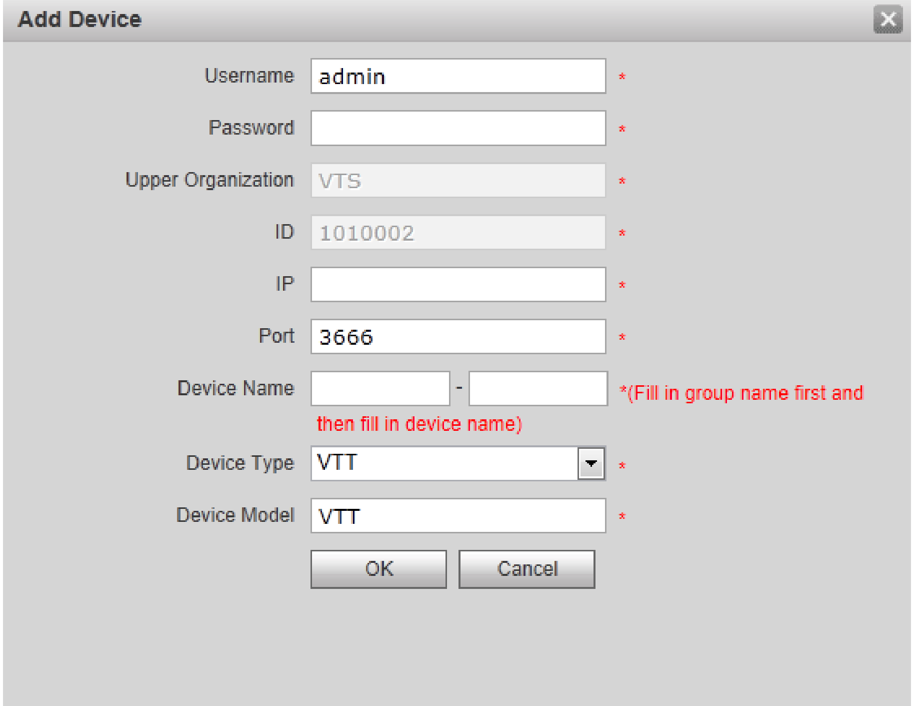
- Bottom VTS

  Click VTS node on left side of the interface, and then click **Add**. See Figure 3-24. Enter the device information of added VTT and VTA, and then click **OK**.

    - **Device Name** is "group name + device name", and it will be displayed in the device tree on the left side of the interface.

  - Make sure that the device model is correct; otherwise the device adding will fail.

Figure 3-24 Add VTT/VTA



Username	admin *
Password	*
Upper Organization	VTS *
ID	1010002 *
IP	*
Port	3666 *
Device Name	- *(Fill in group name first and then fill in device name)
Device Type	VTT *
Device Model	VTT *

- Upper VTS

Click **Edit**. See Figure 3-25. Hover over the device name, and the adding and deleting icons will be displayed. Click ⊕, see Figure 3-26. Enter IP address, username and password, and then click **OK**.

After adding the device, click **Refresh** to display the VTT or VTA information on the interface.

Figure 3-25 Adding VTS

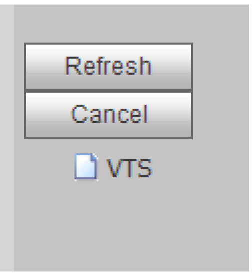
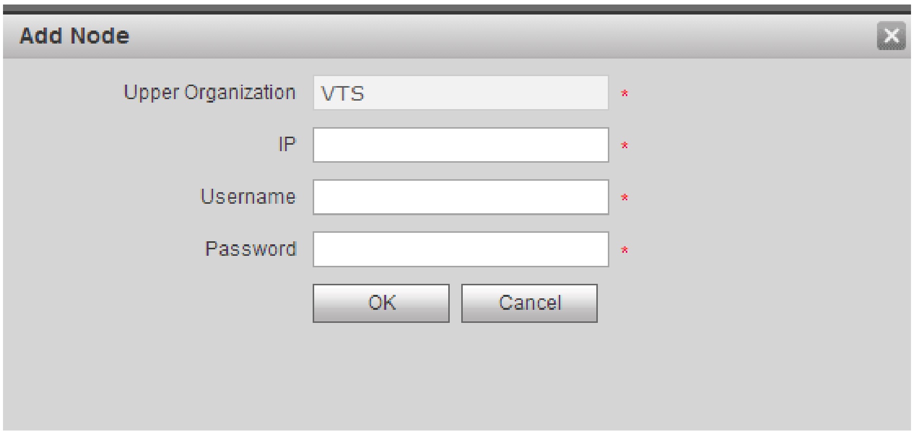


Figure 3-26 Add node


Add Node

Upper Organization: VTS *

IP: *

Username: *

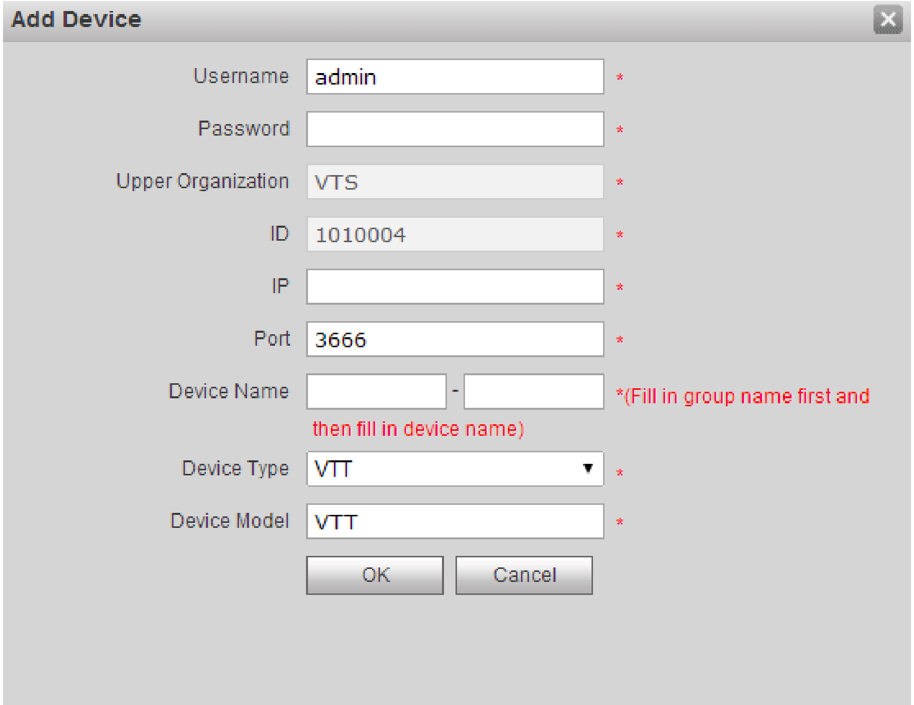
Password: *

3.5.1.1.2 Modifying Device

You can only modify VTT or VTA information.

Click ✎ next to the VTT or VTA information, see Figure 3-27. You can modify username, password, IP address, port, device name, device type and device model.

Figure 3-27 Add device (VTT/VTA)



Add Device

Username	admin	*
Password		*
Upper Organization	VTS	*
ID	1010004	*
IP		*
Port	3666	*
Device Name	-	*(Fill in group name first and then fill in device name)
Device Type	VTT ▾	*
Device Model	VTT	*

3.5.1.1.3 Deleting Device

- Delete VTS

  Click **Edit**, Hover over the device name, and the add and delete icons will be displayed. Click ✖ to delete it.

  Root node cannot be deleted.

- Delete device (VTT or VTA)

  Click ⛔ in the device information bar to delete a device.

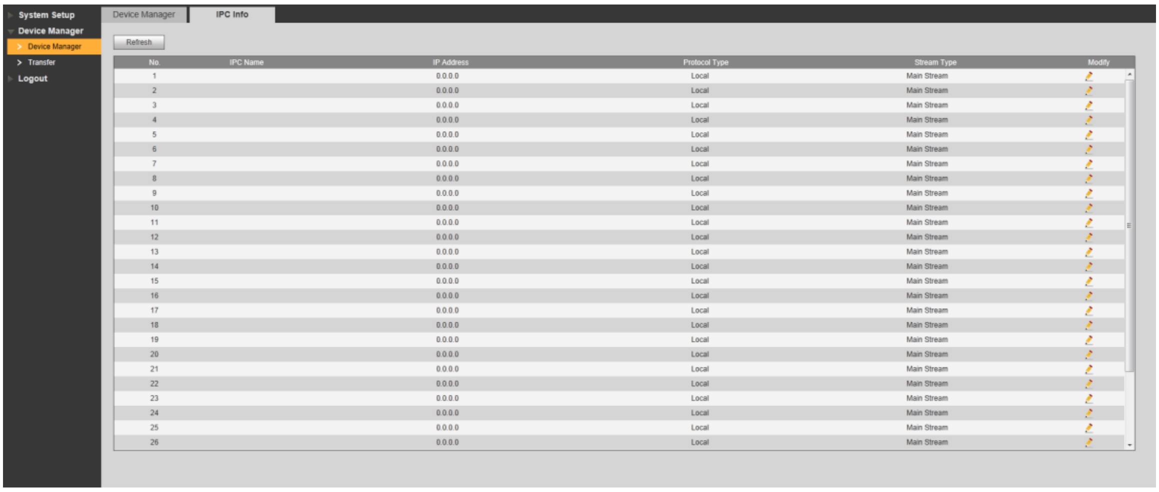
3.5.1.2 IPC Information

Add IPC to do monitoring. And you can add 32 IPCs at most.

Step 1 Select Device **Manager > Device Manager**, and select the **IPC Info** tab.

The **IPC Info** interface is displayed.

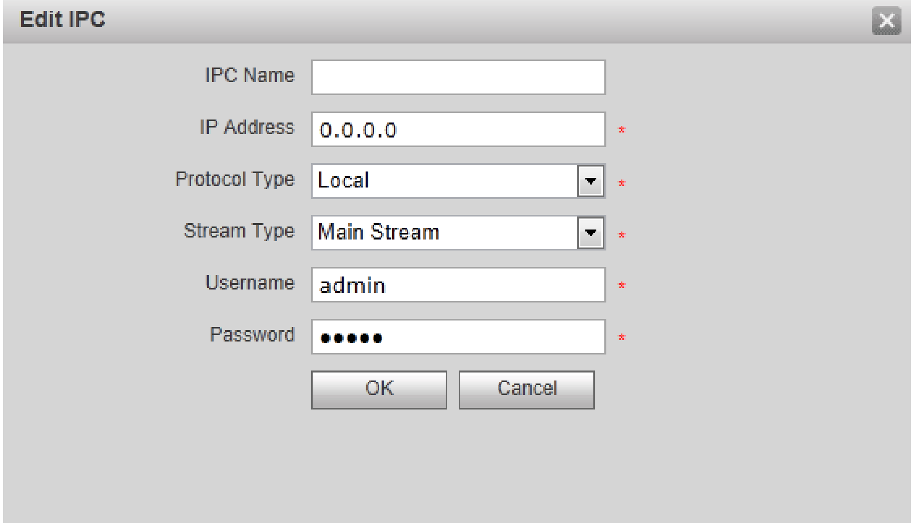
Figure 3-28 IPC Information



No.	IPC Name	IP Address	Protocol Type	Stream Type	Modify
1		0.0.0.0	Local	Main Stream	✎
2		0.0.0.0	Local	Main Stream	✎
3		0.0.0.0	Local	Main Stream	✎
4		0.0.0.0	Local	Main Stream	✎
5		0.0.0.0	Local	Main Stream	✎
6		0.0.0.0	Local	Main Stream	✎
7		0.0.0.0	Local	Main Stream	✎
8		0.0.0.0	Local	Main Stream	✎
9		0.0.0.0	Local	Main Stream	✎
10		0.0.0.0	Local	Main Stream	✎
11		0.0.0.0	Local	Main Stream	✎
12		0.0.0.0	Local	Main Stream	✎
13		0.0.0.0	Local	Main Stream	✎
14		0.0.0.0	Local	Main Stream	✎
15		0.0.0.0	Local	Main Stream	✎
16		0.0.0.0	Local	Main Stream	✎
17		0.0.0.0	Local	Main Stream	✎
18		0.0.0.0	Local	Main Stream	✎
19		0.0.0.0	Local	Main Stream	✎
20		0.0.0.0	Local	Main Stream	✎
21		0.0.0.0	Local	Main Stream	✎
22		0.0.0.0	Local	Main Stream	✎
23		0.0.0.0	Local	Main Stream	✎
24		0.0.0.0	Local	Main Stream	✎
25		0.0.0.0	Local	Main Stream	✎
26		0.0.0.0	Local	Main Stream	✎

Step 2 Click ✎.

Figure 3-29 Add IP



IPC Name:
IP Address: 0.0.0.0 *
Protocol Type: Local *
Stream Type: Main Stream *
Username: admin *
Password: ●●●●● *

Step 3 For details, see Table 3-4.

Table 3-4 IPC parameter description

Parameter	Description
IPC Name	Enter the IPC name.
IP Address	Enter the IP address IPC does device.
Protocol	Includes Local and ONVIF.
Stream Type	Includes **Main Stream** and **Sub Stream**
Username	Enter the user name/password of the device you need.
Password	

Step 4 Click **OK** to finish configuration.

3.5.2 Call Transfer

Configure the calling transfer and receiving of VTS.

For example, you want to transfer the calling of Device 1 to Device 2. Configure forwarding on Device 1, and receiving on Device 2,

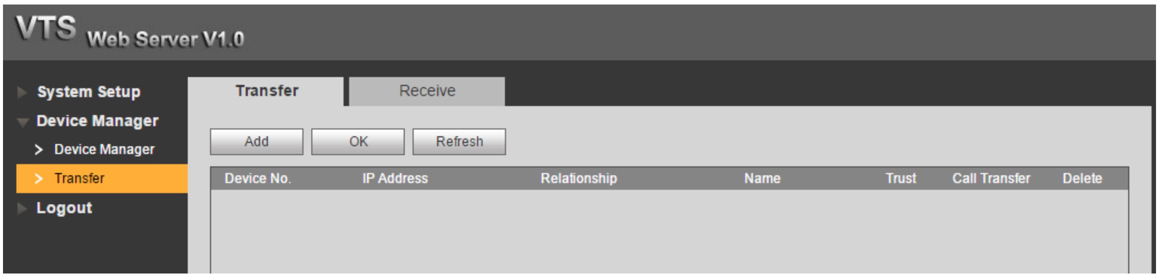
3.5.2.1 Transfer

If you configure calling transfer, when there is calling, the system will transfer the calling to the configured VTS.

When you configure calling transfer on the VTS, you need to configure receiving on the other VTS.

Select **Device Manager > Transfer**, Click the **Transfer** tab. See Figure 3-30.

