Video Door Phone (Version 4.7)

Quick Start Guide

V1.0.0

Foreword

This manual introduces the common configuration of intercom devices. Read carefully before using the device, 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.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	May 2024

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguard and Warnings

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

Installation Requirements

 WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Please follow the electrical requirements to power the device.
  - ◇ Following are the requirements for selecting a power adapter.
    - ○ The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - ○ The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - ○ When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - ◇ We recommend using the power adapter provided with the device.
  - ◇ When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The device must be installed at a height of 2 meters or below.

Operation Requirements

 DANGER

Battery Pack Precautions

Preventive measures (including but not limited to):

- Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.

- Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
- Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Transport, use and store the device under allowed humidity and temperature conditions.
- If the device is powered off for longer than a month, it should be placed in its original package and sealed. Make sure to keep it away from moisture, and store it under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.

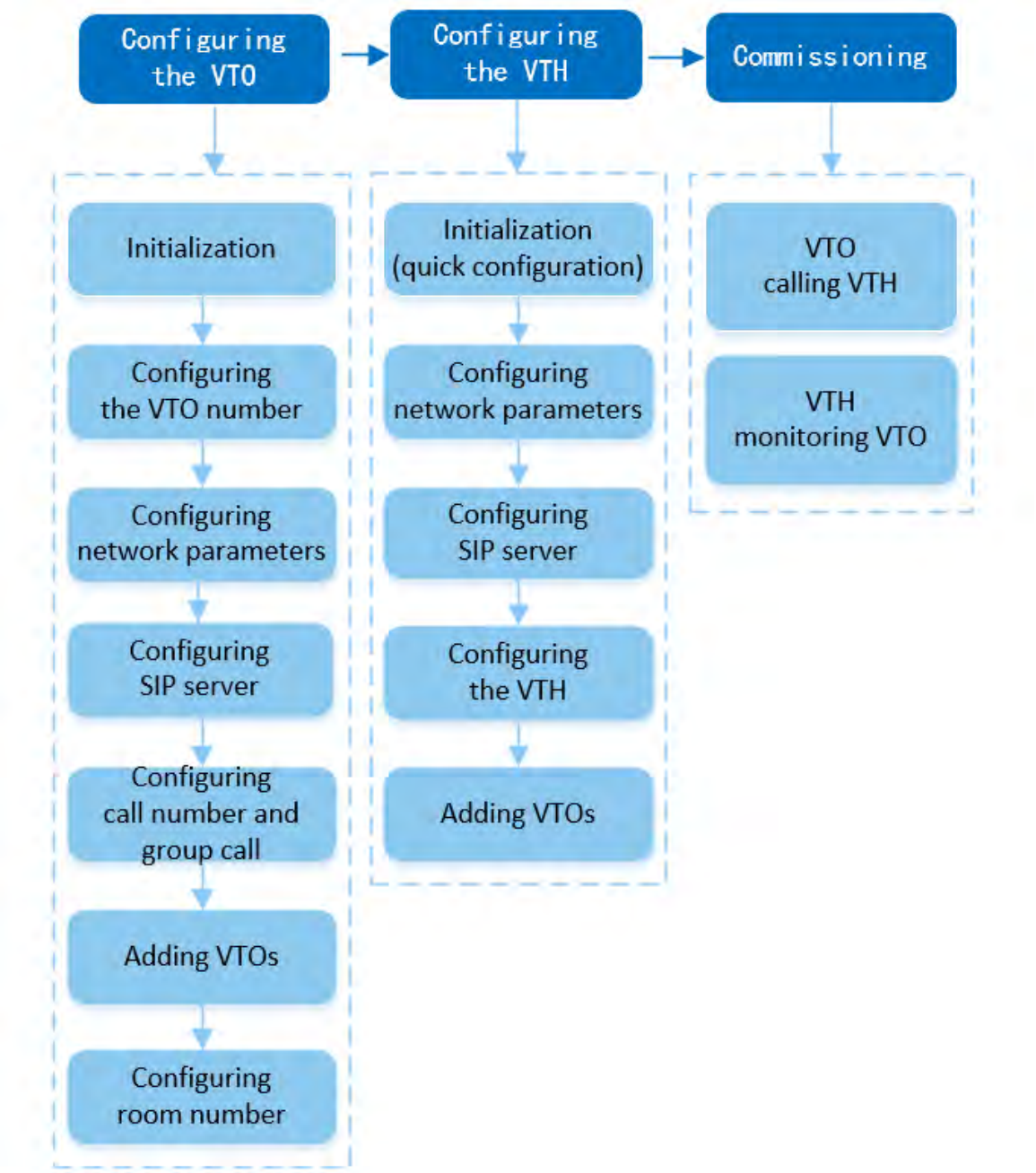
Table of Contents

1 Common Configuration

Follow the configuration procedure and carry out commissioning to ensure that the device can realize basic network access, call and monitoring functions.

1.1 Basic Configuration Procedure

Figure 1-1 Basic configuration procedure



1.2 Preparation

Before the configuration:

- Make sure that there are no short or open circuit in the VTO and VTH.
- Plan IP addresses and numbers (works as phone numbers) for every VTO and VTH.
- Make sure that the VTH and VTO are on the same network segment.

2 VTO Configuration

2.1 Initialization

For first-time login, you need to initialize the VTO.

Prerequisites

Make sure that the computer and the VTO are on the same network segment.

Procedure

Step 1 Turn on the VTO.

Step 2 Enter the IP address of the VTO in the browser.

For first-time login, enter the default IP (192.168.1.108). If you have multiple VTOs, we recommend you change the default IP address to avoid a conflict.

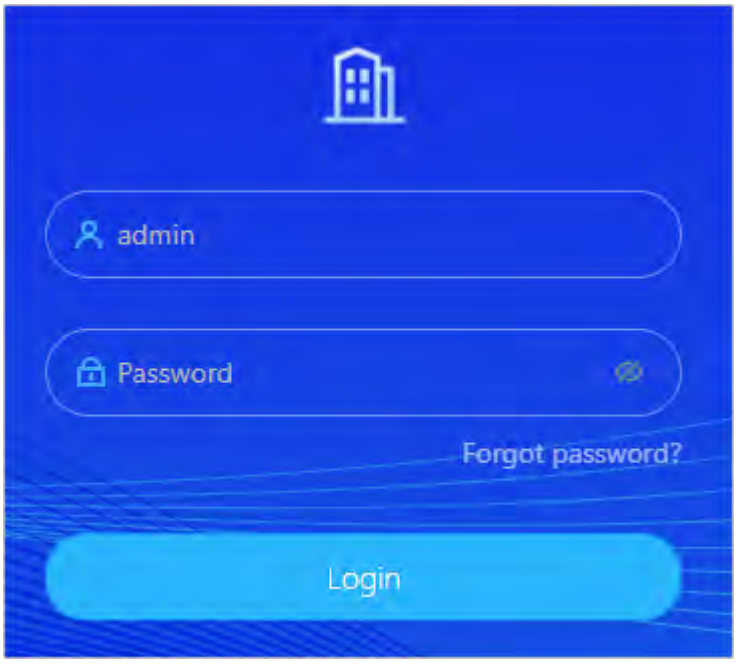
Step 3 Enter and confirm the new password, and then click **Next**.

Step 4 Select **Email** and enter the email address to use to reset your password.

Step 5 Click **Next** , and then click **OK** to go to the login page.

Step 6 Enter username and the new password to log in to the webpage.

Figure 2-1 Login



2.2 Configuring the VTO Number

Configure basic settings of the VTO.

Procedure

Step 1 Log in to the webpage of the VTO.

Step 2 Select **Local Device Config** > **Basic Settings**.

Step 3 Configure the parameters.

Figure 2-2 Basic settings

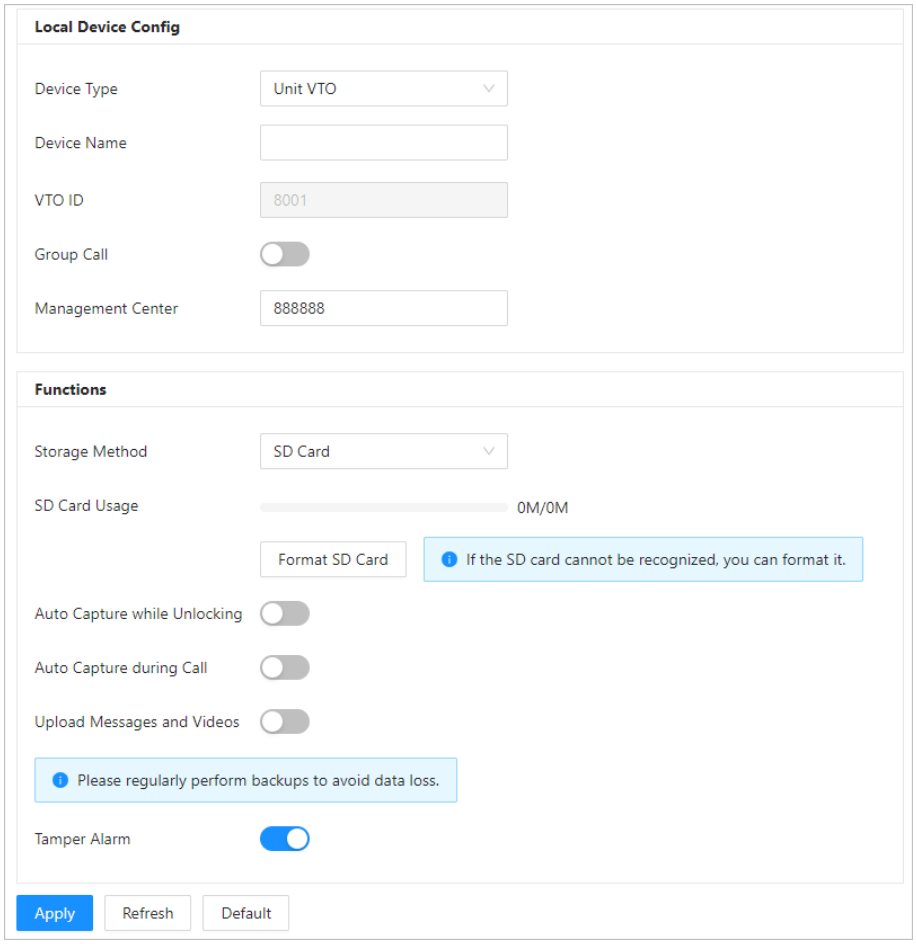


Table 2-1 Basic parameter description

Parameter	Description
Device Type	Select the device type.
Device Name	When other devices are monitoring this VTO, the device name will appear on the monitoring image.
VTO ID	Used to differentiate each VTO, and we recommend you set it according to unit or building number, and then you can add VTOs to the SIP server by using their numbers. The number cannot be changed when the VTO serves as the SIP server.
Group Call	Enable it on the VTO that works as the SIP server, and when a main VTH receives a call, all extension VTHs will also receive the call.
Management Center	888888 by default.
Storage Method	SD card by default.

Parameter	Description
SD Card Usage	Displays the total and used capacity of the SD card. You can click **Format SD Card** to delete all the data in the SD card.
Auto Capture while Unlocking	Take a snapshot and save it in the SD card of the VTO when the VTO is unlocking.
Auto Capture during Call	Take a snapshot and save it in the SD card of the VTO when the VTO is calling.
Upload Messages and Videos	When enabled: • If an SD card is inserted in both the VTH and VTO, the video message will be saved both in the SD cards of the VTH and the VTO. • If an SD card is only inserted in the VTH or the VTO, the video message will be saved only in the SD card of the VTH or the VTO. • If no SD card is inserted in the VTH or VTO, no video message will be saved.
Tamper Alarm	Within 5 minutes after the device is powered on, if you continuously press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information.

