

# **Master Station**

## **Quick Start Guide**






# Foreword

## General

This manual introduces the installation and basic operation of the master station (hereinafter referred to as "VTS").

## Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

| Signal Words   | Meaning   |
|--|---|
|  <b>CAUTION</b> | Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result. |
|  <b>TIPS</b>    | Provides methods to help you solve a problem or save you time.  |
|  <b>NOTE</b>    | 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.



### CAUTION

- Risk of explosion if the battery is replaced by an incorrect type.
- Do not throw or immerse into water, heat to more than 100 °C (212 °F), 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

|   |            |
|---|------------|
| <b>Foreword</b> .....                                 | <b>I</b>   |
| <b>Important Safeguards and Warnings</b> .....        | <b>III</b> |
| <b>1 Structure</b> .....                              | <b>1</b>   |
| 1.1 Front Panel.....                                  | 1          |
| 1.2 Rear Panel .....                                  | 2          |
| <b>2 Cable Connection</b> .....                       | <b>4</b>   |
| 2.1 Important Note .....                              | 4          |
| 2.2 Network Diagram .....                             | 4          |
| <b>3 Web Operations</b> .....                         | <b>5</b>   |
| 3.1 Device Initialization .....                       | 5          |
| 3.2 Login.....  | 6          |
| 3.3 Password Reset.....                               | 6          |
| 3.4 Local Setup .....                                 | 8          |
| 3.5 Device Management .....                           | 9          |
| 3.5.1 Device Manager.....                             | 9          |
| 3.5.2 IPC Information.....                            | 12         |
| 3.6 Logout .....                                      | 13         |
| 3.6.1 Reboot .....                                    | 13         |
| 3.6.2 Logout.....                                     | 13         |
| <b>4 VTS Operations</b> .....                         | <b>14</b>  |
| 4.1 Standby Interface.....                            | 14         |
| 4.2 Monitor .....                                     | 15         |
| 4.2.1 Device .....                                    | 15         |
| 4.2.2 IPC .....                                       | 17         |
| 4.2.3 VTS .....                                       | 18         |
| 4.2.4 4-split .....                                   | 21         |
| <b>Appendix 1 Cybersecurity Recommendations</b> ..... | <b>23</b>  |

# 1 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.

## 1.1 Front Panel

Figure 1-1 Front panel

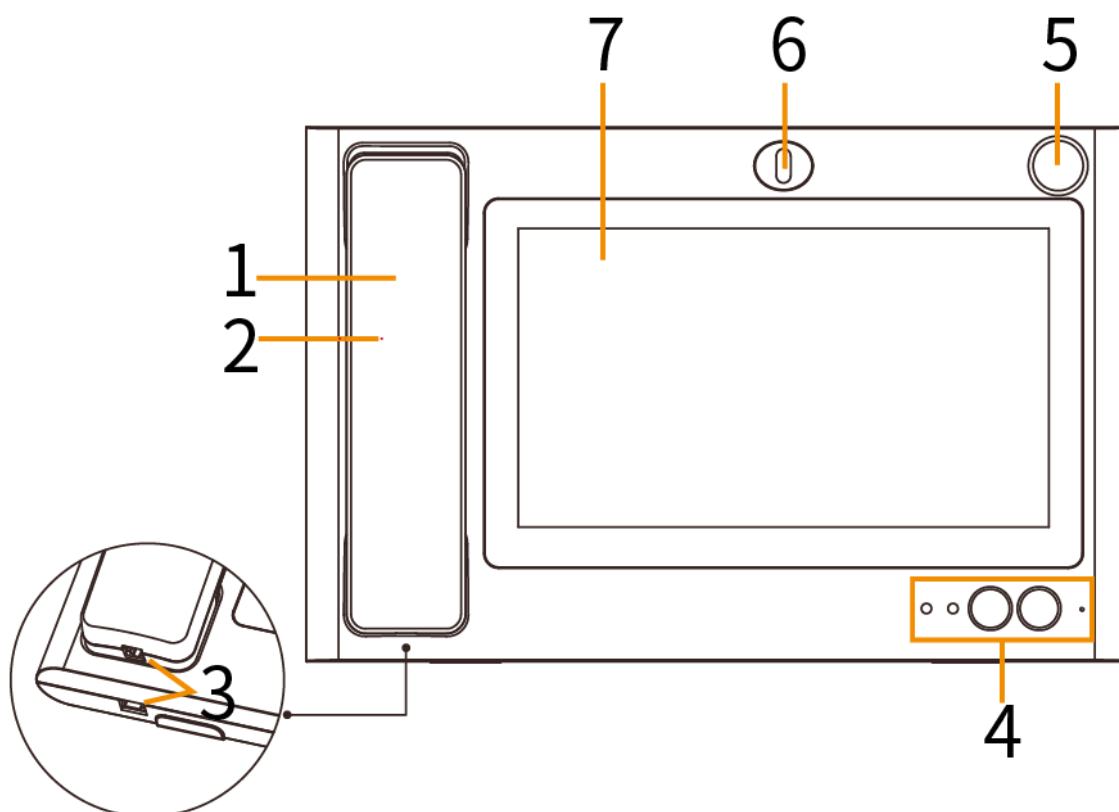



Table 1-1 Front panel description

| No. | Parameter                    | Description  |
|-----|------------------------------|--|
| 1   | Handset                      | Pick up the handset, and the VTS enters handset mode.  |
| 2   | Speaker                      | Outputs audio.   |
| 3   | Telephone line port          | Connected to the VTS and the receiver.   |
| 4   | Indicator lights and buttons | From left to right: <ul style="list-style-type: none"> <li>● Power indicator light<br/>On: Power on; Off: Power off.</li> <li>● Message indicator light<br/>On: There are missed calls; Off: There is no missed call or missed calls have been processed.</li> <li>● Unlock button<br/>(Optional) When the VTS is being called, monitoring or talking, press the button you can open some front</li> </ul> |

| No. | Parameter                | Description  |
|-----|--------------------------|--|
|     |                          | <p>devices which supports unlock function.</p> <ul style="list-style-type: none"> <li>• Handfree button<br/>Answers calls, and switch between handfree mode and handset mode.</li> <li>• Built-in MIC<br/>Inputs audio.</li> </ul> |
| 5   | Speaker port             | <p>(Optional) Connects to a microphone.</p>  <p>This function is only available on the models with built-in camera.</p>                           |
| 6   | Camera                   | (Optional) You can adjust the camera angle manually.   |
| 7   | Display and touch screen | LCD display and touch screen.  |