Figure 3-30 Transfer



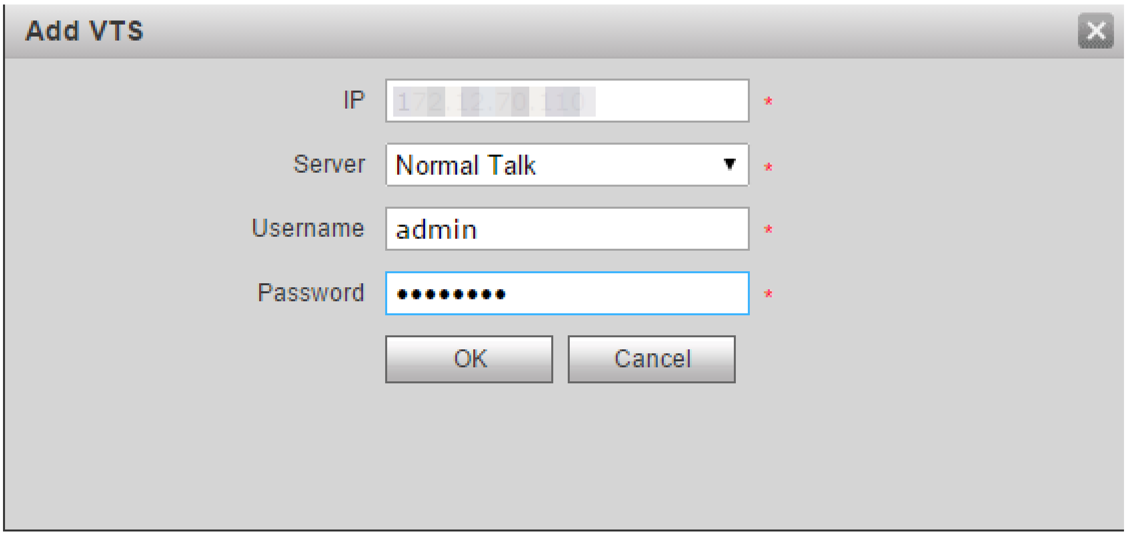
3.5.2.1.1 Adding VTS

Click **Add**. See Figure 3-31. Enter the IP address, username, password, select the server, and then click **OK**.

You can select the server from **Normal Talk**, **Trust,** and **Call Transfer**.

- **Normal Talk**: When there is a call, you can answer the call and talk normally.
- **Trust**: Transfer the call to other VTS.
- **Call Transfer**: When the VTS is busy or nobody answers the call, the call will be transferred to other VTS.

Figure 3-31 Adding VTS



IP: [redacted] *

Server: Normal Talk ▼ *

Username: admin *

Password: •••••••• *

3.5.2.1.2 Deleting VTS

Click ⛔ in the device information bar to delete a certain device.

3.5.2.1.3 TrustING VTS

Click **Trust** to enable the **Trust** function.

3.5.2.1.4 Call Transfer

Click **Call Transfer** to enable the **Call Transfer** function.

📖

You cannot enable **Trust** and **Call Transfer** at the same time.

3.5.2.2 Receive

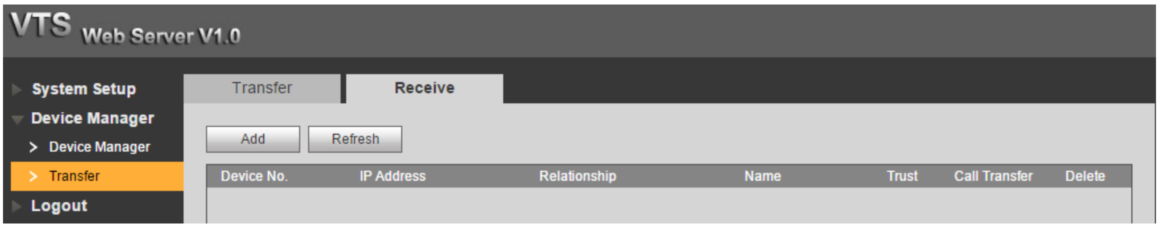
After configuring Receive on the VTS, the VTS will receive the call transferred from other VTS.

⚠

When you configure **Receive** on the VTS, you need to configure Transfer on the other VTS.

Select **Device Manager > Transfer**, and click the **Receive** tab.

Figure 3-32 Receive

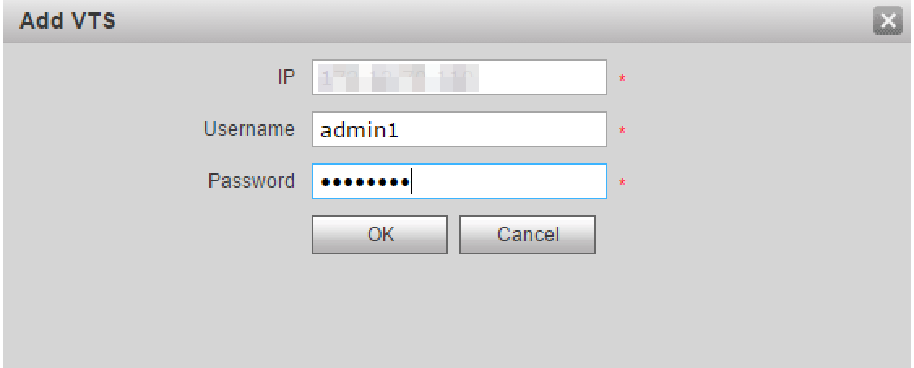


Device No.	IP Address	Relationship	Name	Trust	Call Transfer	Delete

3.5.2.2.1 Adding VTS

Click **Add**. See Figure 3-33. Enter the IP address, username, password, select the server of the VTS that you want to add, and then click **OK**.

Figure 3-33 Adding VTS



IP [redacted] *

Username admin1 *

Password •••••••• *

3.5.2.2.2 Deleting VTS

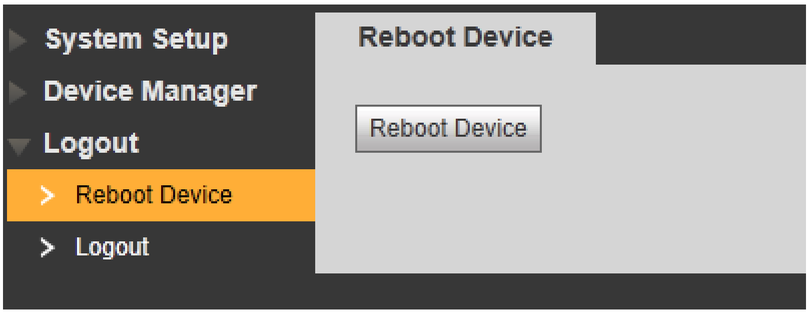
Click ⛔ in the DEVICE information bar to delete a certain device.

3.6 Logout

3.6.1 Reboot

Step 1 Select **Logout > Reboot Device**.

Figure 3-34 Reboot device

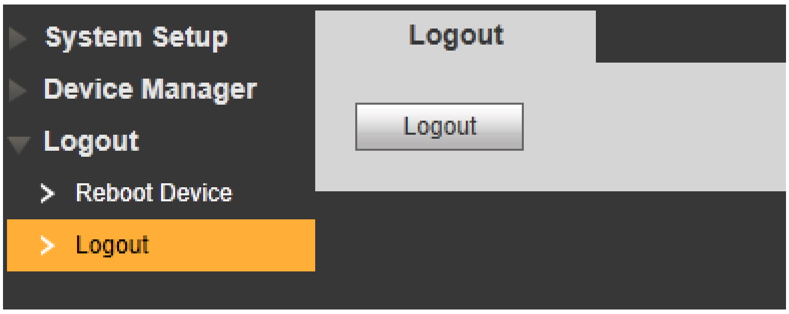


Step 2 Click **Reboot Device** to restart the device.

3.6.2 Logout

Step 1 Select **Logout > Logout**.

Figure 3-35 Logout



Step 2 Click **Logout**.

The login interface is displayed.

4 VTS Operation

⚠

Before operating the VTS, make sure that the cable connection is correct. For details, see “2.1Important Note”

4.1 Standby Interface

After power on, the standby interface is displayed. See Figure 4-1. Tap anywhere to go to the homepage. See Figure 4-2.

Figure 4-1 Standby interface

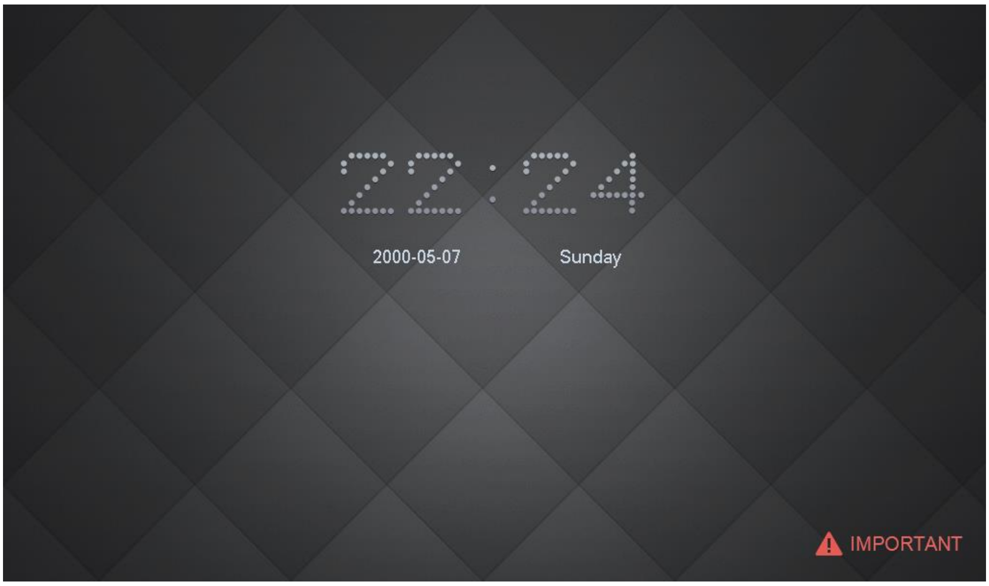
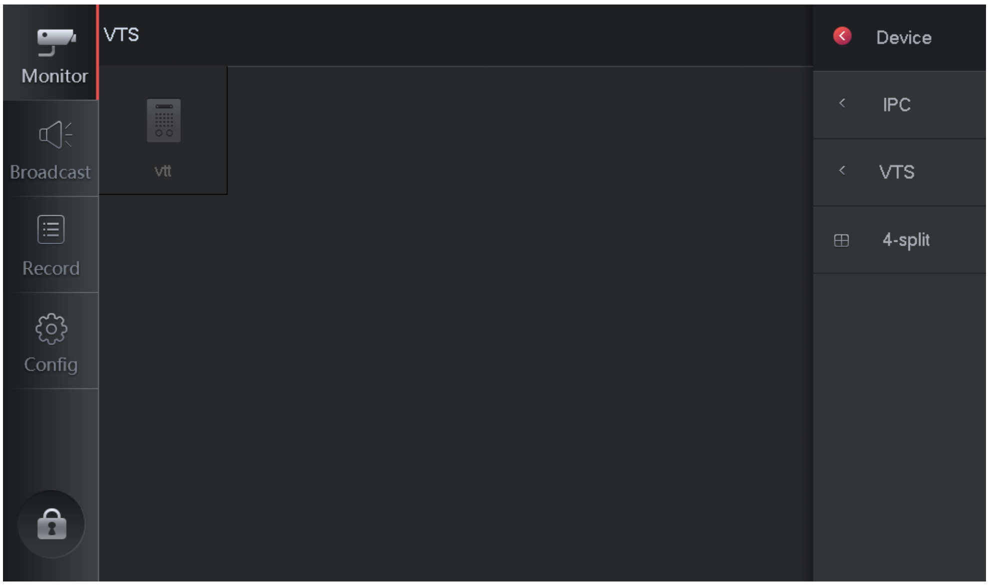


Figure 4-2 Homepage

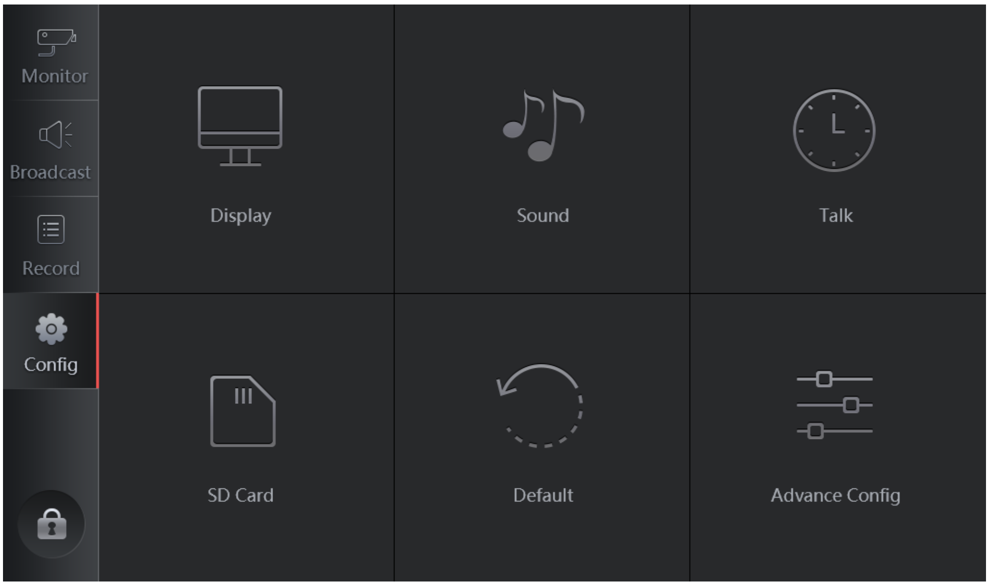


Tap 🔒 , and the system enters the screen saver mode, tap anywhere to cancel the screen saver mode.

4.2 Configuration

Tap **Config** on the homepage to configure display, sound, talk, SD card, default and advance configuration.

