Video Door Phone_(Version 4.8.1)_(VTO, VTS, DSS Agile VDP, DMSS, DoLynk Care, and DoLynk Pro)

Quick Start Guide

V1.0.2

Foreword

This manual introduces the common configuration of intercom devices. And also, it shows the configuration and commissioning among the intercom devices and applications such as DoLynk Pro, DoLynk Care, DMSS, and DSS Agile VDP. 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
V1.0.2	• Added cloud function. • Added deployment solution.	June 2025
V1.0.1	Added distributed configuration.	November 2024
V1.0.0	First release.	October 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 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 procedures and carry out commissions to make sure that the device can realize basic network access, call and monitoring functions.
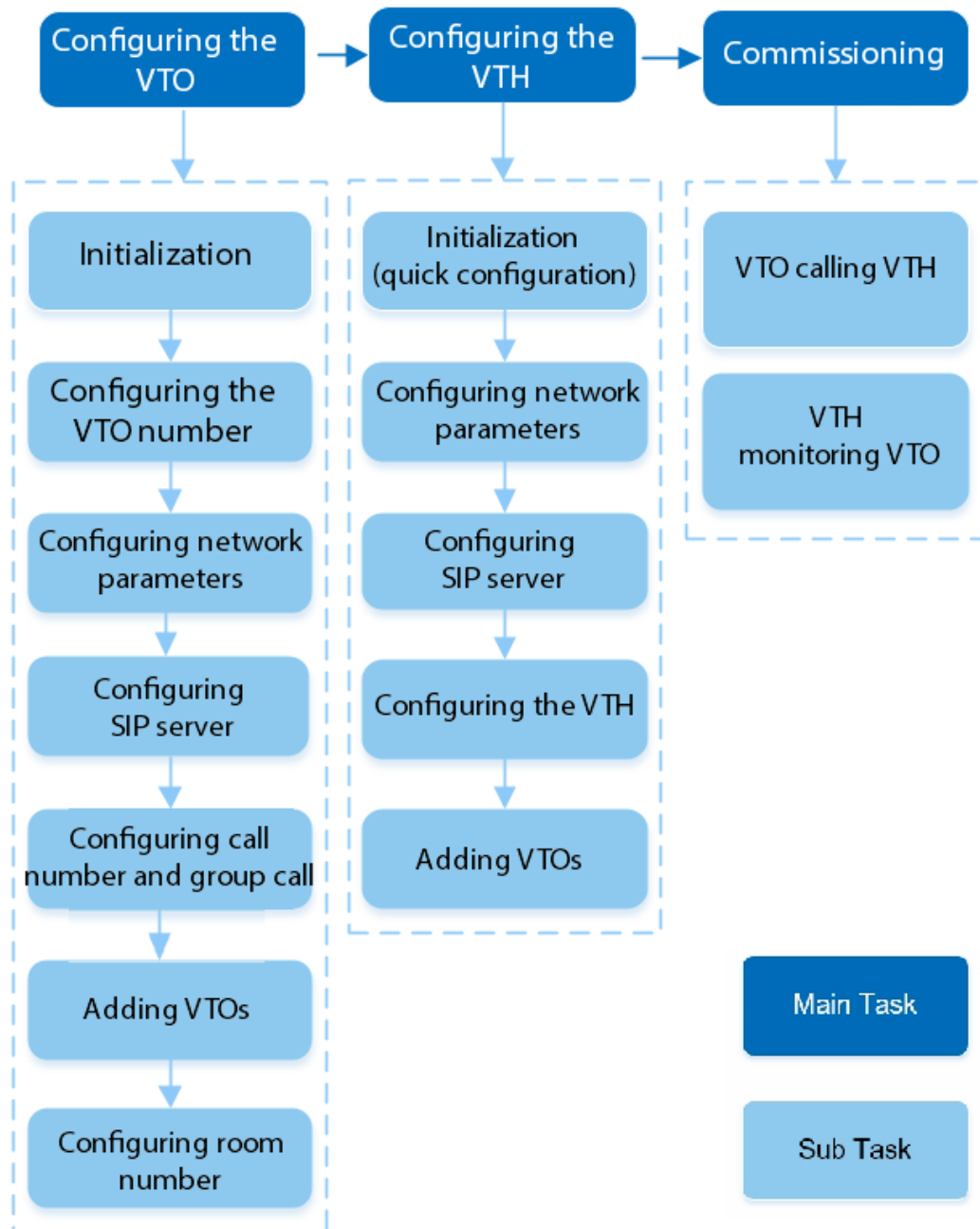
1.1 Preparation

Before the configuration:

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

1.2 Basic Configuration Procedures

Figure 1-1 Basic configuration procedures

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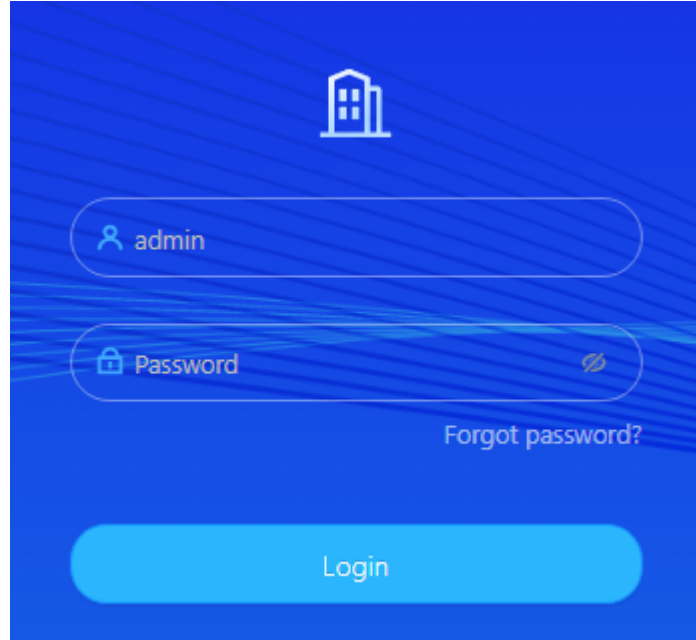
Step 3   Enter and confirm the new password, and then click **Next**.

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 user name and the new password to log in to the webpage.

Figure 2-1 Login

Step 7   Click **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.

Parameter	Description
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.
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.
Auto Record while Calling	Take recording when the VTO is in a call, and save the recording in the SD card of the VTO. 📖 ● This parameter is available only when the device is villa door station. ● When the call time is less than 5 seconds, no video file will be generated. ● If there is a conflict between **Auto Record while Calling** and **Leave Videos**, **Leave Videos** prevails.

Step 4   Click **Apply**.

2.3 Configuring Network Parameters

You need to configure IP address of the VTO to enable communication with other devices.

Procedure

Step 1   Log in to the webpage of the VTO.

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

Step 3   Configure the parameters.

Figure 2-3 TCP/IP

Table 2-2 Description of TCP/IP parameters

Parameter	Description
DHCP	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.
Subnet Mask	
Default Gateway	 • IPv6 address is represented in hexadecimal. • IPv6 version does not require setting subnet masks. • The IP address and default gateway must be in the same network segment.
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. Unicast is not recommended when the platform is being used as an SIP server.

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

Table 2-3 SIP server configuration

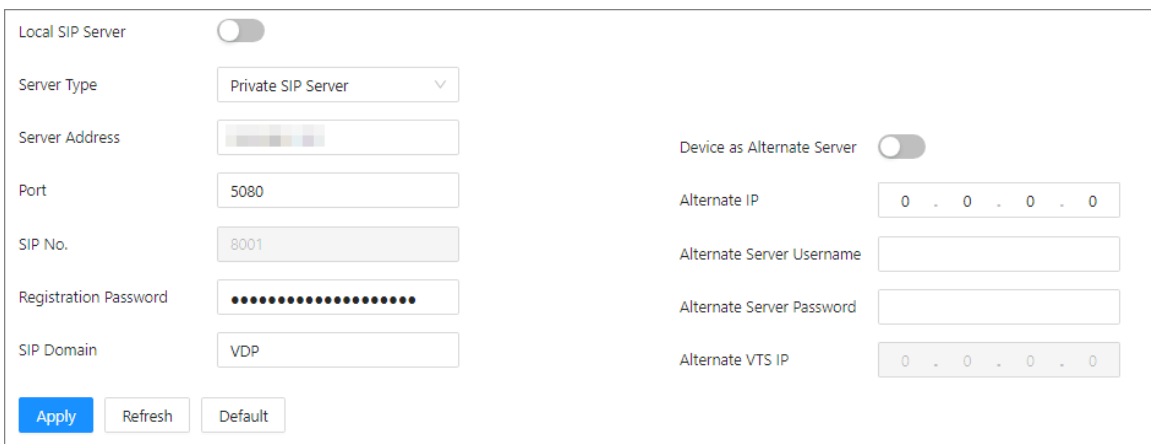| Parameter	Description
Port	5060 by default when the VTO works as an SIP server.
SIP No.	8001 by default when the VTO works as an SIP server.
Registration Password	Leave it as default.
SIP Domain	VDP is by default.

8

Parameter	Description
Cascade SIP Server	Enable the cascade SIP server, and then enter the address, port, SIP No., registration password, the username and password of the cascade SIP server.
Server Address	
Port	
SIP No.	
Registration Password	Generally, the cascade SIP server is a server VTS with port 5060.
Backup SIP Server	• The backup SIP server allows devices under the SIP server to call and intercom normally when the SIP server is abnormal. And make sure the devices are under the smooth netwrok.
Room Number of Backup Server	• All functions can not be restored when the VTO server and VTS server crash at the same time. If such situation occurs, the upper devices only can call the lower devices, but the dual communication is not allowed. • Enable **Backup SIP Server**, and then enter the room number of the server, or you can click **Select Online Device** to select an online server.

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
Server Address	The IP address of the SIP server.
Port	5080 by default when the platform works as the SIP server.
SIP Domain	Keep default value VDP or leave it empty.

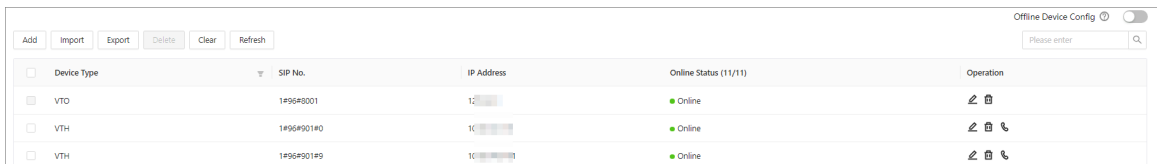| Parameter	Description
Alternate IP	The alternate server will be used as the SIP server when DSS Express or DSS Professional stops responding. We recommend you configure the alternate IP address. 📖 • If you enable **Alternate Server**, the current VTO you have logged in serves as the alternate server. • 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.
Alternate Username/ Password	Used to log in to the alternate server.
Alternate VTS IP	IP address of the alternate VTS.
Device as 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 **VTO** from 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.
Building 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**.