## 1.2 Rear Panel

Figure 1-2 Rear panel

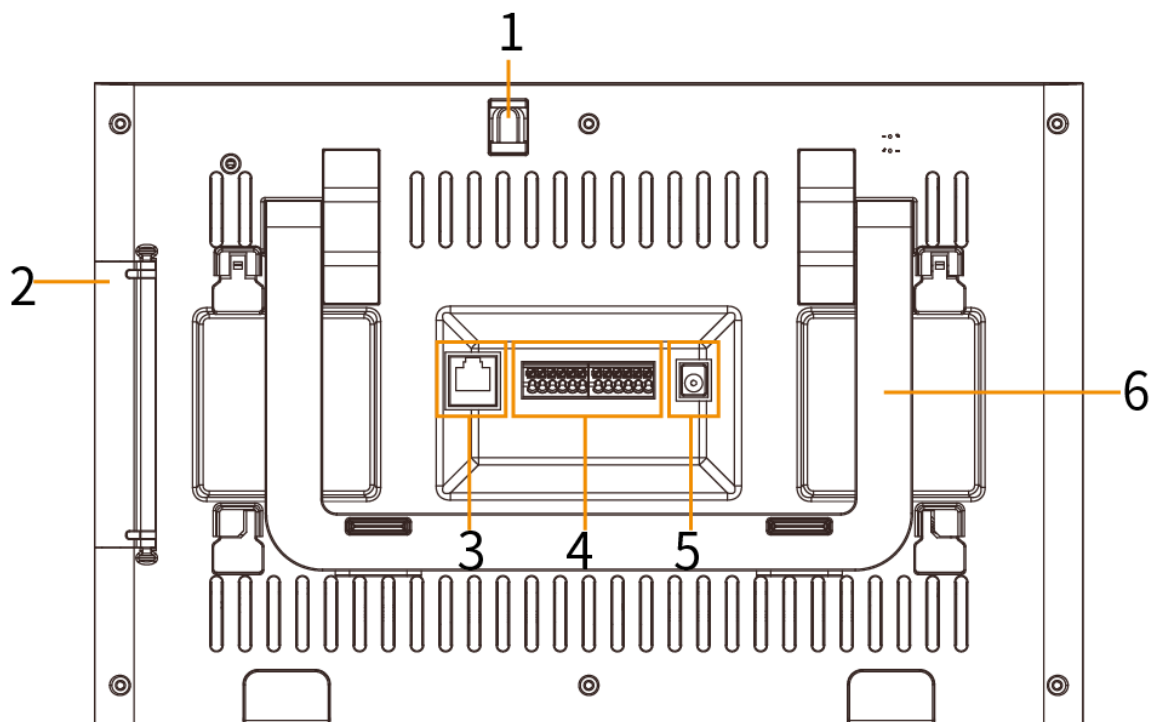


Table 1-2 Rear panel description

| No. | Parameter | Description   |
|-----|-----------|---|
| 1   | Camera    | You can adjust the camera angle manually.   |
| 2   | Port      | <p>Open the cover, ports from top to bottom:</p> <ul style="list-style-type: none"> <li>• HDMI video transmission port, which is used for video transmission.</li> <li>• USB port.</li> </ul> |

| No. | Parameter    | Description  |
|-----|--------------|--|
|     |              | <ul style="list-style-type: none"> <li>● USB port.</li> <li>● SD slot.</li> </ul>  |
| 3   | Network port | Connects to RJ-45 cable.   |
| 4   | 12-Core port | <p>From left to right:</p> <ul style="list-style-type: none"> <li>● Power output port.</li> <li>● Ground.</li> <li>● Alarm input port 1.</li> <li>● Alarm input port 2.</li> <li>● Alarm input port 3.</li> <li>● Alarm input port 4.</li> <li>● Power input port.</li> <li>● Ground port.</li> <li>● RS-485A port.</li> <li>● RS-485B port.</li> <li>● Alarm Output No.</li> <li>● Alarm Output COM.</li> </ul> |
| 5   | Power        | 12V DC power input.  |
| 6   | Bracket      | Adjust the angle within 0°–45° through the bracket on the rear panel.  |



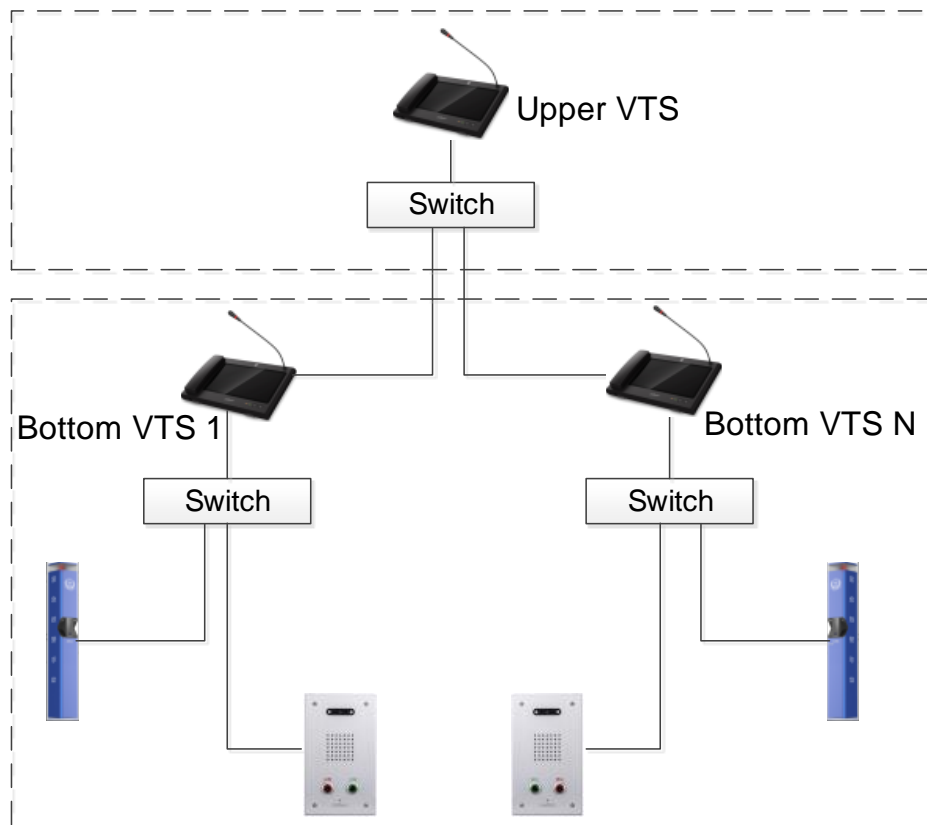
## 2 Cable Connection

### 2.1 Important Note

- Use the standard power adapter. Do not supply power with the adapter of other models.
- Before connecting cables, read "1 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 (192.168.1.108 by default) in the address bar.