Figure 4-3 Configuration interface



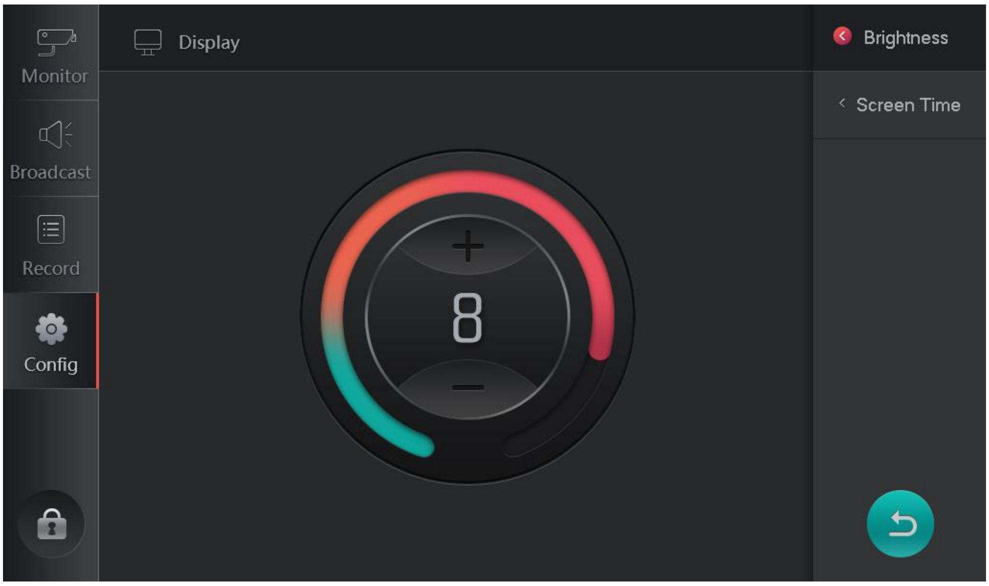
4.2.1 Configuring Display

4.2.1.1 Brightness

Set the brightness of the touch screen

Step 1 Select **Config > Display > Brightness**.

Figure 4-4 Brightness



Step 2 Tap + or – to adjust the brightness.

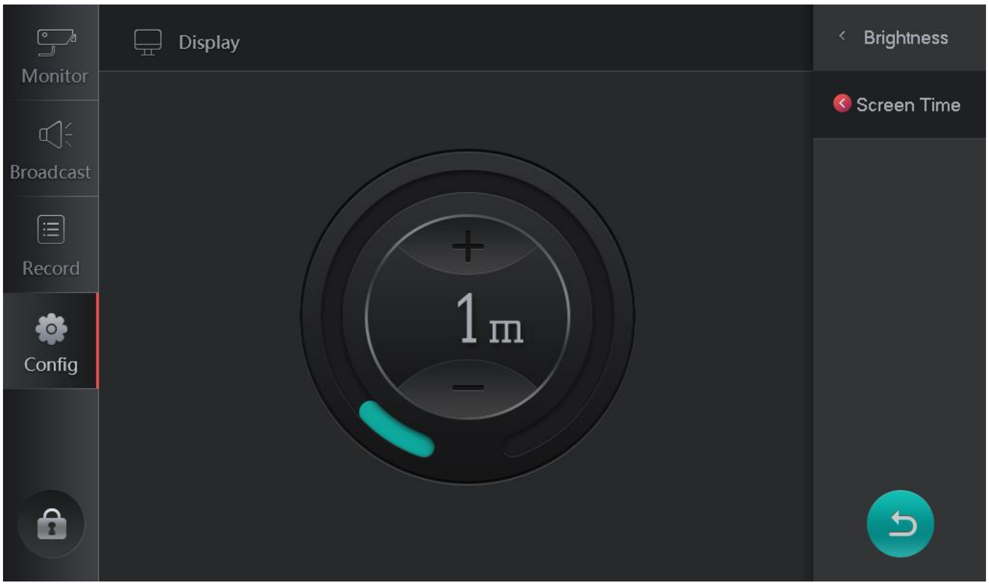
Tap ↶ to go back to the **Config** interface.

4.2.1.2 Screen Time

The system will enter screen saver mode after the configured period.

Step 1 Select **Config > Display > Screen Time**.

Figure 4-5 Screen time



Step 2 Tap + or – to adjust the time, and the unit is minute.

Tap ↶ to go back to the **Config** interface.

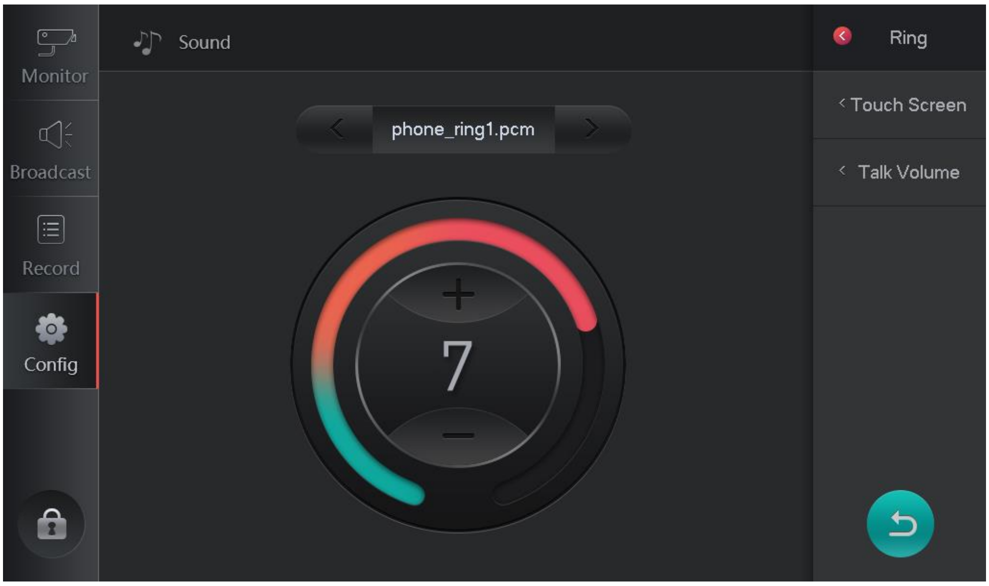
4.2.2 Configuring Sound

4.2.2.1 Ring

You can set the ring tones and volume as needed.

Step 1 Select **Config > Sound > Ring**.

Figure 4-6 Ring



Step 2 Tap the arrow keys (< or >) to select the ring tones.

Step 3 Tap + or – to adjust the volume of the ring.

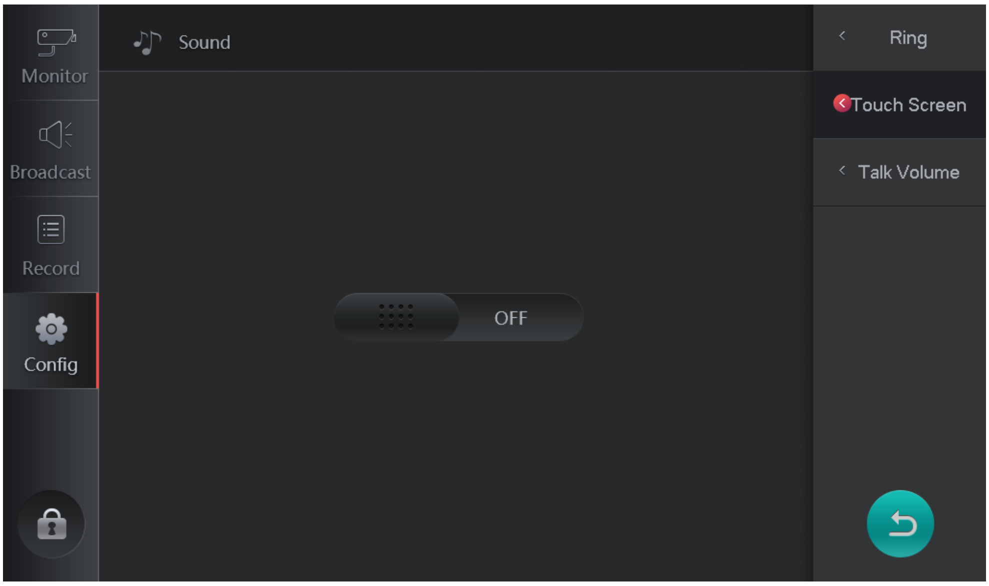
Tap ↩ to go back to the **Config** interface.

4.2.2.2 Touch Screen

Select **Config > Sound > Touch Screen**. See Figure 4-7. Tap ▬ to enable or disable the touch sound as needed.

Tap ↩ to go back to the **Config** interface.

Figure 4-7 Touch screen

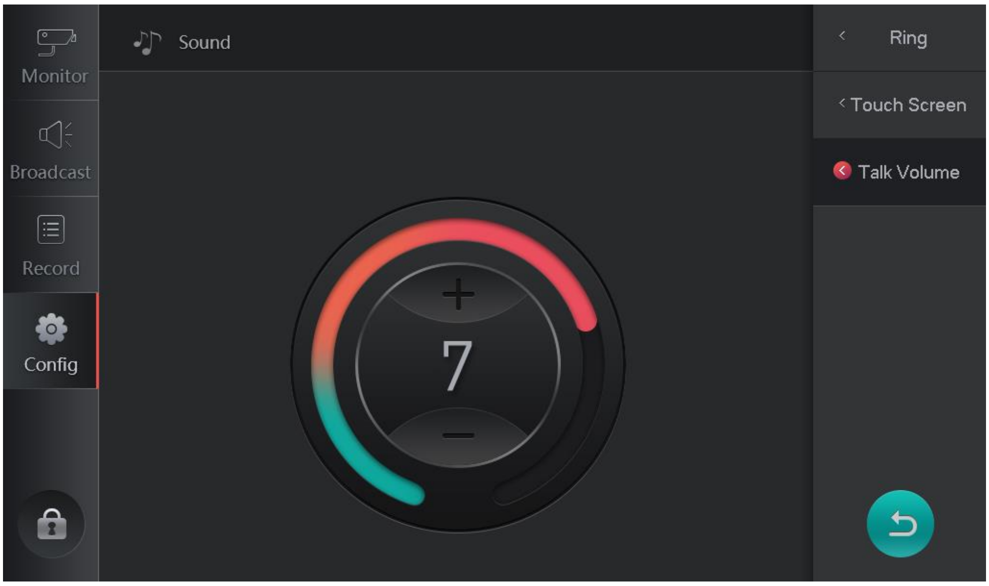


4.2.2.3 Talk Volume

Select **Config > Sound > Talk Volume**. See Figure 4-8. Tap + or – to adjust the volume during talking.

Tap ↩ to go back to the **Config** interface.

Figure 4-8 Talk volume

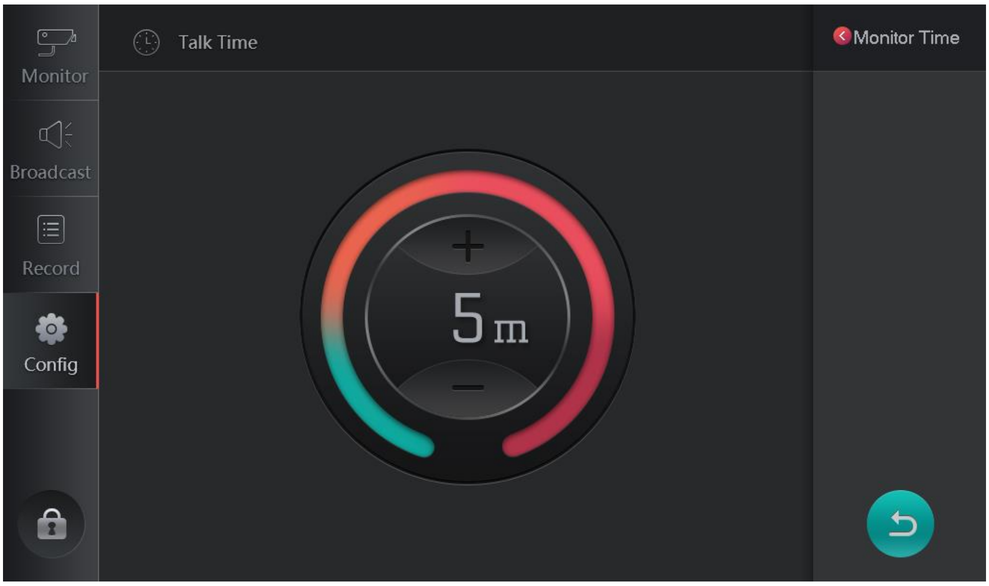


4.2.3 Configuring Talk

Select **Config > Talk**. The **Talk** interface is displayed. See Figure 4-9. Tap + or – to adjust the monitor time.

Tap ↩ to go back to the **Config** interface.

Figure 4-9 Monitor time

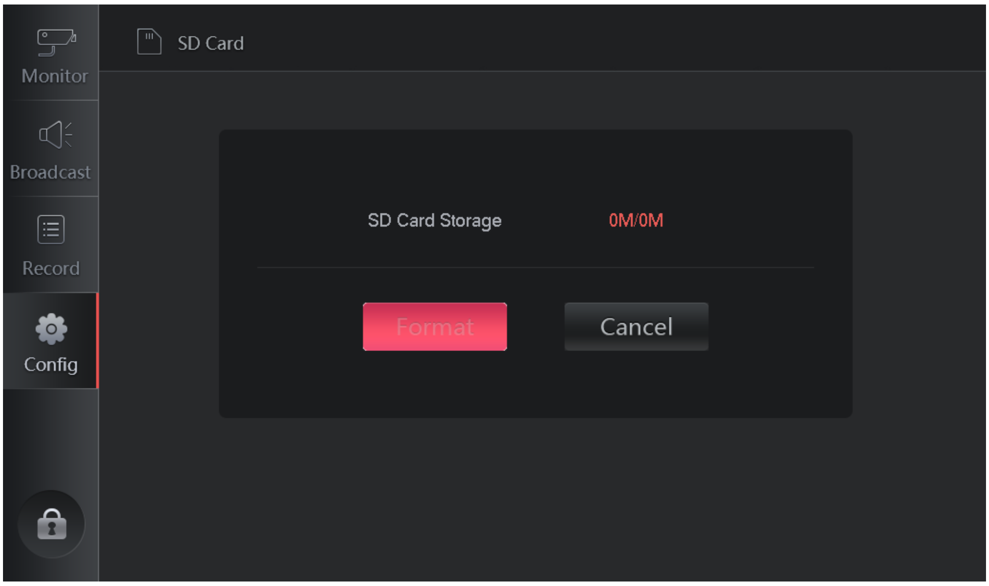


4.2.4 SD Card

Select **Config > SD Card**. The **SD Card** interface is displayed. See Figure 4-10. Tap **Format**, to format the SD card.

Tap **Cancel** to go back to the **Config** interface.