Related Operations

- Click ✎ to edit the VTO.

- Click 🗑 to delete added VTOs, but the one that you have logged in to cannot be modified or deleted.
- Click 📞 or 📞 to call or hang up VTH.

  📖

  ◇ It is only available when SIP function is online.
  ◇ If the group call is enabled, the group call will be performed when call #0 or -0 VTH.
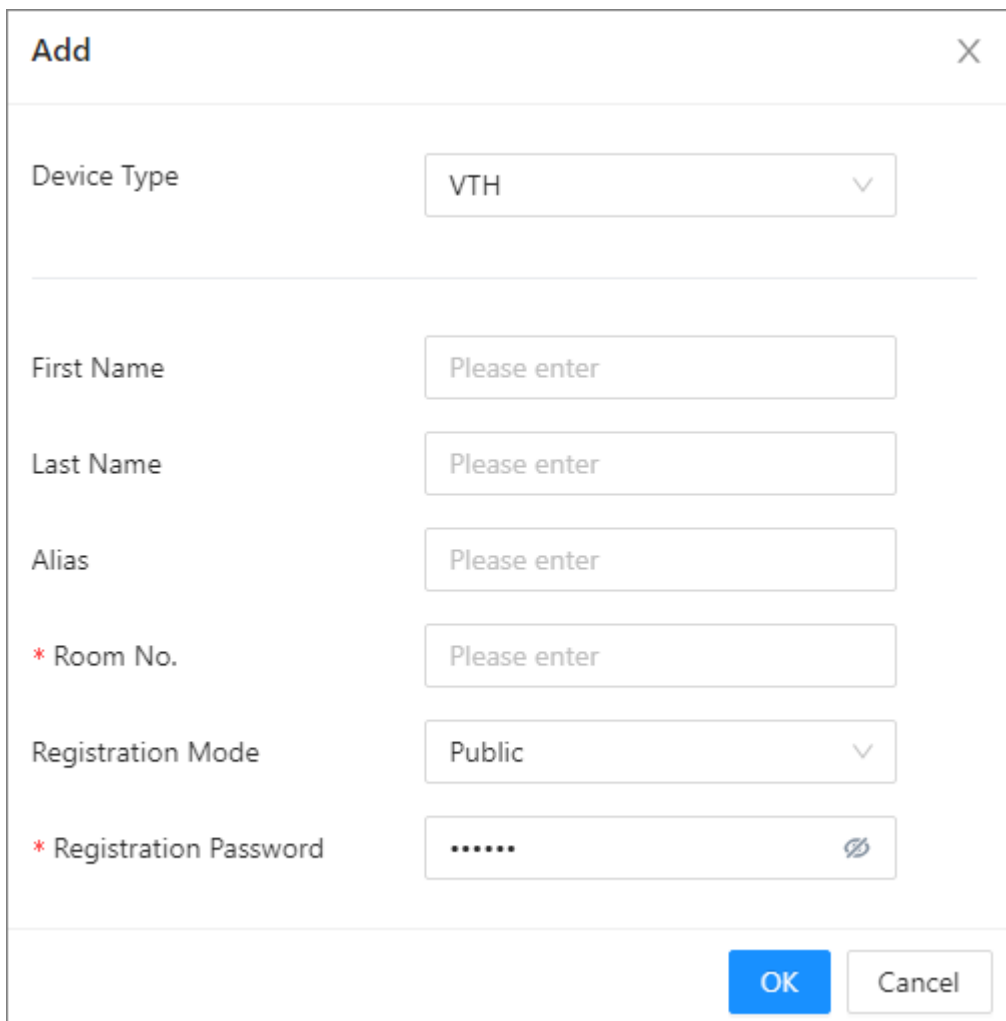
2.6 Adding the VTH

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
First Name	Information used to differentiate each room.
Last Name	
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**.
Registration 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 a 4.3-inch device are similar to those on a 7-inch device.
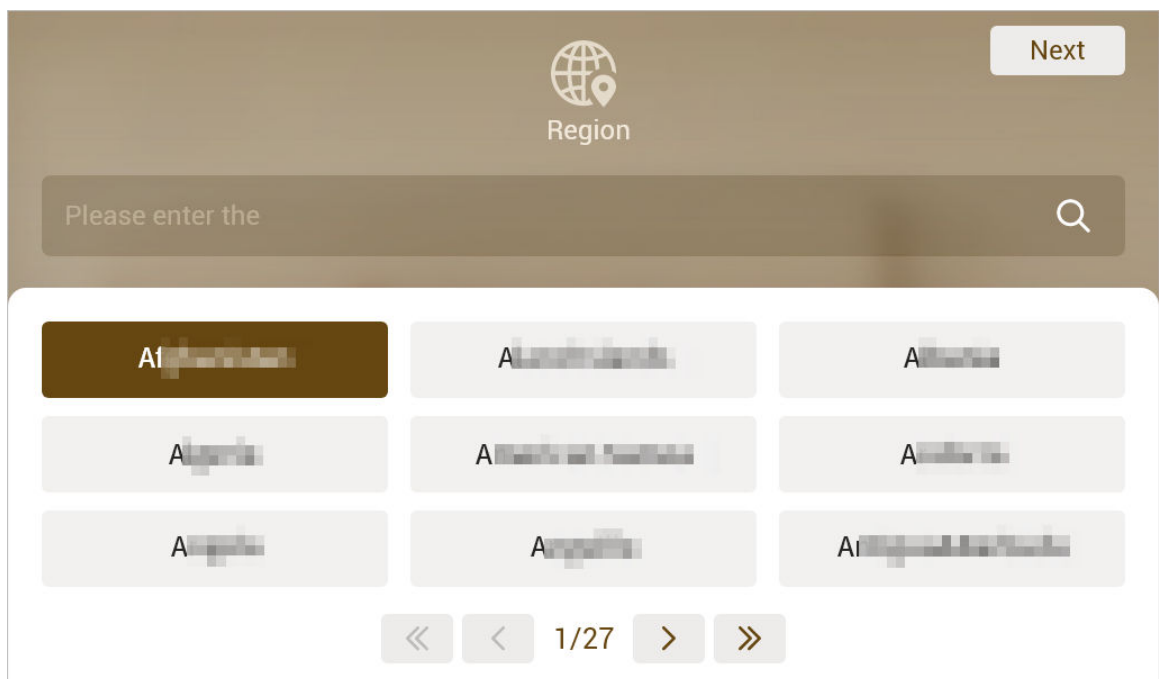
📖

- Quick configuration allows you to configure the parameters of the VTO, VTH and the SIP server at the same time.
- The snapshots are for reference only.

Procedure

Step 1   Turn on the VTH.
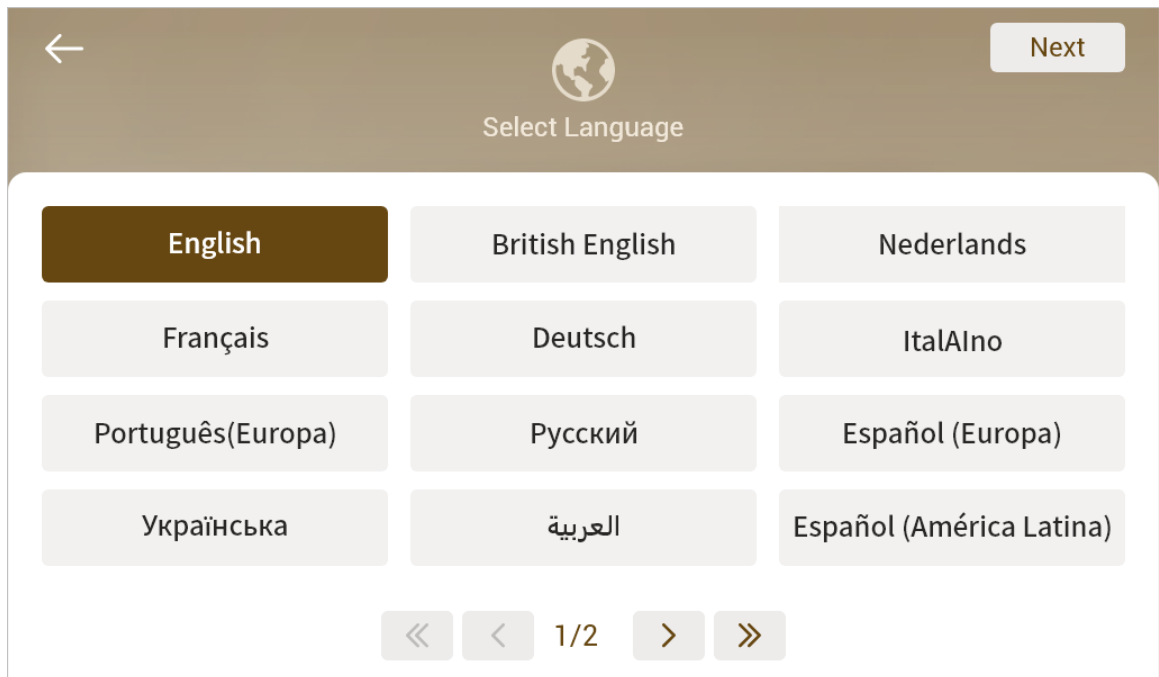
Step 2   Select a region, and then tap **Next**.