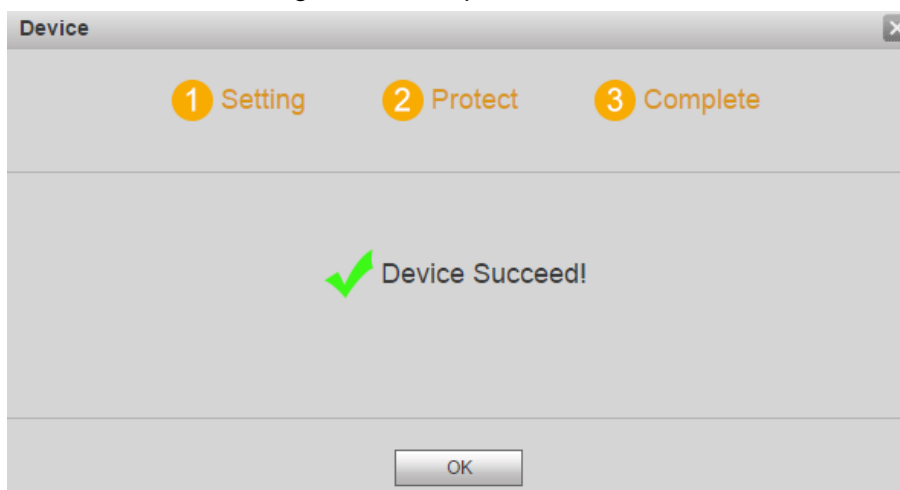
Figure 3-1 Password setting

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

Figure 3-2 Password protection

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

Figure 3-3 Completed



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

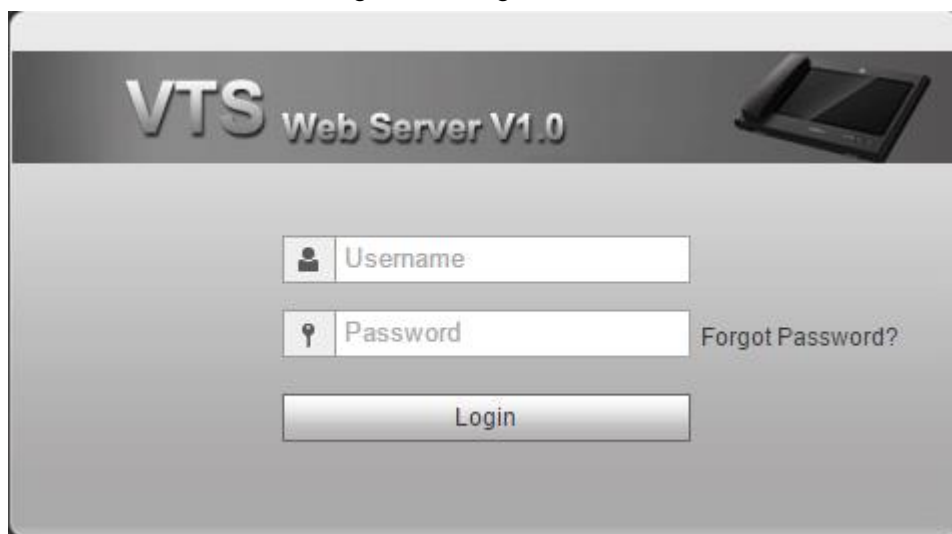
## 3.2 Login

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 with that of the VTS.

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 (1/2)

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\_easy4ip@telecamera.com.

The security code will be delivered to .com

Security code:

Cancel Next

**Step 2** Scan the QR code, and you will get a string.

**Step 3** Send the string to the email address displayed on the QR code interface. A security code will be sent to your email.

**Step 4** Enter the security code that you have received.

**Step 5** Click **Next**.

Figure 3-6 Reset the password (2/2)

Reset the password(2/2)

Username admin

New Password

Weak Middle Strong

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 \\' \\' \\' \\' &)

Cancel OK

**Step 6** 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 7 Click **OK** and password reset is completed.

## 3.4 Local Setup

Set device role, device number and IP address, and more.

Step 1 Select **System Setup > Local Setup**, and then click the **Local Setup** Tab.


Figure 3-7 Local setup



The screenshot shows the 'Local Setup' configuration page. On the left is a navigation menu with 'System Setup' expanded to 'Local Setup'. The main area contains the following fields and controls:

- Device Role:** Dropdown menu set to 'Bottom VTS'. Red asterisk: \* After role is switched, please reboot to take effect
- Device Name:** Text input field with 'VTS'. Red asterisk: \* After role is switched, please reboot to take effect
- Device No.:** Text input field with '101'. Red asterisk: \* Input range 101-999
- IP Address:** IP address input field with red asterisk \*
- Subnet Mask:** Subnet mask input field with red asterisk \*
- Default Gateway:** Default gateway input field with red asterisk \*
- MAC Address:** MAC address input field
- DNS Address:** DNS address input field
- Reboot Date:** Dropdown menu set to 'Tuesday'
- Version Info:** Text field showing '2020-02-22'
- SSH:** Radio buttons for 'On' and 'Off' (selected)
- Buttons:** 'Default', 'Refresh', and 'OK'

Step 2 Configure parameters.

Table 3-1 Local settings

| Parameter   | Description  |
|-------------|--|
| Device Role | <p>Includes 3 role types, and the default one is <b>Bottom VTS</b>.</p> <ul style="list-style-type: none"> <li>● Bottom VTS: When used without platform, VTS can be used as bottom VTS, which has management permission.</li> <li>● 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.</li> <li>● Platform client: When used with platform, VTS can be used as platform client, which does not have the permission to manage device.</li> </ul> |
| Device Name | Customize the name for the device.   |
| Device No.  | <p>Customize the number for the device. Do not modify it arbitrarily.</p> <p> If you modify the number of the VTS of lower level, you need to add the device to the upper VTS again.</p>  |
| IP Address  | Enter the IP address, subnet mask, and gateway.  |

| Parameter       | Description  |
|-----------------|--|
| Subnet Mask     |   |
| Default Gateway | If you modify the IP address of the VTS of lower level, you need to add the device to the upper VTS again.   |
| MAC Address     | The MAC address of the VTS.  |
| DNS Address     | The DNS address of the VTS. 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    | The current version.   |
| SSH             | Enable or disable the SSH debug function.<br><br>If you have enabled the SSH function the <b>Advanced Config</b> on the device, the function is enabled on the web interface. |

**Step 3** Click **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 \* must be configured.
- When the device role is modified, the system will go to the login interface, and you need to log in again.
- When IP Address is modified, the system will go to the login interface, and you need to log in again.

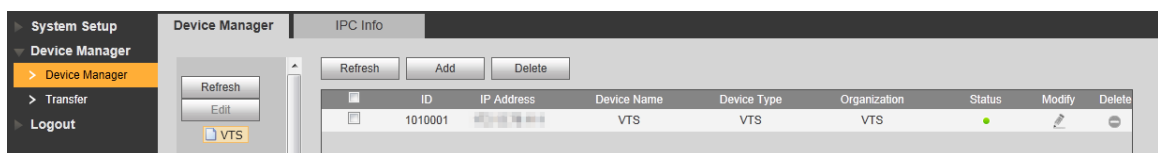
## 3.5 Device Management

### 3.5.1 Device Manager

- When the device role is bottom VTS, it can add the VTT and the VTA
- When the device role is upper VTS, it can add the bottom VTS.

Select **Device Manager > Device Manager**, and click **Device Manager**.

Figure 3-8 Device manager




#### 3.5.1.1 Adding Device

- Bottom VTS  
Click VTS node on left side of the interface, and then click **Add**. See Figure 3-9. Enter the device information of added VTT and VTA, and then click **OK**.



