

Digital VTS

Quick Start Guide






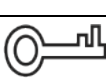

V1.0.0

Foreword

This manual introduces the structure and configuration of digital VTS. Read carefully before using the VTS, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	November 2022

Privacy Protection Notice

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

About the Manual

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

format) cannot be opened.

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

Important Safeguards and Warnings

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

Operation Requirements



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

Installation Requirements



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



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

Table of Contents

Foreword	I
Important Safeguards and Warnings.....	III
1 Device Structure.....	1
1.1 Front Panel.....	1
1.2 Rear Panel.....	3
2 Functions Configuration.....	5
2.1 Initializing VTS	5
2.1.1 Initialization through Local Device	5
2.1.2 Initialization through Webpage.....	5
2.2 Building Scenes	6
2.2.1 Configuring VTS	6
2.2.2 Configuring SIP Server.....	7
2.2.3 Adding VTO/Fence Station.....	8
2.3 Industrial Scenes.....	10
2.3.1 Configuring TCP/IP.....	10
2.3.2 Configuring Device Role.....	12
2.3.3 Adding Device	12
2.3.3.1 Adding VTA.....	12
2.3.3.2 Adding Lower-level VTS	14
3 Verification	15
3.1 Verifying Building Scenes	15
3.2 Verifying Industrial Scenes.....	15
Appendix 1 Cybersecurity Recommendations.....	17