Figure 3-1 Region

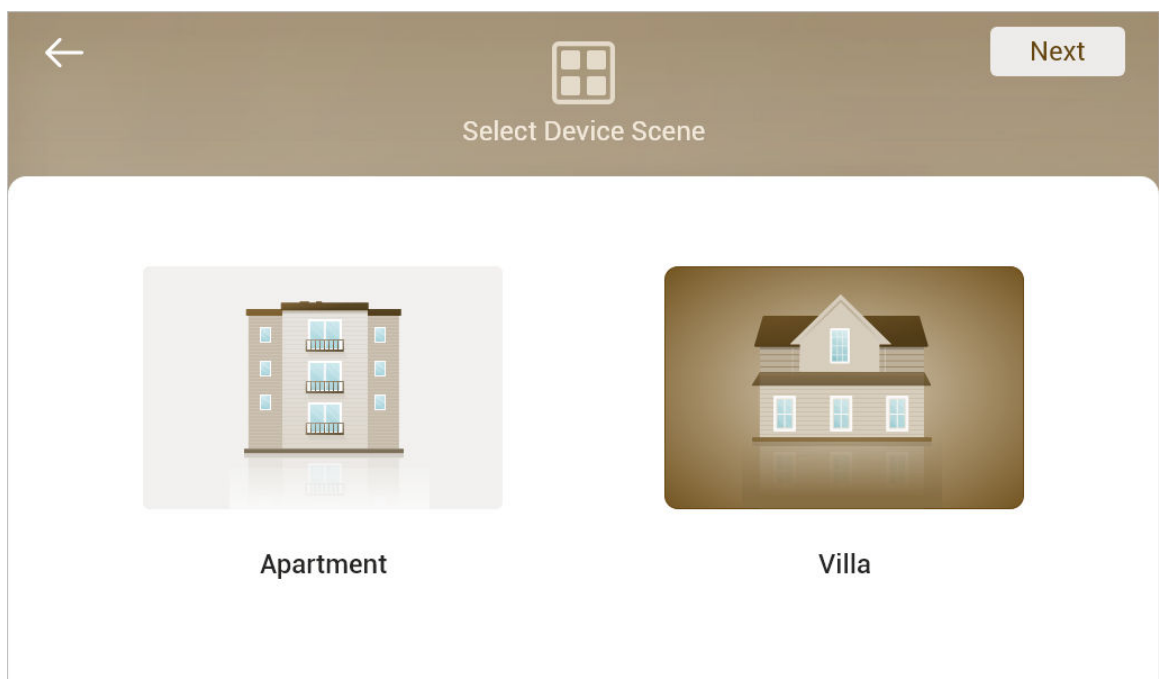Step 3   Select a language, and then tap **Next**.

Figure 3-2 Language

Step 4   Select **Apartment** or **Villa**, and then tap **Next**.
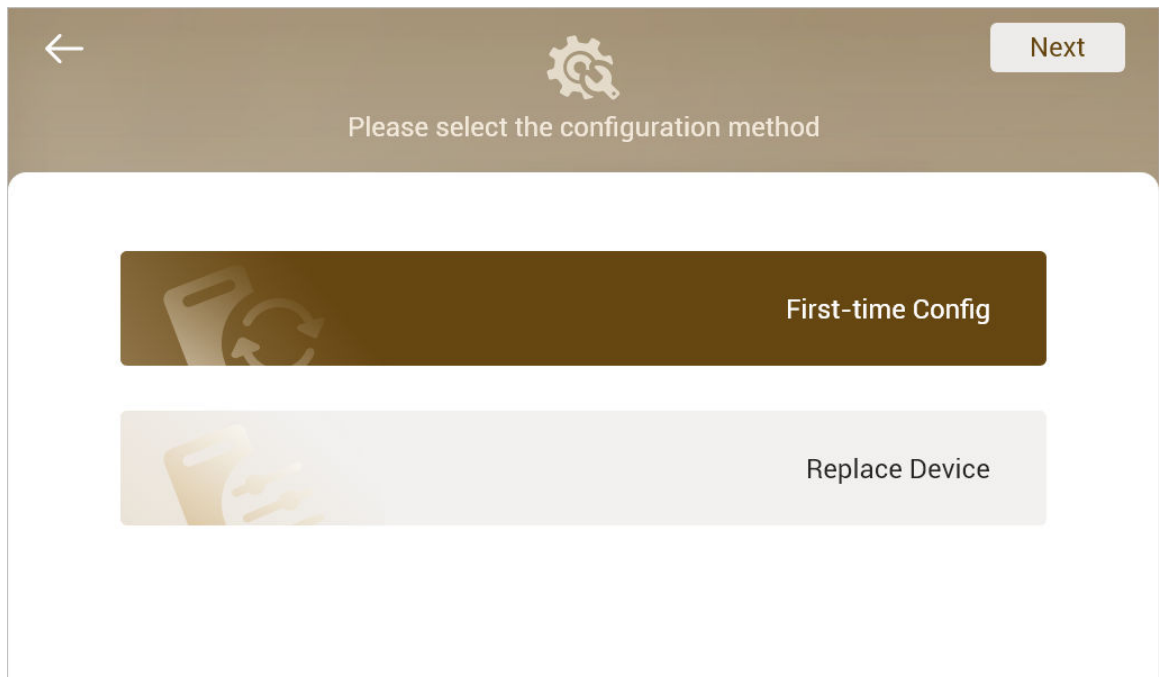
This section takes **Villa** as an example.
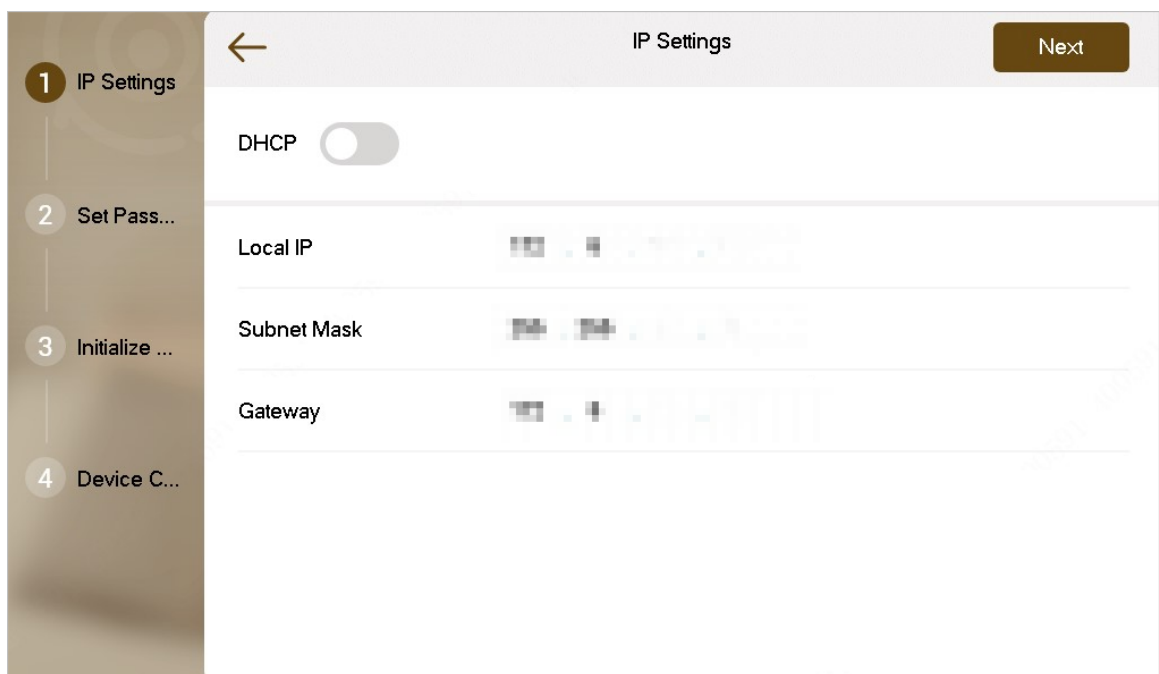
Figure 3-3 Scene

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.
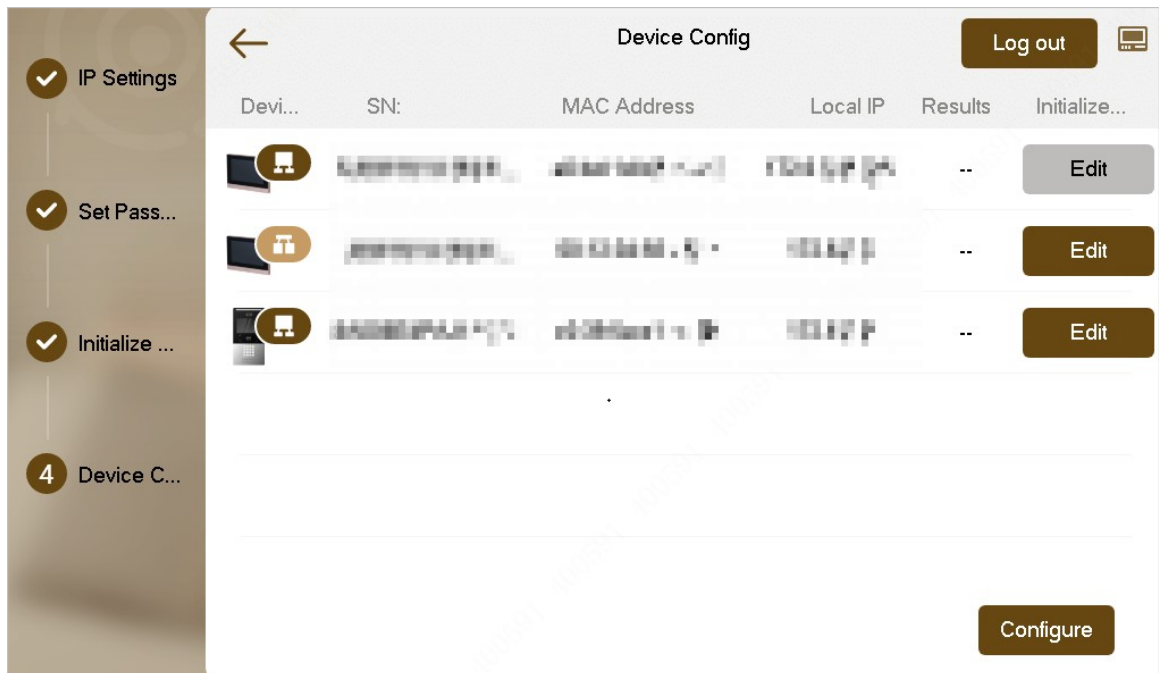
- The device you are using cannot be edited.
- [image] : Indicates that the device is the main device.
- [image] : Indicates that the device is the sub device.
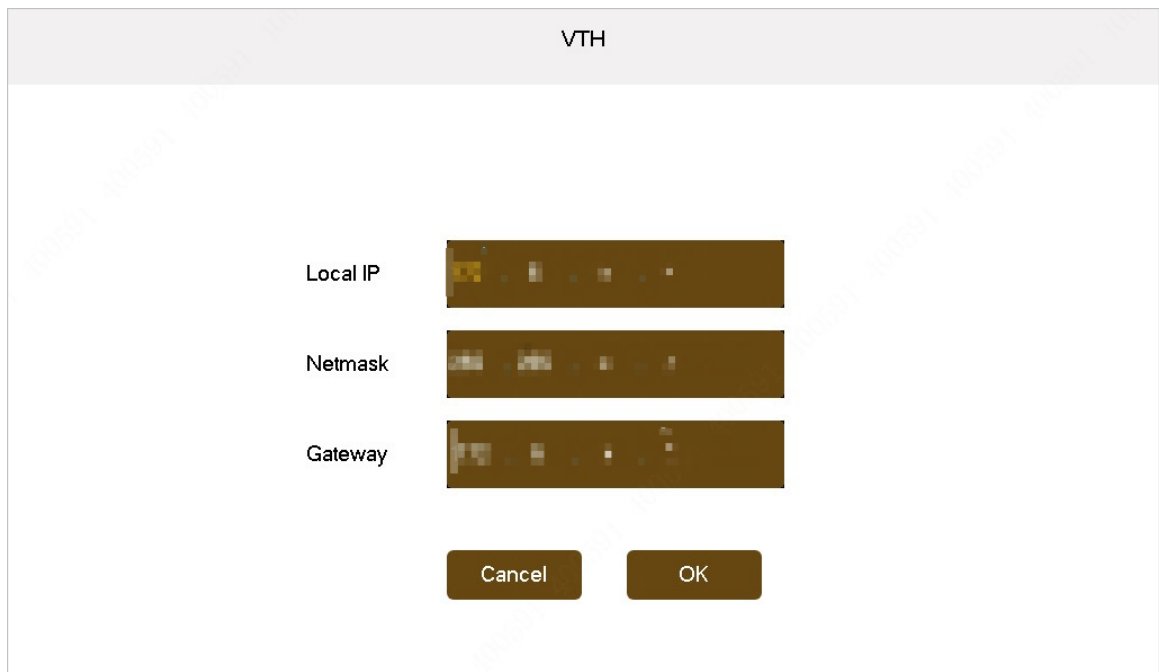
Figure 3-7 Edit the device information