- The **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 3-9 Add device

- Upper VTS  
Click **Edit**. See Figure 3-10. Hover over the device name, and the adding and deleting icons will be displayed. Click , see Figure 3-11. Enter the 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 3-10 Adding VTS

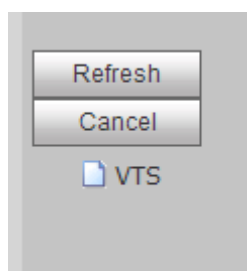


Figure 3-11 Add node

The 'Add Node' dialog box contains the following fields and values:

- Upper Organization: VTS \*
- IP: \*
- Username: \*
- Password: \*

Buttons: OK, Cancel

### 3.5.1.2 Modifying Device

You can only modify VTT or VTA information.


Click  next to the VTT or VTA information, see Figure 3-12. You can modify username, password, IP address, port, device name, device type and device model.


Figure 3-12 Add device (VTT or VTA)

The 'Add Device' dialog box contains the following fields and values:

- 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 \*

Buttons: OK, Cancel


### 3.5.1.3 Deleting Device

- Delete VTS  
Click **Edit**, hover over the device name, and the adding and deleting icons will be displayed. Click  to delete it.





Root node cannot be deleted.

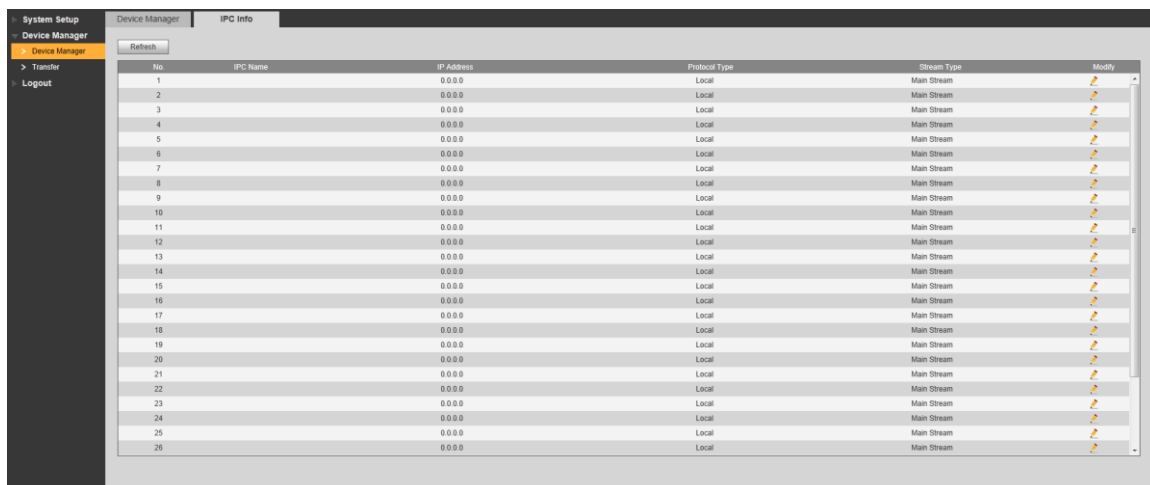
- Delete device (VTT or VTA)  
Click  in the device information bar to delete a device.

### 3.5.2 IPC Information

Add IPC to do monitoring, and you can add 32 cameras at most.

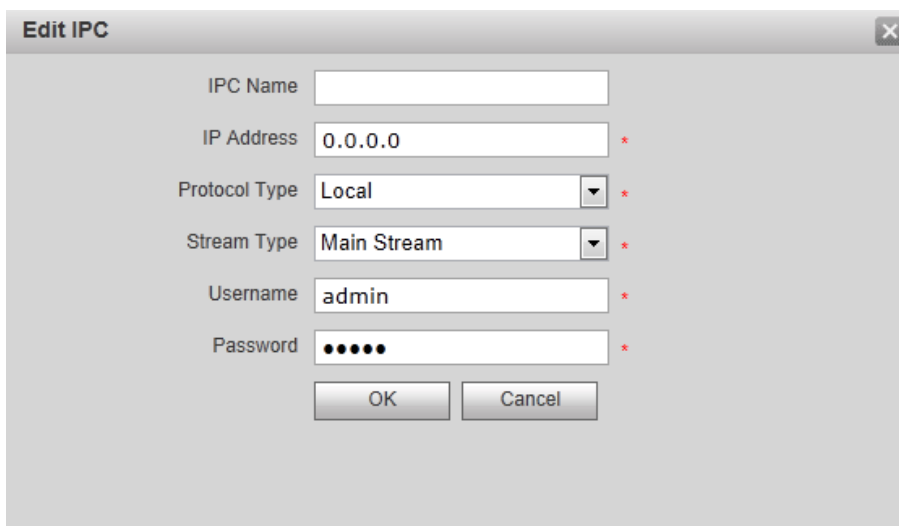
**Step 1** Select **Device Manager > Device Manager**, and click the **IPC Info** tab.

Figure 3-13 IPC information



**Step 2** Click  to edit IPC.

Figure 3-14 Edit IP



**Step 3** Configure the parameters.

Table 3-2 IPC parameter description

| Parameter   | Description                                       |
|-------------|---|
| IPC Name    | Enter the IPC name.                               |
| IP Address  | Enter the IP address of the IPC.                  |
| Protocol    | Includes <b>Local</b> and <b>ONVIF</b> .          |
| Stream Type | Includes <b>Main Stream</b> and <b>Sub Stream</b> |

| Parameter | Description  |
|-----------|--|
| Username  | Enter the user name and password of the IPC that you need. |
| Password  |  |

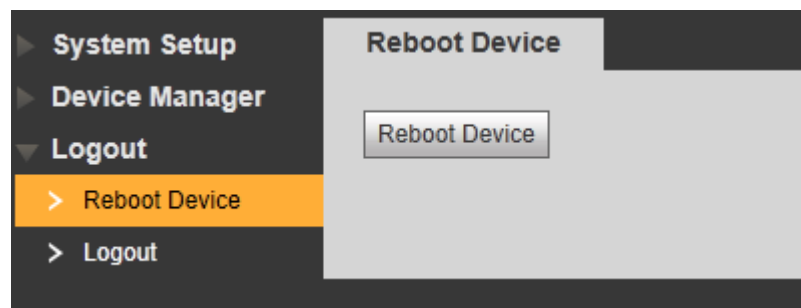
Step 4 Click **OK**.

## 3.6 Logout

### 3.6.1 Reboot

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

Figure 3-15 Reboot device

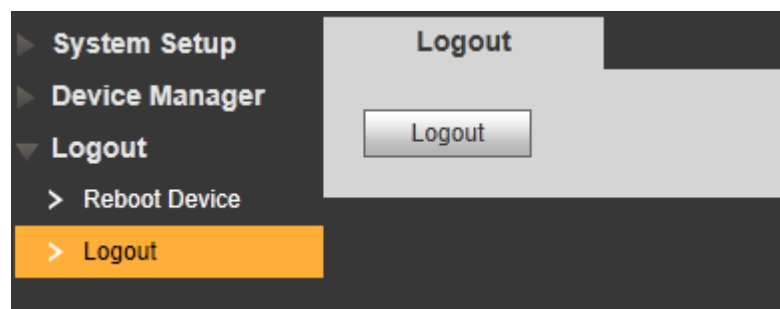


Step 2 Click **Reboot Device** to restart the device.