1 Device Structure

1.1 Front Panel

Figure 1-1 Front panel

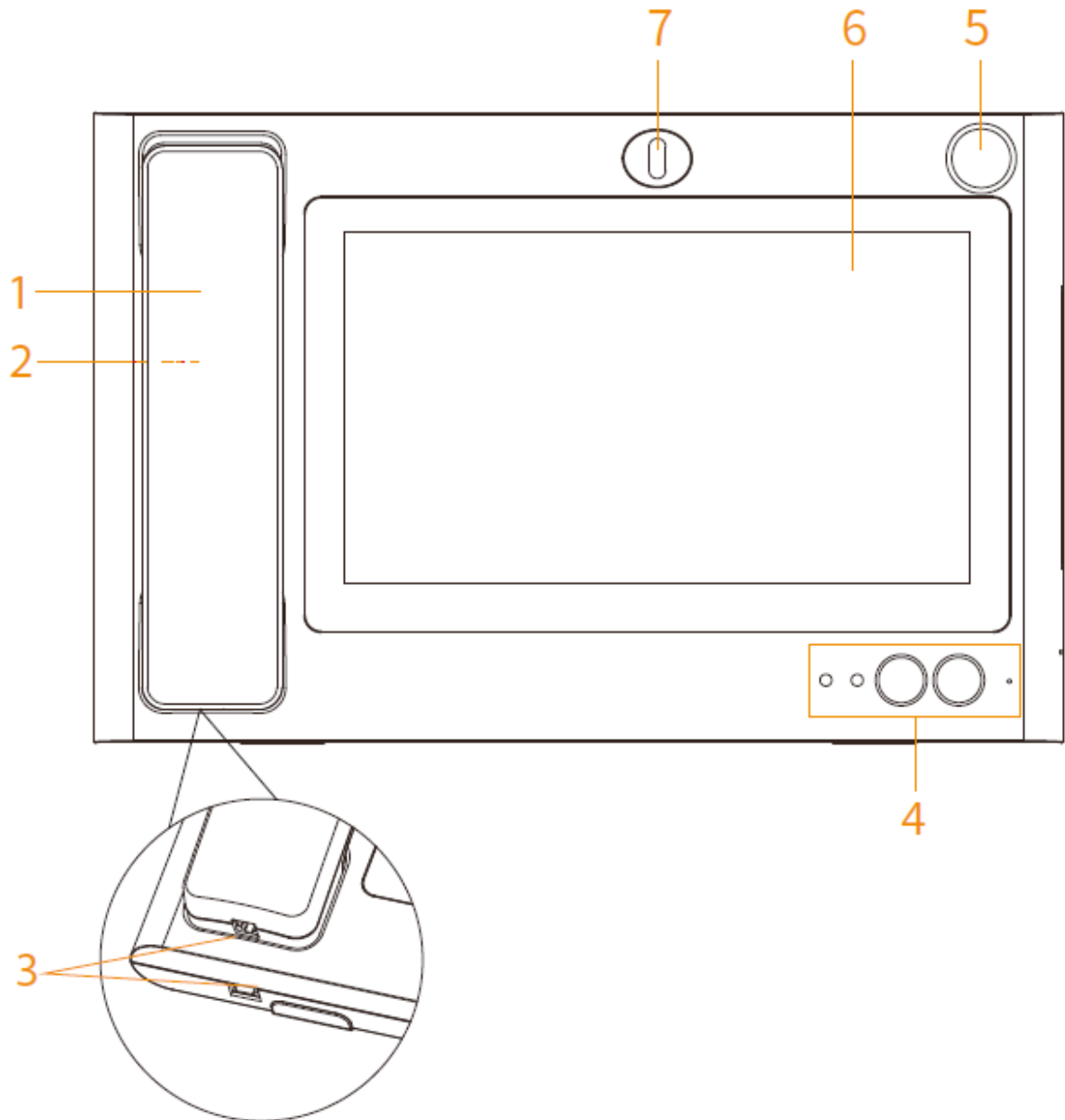





Table 1-1 Front panel description

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

No.	Name	Description
4	Indicator/Button	<p>From left to right:</p> <ul style="list-style-type: none"> ● Power indicator <ul style="list-style-type: none"> ◇ On: The device is powered on. ◇ Off: The device is not connected to the power supply. ● Information indicator <ul style="list-style-type: none"> ◇ On: There is a missed call. ◇ Off: The missed call has been processed or there is no missed call. <p></p> <p>In the industrial scene, if the indicator is on, it indicates that the device has unread alarm records.</p> <ul style="list-style-type: none"> ● Unlock button When you are making calls, watching videos, or talking to others through the VTS, press the unlock button, you can remotely open the door of some front-end devices that support unlocking function. ● Hands-free button Used to answer incoming calls. You can select hands free mode or handset mode. ● Built-in MIC Inputs sound.
5	Gooseneck Microphone Port	<p>Connects to a gooseneck microphone.</p> <p></p> <p>The port is available on select models.</p>
6	Display and Touch	Screen and touch area.
7	Camera	<p>Used to talk with another VTS or the platform.</p> <p></p> <p>The camera is available on select models.</p>