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
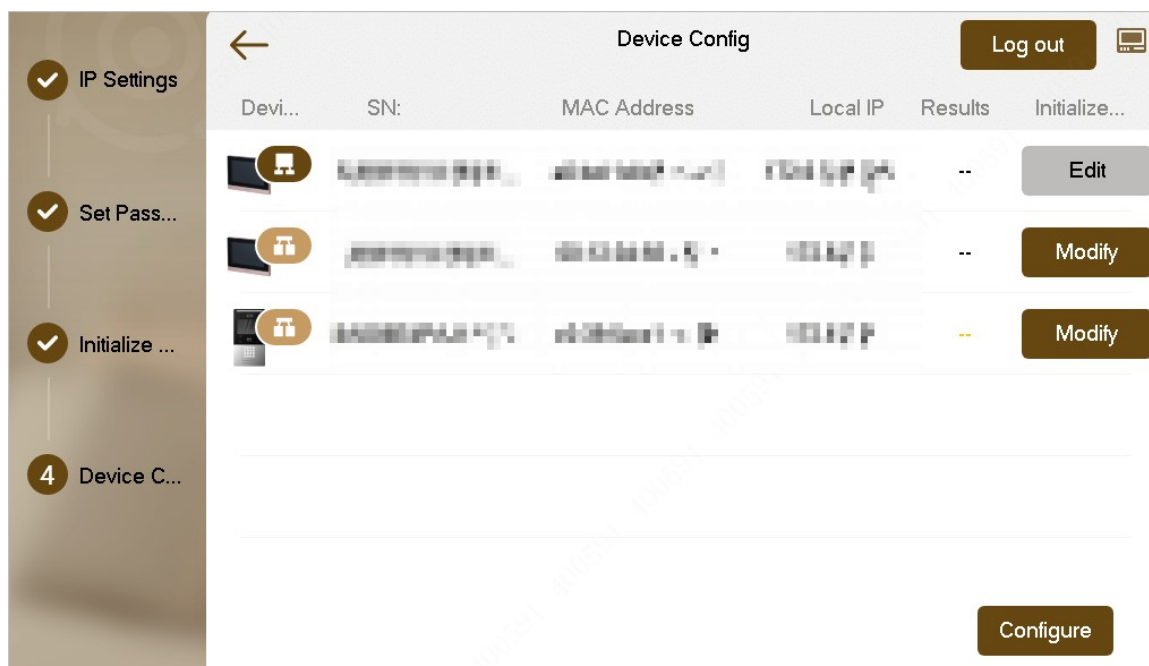

Step 11 Tap **Configure** to finish the initialization.

- **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 that 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** > [icon] > **Project Settings**.

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

Step 3   Tap [icon].

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

Figure 3-12 Network settings (1)
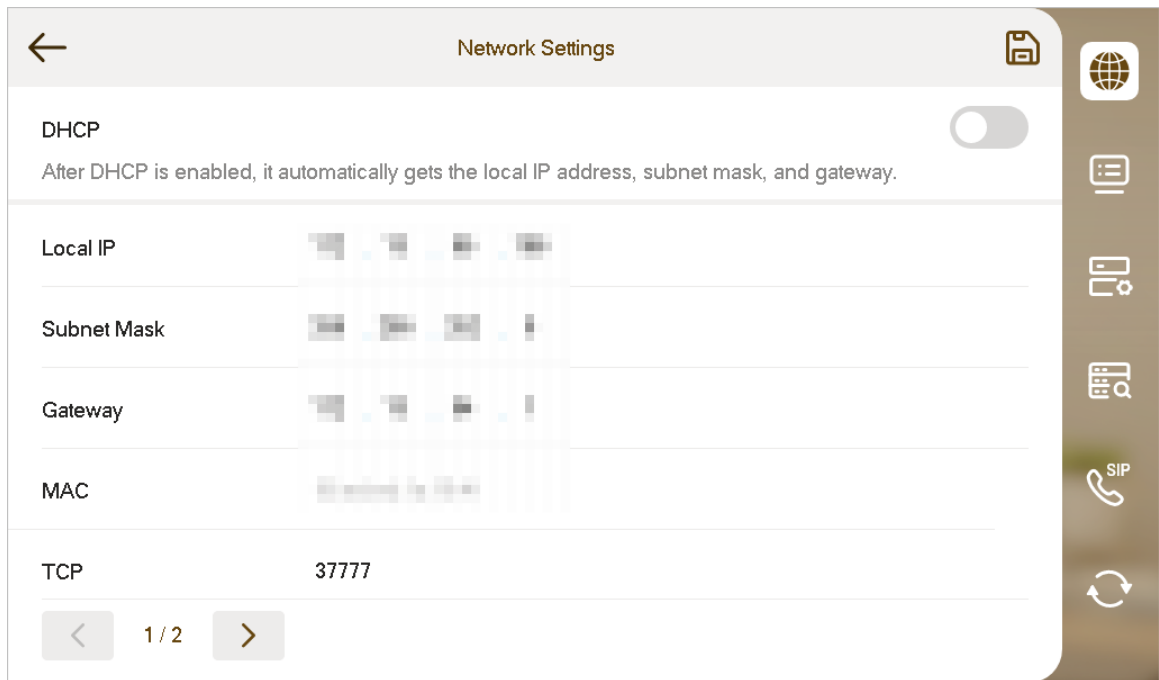
Figure 3-13 Network settings (2)

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** > ![wifi icon], and then tap **WLAN**.
2. Tap ![toggle] , select a Wi-Fi, and then enter the password to connect to the network.

Figure 3-14 Wi-Fi
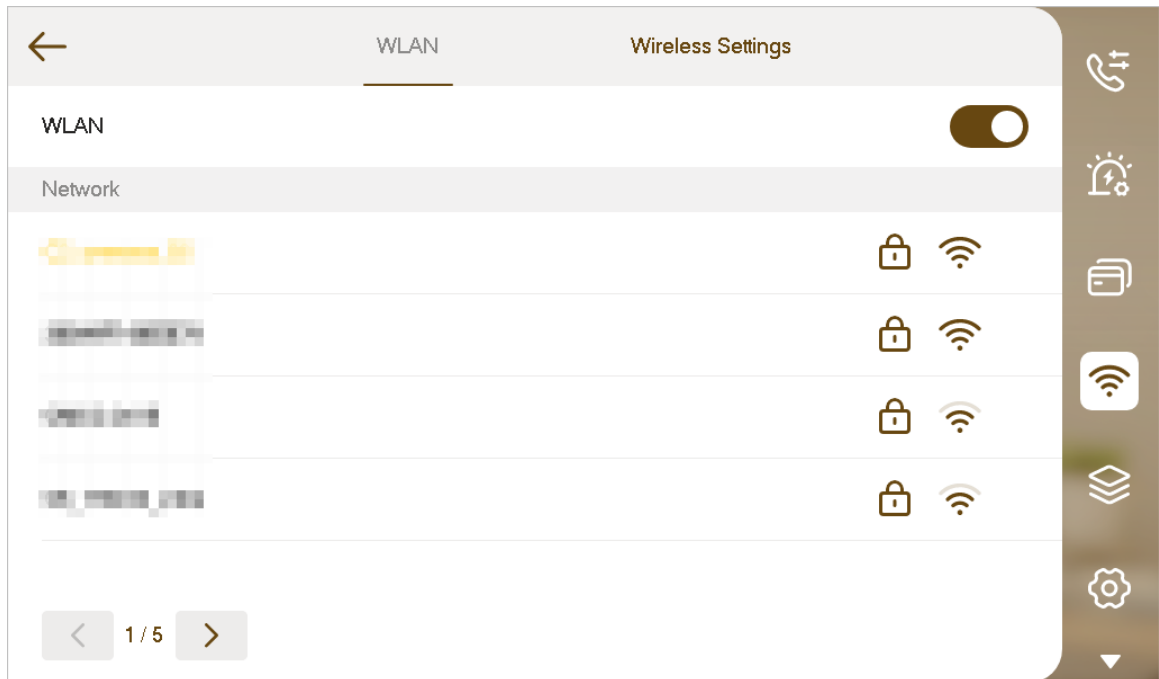
Wireless IP

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

    ![note icon]