Figure 4-10 SD Card



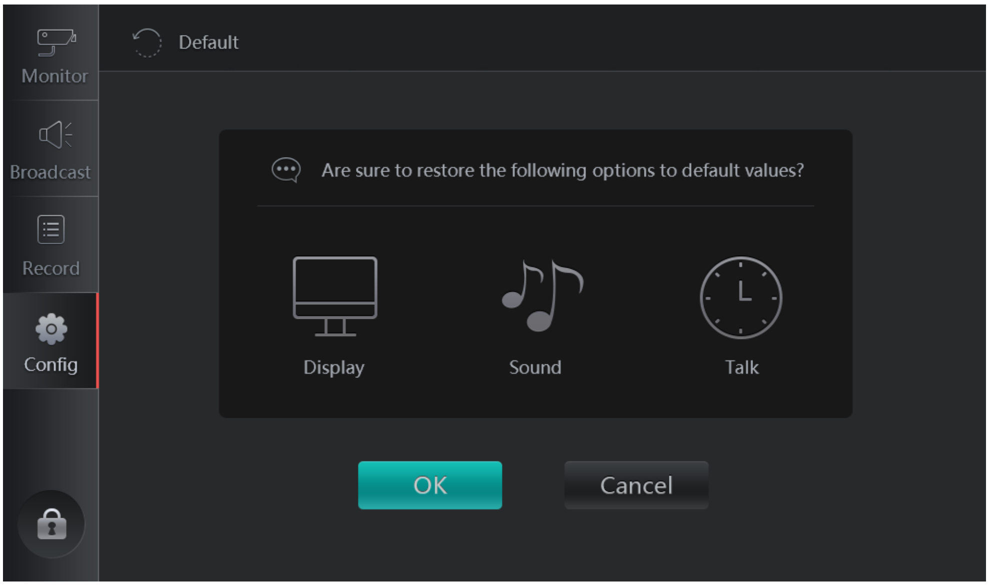
SD Card Storage 0M/0M

4.2.5 Default

Select **Config > Default**. The **Default** interface is displayed. See Figure 4-11. Tap **OK** to restore the display, sound and talk configuration to default value.

Tap **Cancel** to go back to the **Config** interface.

Figure 4-11 Default



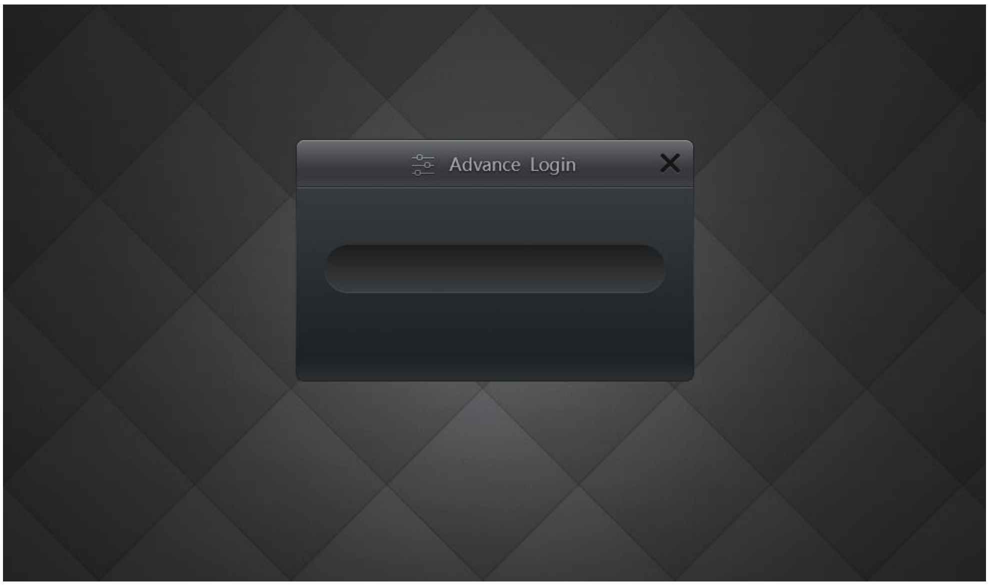
Are sure to restore the following options to default values?

4.2.6 Advanced Config

Set the device number and IP address. You can restore the number to the default value.

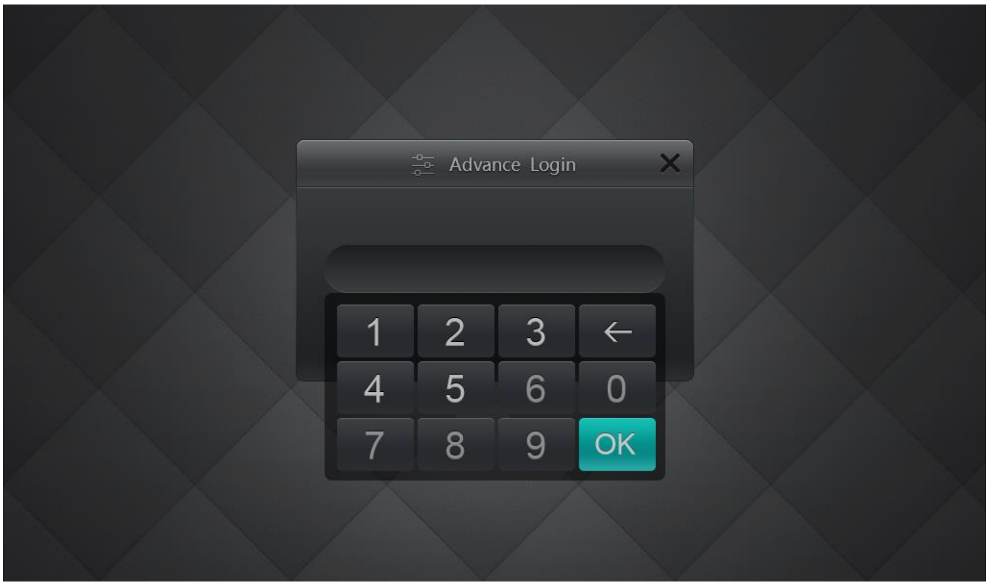
Step 1 Select **Config > Advanced Config**.

Figure 4-12 Advanced login



Step 2 Enter the password.

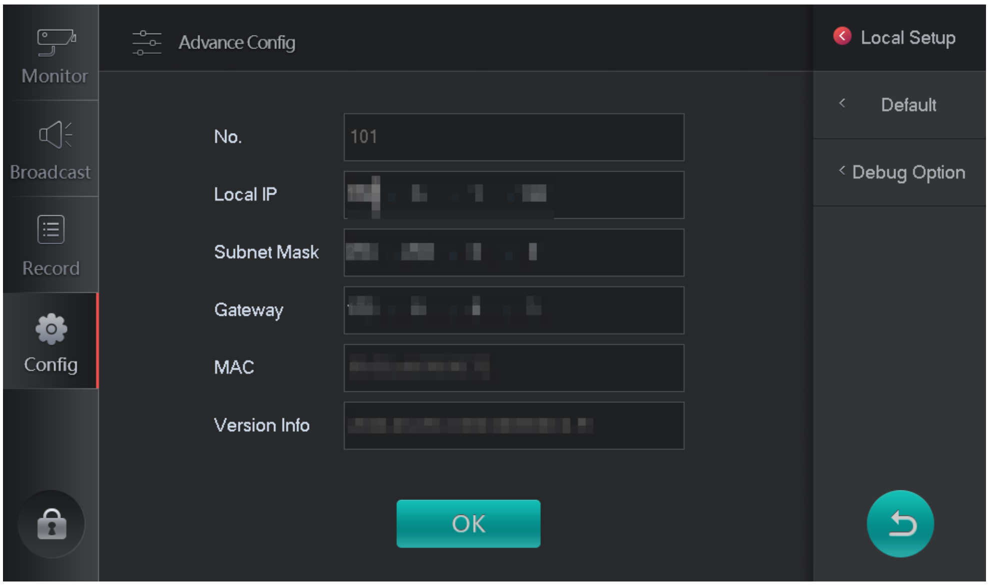
Figure 4-13 Entering password



Step 3 Tap **OK**.

The login password is 888888 by default, and it cannot be modified.

Figure 4-14 Local setup



No. 101

Local IP [redacted]

Subnet Mask [redacted]

Gateway [redacted]

MAC [redacted]

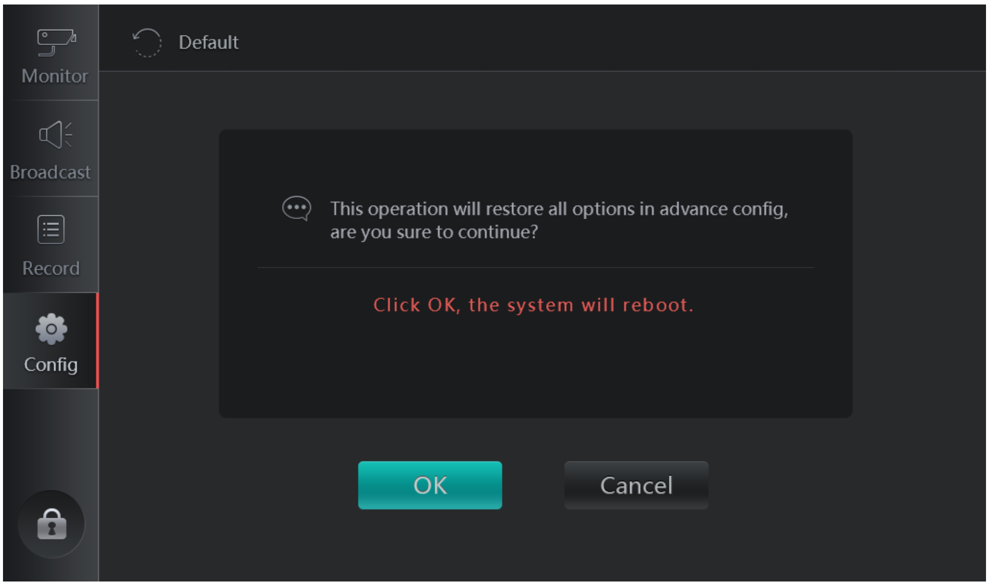
Version Info [redacted]

4.2.6.1 Default

Select **Config > Advanced Config > Default**. The **Default** interface is displayed. See Figure 4-15. Tap **OK** to restore all options except the IP address in advance configuration to the default value, and the device will restart.

After restoring the device, password initialization will be required when you log in to the web interface.

Figure 4-15 Default



This operation will restore all options in advance config, are you sure to continue?

Click OK, the system will reboot.

4.2.6.2 Local Setup

You can modify VTS number, local IP address, subnet mask, and gateway; and view the MAC address and version information. See Figure 4-14.

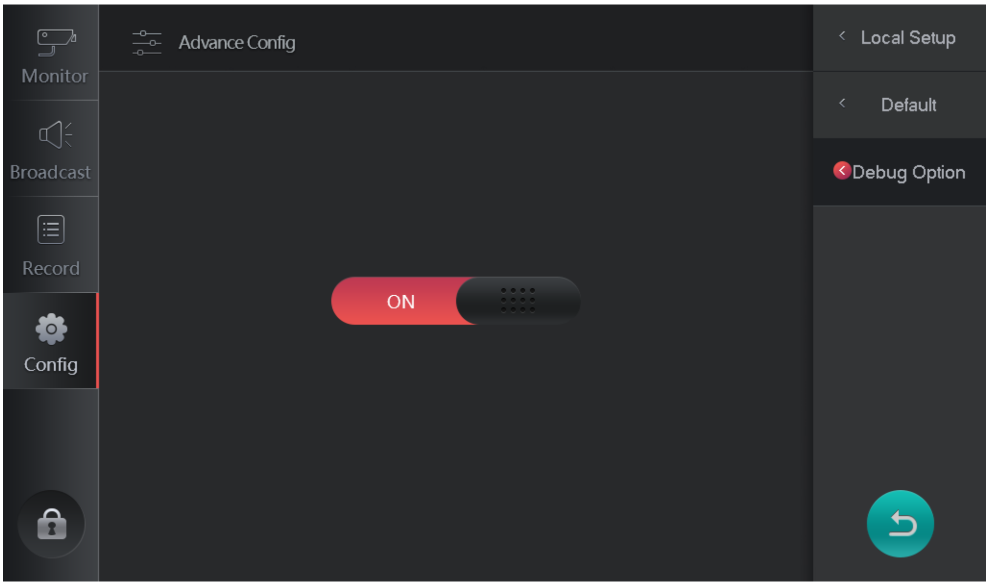
Enter the number according to the actual situation, and tap **OK**.

4.2.6.3 Debug Option

Select **Config > Advanced Config > Debug Option**. The **Debug Option** interface is displayed. See Figure 4-16. Tap to enable or disable the SSH debug function.

If you have enabled the SSH function on the web interface, the function is enabled in this interface. For details, see "3.4.1.1Local Setup."

Figure 4-16 Debug Option



4.3 Monitor

The VTS can monitor the terminals including VTT, VTA, and IPC, and talk with the VTS in the network.

📖

Before monitoring, add the corresponding terminals and IPC. For the detailed operation of adding terminals, see "3.5.1.1.1 Adding Device"; for the detailed operation of adding IPC, see "3.5.1.2 IPC Information."

4.3.1 Device

You can do operations on the added devices (VTT and VTA) such as monitor, switch, call, record, and snapshot.

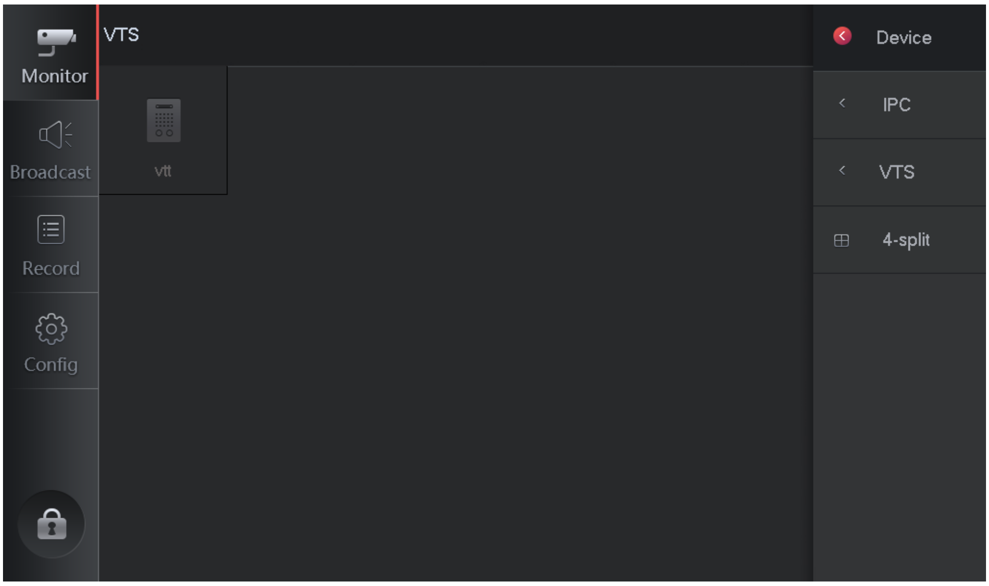
This section takes VTT as an example.

Step 1 Select **Monitor > Device**.