1.2 Rear Panel

Figure 1-2 Rear panel

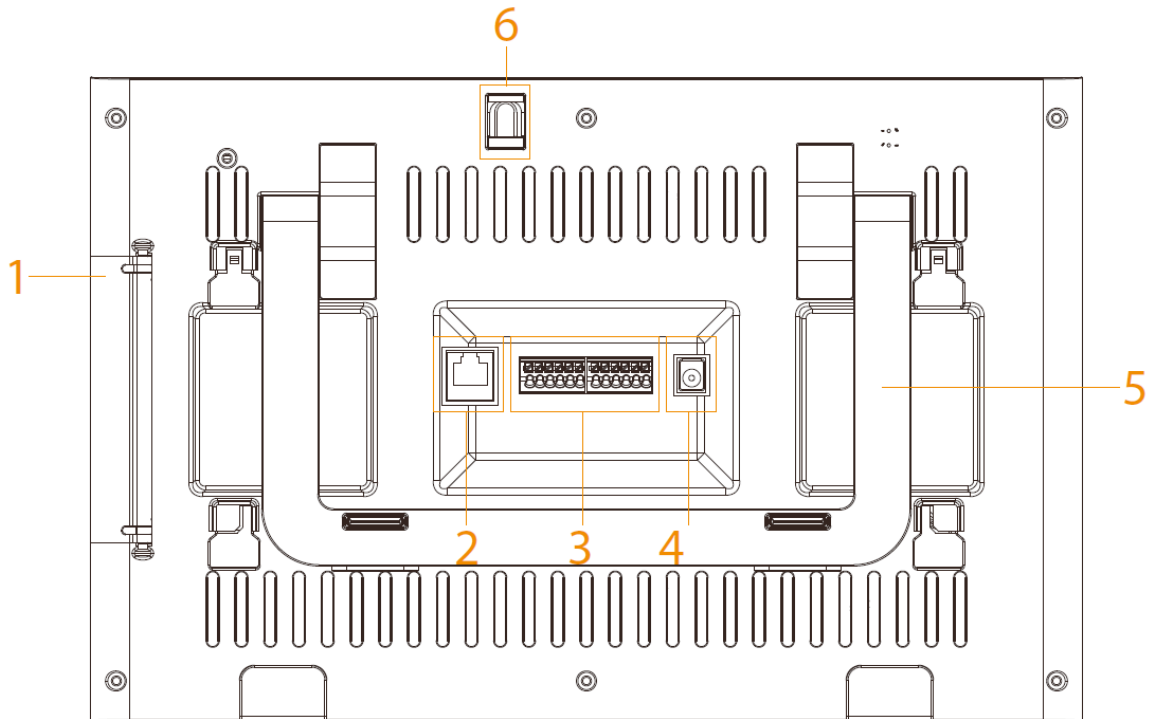



Table 1-2 Rear panel description

No.	Name	Description
1	Port	Open the rear panel and the ports from top to bottom are: <ul style="list-style-type: none"> ● HDMI video transmission port, for video transmission only. ● USB port. ● USB port. ● SD card slot.
2	Network Port	Connects RJ-45 cable.
3	12-pin Port	Ports from left to right are: <ul style="list-style-type: none"> ● Power output port. ● GND. ● Alarm input port 1. ● Alarm input port 2. ● Alarm input port 3. ● Alarm input port 4. ● Power input port. ● GND. ● RS-485A port. ● RS-485B port. ● Alarm output port NO. ● Alarm output port COM.
4	Power Port	12 VDC power.
5	Bracket	Place VTS on the desk. You can adjust the bracket angle to an appropriate position for monitoring.

No.	Name	Description
6	Camera Knob	<p>You can adjust the knob to an appropriate angel for monitoring. You can also hide the camera by adjusting the knob.</p>  <p>The knob is available on select models.</p>