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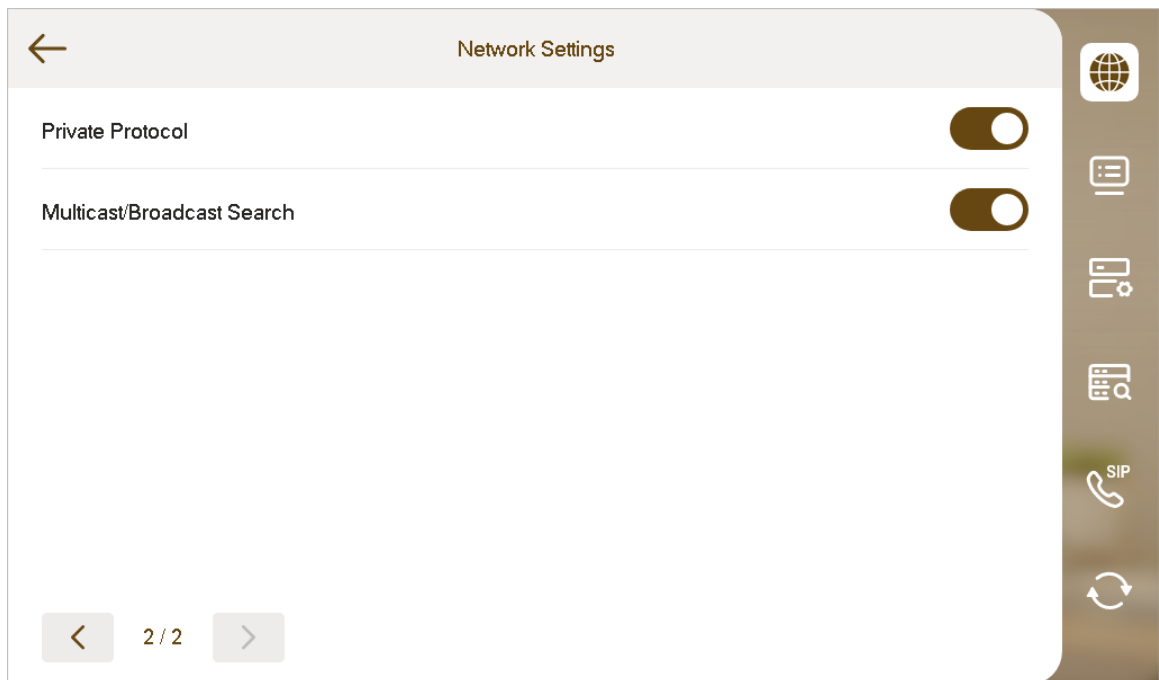
3.2.2 Configuring the SIP Server

Procedure

Step 1   On the main screen, select **Setting** > ![icon] > **Project Settings**.

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

Step 3   Tap ![SIP icon].

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	Leave it as default, or turn on **Custom Name**, and then you can edit the user name.
Registration Password	Leave it as default.
Domain	When a VTO works as the SIP server, it can be **VDP** or null. When it docks to a third-party server, it must be the same as that of the server.
Username	SIP server login user name 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 (1)

Figure 3-18 VTH configuration (2)
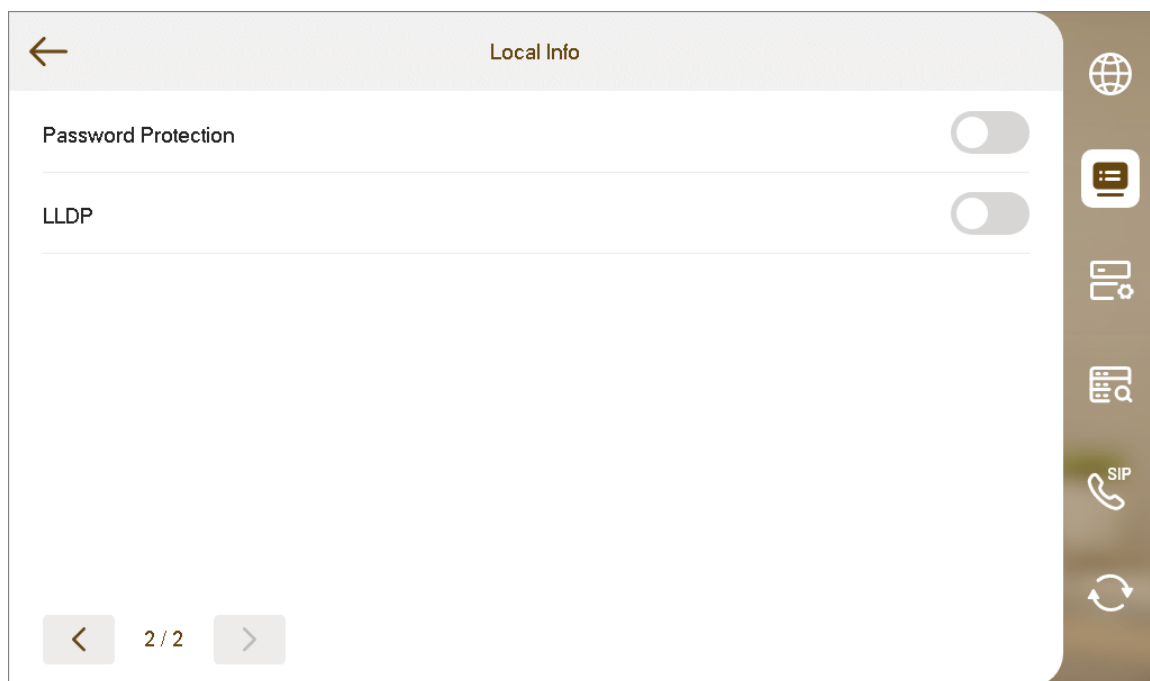
Step 4   Configure VTH information.

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.

> We recommend you turn off SSH, and turn on security mode and password protection. Otherwise, the device might be exposed to security risks and data leakage.
>   ● **LLDP** : Improves the efficiency of information exchange among network devices.

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 🗄️ .
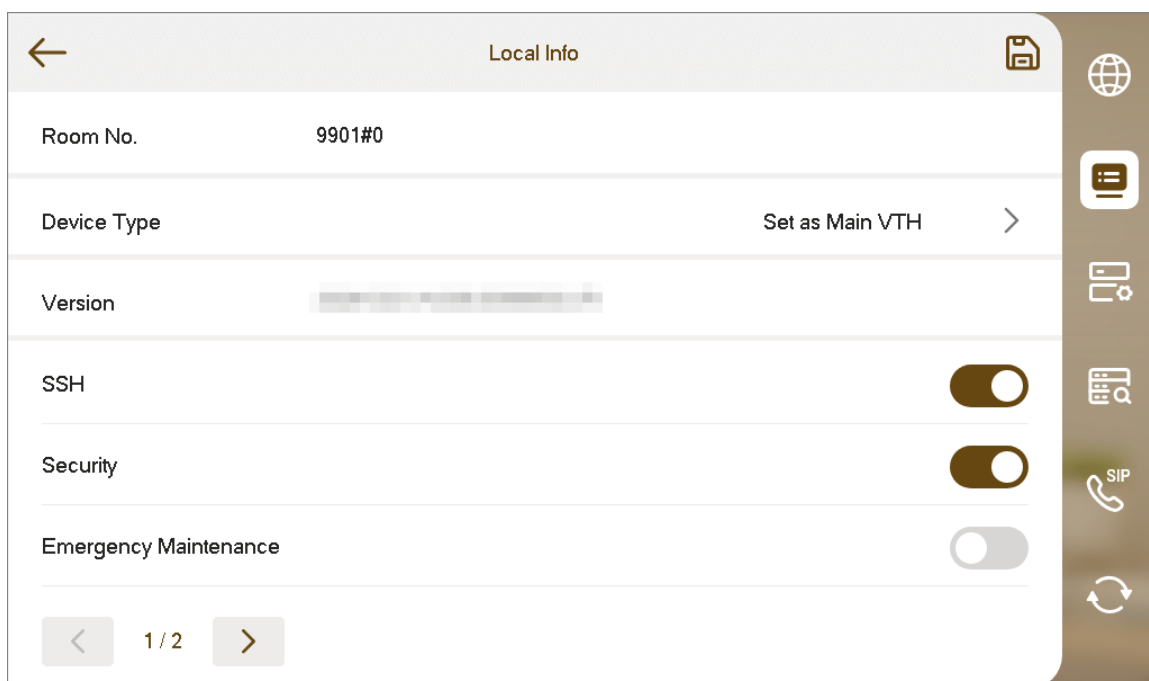
Figure 3-19 VTO configuration
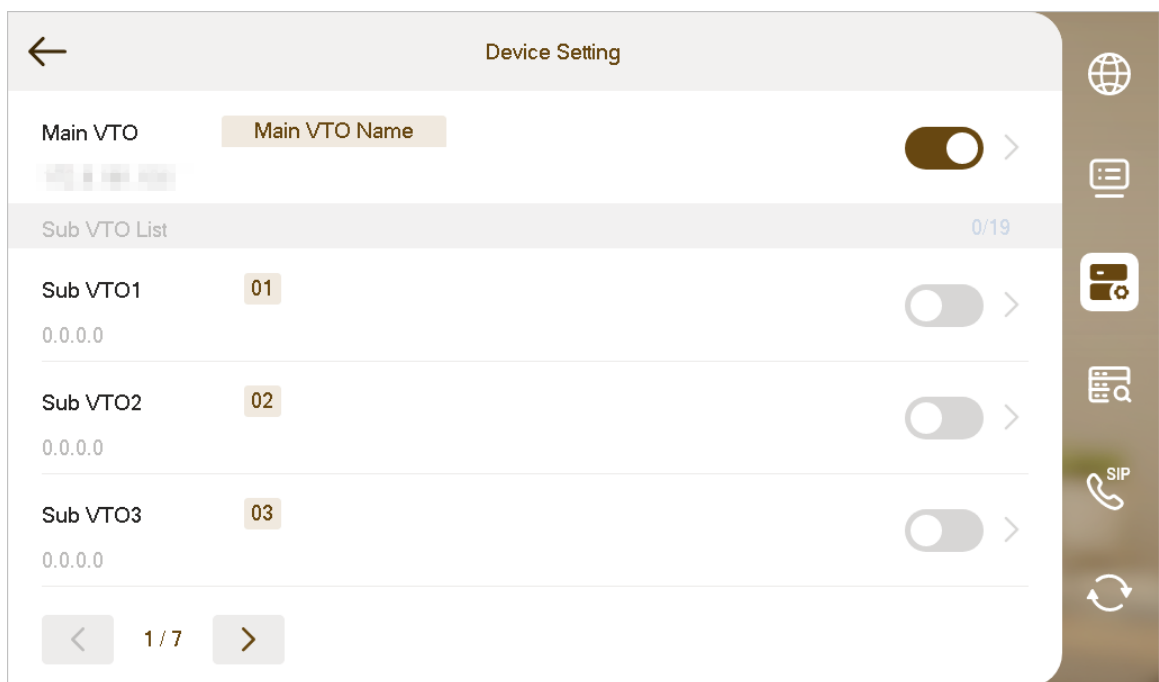
Step 4   Add a VTO or fence station.