Step 4 Click **Apply**.

2.3 Configuring Network Parameters

You need to configure IP address of Device to make sure that it can communicate with other devices.

Procedure

Step 1 Log in to the webpage of the VTO.

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

Step 3 Configure the parameters.

Figure 2-3 TCP/IP

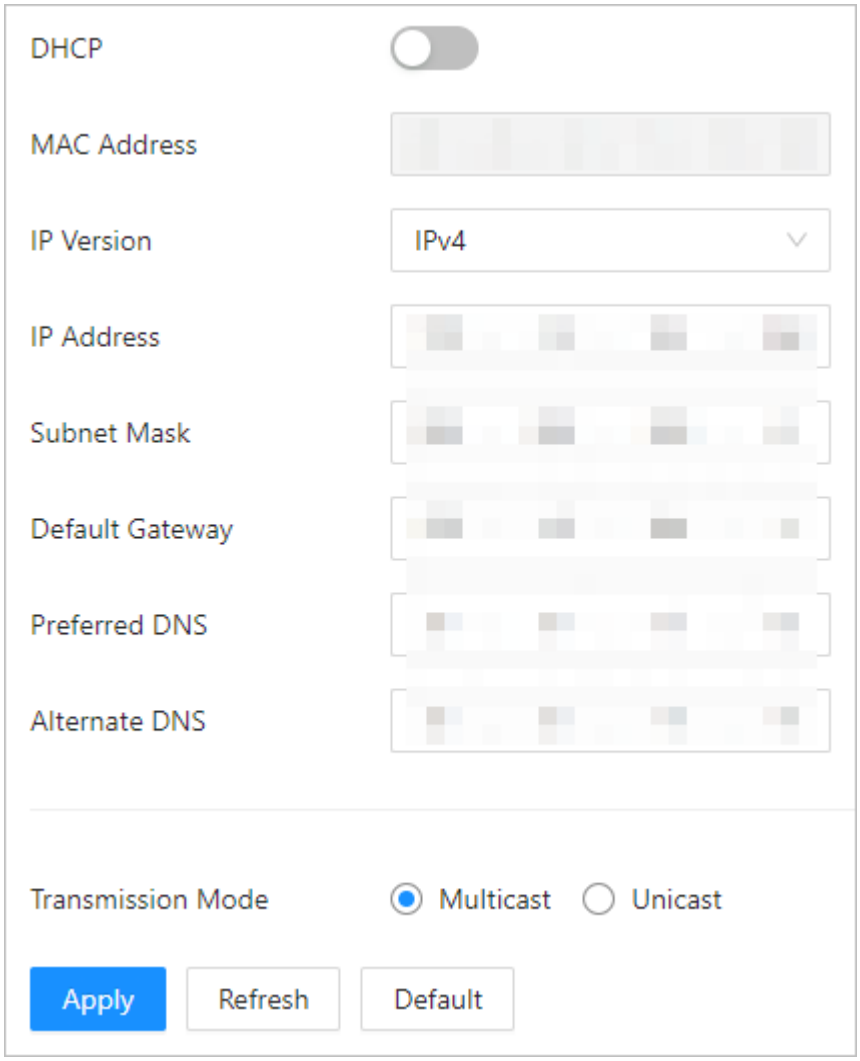


Table 2-2 Description of TCP/IP parameters

Parameter	Description
Mode	DHCP stands for Dynamic Host Configuration Protocol. ● When not enabled, manually enter IP address, subnet mask, and gateway. ● When enabled, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.

Parameter	Description
IP Address	If you set the mode to **Static**, configure the IP address, subnet mask and gateway.  • IPv6 address is represented in hexadecimal. • IPv6 version do not require setting subnet masks. • The IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
Transmission Mode	• Multicast: Ideal for video talk. • Unicast: Ideal for group call.

Step 4 Click **Apply**.

2.4 Configuring the SIP Server

When connected to the same SIP server, all the VTOs and VTHs can call each other. You can use a VTO or another server as the SIP server.

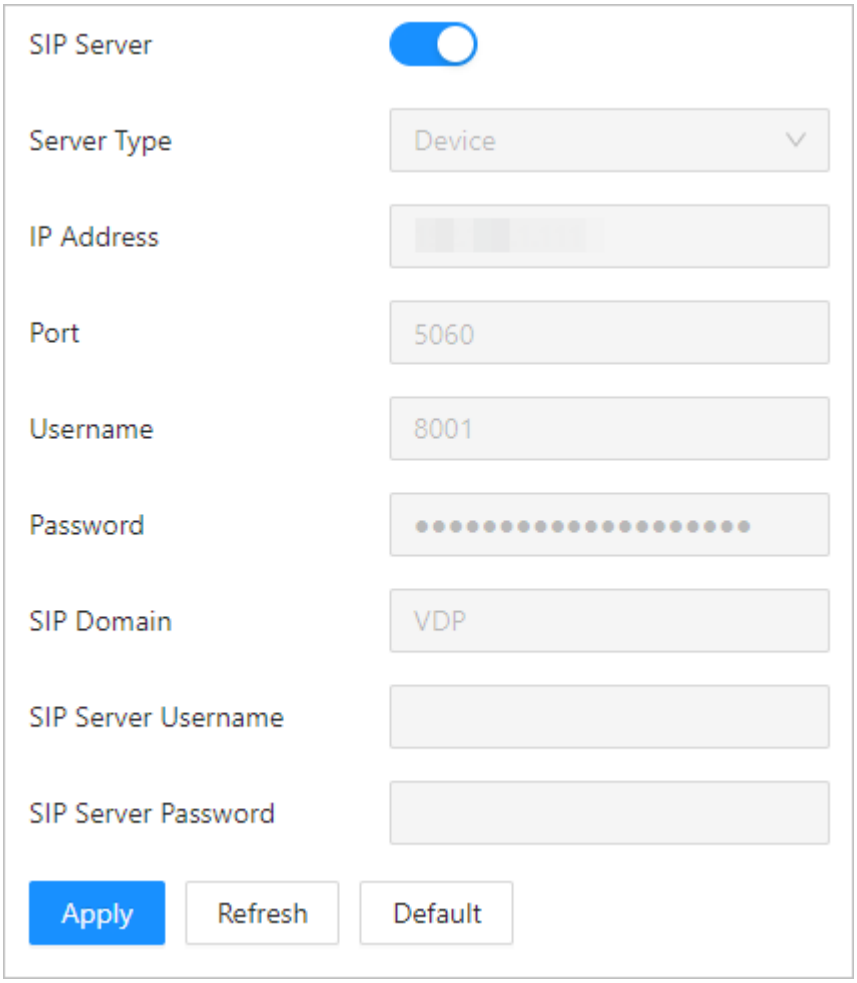
2.4.1 VTO as the SIP Server

Procedure

Step 1 Log in to the webpage of the VTO.

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

Figure 2-4 VTO as the SIP server



Step 3 Configure the parameters.

- If the current VTO works as the SIP server, enable **SIP Server** , and then click **Apply**.

  The VTO will automatically restart, and then you can add other VTOs and VTHs to this VTO.
- If another VTO is working as the SIP server, set **Server Type** as **Device**, configure the parameters, and then click **Apply**.

Table 2-3 SIP server configuration

Parameter	Description
IP Address	The IP address of the VTO that works as the SIP server.
Port	5060 by default when the VTO works as an SIP server.
Username	Default.
Password	
SIP Domain	Default.
SIP Server Username	The username and password of the SIP server.
SIP Server Password	

2.4.2 Platform as the SIP Server

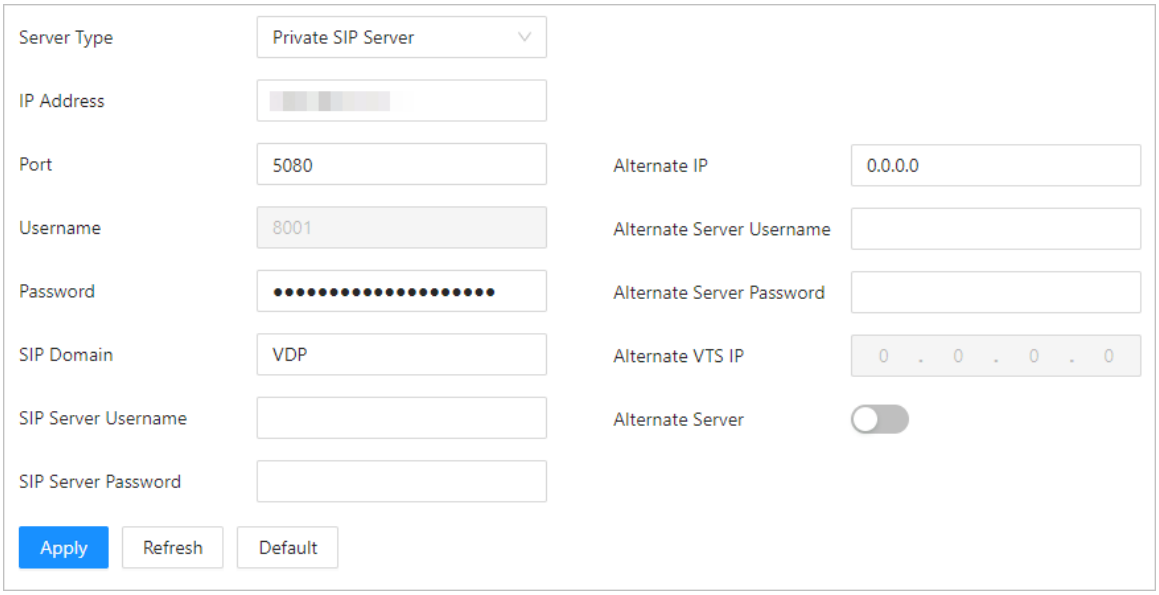
Procedure

Step 1 Log in to the webpage of the VTO.

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

Step 3 Enable **SIP Server** , and then set **Server Type** as **Private SIP Server**.

Figure 2-5 Platform as the SIP server



Step 4 Configure the parameters.

Table 2-4 SIP server configuration

Parameter	Description
IP Address	The IP address of the SIP server.
Port	5080 by default when the platform works as the SIP server.
Username	Default.
Password	
SIP Domain	Keep default value VDP or leave it empty.
SIP Server Username/ Password	The username and password of the SIP server.
Alternate IP	The alternate server will be used as the SIP server when DSSExpress/DSS pro stops responding We recommend you configure the alternate IP address. ● If you enable **Alternate Server**, the current VTO you have logged in serves as the alternate server. ● If you want another VTO serve as the alternate server, you need to enter the IP address of that VTO in the **Alternate IP Addr.** textbox. Do not enable **Alternate Server** in this case.

Parameter	Description
Alternate Username/ Password	Used to log in to the alternate server.
Alternate VTS IP	IP address of the alternate VTS.
Alternate Server	Enable it as needed.

Step 5 Click **Apply**.

2.5 Adding the VTO

Procedure

Step 1 Log in to the webpage of the VTO.

Step 2 Select **Device Setting**.

Figure 2-6 Device setting

Step 3 Click **Add** , select **Door Station** as the device type, and then configure the parameters.

The SIP server must be added.