2 Functions Configuration

2.1 Initializing VTS

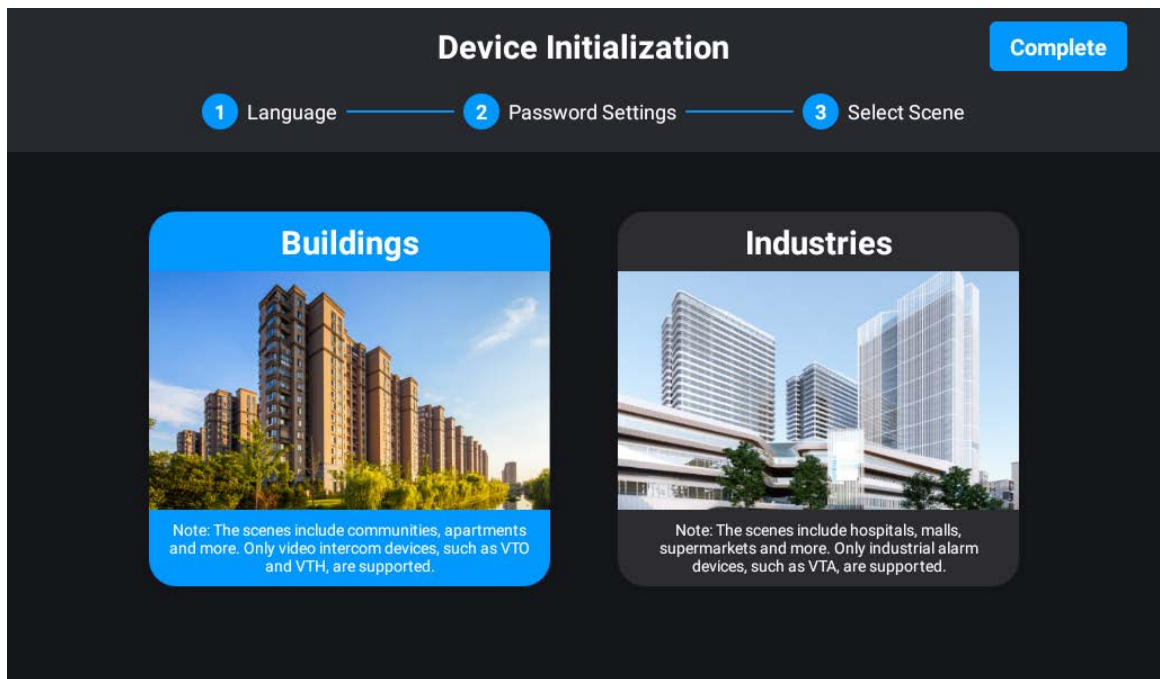
For the first time use or use after resetting, you need to initialize VTS. This chapter introduces initialization through local device and webpage.

2.1.1 Initialization through Local Device

Procedure

- Step 1 Power on the VTS.
- Step 2 Select the language.
- Step 3 Configure password and enter e-mail address.
- Step 4 Select **I have read and agree to the terms and conditions and accept privacy policy and license agreement**, and then tap **Next**.
- Step 5 Select the scene depending on your needs.

Figure 2-1 Initialization through local device



- Step 6 Tap **Complete**.

2.1.2 Initialization through Webpage

Procedure

- Step 1 Enter the IP address of VTS in a browser, and then click **Enter**.
- Step 2 Select the language.
- Step 3 Select **I have read and agree to the terms and conditions and accept privacy policy and license agreement**, and then click **Next**.
- Step 4 Configure password and enter e-mail address, and then click **Done**.
- Step 5 Enter the username and password, and then click **Log in**.

Step 6 Select the scene and click **OK** on the webpage.

2.2 Building Scenes

The building scenes include communities, apartments and more. Only video intercom devices, such as VTO and VTH, are supported. This chapter introduces local operations of VTS.

2.2.1 Configuring VTS

Configure the number and network parameters of VTS.

Procedure



- Step 1 Select **Settings** >  > **Project Setting** on the home screen.
- Step 2 Enter the password you have configured during initialization and tap **OK**.
- Step 3 Tap  and configure the parameters.