### 3.6.2 Logout

Step 1 Select **Logout > Logout**.

Figure 3-16 Logout



Step 2 Click **Logout**.  
The login interface is displayed.

# 4 VTS Operations



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

## 4.1 Standby Interface

After powering 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

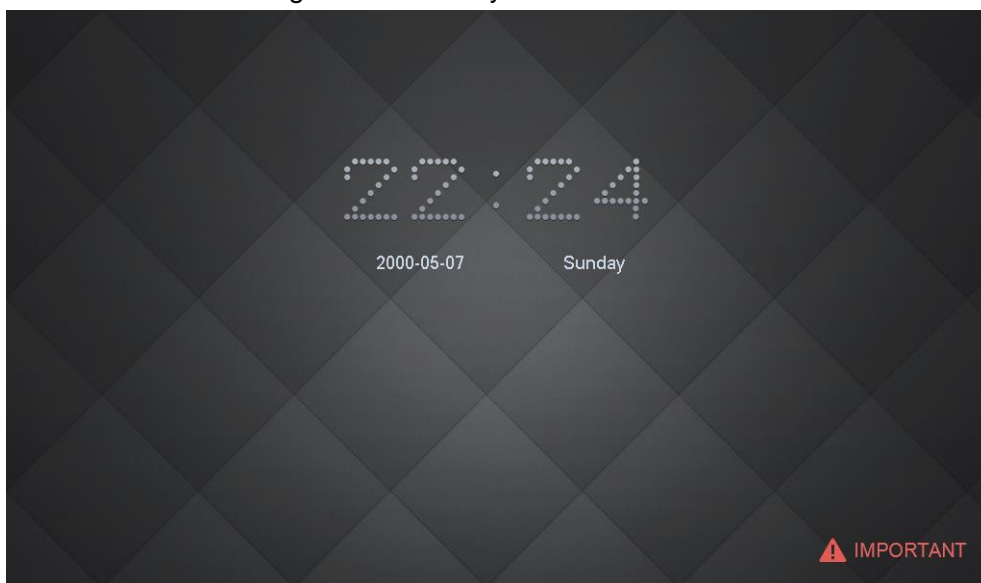
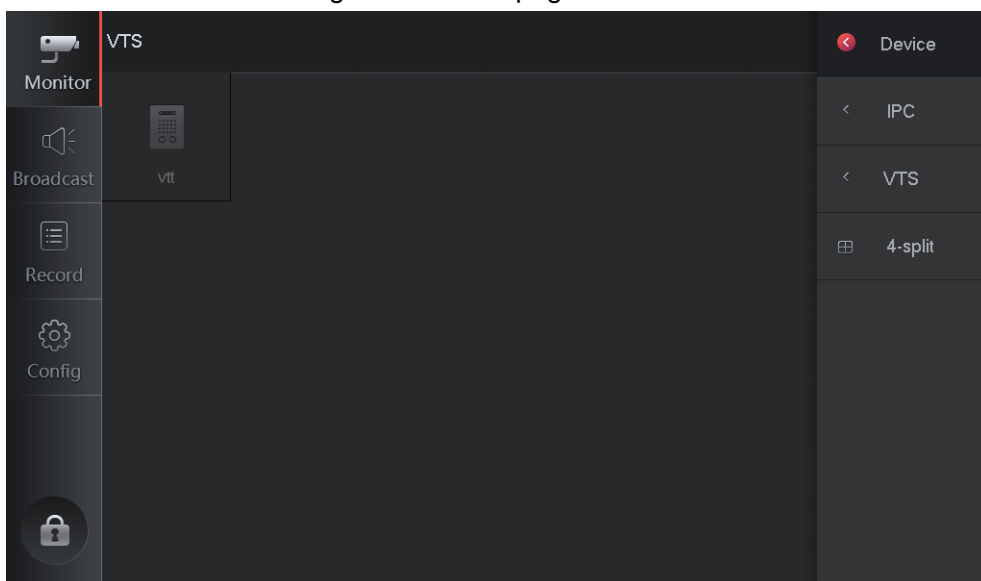



Figure 4-2 Homepage





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

## 4.2 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 Adding"; for the detailed operation of adding IPC, see "3.5.2 IPC Information."

### 4.2.1 Device

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

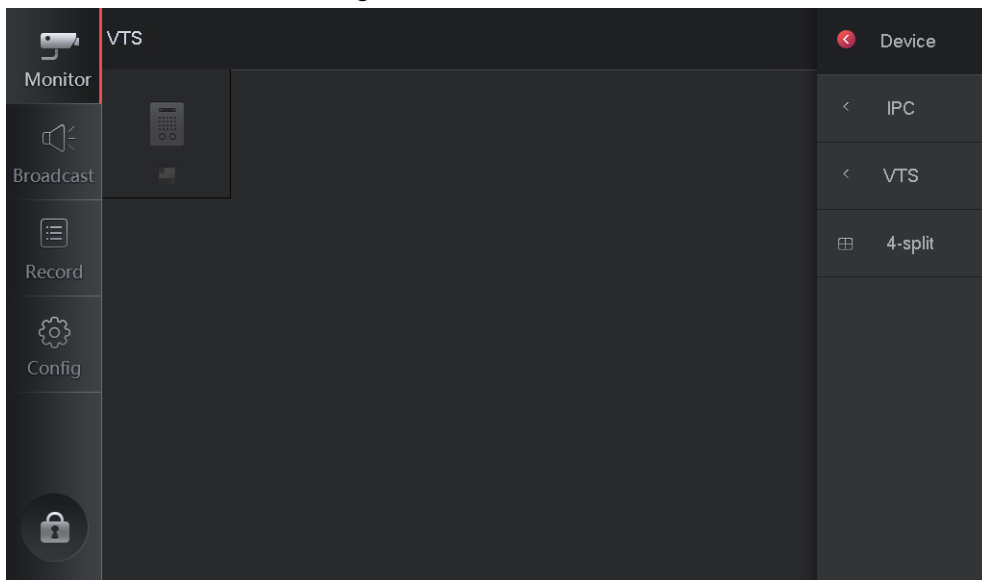
This section takes VTA as an example.