Figure 2-7 Add a VTO

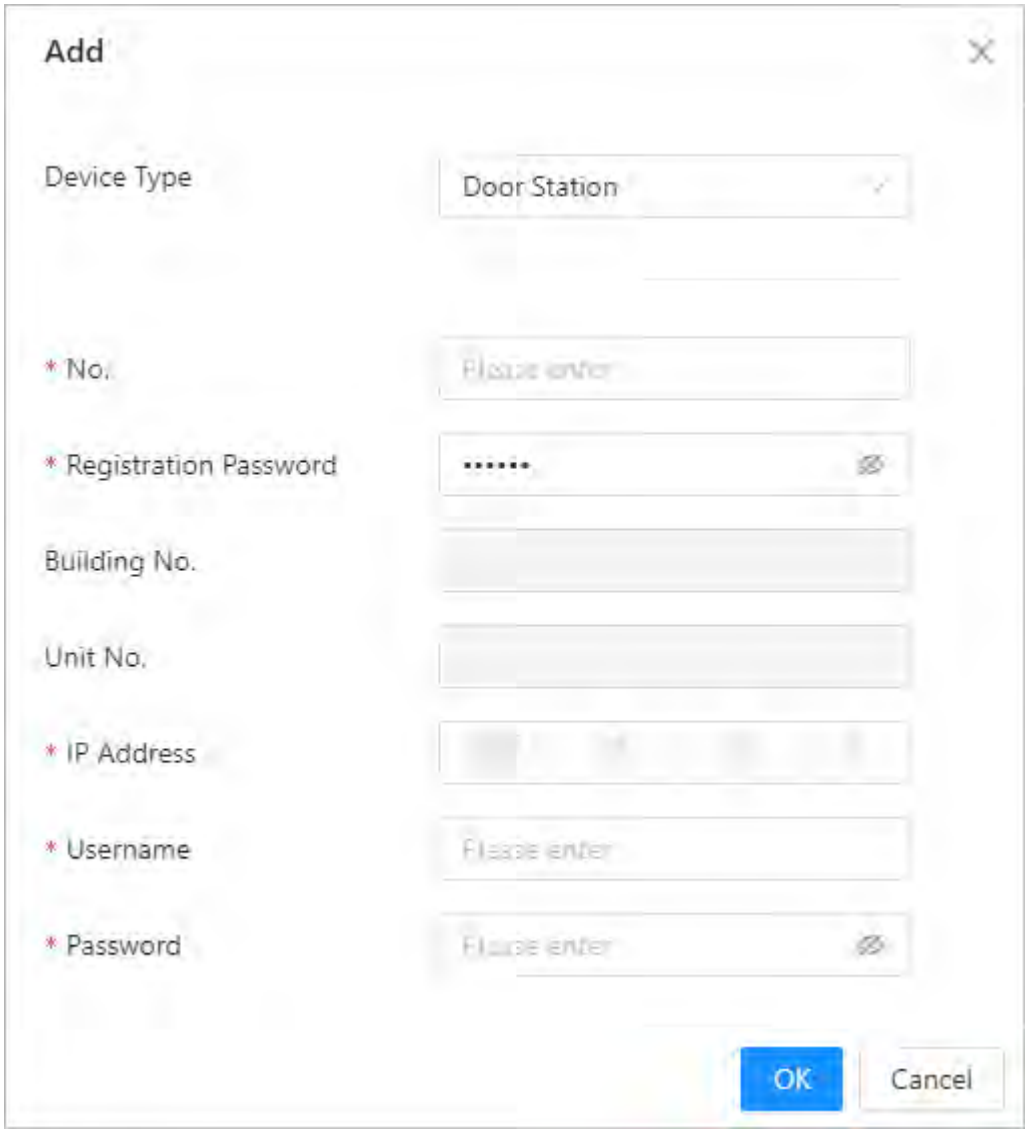


Table 2-5 VTO parameters description

Parameter	Description
No.	VTO number.
Registration Password	Default.
Build No.	Cannot be edited.
Unit No.	
IP Address	VTO IP address.
Username	The username and password of the webpage of the VTO.
Password	

Step 4 Click **OK**.

2.6 Adding the VTH

Procedure

Step 1 Log in to the webpage of the VTO.

Step 2 Select **Device Setting**.

Step 3 Click **Add** , select **VTH** as the device type, and then configure the parameters.

The SIP server must be added.

Figure 2-8 Add a VTH

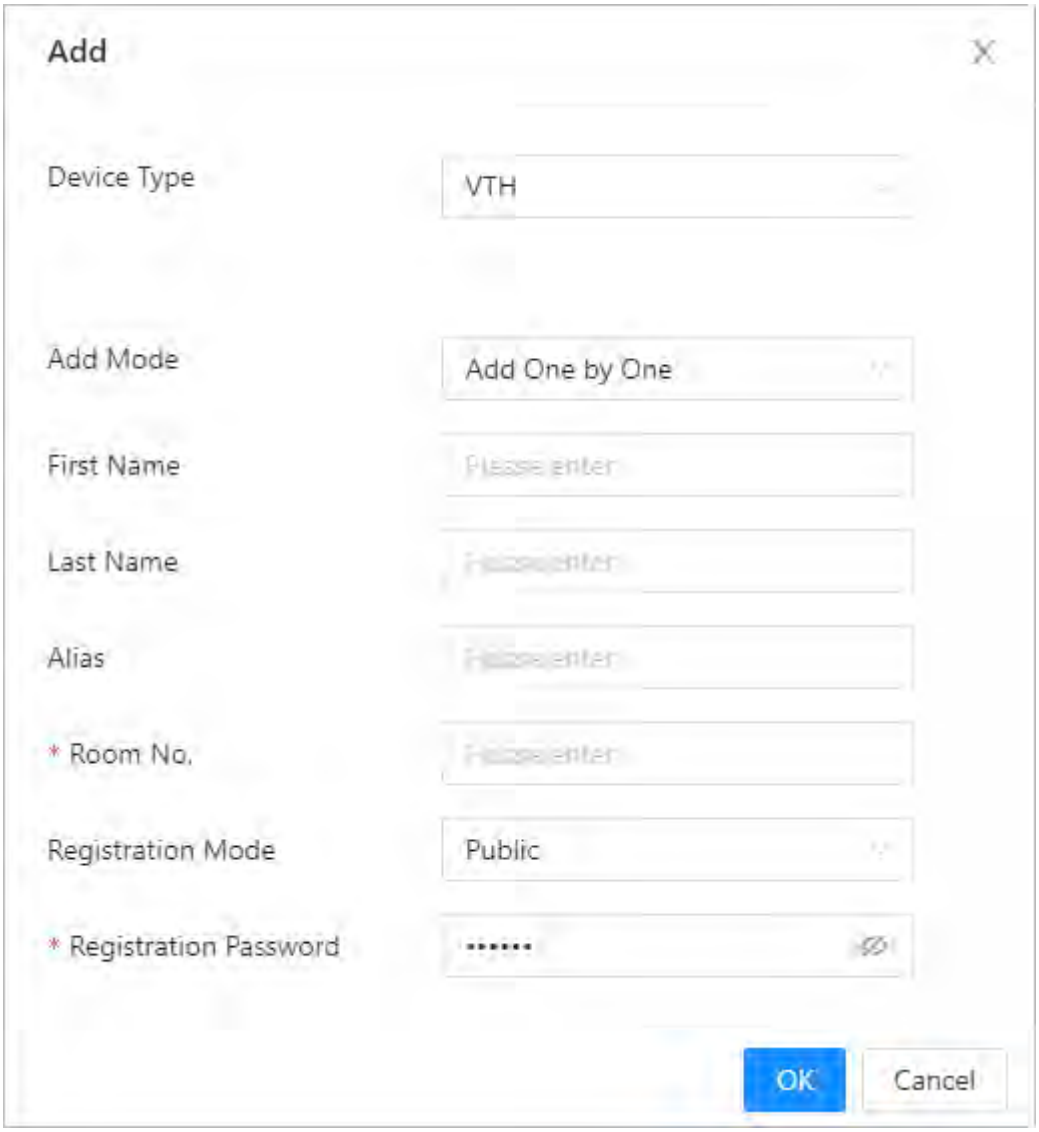


Table 2-6 VTH parameters description

Parameter	Description
Add Mode	Select from **Add One by One** and **Add in Batches**.
First Name	Information used to differentiate each room.
Last Name	

Parameter	Description
Alias	
Room No.	Room number. ● The room number consists of up to 6 characters, and can contain numbers and letters. It cannot be the same as the VTO number. ● When there are multiple VTHs, the room number for the main VTH should end with #0, and the room numbers for the extension VTHs with #1, #2… ● You can configure up to 9 extension VTHs for each main VTH.
Registration Mode	Select **Public**.
Registered Password	Default.

Step 4 Click **OK**.

3 VTH Configuration

This chapter introduces how to configure the VTH and use the intercom function.

3.1 Quick Configuration

For first-time login, you can quickly initialize and configure the VTH through quick configuration. This manual uses the snapshots from 7-inch device as the example. The interfaces on 4.3-inch device is the similar with that on 7-inch device.

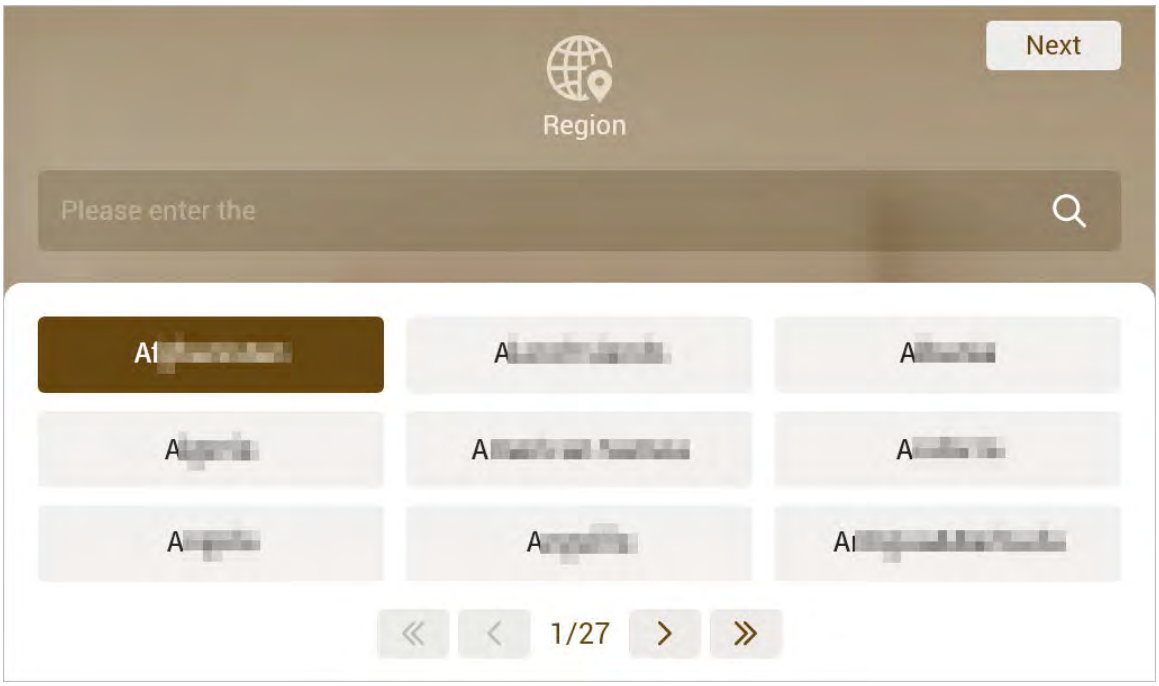
- Quick configuration enables you to configure the parameters of the VTO, VTH and the SIP server at the same time. For more details about modifying the parameters, see "3.2 Manual Configuration".
- The snapshots are for reference only.