📖

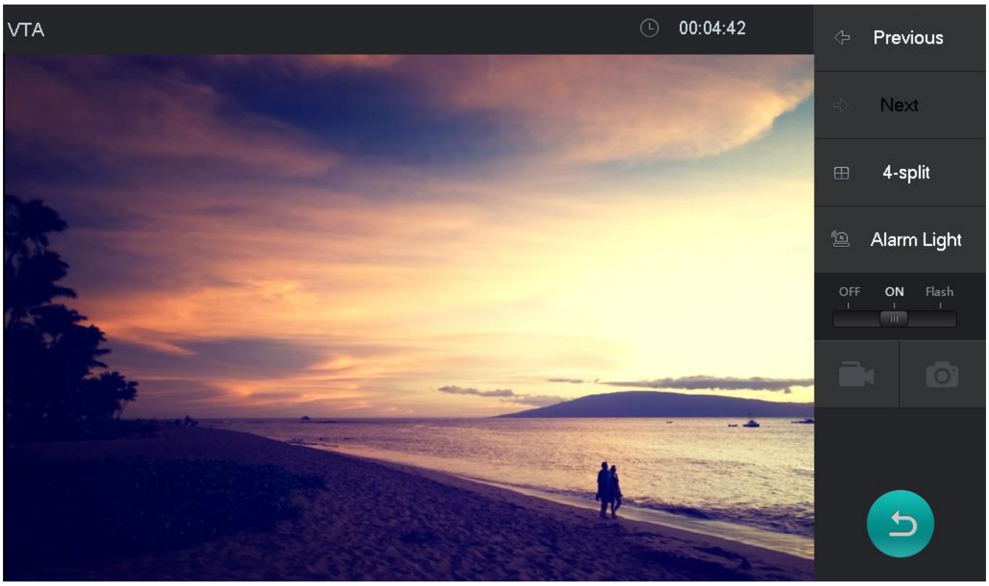
When the icon is highlighted, you can monitor the device.

Figure 4-17 Device



Step 2 Tap the VTT icon.

Figure 4-18 Monitoring

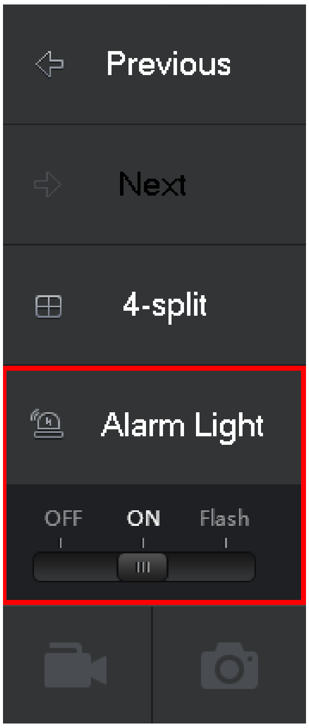


Step 3 Do the operation as the description of Table 4-1.

Table 4-1 Monitor description

Icon/Parameter	Description	
Previous	When the VTS connects to several devices, tap **Previous** or **Next** to switch the monitoring image.	
Next		
Split	Tap **Split**, and the 4-split interface is displayed. For details, see "4.3.4 4-split."	
Alarm light	The function is available on VTA. 1. Tap **Alarm Light**, and the interface shown in Figure 4-19 is displayed. 2. Tap the **OFF, ON** or **Flash** button to make the alarm light of VTS in the corresponding status.	
👂	Tap 👂, you can hear the sound from the device which is calling, and the icon changes to 👂; tap 👂 again to stop monitor.	
📢	Tap 📢, you can talk with the device which is calling, and the icon changes to 📢; tap 📢 to stop the call.	
🎥	Tap 🎥 to start recording video, and the icon changes to ■; tap ■ again to stop the recording video.	📖 ● When there is no SD card in the VTS, the icon is gray. ● The snapshot and recorded videos are stored in the SD card.
📷	Tap 📷 to capture pictures.	

Figure 4-19 Alarm light operation.

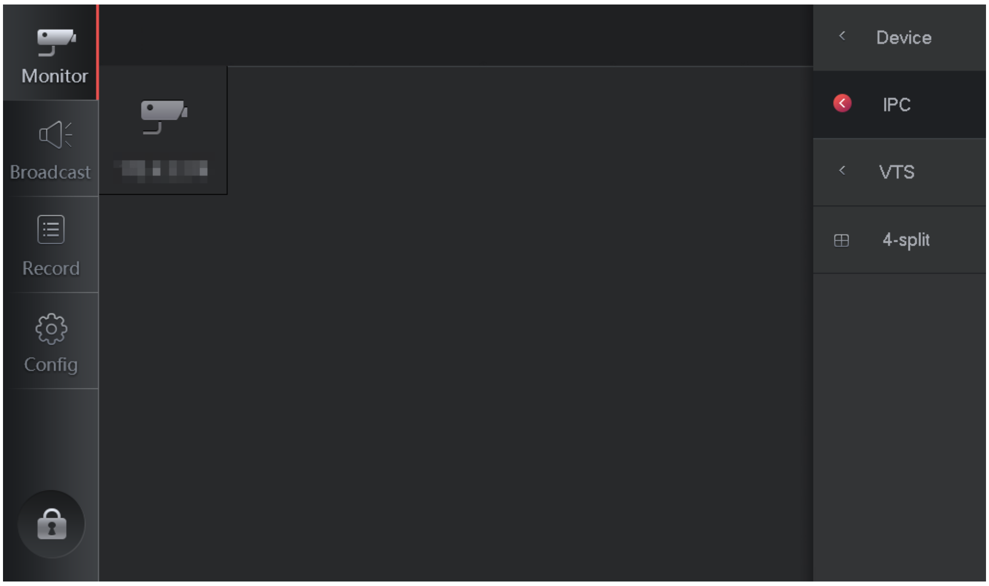


4.3.2 IPC

You can do operations on the added IPC such as monitor, switch, call, record, and snapshot.

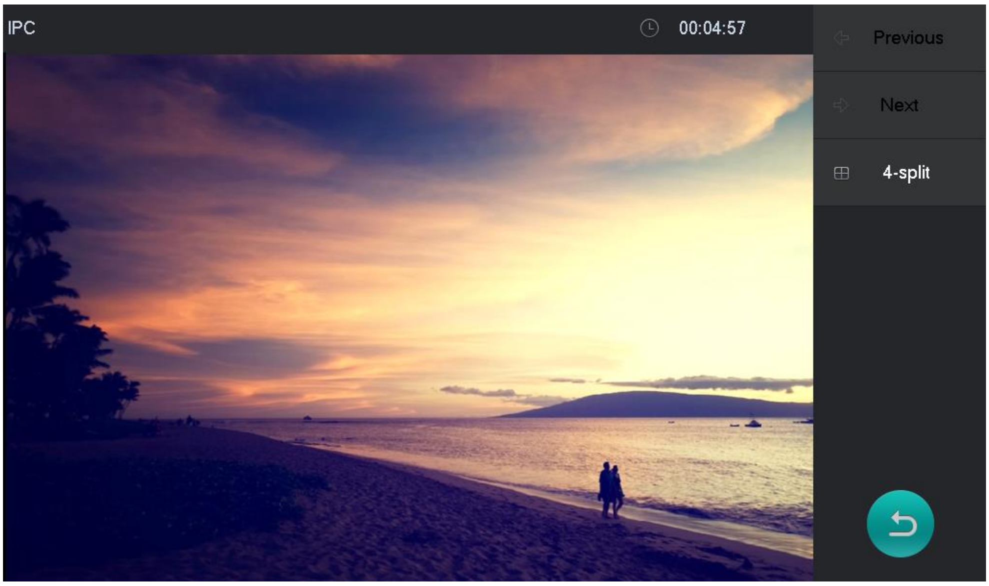
Step 1 Select **Monitor > IPC**.

Figure 4-20 IPC



Step 2 Tap the IPC icon.

Figure 4-21 Monitoring



Step 3 Do the operation as the description of Table 4-1.

4.3.3 VTS

You can call and control the online VTS that has been added.

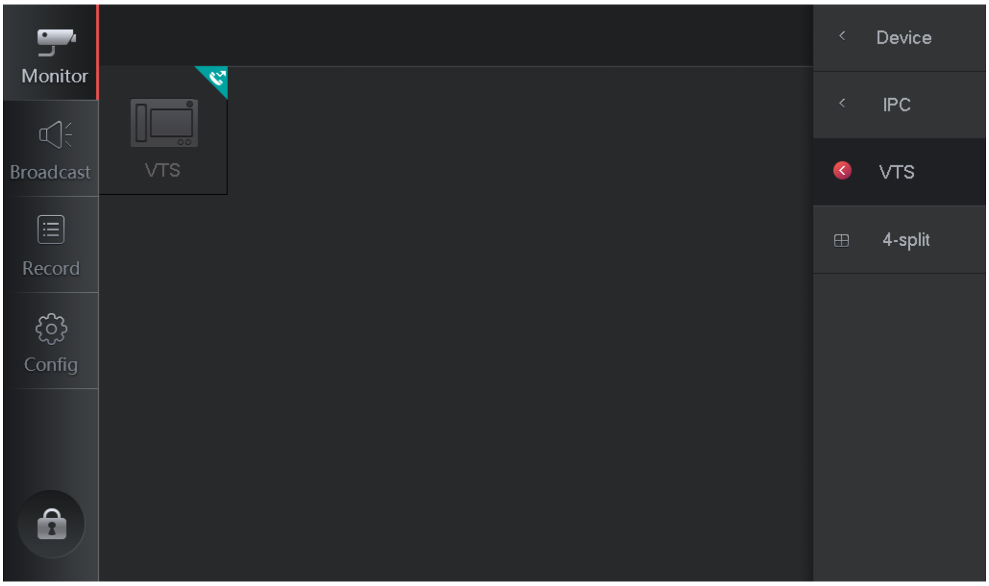
4.3.3.1 Call

Step 1 Select **Monitor > VTS**.

📖

The highlighted icon means the VTS is online, and you can call the VTS.

Figure 4-22 VTS



Step 2 Tap the highlighted icon to call the VTS.

When the other device answers the call, the calling interface is displayed. See Figure 4-24. For details, see Table 4-2.

The camera is not on in Figure 4-24; when the camera is on, there will be monitoring image on the interface.

Figure 4-23 Calling

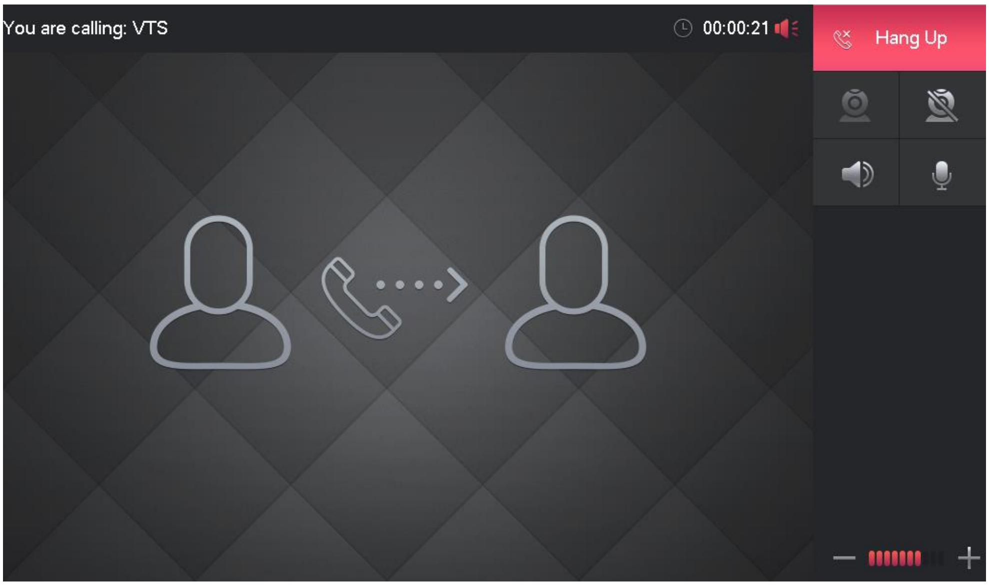


Figure 4-24 Talking

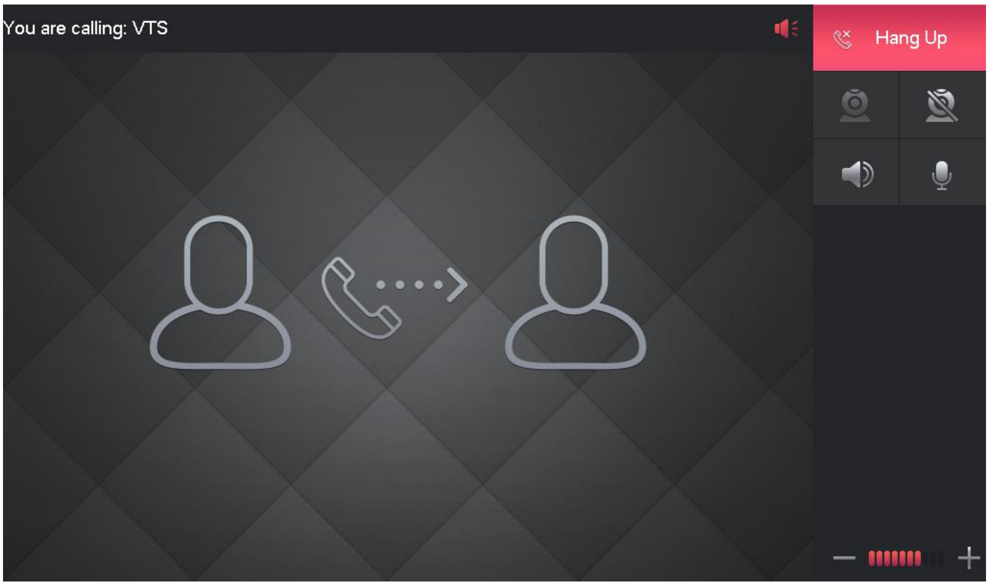


Table 4-2 Icon description

Icon	Meaning
📷	Tap 📷 to allow the other device monitoring the local video.
🚫📷	Tap 🚫📷 to forbidden the other device monitoring the local video.
🔊	Tap 🔊, and the VTS will not play the audio of the other device.
🎙	Tap 🎙, and the other device cannot receive the audio of the VTS.

Icon	Meaning
− ▮▮▮▮▮▮ +	Adjust the talking volume.
🔈	🔈 Indicates that the VTS is in handsfree mode; when you use handset, the icon changes to ☎.

4.3.3.2 Answer

When VTS calls, the answering interface is displayed.