**Step 1** Select **Monitor > Device**.



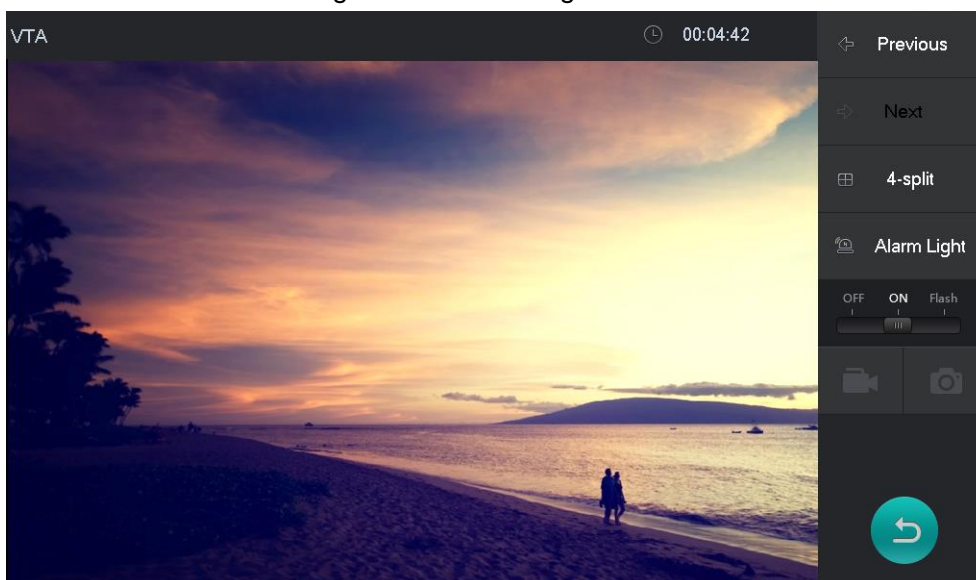
When the icon is highlighted, you can monitor the device.

Figure 4-3 Device



**Step 2** Tap the VTA icon.

Figure 4-4 Monitoring



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

Table 4-1 Monitor description














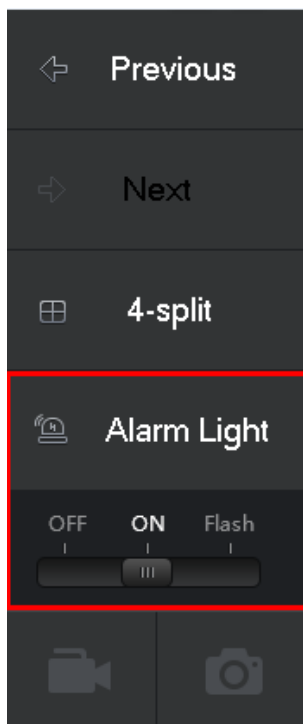
| Icon/Parameter  | Description  |
|---|--|
| Previous  | When the VTS connects to several devices, tap <b>Previous</b> or <b>Next</b> to switch the monitoring image.   |
| Next  |  |
| Split   | Tap <b>Split</b> , and the 4-split interface is displayed. For details, see "4.2.4 4-split."   |
| Alarm light   | The function is available on VTA.<br>1. Tap <b>Alarm Light</b> , and the interface shown in Figure 4-5 is displayed.<br>2. Tap the <b>OFF</b> , <b>ON</b> or <b>Flash</b> 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 the audio monitoring.   |
|  | 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. <ul style="list-style-type: none"> <li>• When there is no SD card in the VTS, the icon is gray.</li> <li>• The snapshot and recorded videos are stored in the SD card.</li> </ul> |
|  |  |

Figure 4-5 Alarm light operation

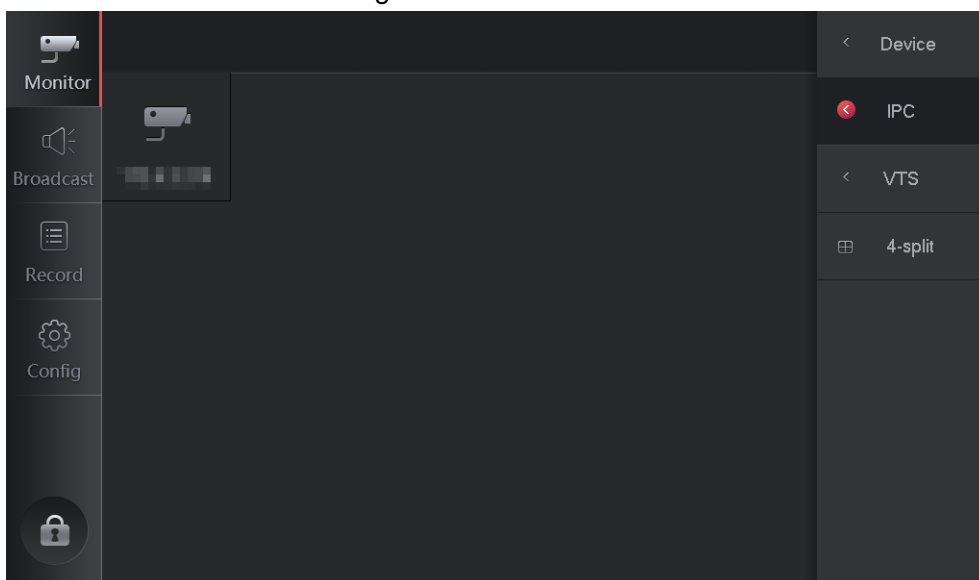


## 4.2.2 IPC

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

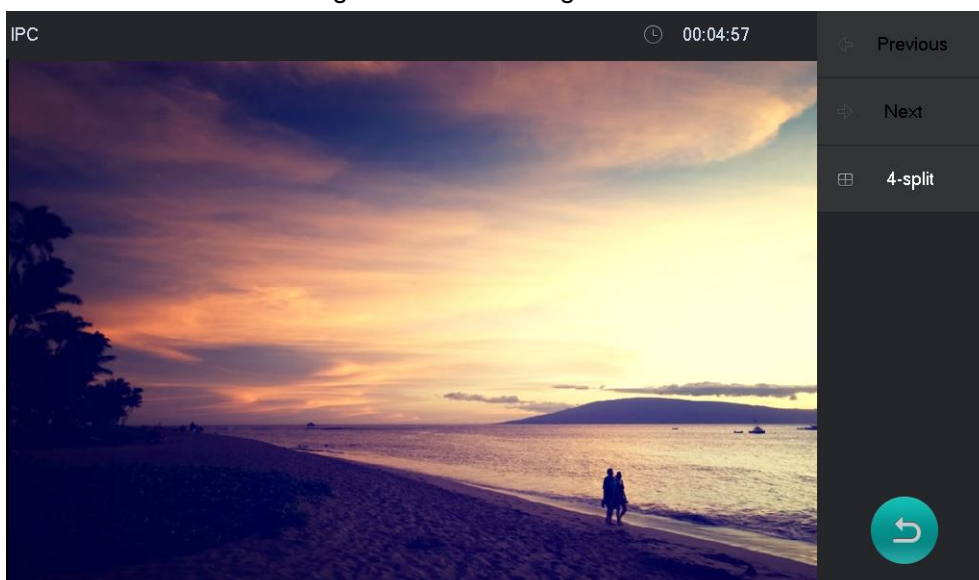
Step 1 Select **Monitor > IPC**.

Figure 4-6 IPC



Step 2 Tap the IPC icon.