Procedure

Step 1 Turn on the VTH.

Step 2 Select a region, and then tap **Next**.

Figure 3-1 Region



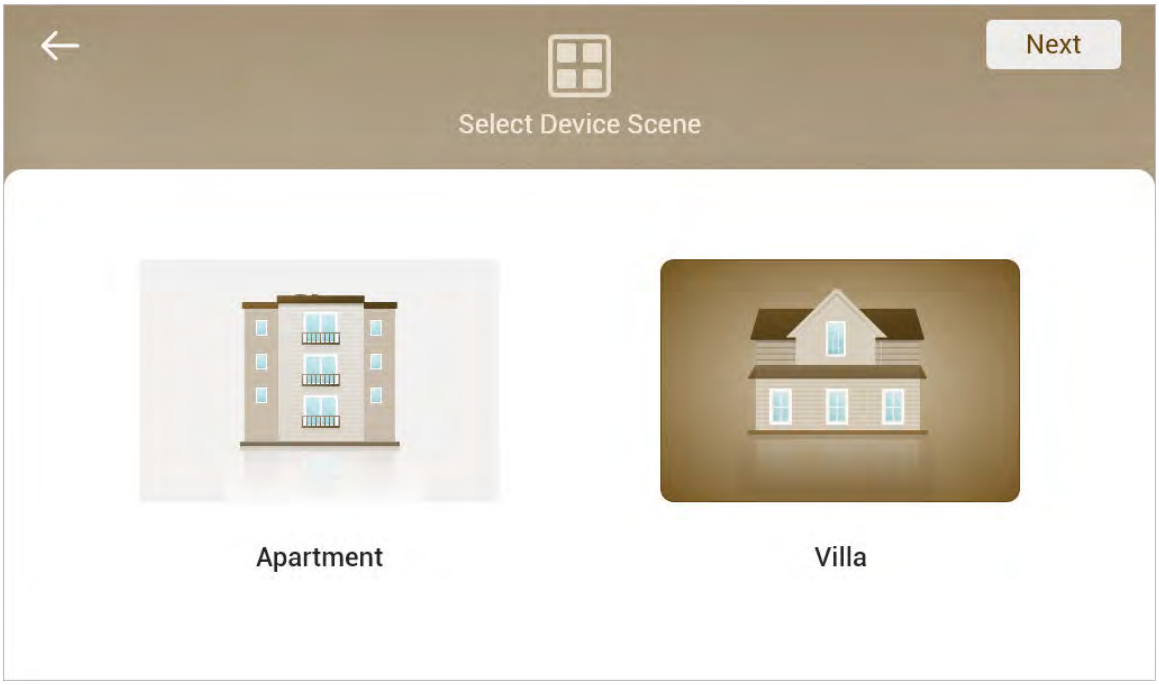
Step 3 Select a language, and then tap **Next**.

Figure 3-2 Language

Step 4 Select **Apartment** or **Villa**, and then tap **Next**.

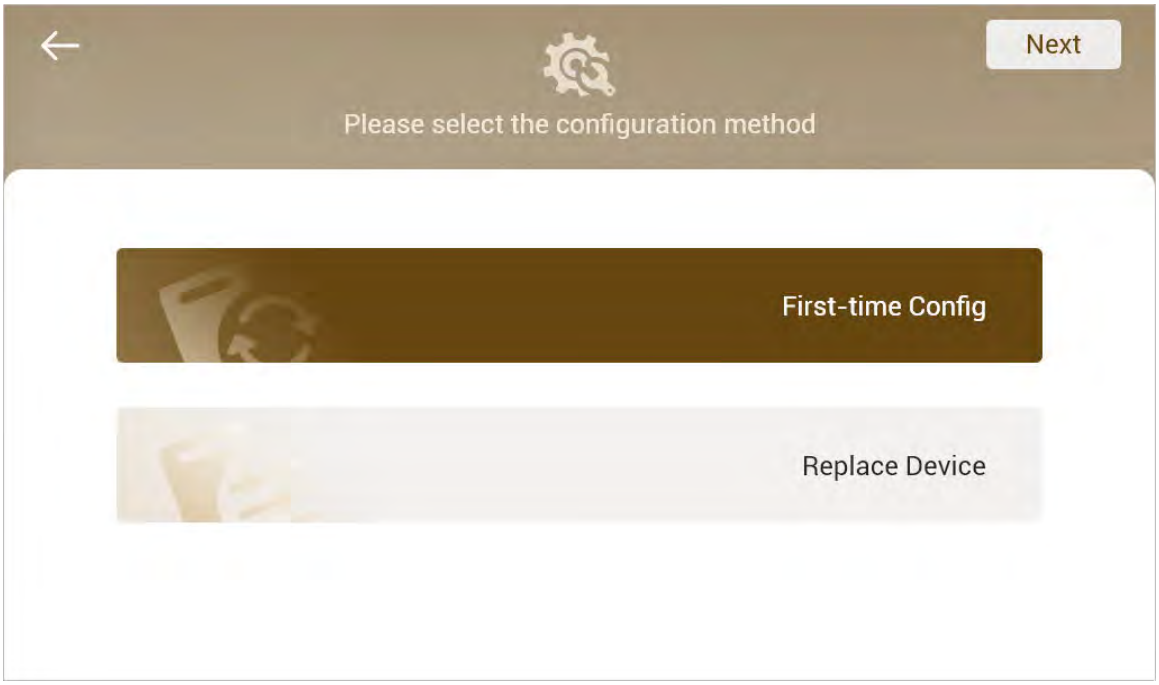
This section takes **Villa** as an example.

Figure 3-3 Scene



Step 5 Select **First-time Config** , and tap **Next**.

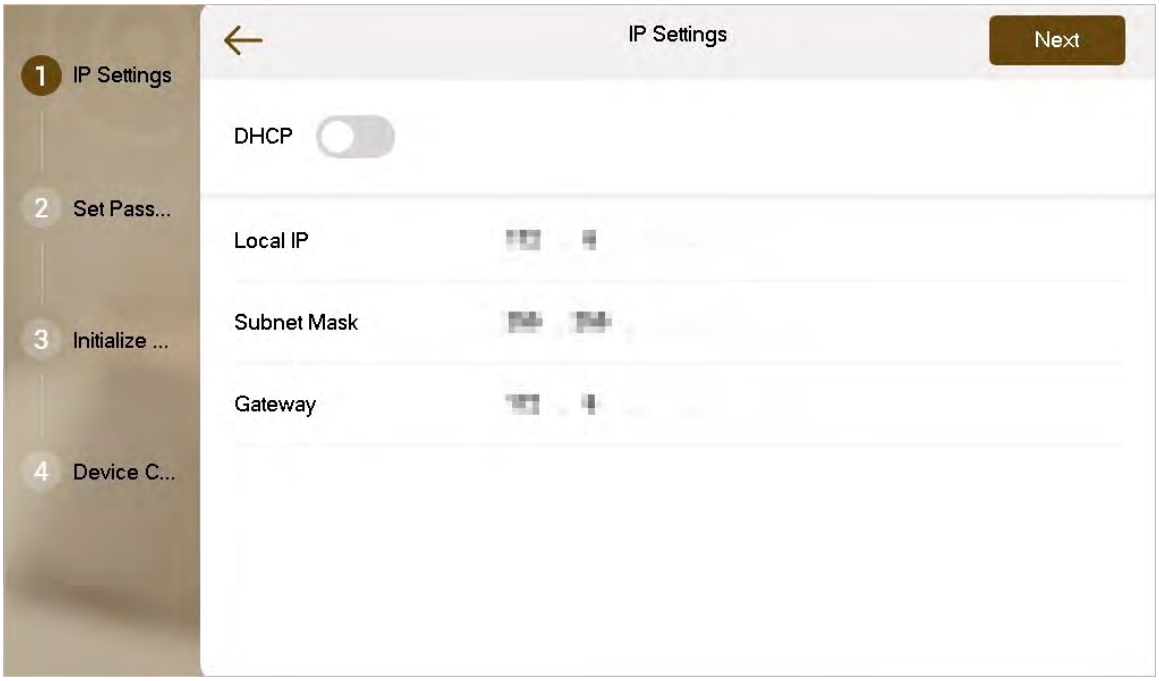
Figure 3-4 First-time configuration



Step 6 Configure the network parameters, and then tap **Next**.

You can also enable **DHCP** , and then tap **Next**.

Figure 3-5 IP settings

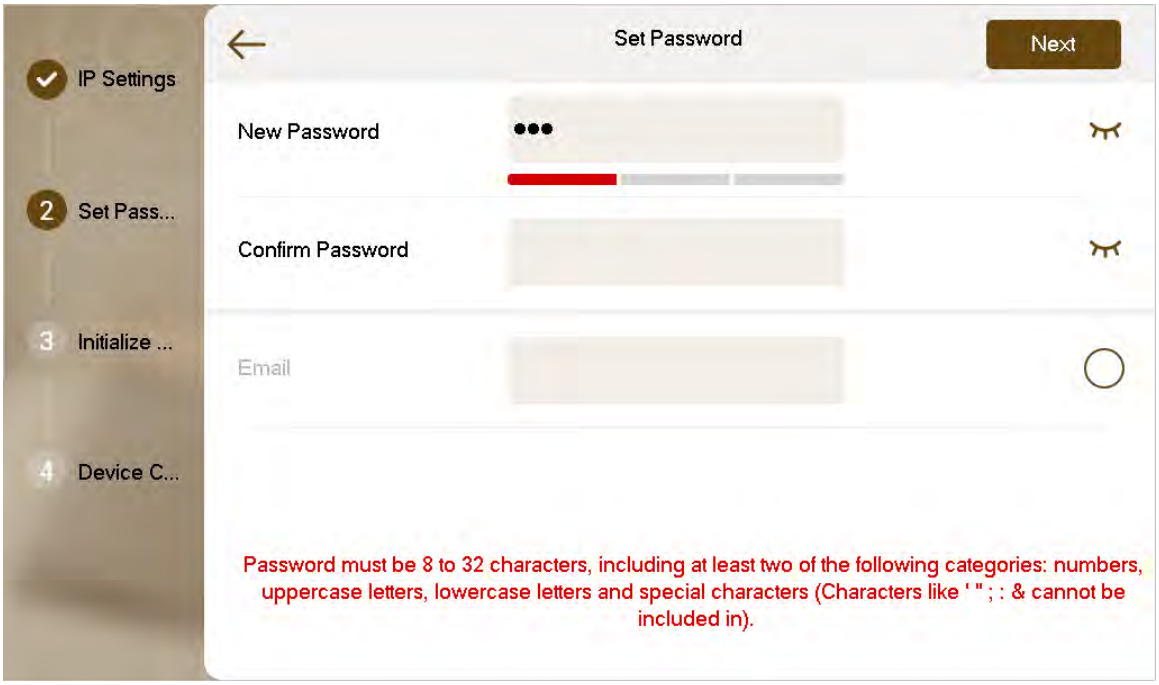


Step 7 Set a password for the VTH, and then tap **Next**.

You can select the **Email**, and then enter the email address for resetting the password.

- The password is used to enter project setting.
- If you select **Apartment** in Step 2, initialization is completed with this step.