   ● Add a main VTO.

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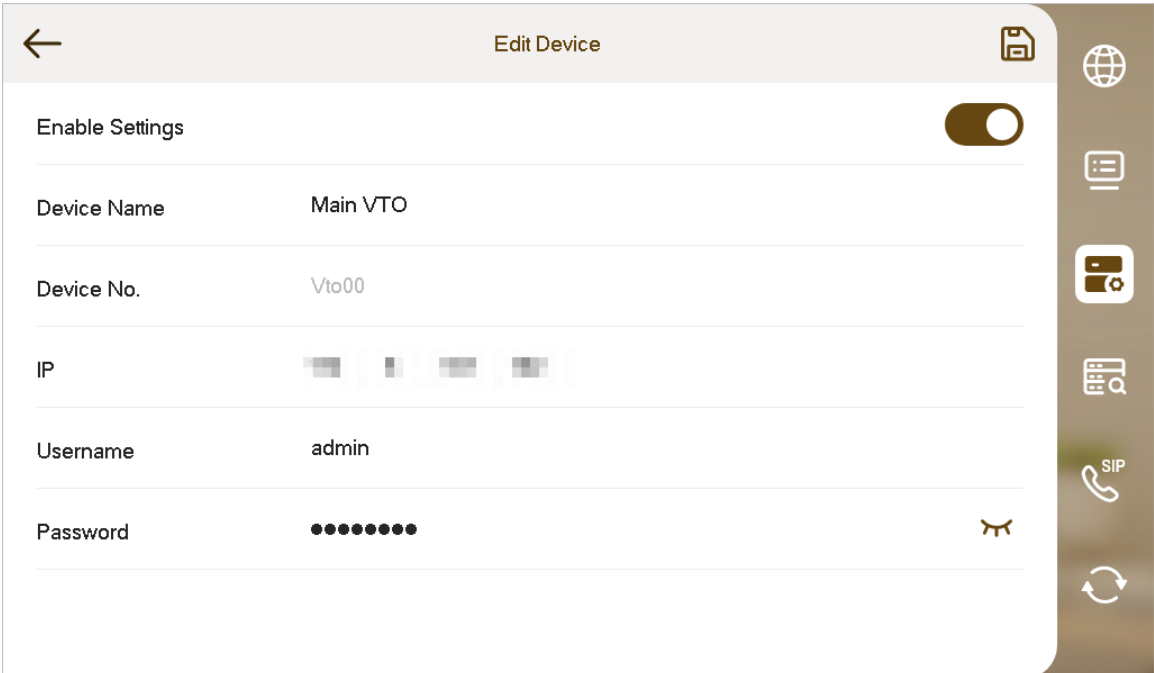
   2. Tap ⬭ .

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

3. Tap ![save icon].

Figure 3-20 Main VTO configuration

- Add a sub VTO or fence station.

    1. Tap ![arrow icon] next to the sub VTO, and then enter the sub VTO or fence station name, IP address, username and password.

    2. Tap ![toggle icon].

        Tap ![left arrow] or ![right arrow] to turn page and add more sub VTOs or fence stations.

    3. Tap ![save icon].

Figure 3-21 Sub VTO configuration

4 VTS as SIP Server Configuration

This chapter introduces how to cascade the devices when the VTS as the SIP server through ConfigTool.

Prerequisites

- Make sure that the ConfigTool has been installed on your computer.
- Make sure that the devices to be cascaded are under the smooth network and can be searched by the ConfigTool.

Procedure

Step 1   Log in to the ConfigTool.

Step 2   Search for and connect the devices (VTOs, VTHs, and VTSs) to be cascaded on the ConfigTool.

Step 3   Select **Building Config**.

Step 4   Select **Global Cascade** from the **Cascade Config** drop-down list, and then click **Global Parameters**.

Step 5   Configure the global parameters, and then click **OK**.

Figure 4-1 Global parameters
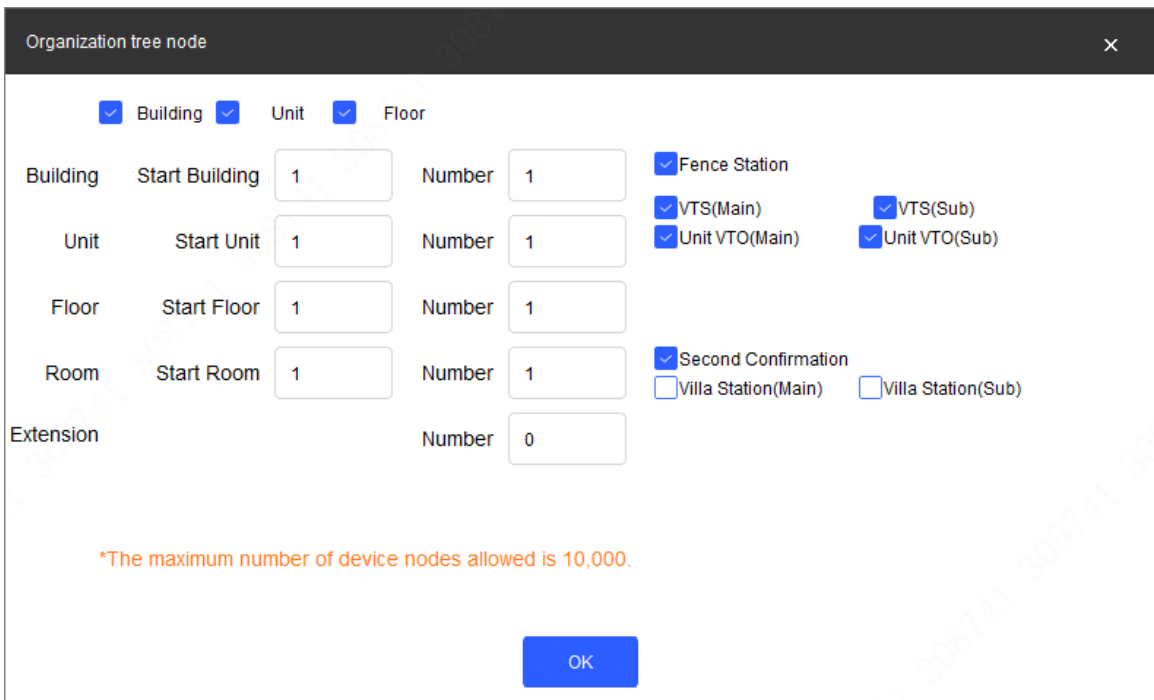
Table 4-1 Global parameters description

Parameter	Description
Center Number	It is 888888 by default.
Server Type	Leave it by default.
Server Address	The address of main server. 📖 The server here refers to the VTS.

Parameter	Description
Server Port	It is 5060 by default.
Server Username	The user name and password of the server.
Server Password	
Sip Domain	It is VDP by default.
Registered PWD	It is 123456 by default. 📖 You can also customize it.
VTO Username	The user name and password of the VTO to be cascaded.
VTO Password	
VTH Username	The user name and password of the VTH to be cascaded.
VTH Password	
VTS Username	The user name and password of the VTS to be cascaded.
VTS Password	

Step 6   Click **Add Node** to add organization tree nodes.

Figure 4-2 Add organization tree nodes

1. Select **Building** , **Unit**, or **Floor** to set in the organization tree.
2. Set the start number and quantity of **Building** , **Unit**, and **Floor** respectively.
3. Click **OK**.

Step 7   Associate the device with the organization tree node.

Figure 4-3 Add organization tree nodes
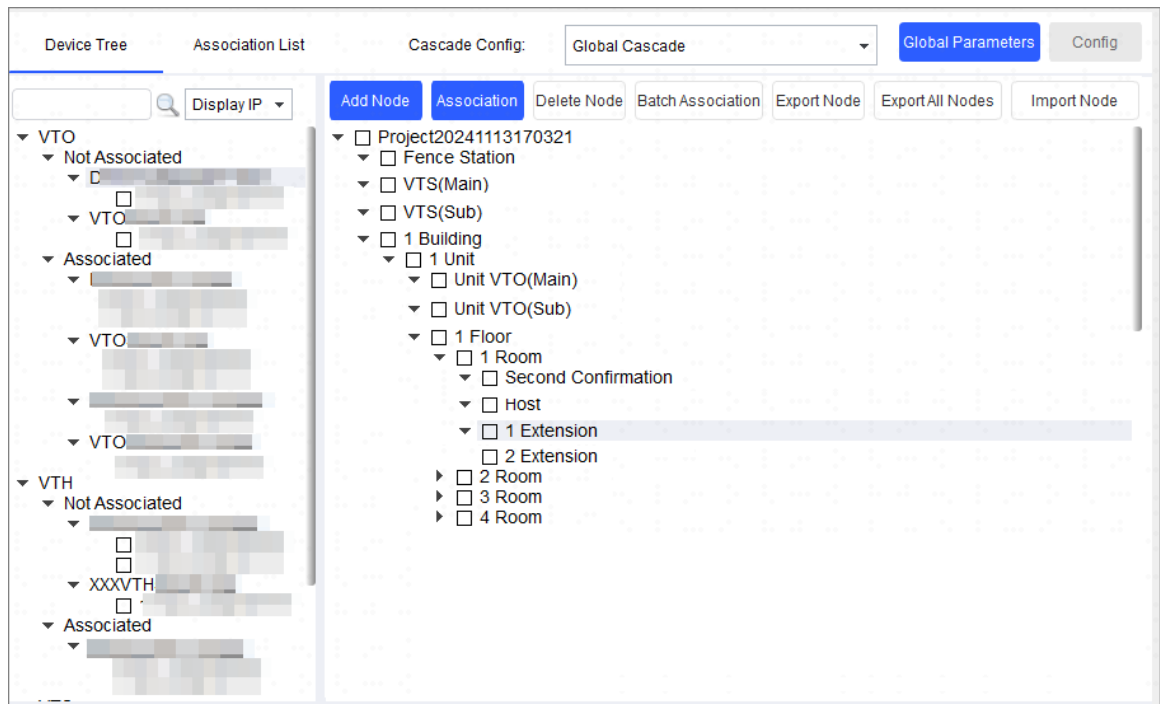
1. Select the device to be associated from the **Device Tree**.
2. Select the node to be associated from the **Node Tree**.
3. Click **Association**.

   📖

   - Fence station can be associated with 99 devices.
   - Main device only can be associated with 1 device.