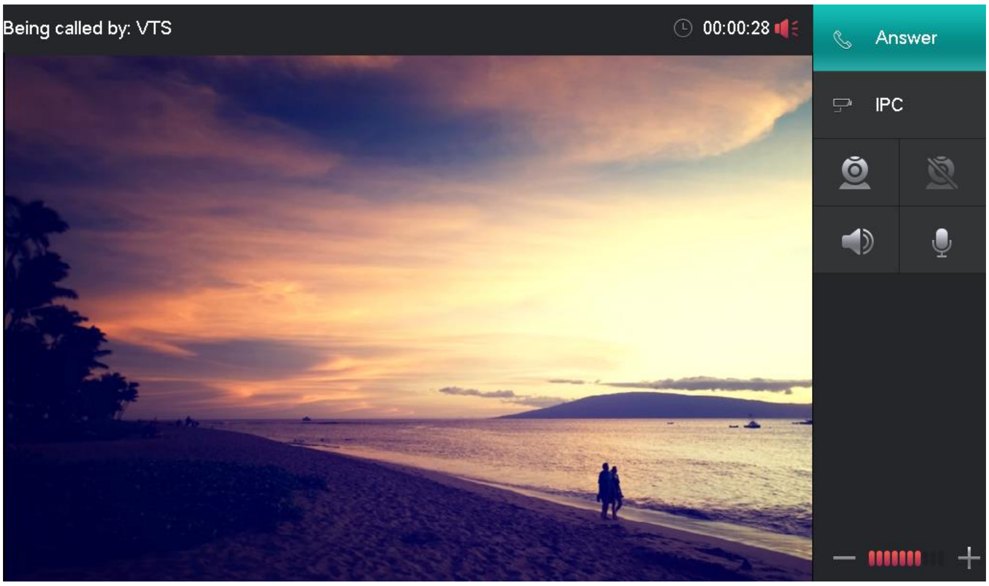


Figure 4-25 Calling status

Step 1 Tap **Answer** or the handsfree button to answer the call. See Figure 4-26. For details, see Table 4-2.

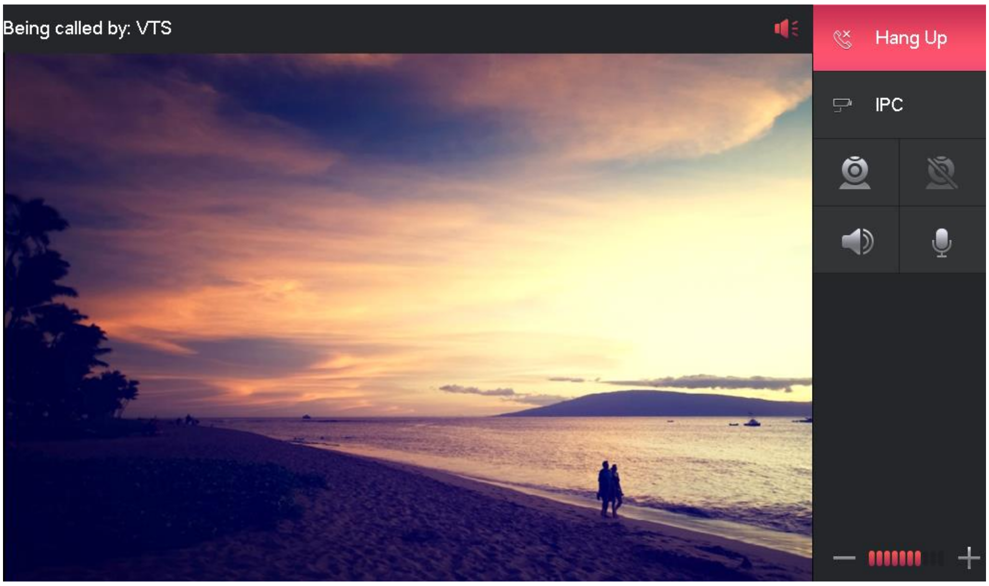
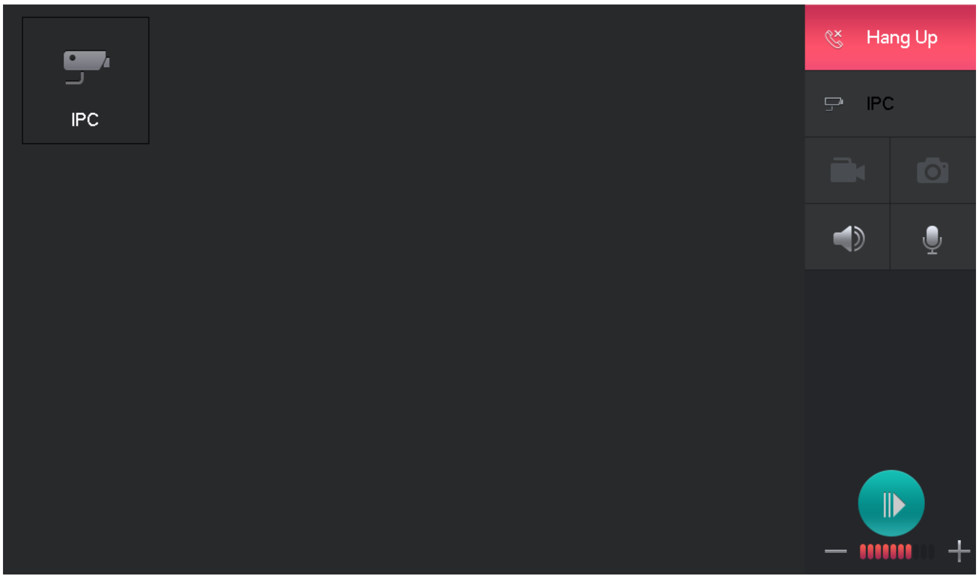


Figure 4-26 Busy

Step 2 (Optional) Tap **IPC** to enter the device list. See Figure 4-27. Select an IPC to do monitoring operation. Tap ▶ to go to the calling interface.

Figure 4-27 IPC monitoring



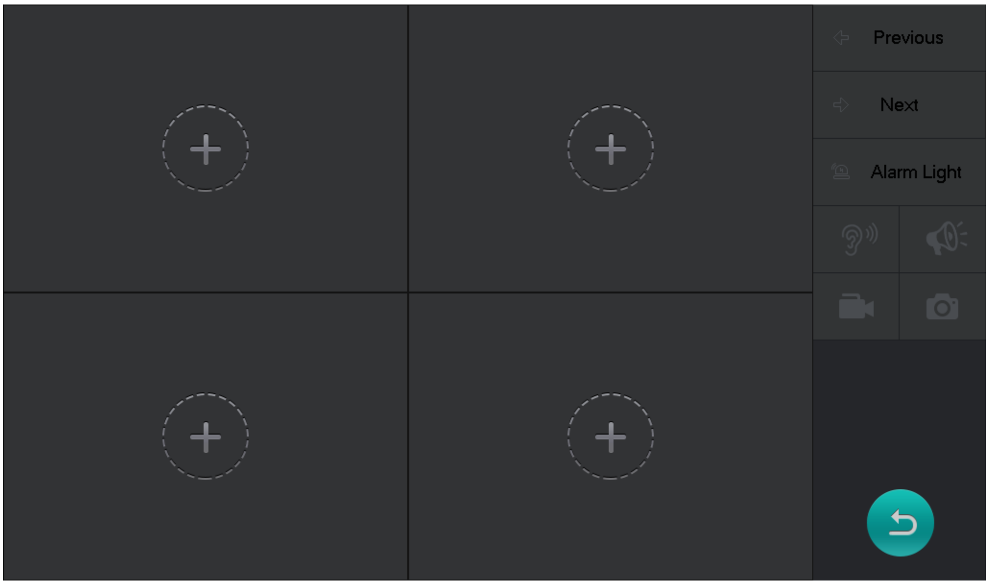
Step 3 Tap **End** to end the call.

4.3.4 4-split

You can monitor max. 4 terminals and IPCs at same time, and do operations on them.

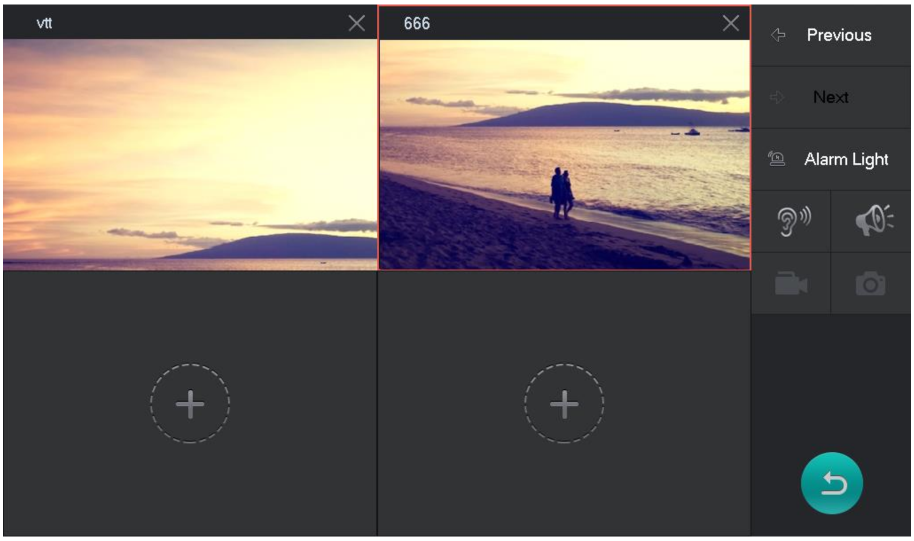
Step 1 Select **Monitor > 4-split**.

Figure 4-28 4-split



Step 2 Tap ⊕, and select the terminal or IPC as needed.

Figure 4-29 4-Split monitoring



Step 3 Tap the window of a certain device to control the device. For details, see Table 4-1.

4.4 Broadcast

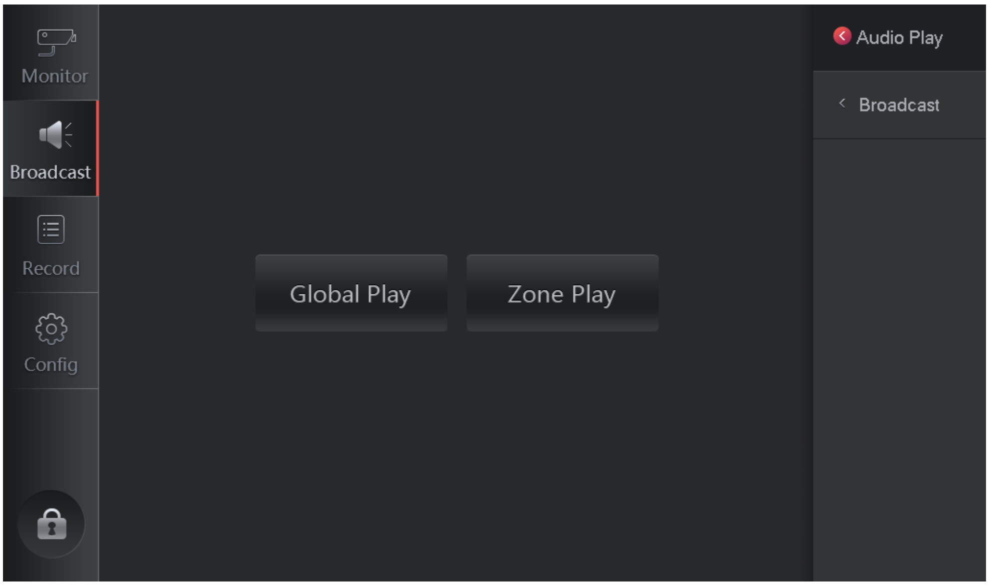
It is used for audio play or broadcast.

4.4.1 Audio Play

4.4.1.1 Global Play

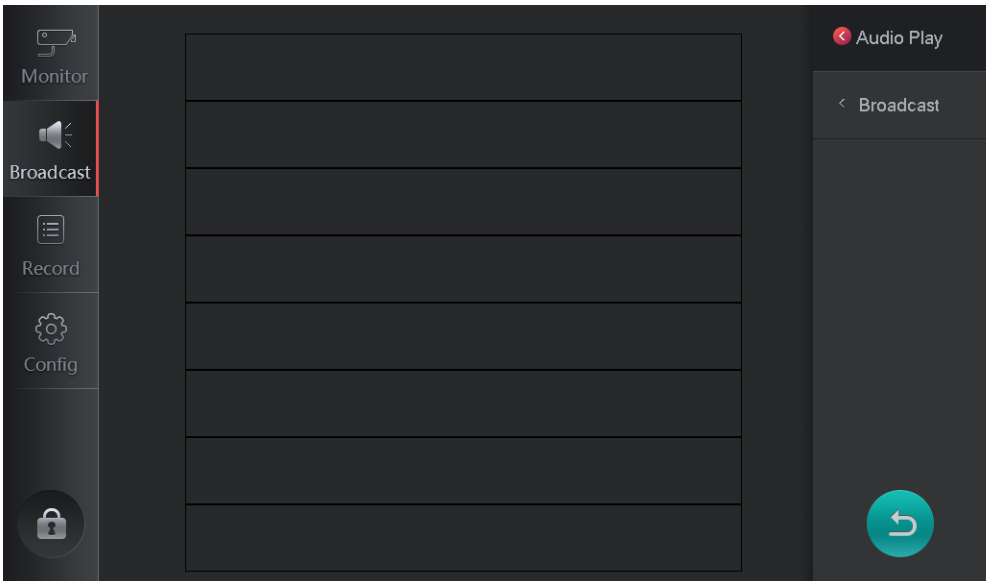
Step 1 Select **Broadcast > Audio Play**.

Figure 4-30 Audio play



Step 2 Tap **Global Play**.

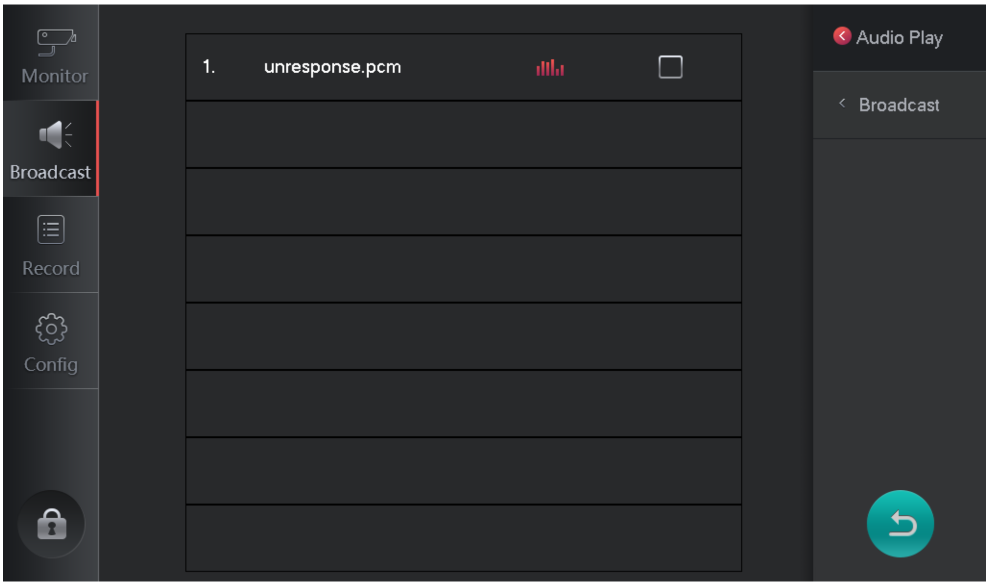
Figure 4-31 File list



Step 3 Tap ▷ to start playing the audio files of terminal devices. See Figure 4-32.