Figure 3-6 Password setting



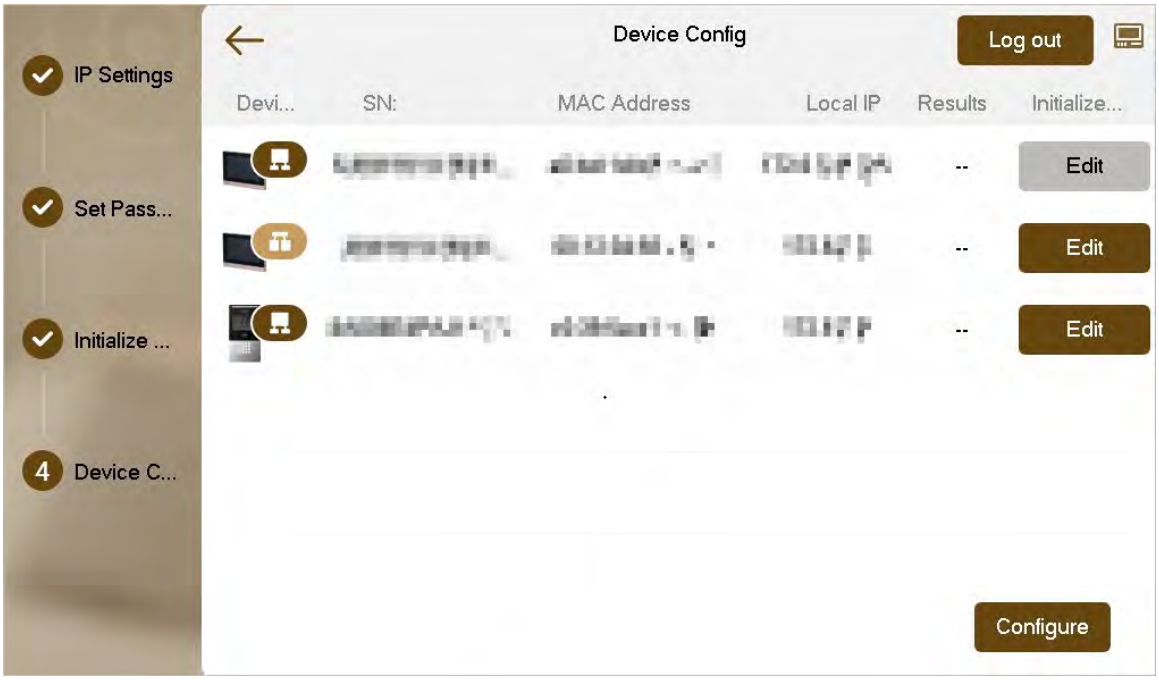
Step 8 Tap **Uninitialized** to initialize a single device, and then tap **Next**.

Initialize All : If there are many devices, tap to initialize all devices that are displayed in the list.

Step 9 After initialization, tap **Edit** to configure the detailed information of the device.

- The device you are using cannot be edited.
- : Indicates that the device is the main device.
- : Indicates that the device is the sub device.

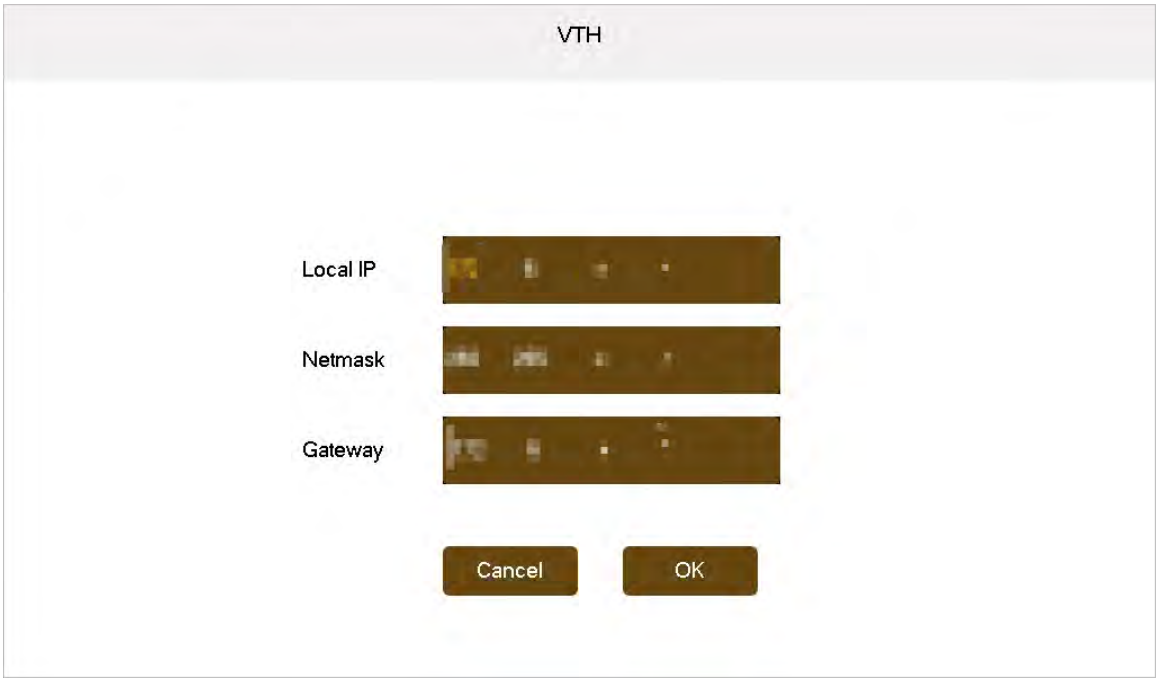
Figure 3-7 Edit the device information



Step 10 Configure the parameters, and then tap **OK**.

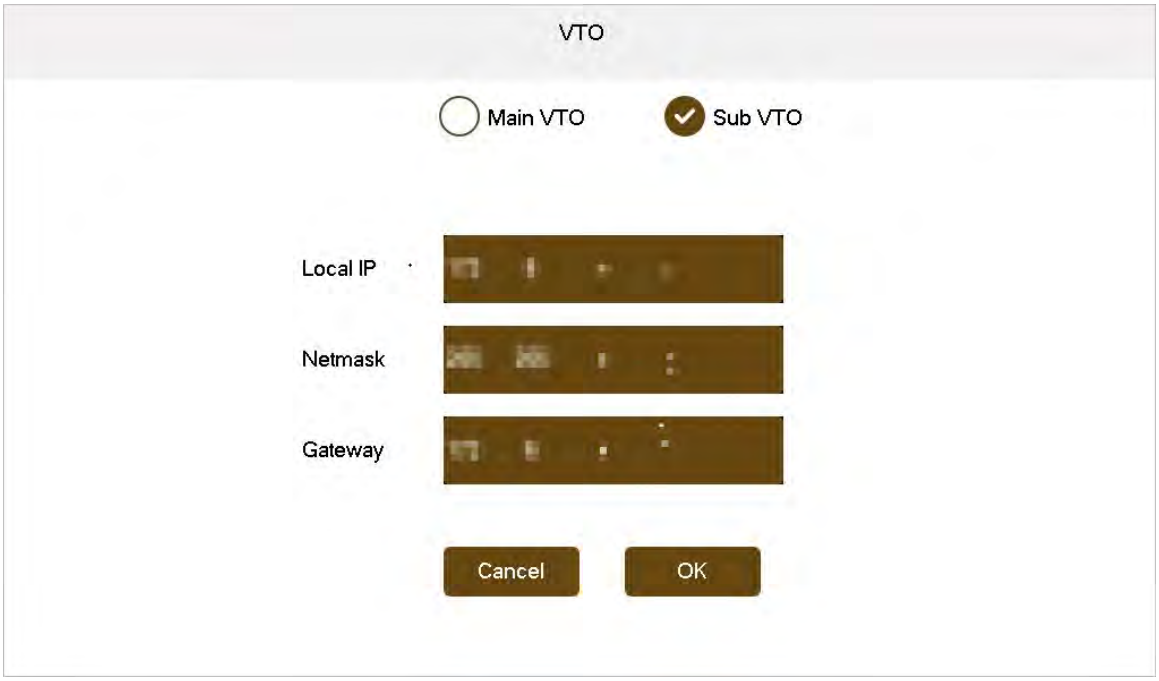
- Configure the network parameters if you want to configure the VTH.

Figure 3-8 Configure the VTH



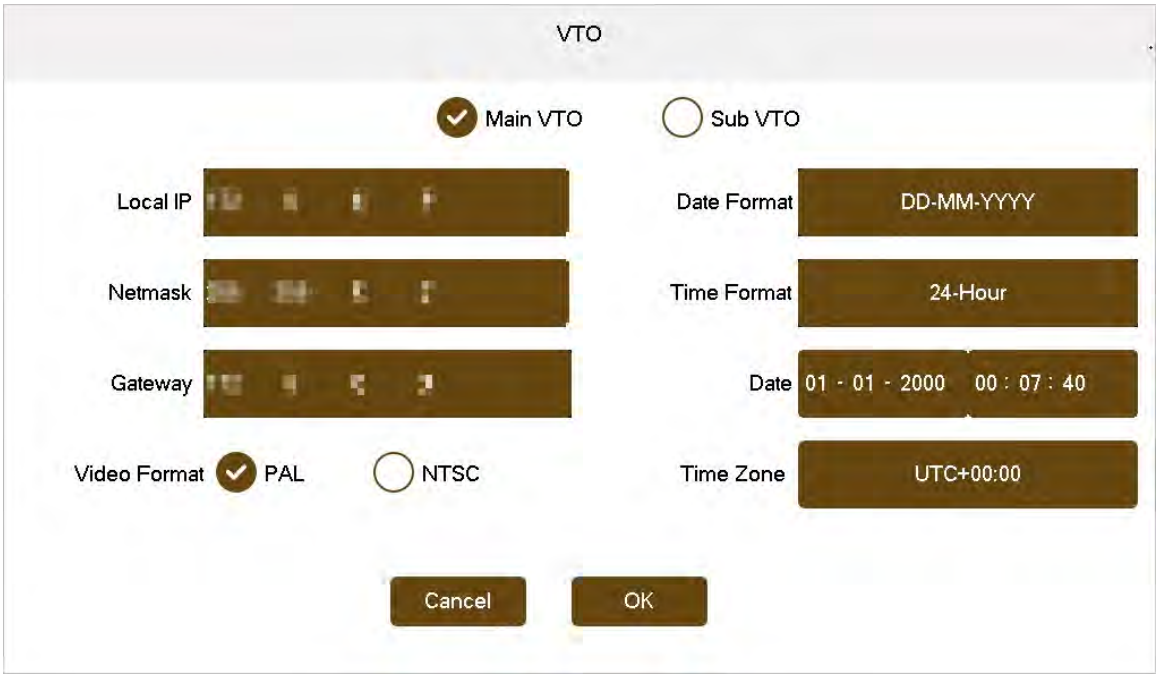
- Configure the network parameters if you want to configure the sub VTO.

Figure 3-9 Configure the sub VTO



- Configure the network parameters and the time if you want to configure the main VTO.