Step 8   Configure the association list.

1. Click **Association List**.
2. Select the cascading models to be configured.
3. Click **Config**.

Figure 4-4 Association list

Step 9   Wait for the ConfigTool to send the task.

Figure 4-5 Successful sending
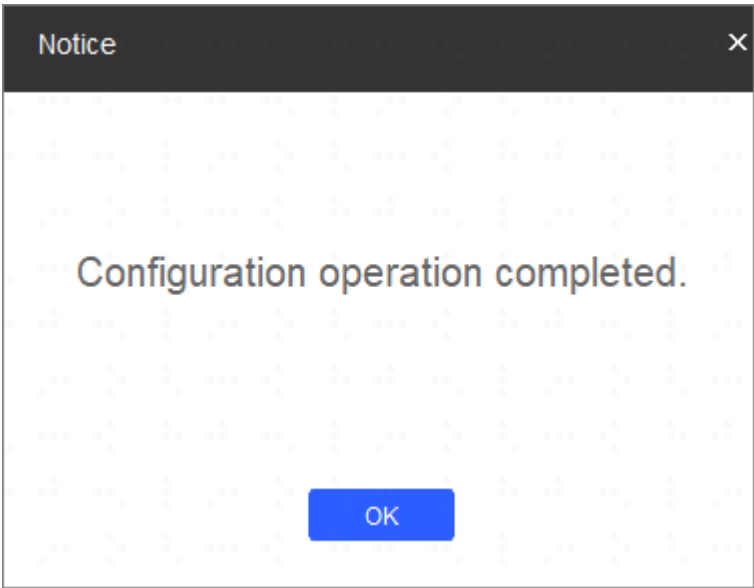
If the sending failed, click ⚠ behind the failed devices to figure out the reason.

Results

All cascading devices will restart.

5 DSS Agile VDP

You can download DSS Agile VDP (hereinafter referred to as the "app") and link your VTH to the app to unlock the door, talk to connected VTO devices, call the management center, and view call records and messages.

5.1 Downloading the App

Prerequisites

Before you start, make sure the VTO, VTH, and DSS server are properly connected.

Procedure

Step 1 On the VTH main screen, tap ▨ .

Step 2 Scan the **Download App** QR code with your smart phone, and then download and install the app.

Figure 5-1 QR code (without DMSS QR code)
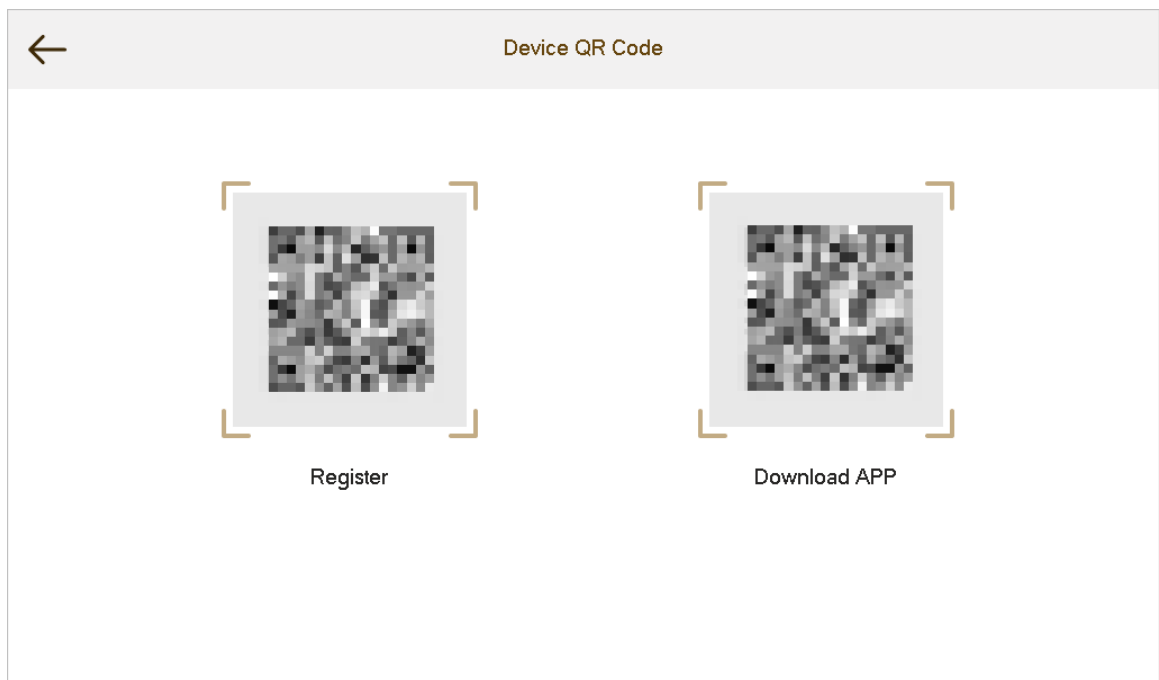
5.2 Registration and Login

After registration and login, you can bind indoor monitors (VTH) to the app to unlock doors, call door stations (VTO) and the management center, view unlocking and alarm messages, manage visitors, and more.

Procedure

Step 1 On your phone, tap ⬙ .

Step 2 On the welcome screen, tap **Scan Now**.

Step 3 Log in with an account.

5.3 Call Functions

You can receive the forwarded calls, remotely unlock the door, view live video of the VTO, and more.

📖

To receive push notifications of call messages on the mobile phone, make sure that notifications of the app are enabled on your smart phone, and you are logged in to the app.

5.3.1 Call Forward

Get your SLP ID, and then configure all forward on the VTH. If the VTH is being called, you will receive the call on the phone.

Procedure

Step 1   Log in to the app, and then tap **Me**.

Step 2   On the VTH main page, tap **Setting**.

Step 3   In the **Password Verification** dialog box, enter the password, and then tap **Forward**.

You can select the forward type as needed.

- **Always** : All the incoming calls to this VTH will be forwarded.
- **Busy** : If the VTH is busy, the call will be forwarded.
- **No Answer** : Calls not answered within defined period will be forwarded.

Step 4   Enter the SIP code in the input box of the forward type as needed.

- Forward calls to a specific user: Enter the SIP code of that user.
- Forward calls to every user: Change the last three numbers of the SIP code to 100, and then all the App users bound to the VTH will receive the forwarded call on their phone simultaneously.

Step 5   Tap 🔲ᴼᶠᶠ to enable the function, and then tap **OK** to save configurations.

5.3.2 Calling Operations

You can receive and answer calls from intercoms such as VTO and the management center.

For example, when the VTO is calling, you can answer the call, view live video, and unlock the door remotely if the VTO has connected to a lock.

5.4 Monitor

After a VTO is added, you can view its live video, have two-way audio talk with it, call management center, and unlock the door connected to it.

Procedure

Step 1   Log in to the app, and then tap **Home**.

Step 2   Select the VTO from the channel list as needed, and then the live view is displayed.

- Tap **Open door** to open the door remotely.
- Tap **Intercom** to enable two-way audio talk with the VTO.
- Tap **Unlock & Give lift Permission** to unlock and give lift permission remotely.

- Tap 📞 to call the management center.

- Tap ⓘ to stop viewing live video.
- Tap ◁× to enable the sound.
- Tap ⬛ᴹˢ to switch main stream to sub stream.

5.5 Records

You can view the incoming and outgoing call records.

Log in to the app, and then tap **Home**.

5.6 Visitor

You can create a pass for a visitor to have access permission. The pass is invalid after it is manually invalidated, the visiting period expires, or the visit is ended. You can also view visit records.

5.6.1 Generating Pass

Procedure

Step 1   Log in to the app, and then tap **Visitor** at the bottom of the screen.
Step 2   Generate a pass QR code for the registered visitor.

1. Tap ⊕, select a visitor in the list, and then tap **Confirm** to add visitor information.
2. Tap **Generate Visitor Pass** to directly generate a pass QR code.

5.6.2 Visitor Records

You can view the visitor status and modify the pass information.

- View visitor status: Log in to the app, tap 📇, and then tap 📅.
- View and modify pass: Tap a visitor in the list, and then you can view the detailed pass information.

6 DMSS App

You can download DMSS App and link your VTH to the app to unlock the door, talk to connected VTO devices, call the management center, and view call records and messages.

6.1 Installing the DMSS and Signing up

You can sign up an account with an email address or phone number.

Procedure

Step 1   Search for DMSS in the App store, and then download the app.

Step 2   On your phone, tap to start the app.

Step 3   Create an account as the instructions.

Step 4   On the **Log in** screen, enter your email/phone number, and password, and then tap **Log in**.

6.2 Adding VTH to DMSS

Prerequisites

Power on the VTH.

Procedure

Step 1   On the **Home** screen of the app, tap, and then select **SN/Scan**.

Step 2   Scan the QR code at the rear panel of the VTH to obtain the information.

Step 3   On the **Add Device** screen, enter the device name of the VTH, user name and password of the VTH, and then tap **Save**.

Step 4   Configure the time zone, and then tap **Done**.

6.3 DMSS Operating the VTO/VTH

You can watch the live view, access video intercoms, make video calls between the device and the app, lock and unlock doors, and more. Here uses the VTO as the example.

Procedure

Step 1   On the **Device** screen, tap a VTO.

Step 2   Tap **Preview** to go to the live video page of the VTO.

Step 3   Operate the VTO as needed.

6.4 DMSS Configuring Arm and Disarm

Prerequisites

Make sure that the VTH and VTO are properly connected.

Procedure

Step 1   On the **Home** screen, tap, select the VTH you have just added, and then tap **Device Details**.

Step 2   Tap **Disarm** or **Arm** to disarm or arm the VTH.

Step 3   Select the arm/disarm mode as needed.

6.5 Sharing Devices

You can share devices with up to 6 DMSS users.

Procedure

Step 1   On the **Device** screen, tap ● ● ● next to a device, and then tap **Share Devices**.

Step 2   On the **Share Devices** screen, share the device with the user by entering their DMSS account or scanning their QR code. You can also enter the phone number to share the devices.

📖

Device sharing via phone number is only supported in selected countries or areas.

Step 3   Select permissions as needed.

Step 4   Tap **OK**.

6.6 Entrusting Devices to Dolynk Care via DMSS

You can entrust devices one by one or in batches.

If the system cannot work properly, the installation maintenance service is needed.

6.6.1 Entrusting the Device One by One

Prerequisites

You have bound with a service provider.

Procedure

Step 1   On the **Device** screen, tap ● ● ● next to a device, and then tap **Device Details** > **Device Info**.