Figure 2-2 Configure the parameters

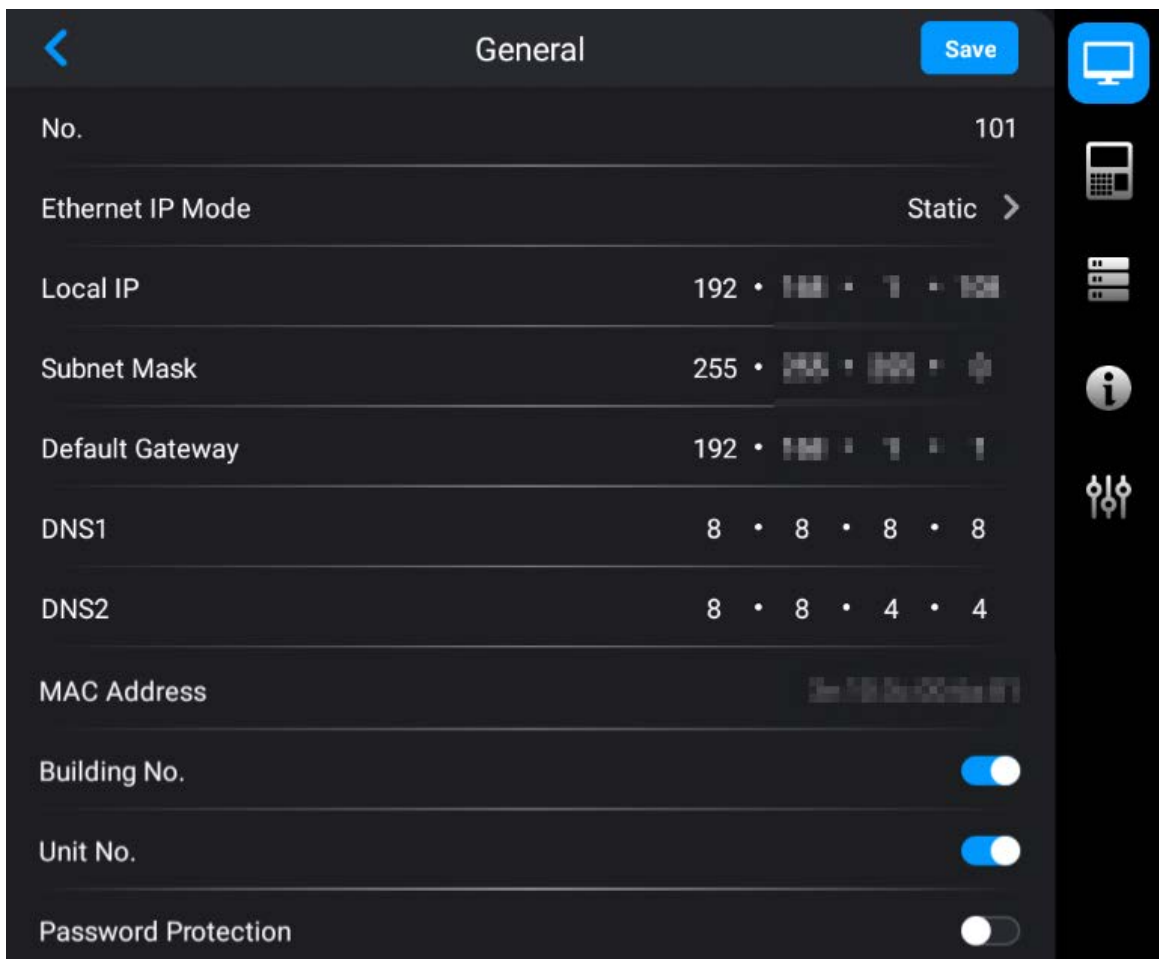



Table 2-1 Parameters description

Parameter	Description
No.	User-defined. You can configure the number from 101 to 999.

Parameter	Description
Ethernet IP Mode	Configure the mode to get the IP. <ul style="list-style-type: none"> • Static: Manually set Local IP, Subnet Mask and Default Gateway. • DHCP (Dynamic Host Configuration Protocol): Select DHCP if there is a DHCP server. The device automatically gets dynamic IP address.
Local IP	If you select Static in Ethernet IP Mode , configure the IP address, subnet mask and default gateway according to the network planning.
Subnet Mask	
Default Gateway	
DNS 1	IP address of DNS server.
DNS 2	Standby IP address of DNS server.
Building No.	<ul style="list-style-type: none"> • If the platform is used as the SIP server, make sure that the configuration status of building and unit number is the same in the platform, VTS and VTO. • If the VTO is used as the SIP server, make sure that the configuration status of building and unit number is the same in VTS and VTO.  <p>You cannot get the device information of VTO on the monitoring screen.</p>
Unit No.	
Password Protection	Switch on password protection. The password is transferred in encryption when the device is registered on the platform through SIP.