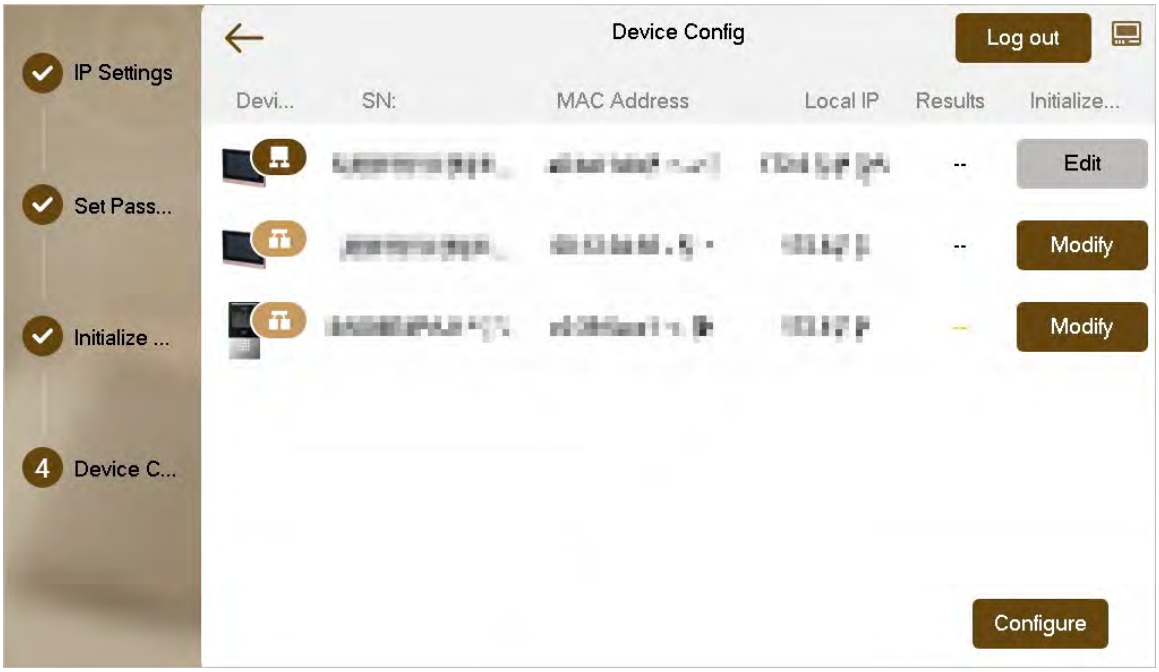
Figure 3-10 Configure the main VTO



Step 11 Tap **Configure** to finish the initialization.

- **Log out** : Tap to directly go to the home screen. If you edit the parameters, and tap **Log out**, the configurations for the device are invalid.
- **Modify** : Tap to modify the device configurations.

Figure 3-11 Configure the device



3.2 Manual Configuration

You can manually configure the parameters you want to modify.

3.2.1 Configuring Network Parameters

You can choose to connect the VTH to the network either through WLAN or LAN.

3.2.1.1 LAN

Procedure

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

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

Step 3 Tap .

Step 4 Enter the information, and then tap ; or turn on **DHCP** to obtain the information automatically.

Figure 3-12 Network settings (1)

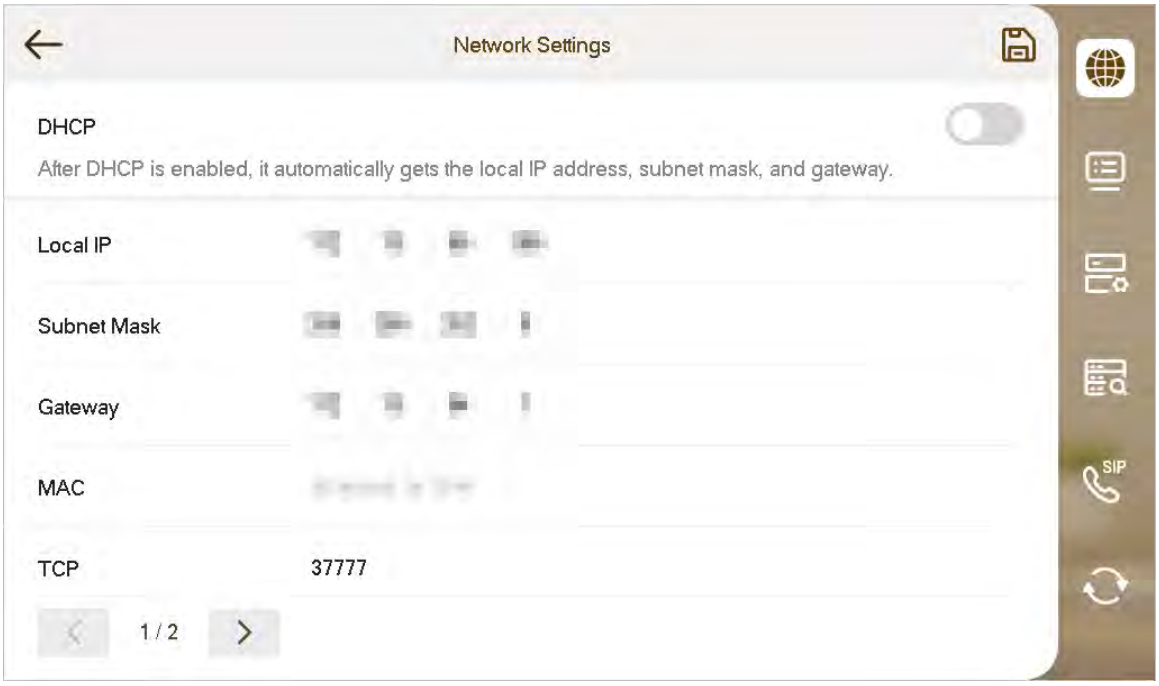
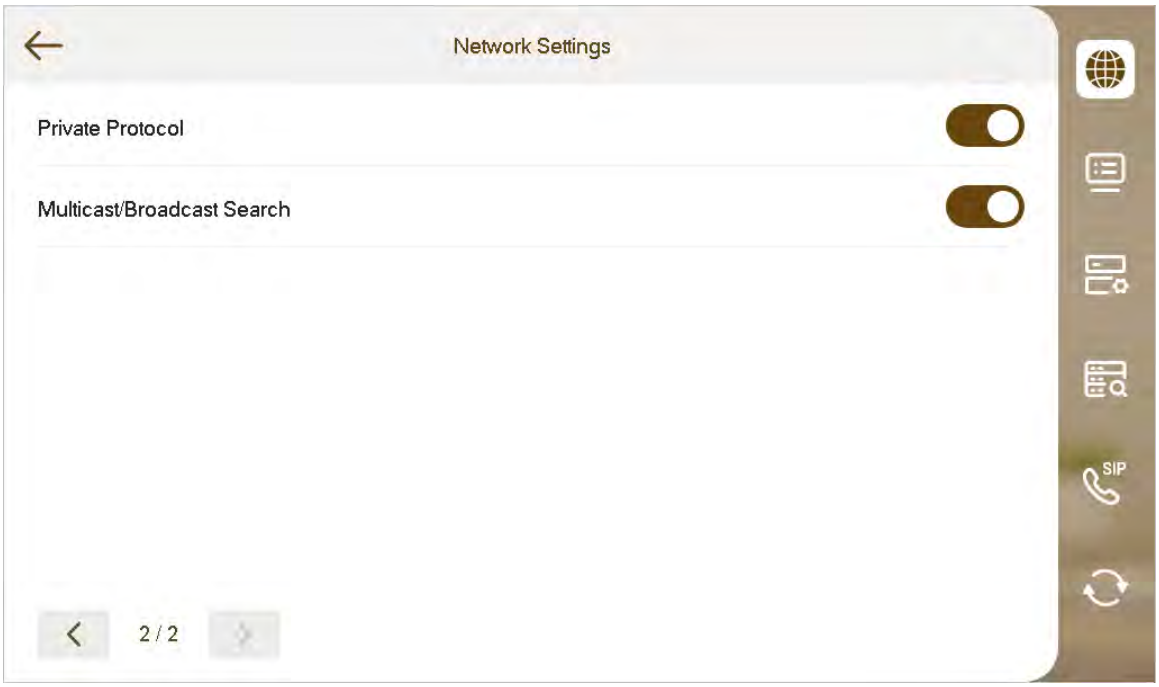


Figure 3-13 Network settings (2)



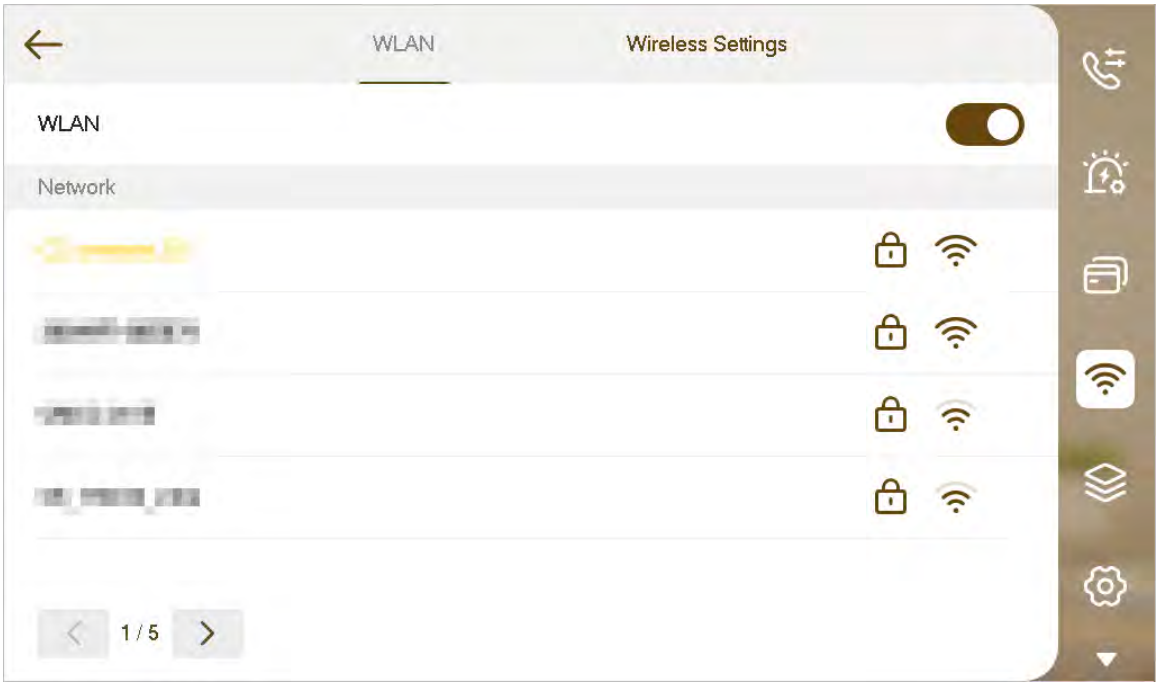
3.2.1.2 WLAN

- The WLAN function is only available on select models.
- Use a router with secured encryption protocols.
- The wired network IP and the WLAN IP cannot be set in the same segment.

WLAN

1. Select **Setting** > , and then tap **WLAN**.
2. Tap , select a Wi-Fi, and then enter the password to connect to the network.

Figure 3-14 Wi-Fi



Wireless IP

1. Select **Setting** > .
2. Tap **Wireless Settings**.
3. Enter the IP address, subnet mask and the gateway, and then tap **OK**.

You can also tap **Wireless Settings**, and turn on **DHCP** to obtain the information automatically.

3.2.2 Configuring SIP Server

Procedure

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

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

Step 3 Tap .