Figure 4-7 Monitoring



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

## 4.2.3 VTS

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

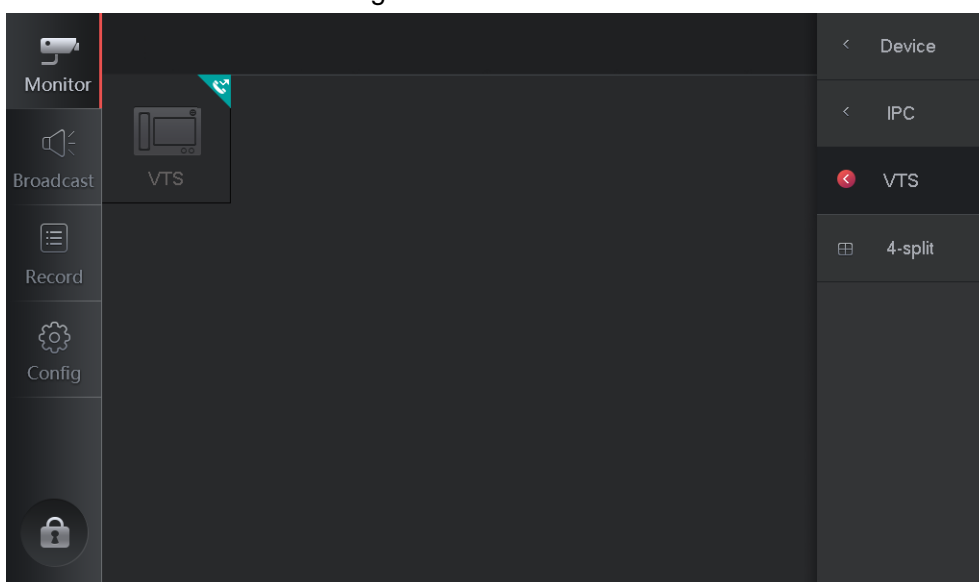
### 4.2.3.1 Call

**Step 1** Select **Monitor > VTS**.



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

Figure 4-8 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 4-10. For details, see Table 4-2.



The camera is not on in Figure 4-10; when the camera is on, there will be monitoring image on the interface.

Figure 4-9 Calling

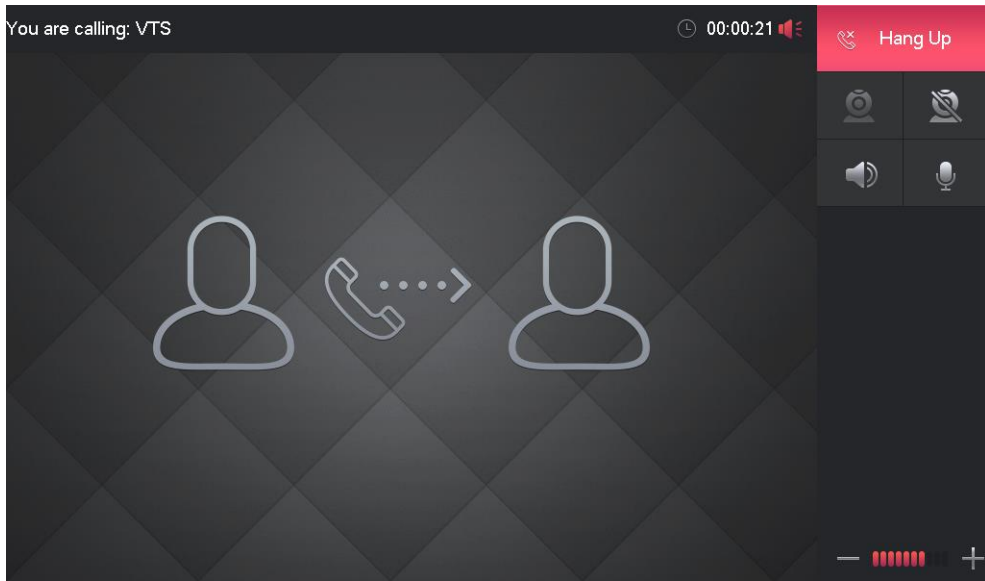


Figure 4-10 Talking

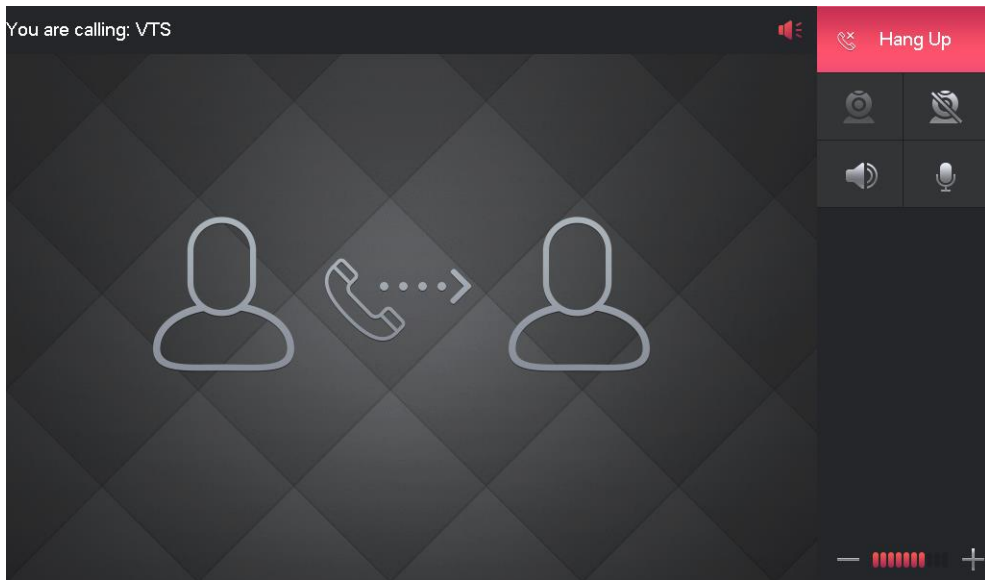














Table 4-2 Icon description

| Icon  | Meaning   |
|---|---|
|  | Tap  to allow the other device monitoring the local video.       |
|  | Tap  to forbid 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. |
|  | Adjust the talking volume.  |

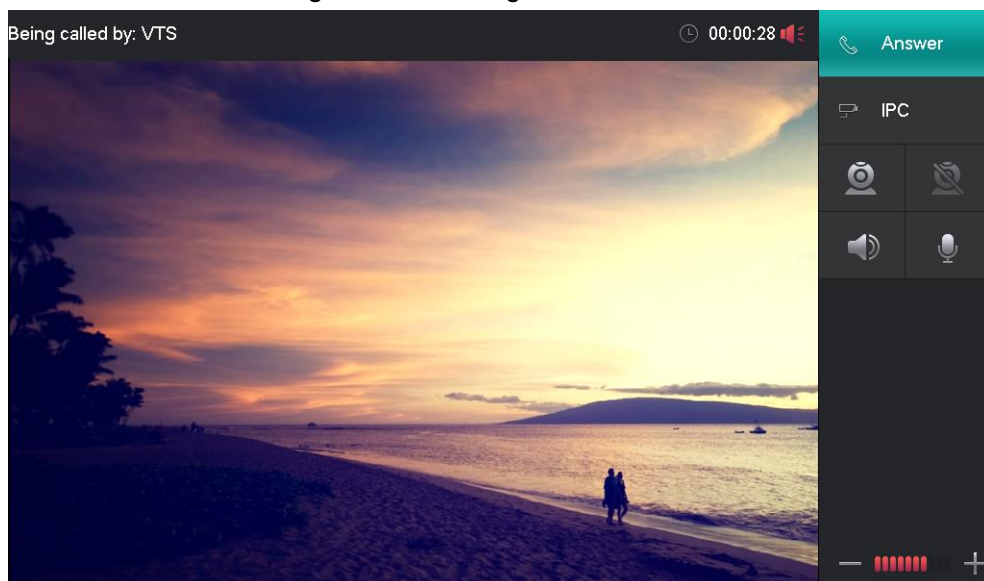


| Icon  | Meaning  |
|---|--|
|  | <p>  indicates that the VTS is in handsfree mode; when you use handset, the icon changes to .                 </p> |