2.2.2 Configuring SIP Server

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

Procedure



- Step 1 Select **Setting** >  > **Project Setting** on the home screen.
- Step 2 Enter the password you have configured during initialization and tap **OK**.
- Step 3 Tap  and configure the parameters.

Figure 2-3 Configure the parameters



Table 2-2 Parameters description

Parameter	Description
IP Address	IP address of SIP server.
Network Port	Network port number of SIP server. <ul style="list-style-type: none"> • VTO as the SIP server: 5060. • The platform as the SIP server: 5080.
Username	Default.
Password	Default.
Domain Name	Keep consistent with the SIP server as VDP by default.

Step 4 Tap **Save**.

2.2.3 Adding VTO/Fence Station

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

Procedure



- Step 1 Select **Settings** >  > **Project Setting** on the home screen.
- Step 2 Enter the password that you configured during initialization and tap **OK**.
- Step 3 Select  > **Add device**.
- Step 4 Add VTO or fence station.
 - Add VTO or fence station one by one.

Figure 2-4 Add VTO or fence station one by one

The screenshot shows a dark-themed 'Add Device' form. At the top left is a back arrow, and at the top right is a 'Save' button. The form contains the following fields:

- Device Type:** Door Station (with a right arrow)
- Add Mode:** Add One by One (with a right arrow)
- Name:** 20 characters at most
- Medium Number:** (empty field)
- IP Address:** 0 • 0 • 0 • 0
- Username:** 32 characters at most
- Password:** 32 characters at most (with an eye icon for visibility)
- Network Port:** 5000
- Enable:** A toggle switch that is currently turned off.

- Add VTO or fence stations in batches.


Figure 2-5 Add VTO or fence stations in batches

The screenshot shows a dark-themed 'Add Device' form. At the top left is a back arrow, and at the top right is a 'Save' button. The form contains the following fields:

- Device Type:** Door Station (with a right arrow)
- Add Mode:** Add in Batches (with a right arrow)
- Start IP:** 0 • 0 • 0 • 0
- End IP:** 0 • 0 • 0 • 0
- Username:** 32 characters at most
- Password:** 32 characters at most (with an eye icon for visibility)

Table 2-3 Parameters description

Parameter	Description
Device Type	You can select VTO, fence station or IPC.

Parameter	Description
Add Mode	Supports adding devices one by one or in batches.  Only VTO supports adding devices in batches.
Name	User-defined. You can configure the name that distinguishes the device.
Medium Number	Cannot be edited.
IP Address	The IP, username and password of the device that you added.
Username	
Password	
Enable	After switching on, select Monitor > ALL to monitor the screen.
Start IP	The start and end IP address of the device if you add devices in batches.
End IP	

Step 5 Tap **Save**.

2.3 Industrial Scenes

The industrial scenes include hospitals, malls, supermarkets and more. Only industrial alarm devices, such as VTA, are supported. This chapter introduces operations on the webpage of the VTS.

2.3.1 Configuring TCP/IP

Procedure


- Step 1 Log in to the device webpage.
- Step 2 Select **Network Settings** > **TCP/IP**.
- Step 3 Configure the parameters.

Figure 2-6 Configure the parameters

The screenshot shows a network configuration form with the following fields and controls:

- NIC:** A dropdown menu currently set to "NIC 1".
- Mode:** Two radio buttons, "Static" (selected) and "DHCP".
- MAC Address:** A field with a grid of input boxes for hexadecimal characters.
- IP Version:** A dropdown menu currently set to "IPv4".
- IP Address:** A field with a grid of input boxes for IP address octets.
- Subnet Mask:** A field with a grid of input boxes for subnet mask octets.
- Default Gateway:** A field with a grid of input boxes for the default gateway IP address.
- Preferred DNS:** A field with a grid of input boxes for the preferred DNS server IP address.
- Alternate DNS:** A field with a grid of input boxes for the alternate DNS server IP address.
- MTU:** A text input field containing the value "1500".
- Buttons:** "Apply" (blue), "Refresh", and "Default" (grey).