Figure 3-15 SIP server (1)

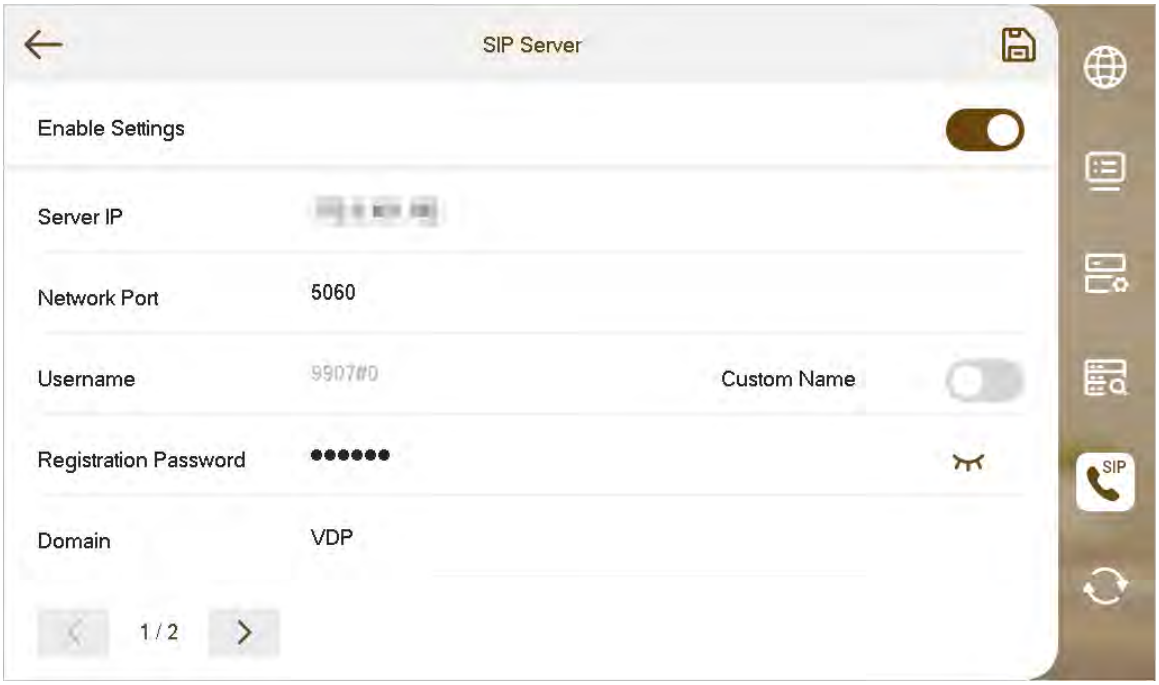
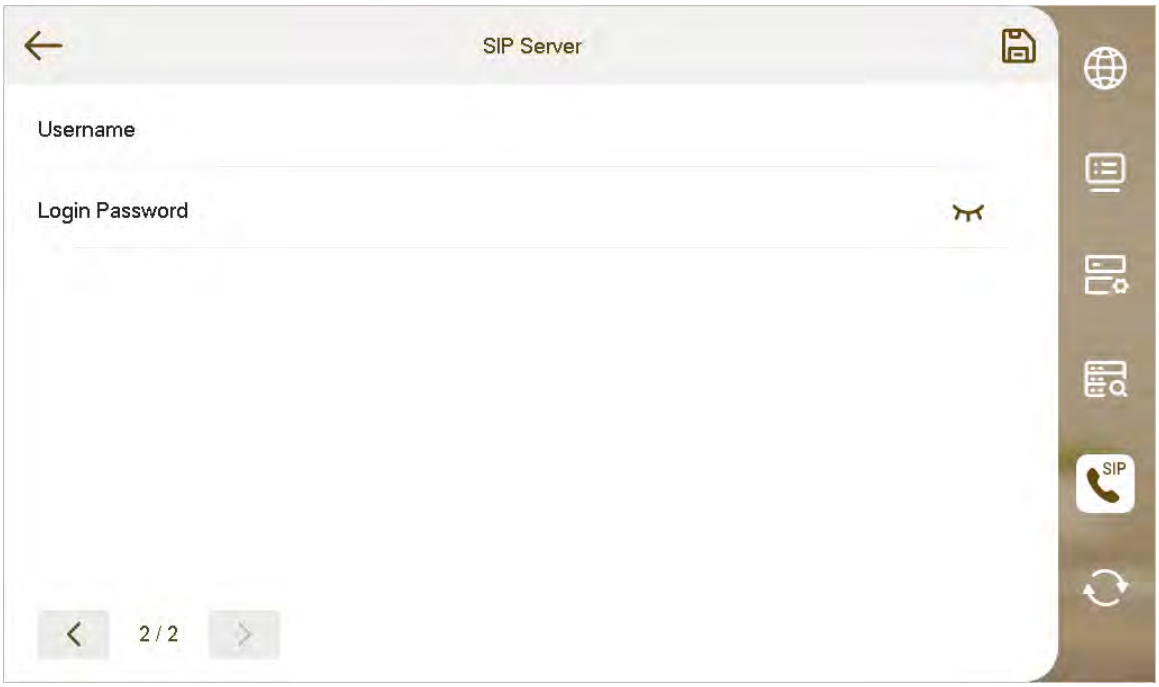


Figure 3-16 SIP server (2)



Step 4 Configure the parameters.

Table 3-1 Description of SIP server parameters

Parameter	Description
Server IP	• When a platform works as the SIP server, it is the IP address of the platform. • When a VTO works as the SIP server, it is the IP address of the VTO.

Parameter	Description
Network Port	• 5080 when a platform works as the SIP server. • 5060 when a VTO works as the SIP server.
Username	Keep it default, or turn on **Custom Name**, and then you can edit the username.
Registration Password	Keep it default.
Domain	When a VTO works as the SIP server, it must be VDP; otherwise, it can be null.
Username	SIP server login username and password.
Login Password	

Step 5 Tap next to **Enable Settings** to enable the SIP server function.

Step 6 Tap .

3.2.3 Configuring VTH

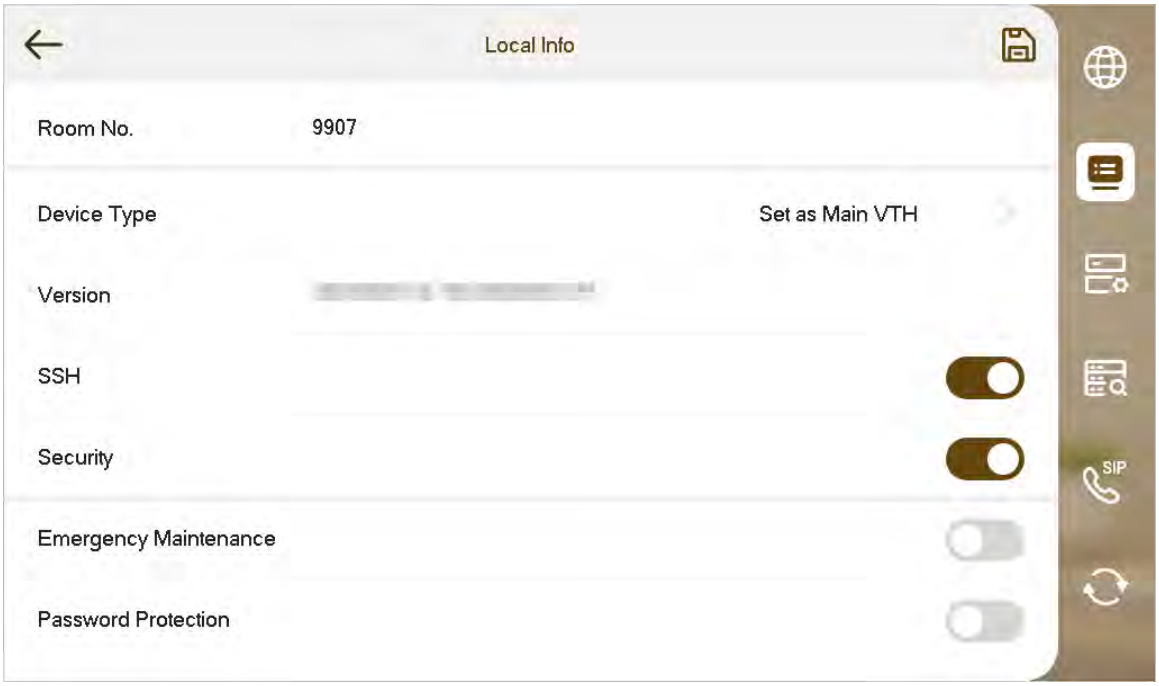
Procedure

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

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

Step 3 Tap .

Figure 3-17 VTH configuration



Step 4 Configure VTH information.

Select the device type from **Set as Main VTH** and **Set as Sub VTH**.

- Set as Main VTH.

Enter the room number (such as 9901 or 101#0).

Room number must be the same with **Room No.**, which is configured when adding VTHs on the VTO webpage. Otherwise, it will fail to connect to the VTO. When there are extension VTHs, room numbers must end with #0. Otherwise, it will fail to connect to the VTO.

- Set as Sub VTH.

  Enter the room number (such as 101#1), IP address, username and password of the main VTH.

  Default username is admin, and the password is the one set during initialization.

Step 5 Turn on the following functions as needed.

- **SSH** : The debugging terminal will connect to the VTH remotely through SSH protocol.
- **Security Mode** : Log in to the VTO in a secured way.
- **Emergency Maintenance** : The device information will be displayed when there are abnormalities.

  We recommend you turn on the function for better after-sale service. If the function is not enabled manually, and there are problems with the key functions (like upgrade), the device will automatically enable it.
- **Password Protection** : Encrypt the password before sending out.

  It is recommended to turn off SSH, and turn on security mode and password protection. Otherwise, the device might be exposed to security risks and data leakage.

Step 6 Tap  .

3.2.4 Configuring VTO

Background Information

Add VTOs and fence stations to bind them with the VTH.

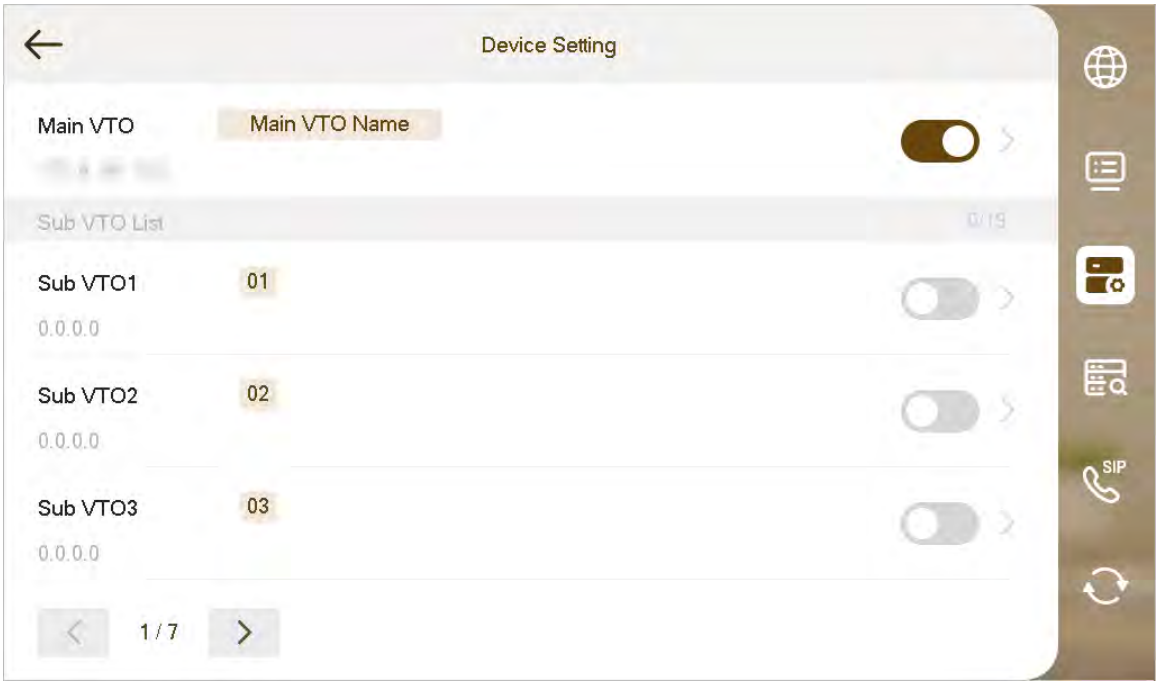
Procedure

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

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

Step 3 Tap  .