Tap □ to stop playing.

Figure 4-32 Playing audio

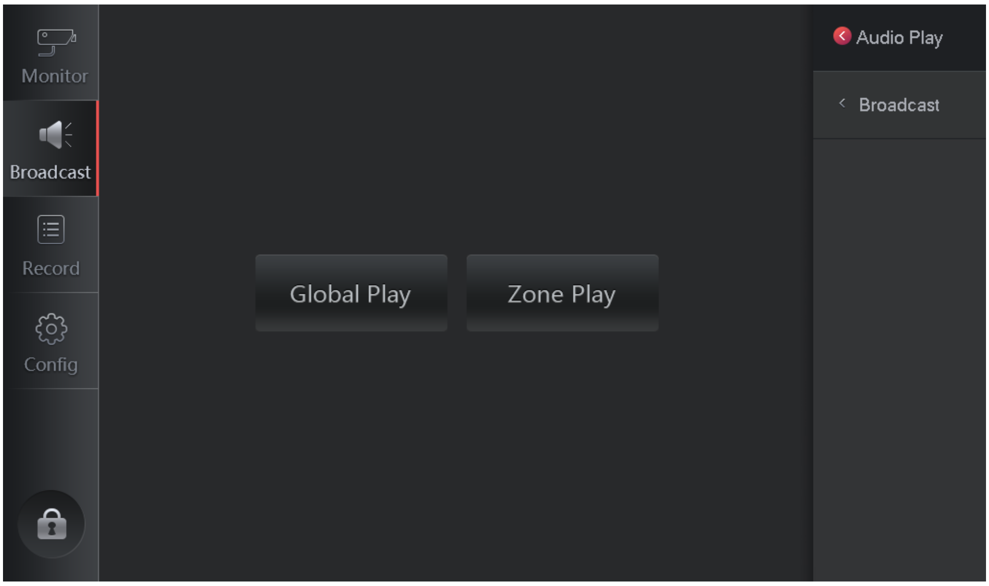


1. unresponse.pcm □

4.4.1.2 Zone Play

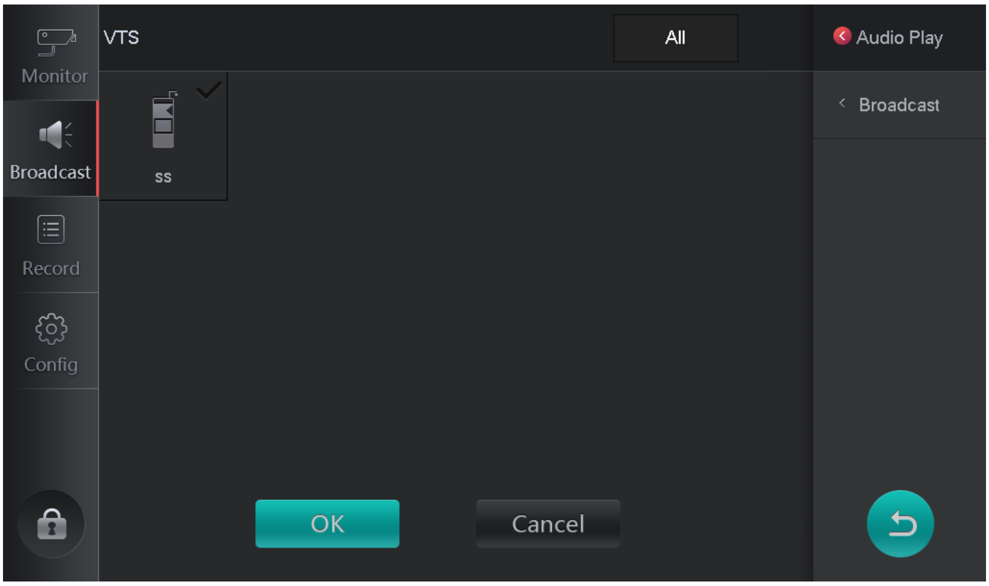
Step 1 Select **Broadcast > Audio Play**.

Figure 4-33 Audio play



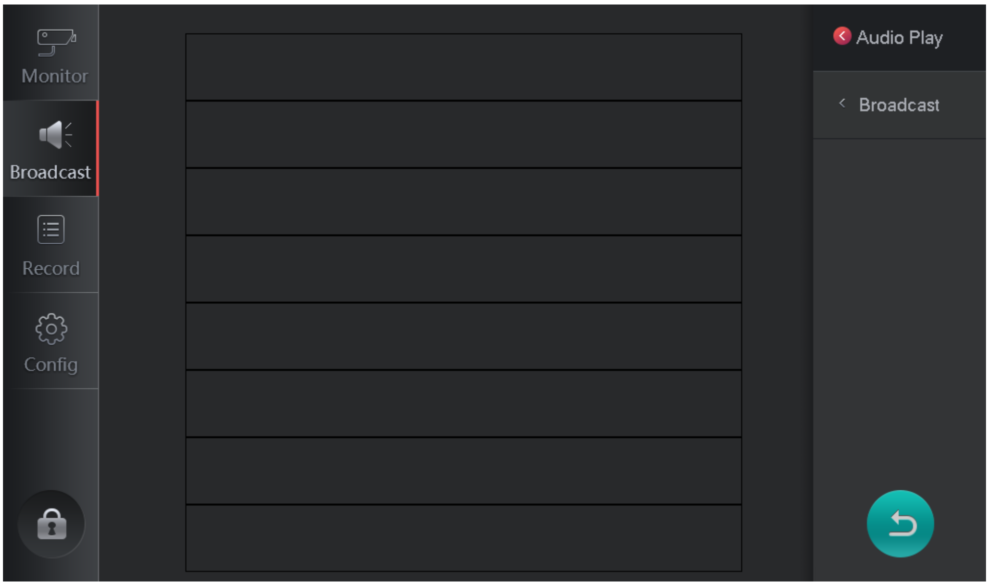
Step 2 Tap **Zone Play**.

Figure 4-34 Select the device



Step 3 Select the device, and tap **OK**.

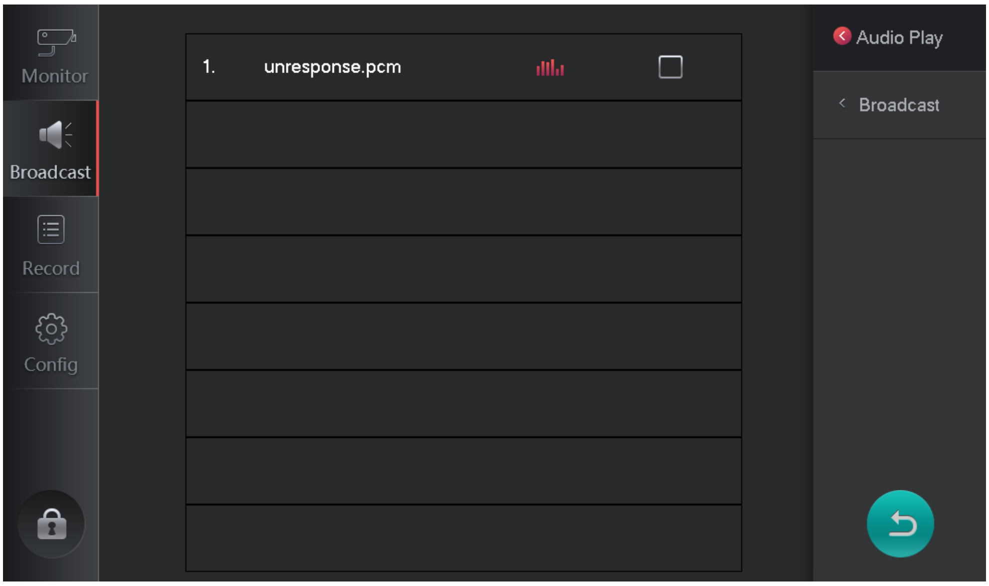
Figure 4-35 File List



Step 4 Tap ▷ to start playing the audio files of terminal devices. See Figure 4-32.

Tap □ to stop playing.

Figure 4-36 Playing audio



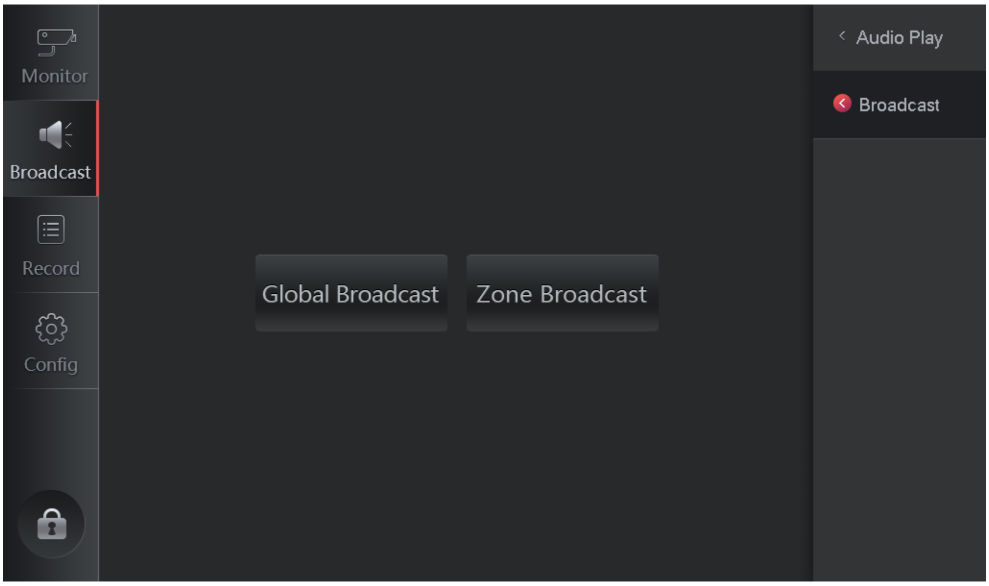
1. unresponse.pcm

4.4.2 Broadcast

4.4.2.1 Global Broadcast

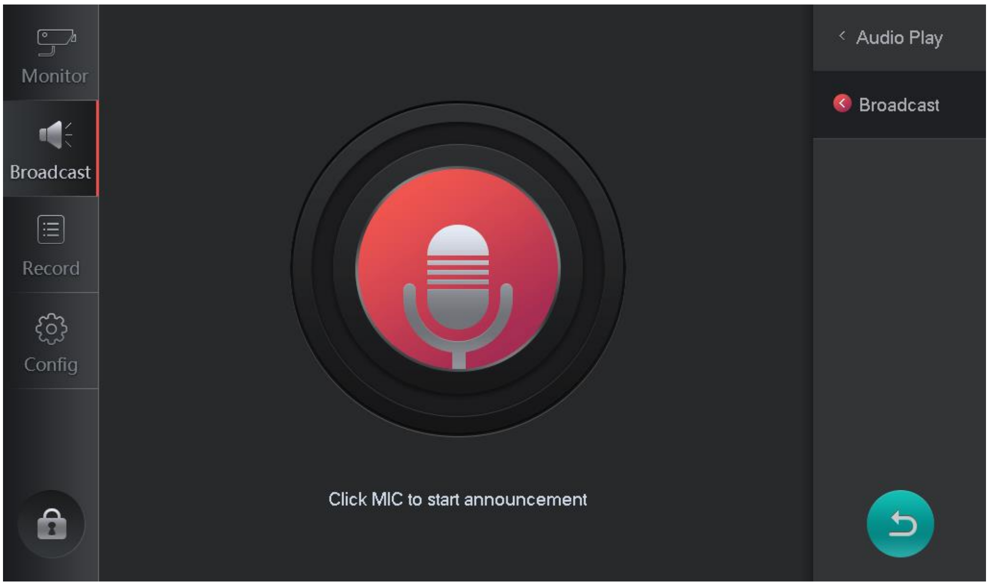
Step 1 Select **Broadcast > Broadcast**.

Figure 4-37 Broadcast



Step 2 Tap **Global Broadcast**.

Figure 4-38 Broadcast

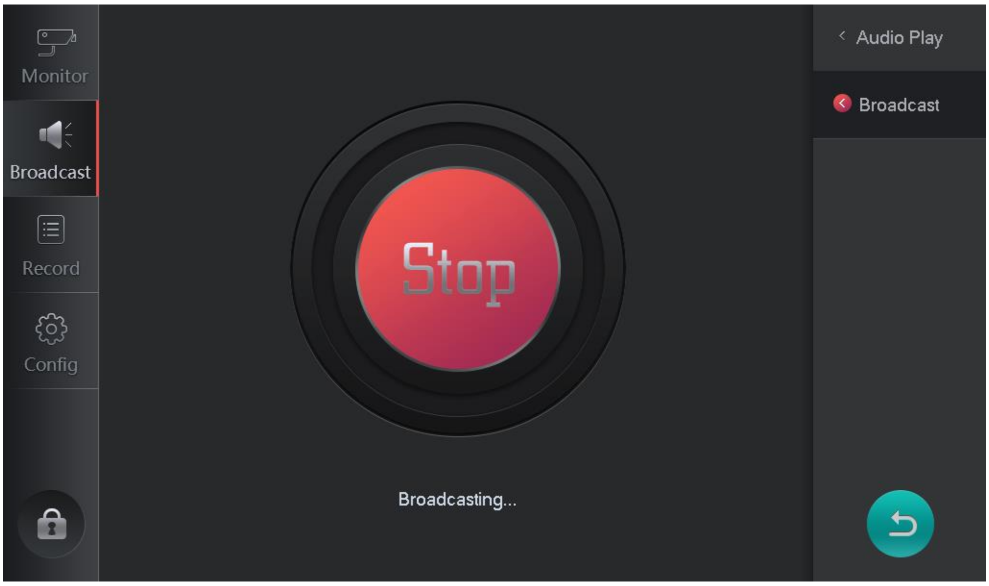


Click MIC to start announcement

Step 3 Tap to talk with the terminal devices or IPC. See Figure 4-39.

Tap to stop broadcast.