### 4.2.3.2 Answer

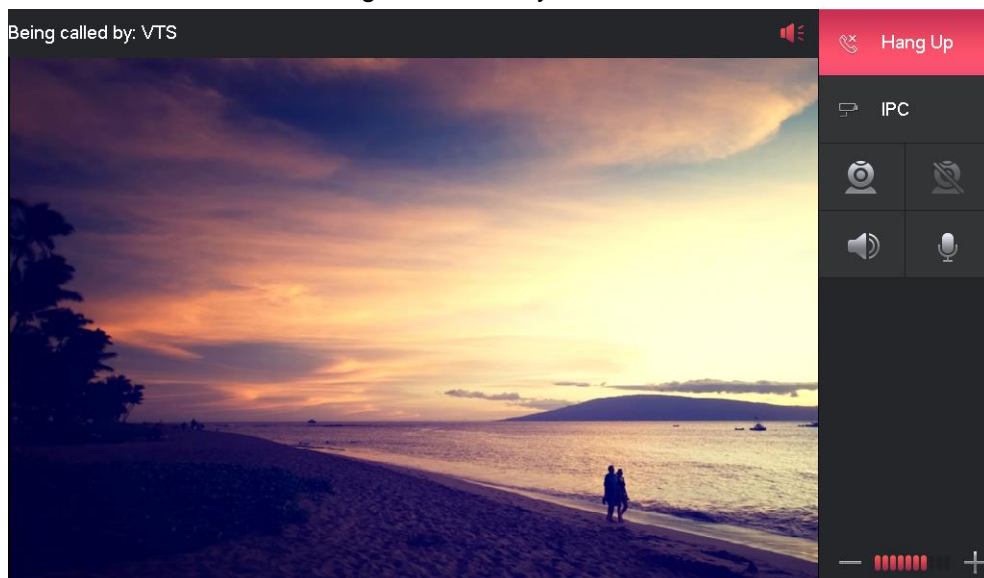
When VTS calls, the answering interface is displayed.

Figure 4-11 Calling status



**Step 1** Tap **Answer** or the handsfree button on the device to answer the call. See Figure 4-12. For details, see Table 4-2.

Figure 4-12 Busy




**Step 2** (Optional) Tap **IPC** to enter the device list. See Figure 4-13. Select an IPC to do monitoring. Tap  to go to the calling interface.

Figure 4-13 IPC monitoring



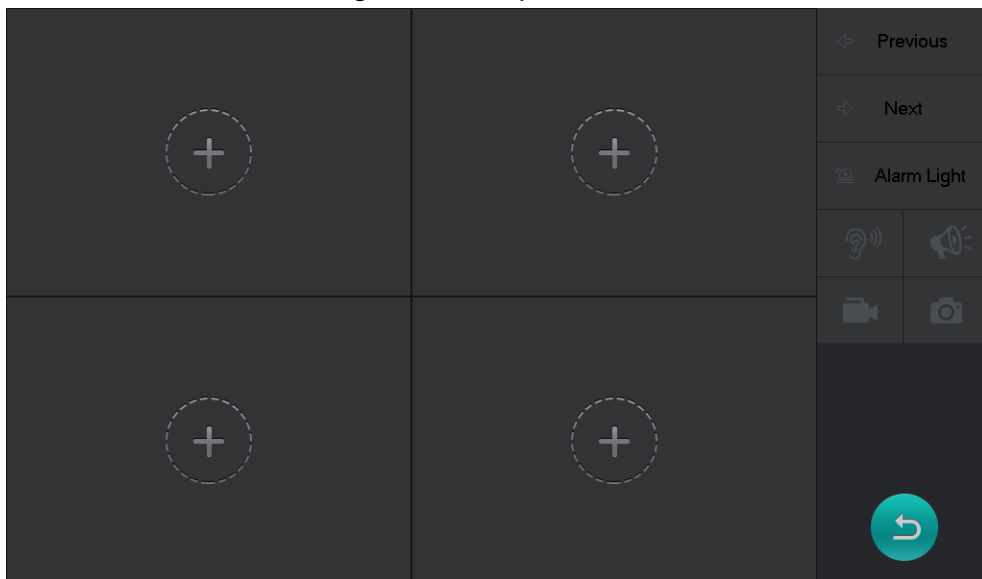
Step 3 Tap **End** to end the call.

## 4.2.4 4-split

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

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

Figure 4-14 4-split




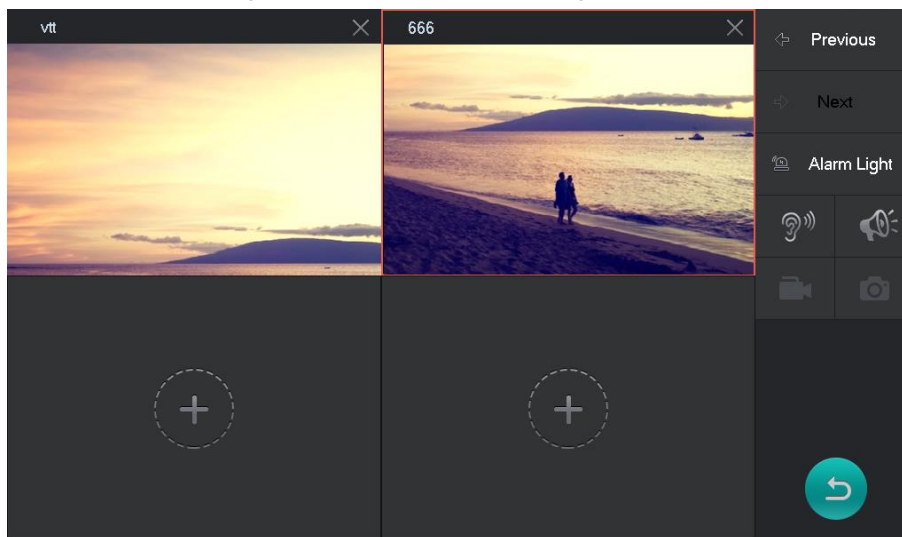
Step 2 Tap , and select the terminal or IPC as needed.

Figure 4-15 4-Split monitoring



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

# 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.