Table 2-4 Parameters description

Parameter	Description
Mode	<ul style="list-style-type: none"> • Static: Manually configure IP, Subnet Mask and Default Gateway. Click Apply and the webpage automatically goes to the login page of the IP that you configured. • DHCP (Dynamic Host Configuration Protocol): Select DHCP if there is a DHCP server. The device automatically gets a dynamic IP address.
MAC Address	MAC (Media Access Control) address of the device.
IP Version	IPv4 as default.
IP Address	If you select Static in Mode , enter the IP address, subnet mask and default gateway according to the network planning.  IP address and default gateway should be on the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of DNS server.
Alternate DNS	Alternate IP address of DNS server.

Step 4 Click **Apply**.

2.3.2 Configuring Device Role

Procedure

- Step 1** Log in to the device webpage.
- Step 2** Select **System > General**.
- Step 3** Configure the parameters.

Figure 2-7 Configure the parameters

The screenshot shows a configuration form with three input fields and three buttons. The 'Device Role' field is a dropdown menu currently set to 'Lower-level VTS'. The 'Device Name' field is a text box containing 'VTS'. The 'Device No.' field is a text box containing '101'. Below the fields are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Table 2-5 Parameters description

Parameter	Description
Device role	Select from lower-level VTS, upper-level VTS and platform client. The information saved on the device will be cleared after you change the device role. <ul style="list-style-type: none">• Lower-level VTS: Used as the lower-level VTS if there is no platform. It has the management permission of the device.• Upper-level VTS: Used as the upper-level VTS if there is no platform. It has permissions to add lower-level VTS. It does not have permission to manage organizational structure.• Platform client: Used as the platform client if there is the platform. It does not have the management permission of the device.
Device name	You can configure the name that distinguishes the device.
Device No.	You can configure the number from 101 to 999.

- Step 4** Click **Apply**.

2.3.3 Adding Device

- If the device is used as the lower-level VTS, you can add VTA.
- If the device is used as the upper-level VTS, you can add lower-level VTS.

2.3.3.1 Adding VTA

Procedure

- Step 1** Log in to the webpage of the device.
- Step 2** Select **Device Setting > Terminal Management**.
- Step 3** Click **Add**, and then configure the parameters.

Figure 2-8 Add VTA

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and values:

- Device No.: 1010002
- Device Type: VTA (dropdown menu)
- Group: test
- Device Name: Alarm
- Device Model: VTA
- Upper Level: VTS
- Add Mode: IP Address (dropdown menu)
- IP Address: [] . [] . [] . []
- Username: admin
- Password: [masked with dots]

At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (white).

Table 2-6 Parameters description

Parameter	Description
Group	Select Monitor > Terminal Management on local VTS, and then you can view the devices of the group that you configured.
Device name	User-defined.
Device model	Enter the complete device model that you can get from the device label.
Add mode	You can add VTA in the following 2 ways. <ul style="list-style-type: none"> ● IP address: Enter the IP address of the device. ● Register: Configure the parameters for registering on the device.
Username	Enter the username and password of the device that you added.
Password	

Step 4 Click **OK**.

2.3.3.2 Adding Lower-level VTS

Procedure

- Step 1 Log in to the webpage of the device.
- Step 2 Select **Device Setting > Terminal Management**.
- Step 3 Click **Add**.
- Step 4 Enter IP address, username and password of the VTS.

Figure 2-9 Add lower-level VTS

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields:

- Upper Level:** A text input field containing the text "VTS".
- Add Mode:** A dropdown menu currently showing "IP Address".
- IP Address:** A text input field containing a dotted pattern representing an IP address.
- Username:** A text input field containing the text "admin".
- Password:** A password input field containing a series of dots.