Figure 3-18 VTO configuration



Step 4 Add a VTO or fence station.

- Add a main VTO.

1. Tap next to the main VTO, and then enter the main VTO name, VTO IP address, username and password.
2. Tap .

Username and **Password** must be consistent with the login username and password of the VTO webpage.

3. Tap .

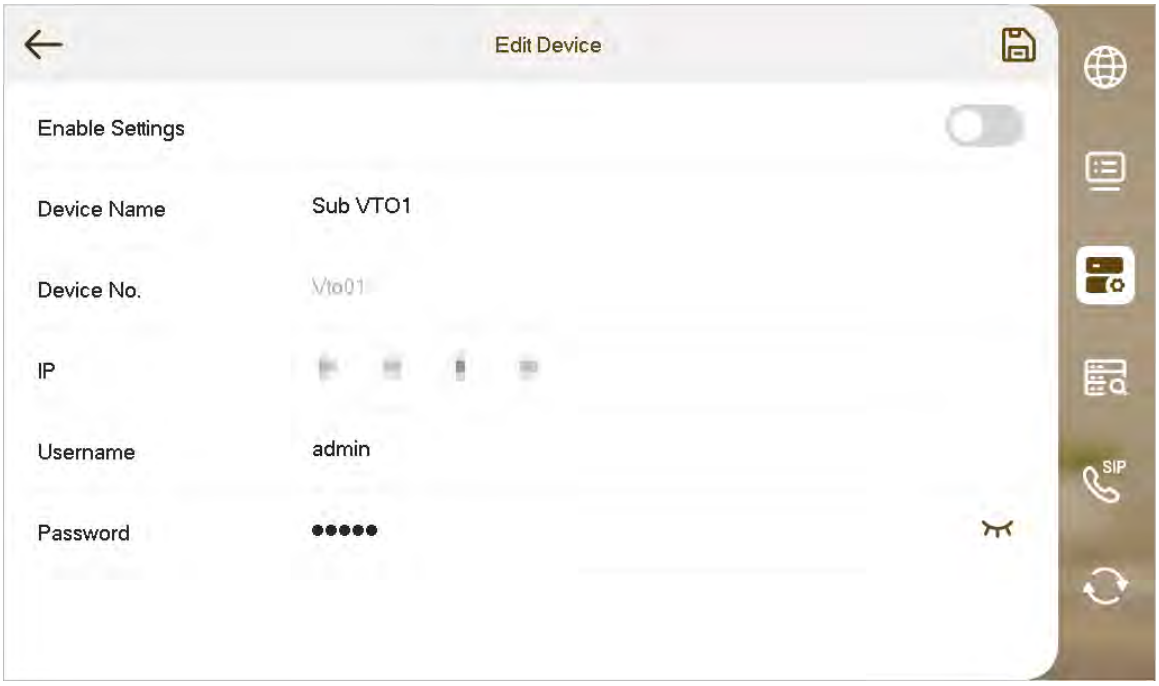
Figure 3-19 Main VTO configuration

- Add a sub VTO or fence station.

1. Tap next to the sub VTO, and then enter the sub VTO or fence station name, IP address, username and password.
2. Tap .

   Tap or to turn page and add more sub VTOs or fence stations.
3. Tap .

Figure 3-20 Sub VTO configuration



4 Commissioning

4.1 Using the VTO to Call the VTH

Procedure

Step 1 Dial VTH room number (such as 9901) at VTO, to call VTH.

Step 2 On the VTH screen, tap **Answer**.

If the network connection is bad, the device will adjust the video stream according to the actual situation.

Figure 4-1 Call from VTO

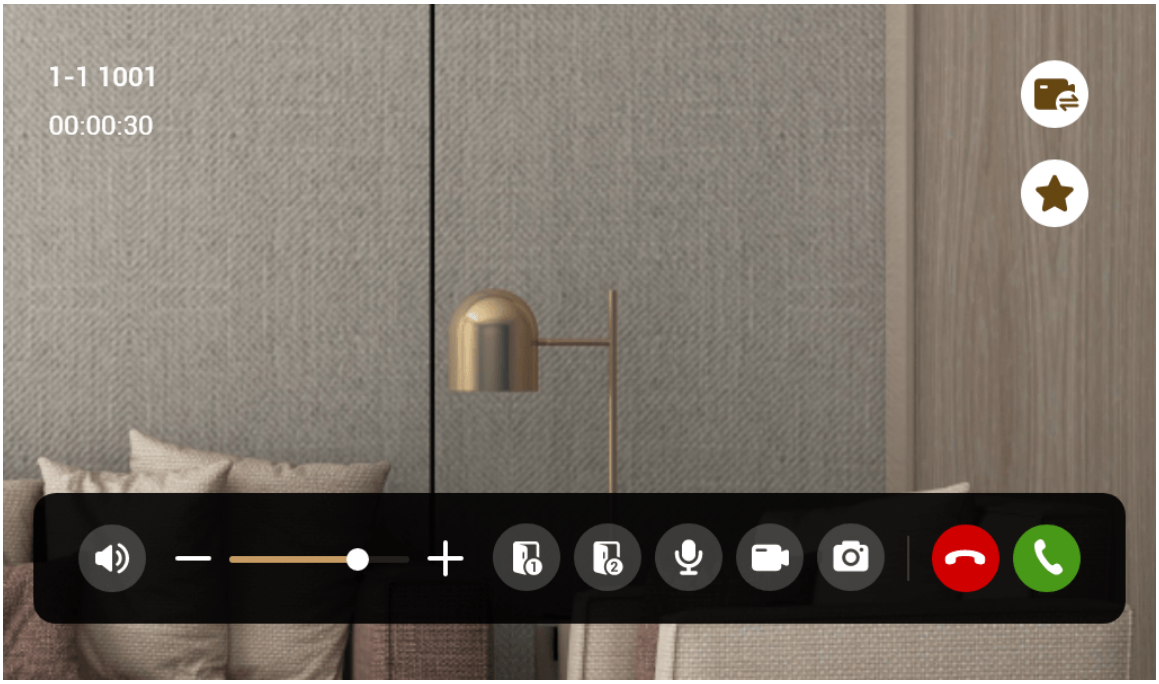


Table 4-1 Call screen description

Key	Description
	Remotely unlock the door where the VTO is installed. The system provides 2-channel unlock. If the icon is gray, it means that the unlock function of this channel is not available.
	The microphone can be used. Tap the icon, and the microphone cannot be used.
	Tap to switch the IPC that is linked.

Key	Description
	Select an IPC in **Favorite** to monitor.
	Take snapshot. This key will be gray if SD card is not inserted. The SD card is available on select models.
	Take recording. Complete recording when the call is completed or by tapping the stop icon. This key is gray if SD card is not installed. Videos are stored in SD card of this VTH. If SD card is full, the earlier videos will be covered. The SD card is available on select models.
–	Reduce volume.
+	Increase volume.
	Answer calls.
	Hang up.

4.2 Using the VTH to Monitor the VTO

When adding VTOs, make sure that the username and password of each device is consistent with the web login username and password. Otherwise, monitoring will not work properly.

Procedure

Step 1 On the main screen of the VTH, select **Monitor** >  .

Figure 4-2 VTO list

: Add the VTO or fence station to **Favorites**.

Step 2 Tap .

Figure 4-3 Monitoring VTO

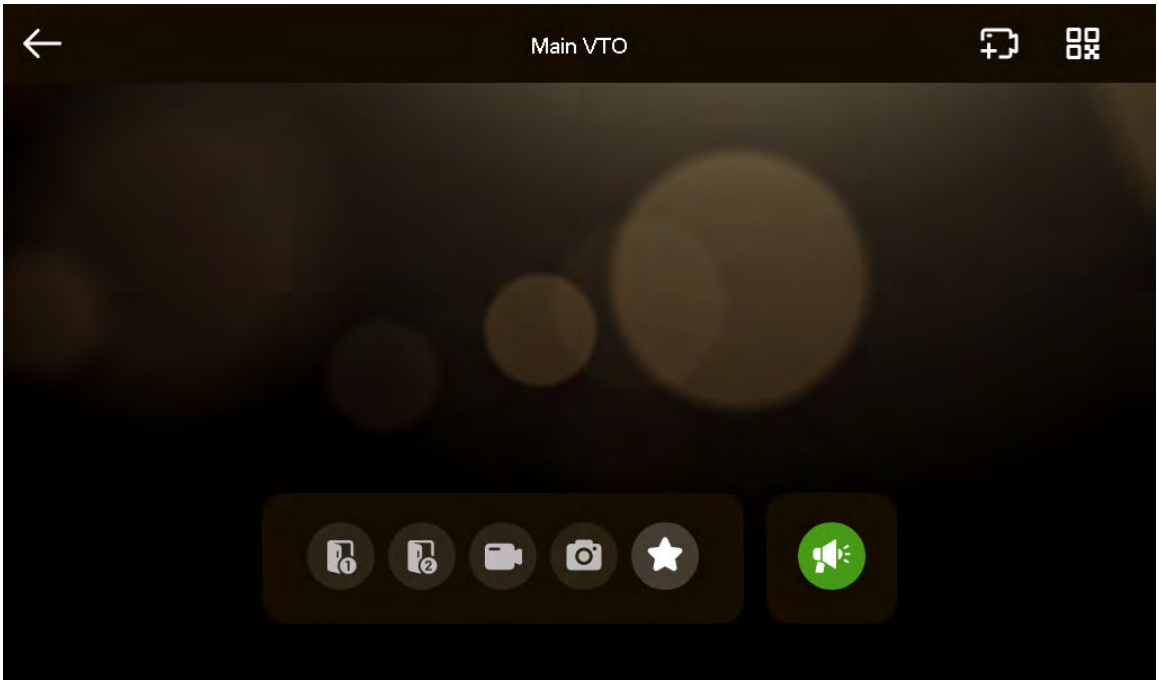


Table 4-2 Interface description

Icon	Description
	Remotely unlock the door where the VTO is located. The system provides 2-channel unlock function. If the icon is gray, it means that unlock function of this channel is not available.
	Take snapshot. ● An SD card is needed to use this function. ● The SD card is available on select models.
	Tap to start recording, and it will stop when the call is completed or by tapping the stop icon. If the SD card is full, the oldest videos will be overwritten. ● An SD card is needed to use this function. ● The SD card is available on select models.
	The VTO has been added to **Favorites**.
	If the VTH is connected to multiple VTOs/IPCs, tap and  to switch device. If the VTH is connected to one VTO, the icon will not be displayed.
	Exit monitoring.
	Tap to speak to the other end device.
	Select an IPC, and when this VTO or fence station calls, you will see the monitoring image from this IPC.
	Display the serial number of the VTO or fence station in QR code. Scan the QR code in the app to add it to the app, and then you can monitor the VTO from your smart phone.

Appendix 1 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

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

Service Configuration

1. **Enable HTTPS**

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

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

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

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

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

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

Network Configuration

1. **Enable Allow list**

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

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

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

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

Security Auditing

1. **Check online users**

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

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

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

Software Security

1. **Update firmware in time**

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

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

Physical Protection

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

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