Figure 4-39 Playing broadcast



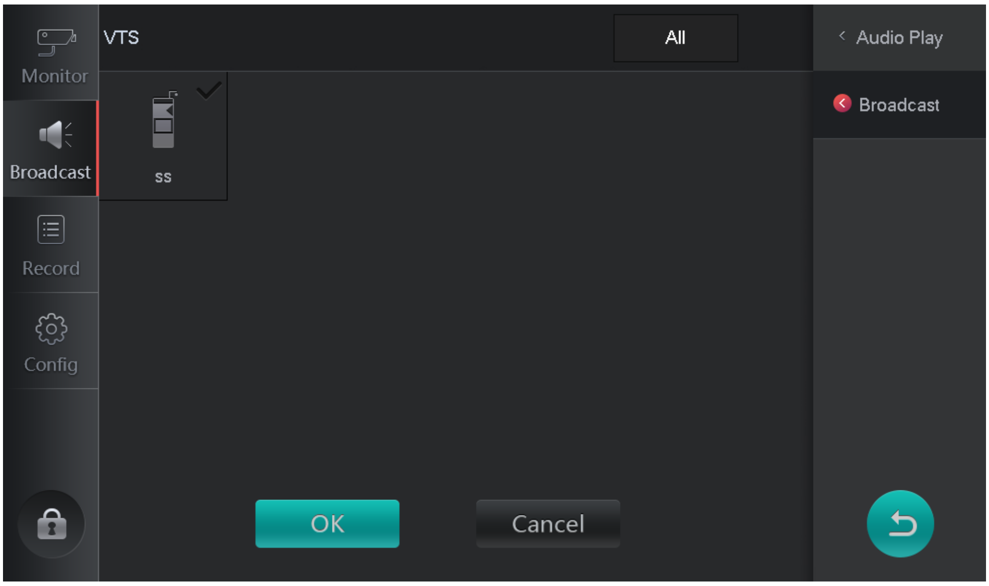
Broadcasting...

4.4.2.2 Zone Broadcast

Step 1 Select **Broadcast > Broadcast** (Figure 4-37).

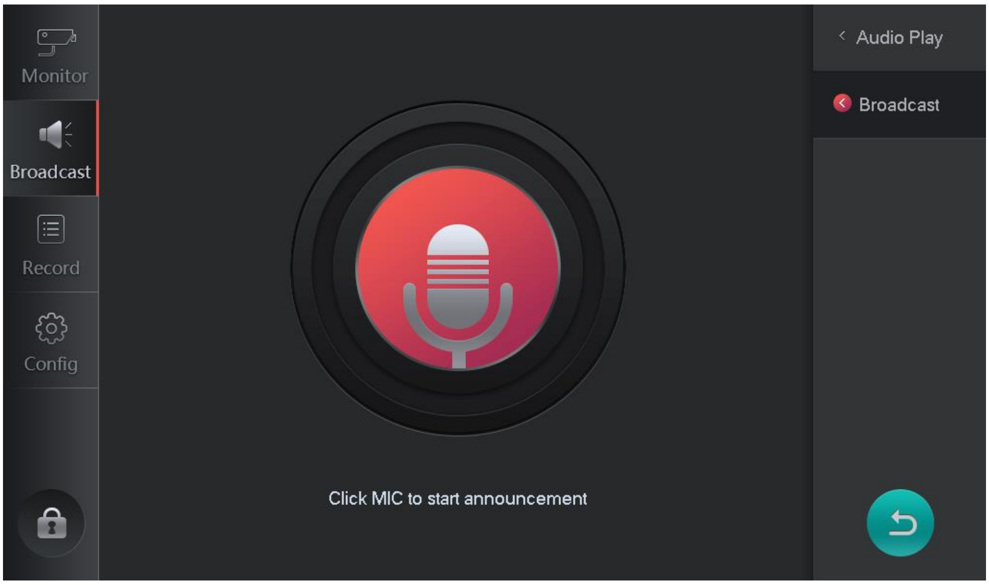
Step 2 Tap **Zone Broadcast**.

Figure 4-40 Select the device



Step 3 Select the device, and tap **OK**.

Figure 4-41 Broadcast

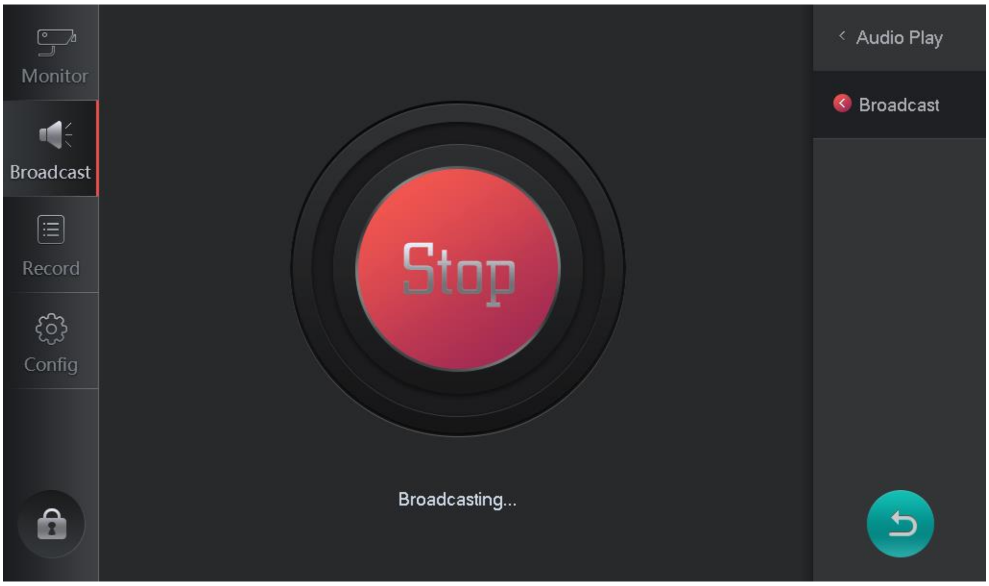


Click MIC to start announcement

Step 4 Tap to talk with the terminal devices or IPC. See Figure 4-39.

Tap to stop broadcast.

Figure 4-42 Playing broadcast



4.5 Record

You can view missed calls, answered calls, dialed calls, record, and snapshot.

4.5.1 Missed, Answered, Dialed

This section takes Missed as an example.

Select **Record > Missed**. See Figure 4-43. White indicates read, and red indicates unread.

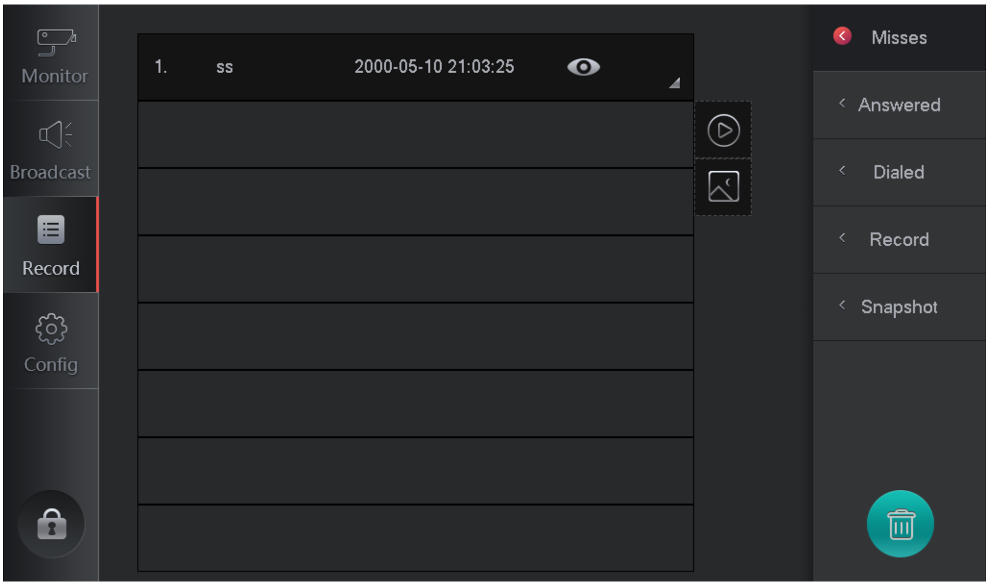
- Tap to go to the monitoring image of corresponding device.

  If the terminal device is VTS, the icon will not be displayed. You cannot do monitoring.

- If there is snapshot or recorded video during this record, will be displayed. Tap it, and will be displayed. Tap it to play the snapshot or recorded video.

Tap to delete all Missed records.

Figure 4-43 Missed records



1. ss 2000-05-10 21:03:25

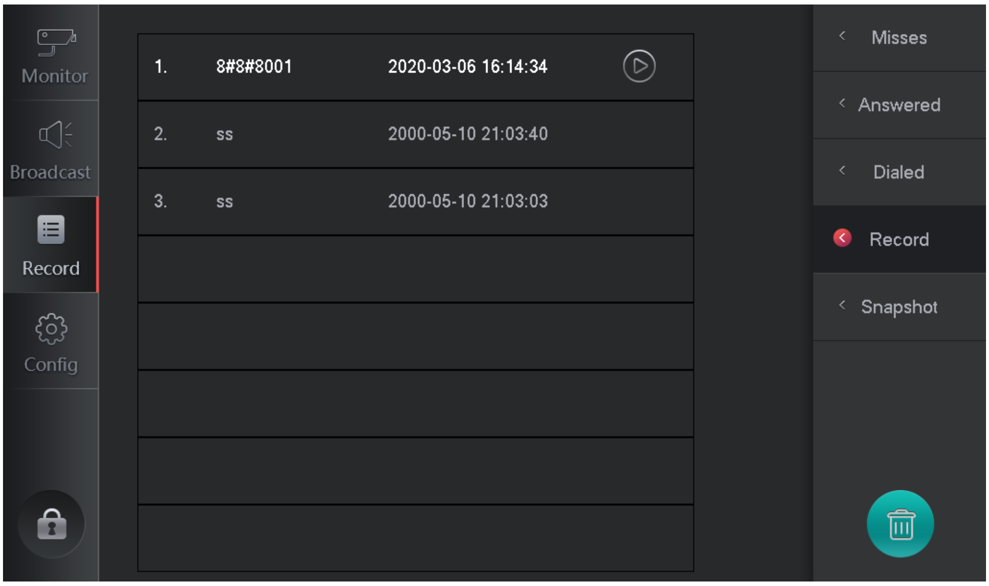
4.5.2 Video Recording

Select **Record > Record**. See Figure 4-44. Select a record, and then tap ▷ to play the recorded video. See Figure 4-45. Tap ↩ to exit the playback interface.

📖

Tap 🗑 to delete all records.

Figure 4-44 Video recording

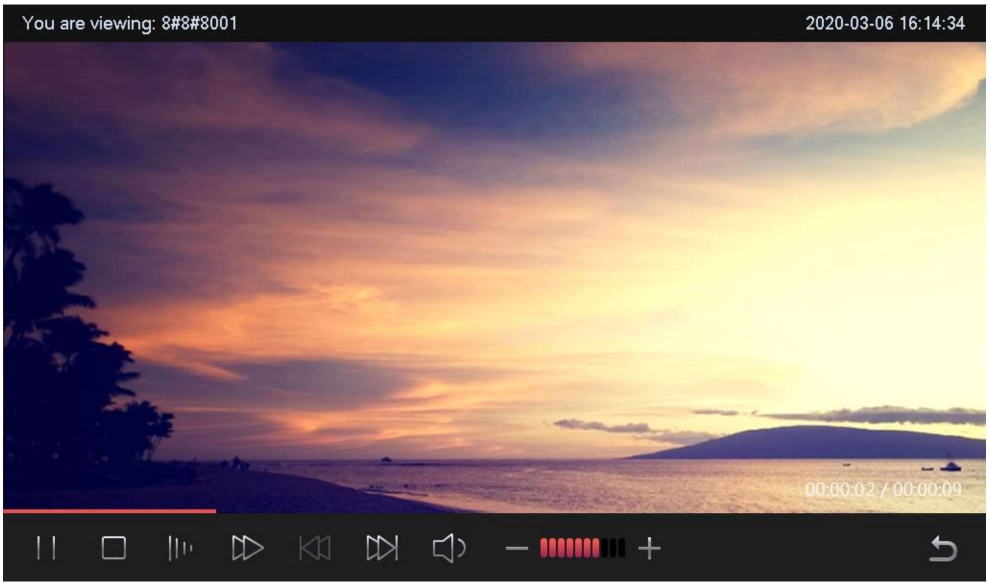


1. 8#8#8001 2020-03-06 16:14:34

2. ss 2000-05-10 21:03:40

3. ss 2000-05-10 21:03:03

Figure 4-45 Recording playback

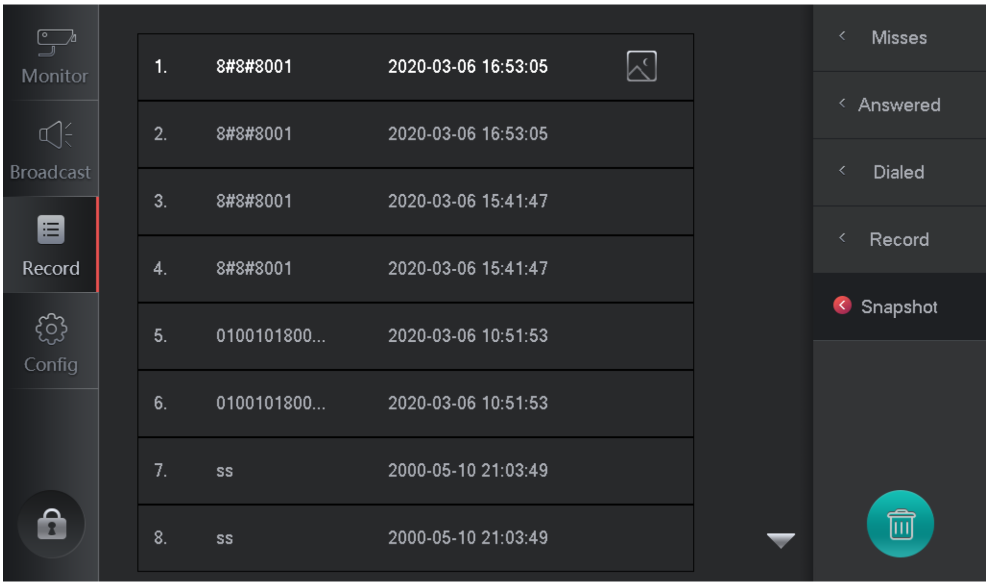


4.5.3 Snapshot

Select **Record > Snapshot**. See Figure 4-46. Select a record, and then tap to view snapshots.

Tap to delete all snapshot records.

Figure 4-46 Snapshot



1.	8#8#8001	2020-03-06 16:53:05
2.	8#8#8001	2020-03-06 16:53:05
3.	8#8#8001	2020-03-06 15:41:47
4.	8#8#8001	2020-03-06 15:41:47
5.	0100101800...	2020-03-06 10:51:53
6.	0100101800...	2020-03-06 10:51:53
7.	ss	2000-05-10 21:03:49
8.	ss	2000-05-10 21:03:49

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **MAC Address Binding**

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

9. **Assign Accounts and Privileges Reasonably**

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

10. **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.

11. **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.

12. **Secure Auditing**

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

13. **Network Log**

    Due to the limited storage capacity of the equipment, 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.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment 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.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.