At the bottom right of the dialog, there are two buttons: a blue "OK" button and a white "Cancel" button.

- Step 5 Click **OK**.

3 Verification

3.1 Verifying Building Scenes

You can call VTH and VTO on the VTS.

Call VTH


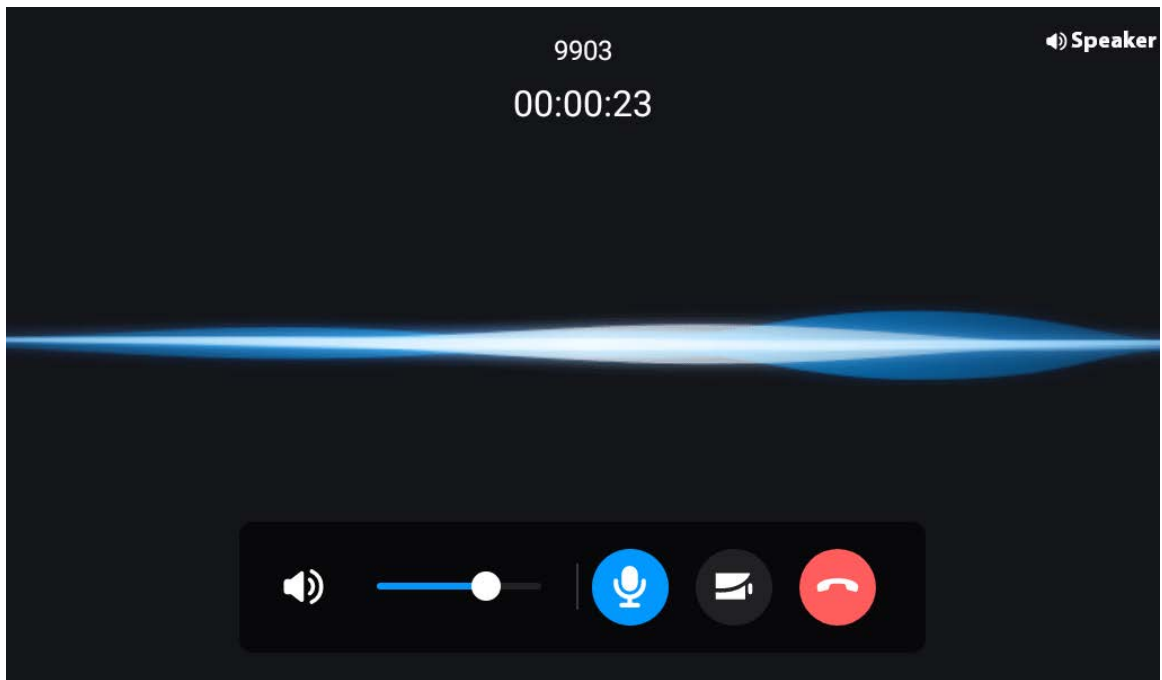
Tap **Call** on the home screen of the VTS. Enter the number of VTH, and then tap .

Figure 3-1 Call VTH



Monitor VTO

Tap **Monitor** on the home screen of the VTS, and then tap the icon of VTO to monitor VTO.

3.2 Verifying Industrial Scenes

- If VTS is used as the lower-level VTS, it supports monitoring and calling VTA. You can also call VTS through VTA and answer the call on VTS.
- If VTS is used as the upper-level VTS, it supports monitoring and calling VTA. Tap **Monitor** on the home screen of the VTS. Tap the icon of VTA to monitor VTA.

Figure 3-2 Monitor VTA



Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

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

2. Update Firmware and Client Software in Time

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

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

1. Physical Protection

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

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

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

4. Enable Account Lock

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

5. Change Default HTTP and Other Service Ports

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

6. Enable HTTPS

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

7. MAC Address Binding

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

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a

minimum set of permissions to them.

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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