Step 2   Tap **Entrust**.

Step 3   Select entrusting periods and permissions, and then tap **OK**.

Step 4   Read and select **I have read and agree User Agreement**, and then tap **Next**.

6.6.2 Entrusting Devices in Batches

Procedure

Step 1   On the **Device** screen, select **Me** > **Service** > **Service Provider**, and then tap ⊕.

Step 2   Confirm the information of the bound service provider.

Step 3   Select the devices to be entrusted.

7 Dolynk Care

7.1 DoLynk Care Client

7.1.1 Signing Up and Login

Procedure

    Step 1   Open the browser, enter the web address, and then press the Enter key.

    Step 2   Click **Create Account** to create an account.

    Step 3   Enter the verification code that was sent to the registered email or phone number, and then read and select **I have read and agree to Privacy Policy and Terms and Conditions** . Click **Sign up**.

    Step 4   On the login page, enter email or phone number, and password, and then click **Log in**.

7.1.2 Adding Sites

Procedure

    Step 1   Log in to the platform.

    Step 2   Click **Sites** on the console page.

    Step 3   Add a site and configure the parameters according to the actuality.

    Step 4   Click **OK**.

7.1.3 Adding Devices

Procedure

    Step 1   Log in to the platform.

    Step 2   Select the site that you want to add the device to.

    Step 3   Add devices as needed.

7.1.4 Delivering Devices

    You can deliver devices to customers.

Procedure

    Step 1   Click a site on the site list page.

    Step 2   Click **Deliver**.

        1. Select the devices that you want to deliver.

        2. Deliver the device to the binding customer of the site.

        3. Confirm the customer information, including the customer name and email.

        4. Select the device that you want to deliver, and then read and select **I have read and agree to Service Provider Agreement**.

        5. Click **Next**.

        6. (Optional) Request permissions.

Table 7-1 Instruction of permissions

Permission	Description	Note
Health Management	Select by default, which cannot be canceled.	—
Video Devices	You can request for the permissions of device configuration, live video and playback. • Configuration permissions: Including restart and upgrade the device, format SD card and configuration plug-in. • Live video and playback: View the live video, playback the recordings and the video permission of the plug-in.	You can choose temporary permissions, such as 1 hour or 4 hours, or opt for authorization during the whole entrusting period.
Alarm Devices	You can request for the permissions of device configuration and operation.	
Video Interconnect Devices	You can request for the permissions of device configuration and operation.	

Step 3   Click **OK**.

7.1.5 Lending Devices

The users of DoLynk Care lend the video devices and alarm devices to DMSS users. Supports configuring the lending period and permissions.

Procedure

Step 1   Select a site on the site list page.

Step 2   Click **More** > **Lend**.

Step 3   Set the lending period.

Step 4   Select the devices that you want to lend, read and then select **I have read and agree to Rules for Entrusting**.

Step 5   Configure the permissions.

Step 6   Click **OK**.

7.1.6 Entrusting Device

For the delivered devices, DoLynk Care users can request for device entrusting from DMSS users to be authorized for device configuration and operation.

Procedure

Step 1   Select a site on the site list page.

Step 2   Select **More** > **Entrusting**。

Step 3   Set the entrusting period.

Step 4   Select the devices that you want to entrust, read and then select **I have read and agree to Service Provider Agreement**.

Step 5   Configure the permission.

Step 6   Click **OK**.

7.1.7 Requesting for Operation Permissions

You can apply for permissions on the devices that have been entrusted or lent.

Procedure

Step 1　　Select the site on the site list page.

Step 2　　Select **More** > **Apply for Permission**.

Step 3　　Select the device that you want to request for permissions, and then click **Next**

Step 4　　Configure the permission types and period.

Step 5　　Click **OK**.

7.2 DoLynk Care App

7.2.1 Installing Dolynk Care and Signing Up

Procedure

Step 1　　Search for DoLynk Care in App store, and then download the app.

Step 2　　On your phone, tap 📱 to start the app.

Step 3　　Create an account as the instruction.

Step 4　　On your phone, tap 📱 to start the app.

Step 5　　Enter your email address or phone number, and password, and then tap **Log in**.

7.2.2 Adding Sites

In DoLynk Care, devices are managed in sites.

Procedure

Step 1　　Tap ⊕ on the upper-right corner of the screen.

Step 2　　Tap **Add Site**.

Step 3　　Configure the parameters as needed.

7.2.3 Adding Devices to a Site One by One

Add devices to the app for management and maintenance. You can add the VTO or VTH by entering the SN or scanning the QR code. Supports searching for the devices in the same LAN.

📖

- Before adding devices, make sure that the device is connected to the power and the network.
- Make sure that your phone has enabled Wi-Fi function.

7.2.3.1 Adding by SN/QR Code

You can add devices by scanning the QR code of the device or manually entering device SN in the wireless or wired network.

Procedure

Step 1   On the home screen, tap ⊕.

Step 2   Scan device QR code.

Step 3   Select a site, and then tap **OK**.

Step 4   Select a device type.

Step 5   Tap **Completed**.

7.2.3.2 Adding by LAN Searching

Tap ⊕ > **Discover LAN** on the upper-right corner of the home screen. You can search for devices and add them. Make sure that your phone and the devices are connected to the same network.

7.2.4 Adding Devices to Dolynk Care Cloud in Batch

Prerequisites

If you add the devices to cloud in batches, the device user name and password must be the same, or you can use the preset user name and password.

Procedure

Step 1   Log in to the app.

Step 2   Tap **Tools** on the bottom of home screen.

Step 3   Tap **Add Device to Cloud**.

Step 4   Select the devices, and configure the cloud platform parameters.

Step 5   Tap **OK**.

Step 6   Select the site that you want to bind the device to.

Step 7   Tap **Save**.

7.2.5 Delivering Devices

You can deliver devices to the customers. Offline and entrusted devices cannot be delivered.

Procedure

Step 1   Tap **Sites** on the bottom of the screen.

Step 2   Tap a site on the site list.

Step 3   Deliver devices as instruction.

Step 4   Tap **OK**.

8 DoLynk Pro

8.1 DoLynk Pro Client

8.1.1 Signing Up and Logging In

You need to create an account for your first-time login.

Procedure

Step 1   Open the browser, enter the address, and then press Enter.

Step 2   Create an account according to the actuality.

Step 3   Enter the verification code and click **I have read and agree Privacy Policy and User Agreement and DoLynk Pass Privacy Policy**.

Step 4   Click **Register**.

Step 5   Enter the email address or phone number, and password, and then click **Log in**.

8.1.2 User and Role Management

You can create roles and add users to the platform. The users are assigned with different roles, which determines that they have different permissions for sites, operations and menus.

8.1.2.1 Adding Roles

A role is a set of permission.

Procedure

Step 1   Log in to the platform.

Step 2   Select **Users** > **Role**.

Step 3   Click **Add**.

Step 4   Enter the name of the role, and then select the menu permissions of webpage and app.

Step 5   Click **OK**.

8.1.2.2 Adding Users

You can add the user to manage and operate the platform.

Prerequisites

You have created roles.

Procedure

Step 1   Log in to the platform.

Step 2   Select **Users** > **Users**.

Step 3   Click **Add**, and then configure the parameters according to the actuality.

Step 4   Click **OK**.

8.1.3 Adding Devices

Prerequisites

You have added the sites.

Procedure

Step 1   Log in to the platform.

Step 2   Click **Device**.

Step 3   Click **Add Device** > **Add Device**.

Step 4   Select the site for the device.

Step 5   Configure the device information.

Step 6   Follow the guide to add the device.

Step 7   Click **OK**.

8.1.4 Site Management

The user who has the permission can add, edit and delete the sites.

Procedure

Step 1   Log in to the platform.

Step 2   Click **Sites**.

Step 3   Enter the site name to add a site, and then click **OK**.

8.1.4.1 Managing Device in Site

You can manage the devices in the site, including adding, viewing, moving and deleting devices.

Procedure

Step 1   Click **Sites**.

Step 2   Select **Device**.

Step 3   Managing devices in the site, such as adding, moving, viewing and set the devices.

8.1.4.2 Entrusting the Site

Supports entrusting the site to the bound installer.

Procedure

Step 1   Click **Site** on the console page.

Step 2   Select the site that you need to entrust.

Step 3   Configure the entrusting period and permissions.

Step 4   Read **User Entrusting Rule** , and then select **I have read and agree to User Entrusting Rule**.

Step 5   Click **OK**.

8.2 DoLynk Pro App

8.2.1 Installing the DoLynk Pro and Signing up

When the users log in to the app for the first time, if you already have the accounts, you can log in directly.

Procedure

Step 1   Search for the DoLynk Pro app in App Store or Google Play to download and install the app.

Step 2   Tap 🔷 to start the app.

Step 3   Enter the email/mobile phone number and password.

Step 4   Read and select policies, and then tap **Login**.

8.2.2 Adding Devices

The admin accounts can add devices by scanning QR code or online searching on device management screen.

8.2.2.1 Adding by SN/QR Code

You can add devices by scanning the QR code of the device or manually entering device SN in the wireless or wired network.

Prerequisites

- The device has been connected to the power and initialized in the same LAN with your mobile phone.
- The device has been connected to the network wireless or wired.

Procedure

Step 1   Log in to the app.

Step 2   Tap ✛, and then select **SN/Scan**.

Step 3   On the **Add Device** screen, select a device type.

Step 4   Enter the password of the device, and then tap **Save**.

8.2.2.2 Adding through AP Configuration

You can add devices through AP configuration.

Procedure

Step 1   Log in to the app.

Step 2   On the **Add Device** screen, select a device type.

Step 3   Follow the instructions to configure network.

Step 4   Select **Switch to AP configuration** . Follow the on-screen instructions to enable the device hotspot, and then tap **Next**.

Step 5   Following the on-screen instructions to connect your mobile phone to the Wi-Fi.

Step 6   Enter the device password, and then tap **Next**.

8.2.2.3 Adding by LAN Searching

When your mobile phone and the devices are connected to the same network, you can search for devices and add them.

Procedure

    Step 1   Log in to the app.

    Step 2   Tap ┼, and then select **Online Search**.

    Step 3   Select the device that you want to add on the search result screen.

    Step 4   Enter the password of the device, and then tap **Save**.

8.2.3 Sites Management

Manage sites information. You can add, delete, modify and fuzzy search for sites.

Procedure

    Step 1   Log in to the app.

    Step 2   Select **Me** > **Sites**.

    Step 3   Tap ⊕, enter the site name and tap **Save**.

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).