Digital Face Recognition Door Station

Quick Start Guide

V1.0.1

Foreword

General

This manual introduces the structure, mounting process, and basic configuration of the device.

Update Instruction

During update, keep the power on until the update is completed.

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.0.1	Add description of car issuing and face recogniton on the VTO.	November 2021
V1.0.0	First release.	September 2020

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit

our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Operation Requirements

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

Installation Requirements

 **WARNING**

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

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- Make sure the power supply meets the SELV (Safety Extra Low Voltage) requirements, and rated voltage conforms to the IEC60065, IEC60950-1 or IEC62368-1 standard. The requirements of the power supply are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Table of Contents

1 Overview

1.1 Introduction

This Digital Face Recognition Door Station (hereinafter referred to as "VTO") can be connected to the indoor monitors (VTHs), VTS, or third party servers to form a video intercom system.

The VTO supports fingerprint unlock, face unlock, card unlock and other functions including emergency call, announcement, and history viewing.

1.2 Features

- Voice/video calls: Make voice/video calls to VTS or VTH.
- Group call: Call multiple VTHs at a time.
- Video surveillance: Monitor areas around the VTO from VTH or management center.
- Emergency call: Press a key to call the Center in case of an emergency.
- Auto-snapshot: Take pictures automatically during unlocking or call, and store them in FTP.
- Alarm: Support various alarms, including tampering and door contact. Once an alarm is triggered, a report will be sent to the management center.
- Unlocking: Card, fingerprint, face and remote unlock.
- Announcement: Send messages to multiple VTHs.
- History viewing: View call, alarm and unlocking history.

2 Appearance

Slight differences might be found in the front and rear panel of different models of the VTOs.

Figure 2-1 Dimensions (mm [inch])

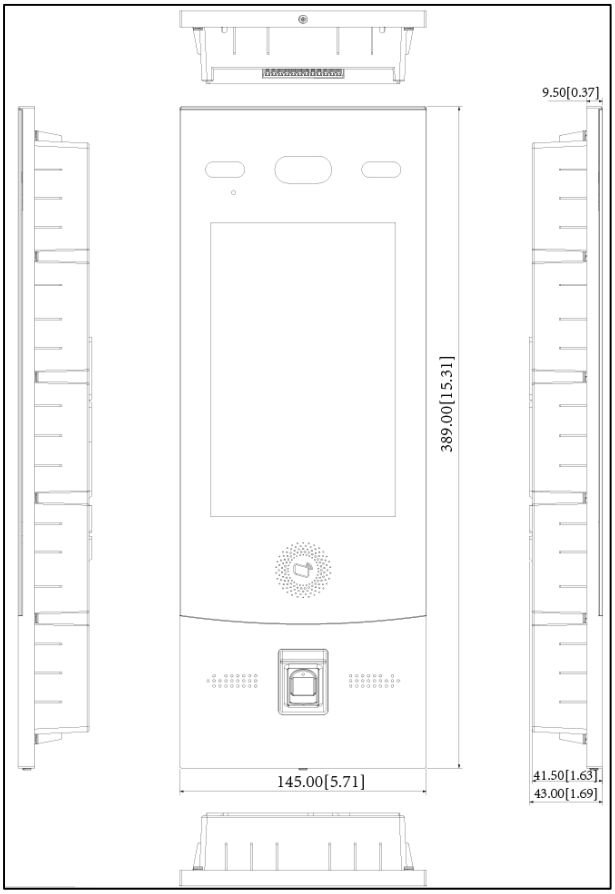


Figure 2-2 Components

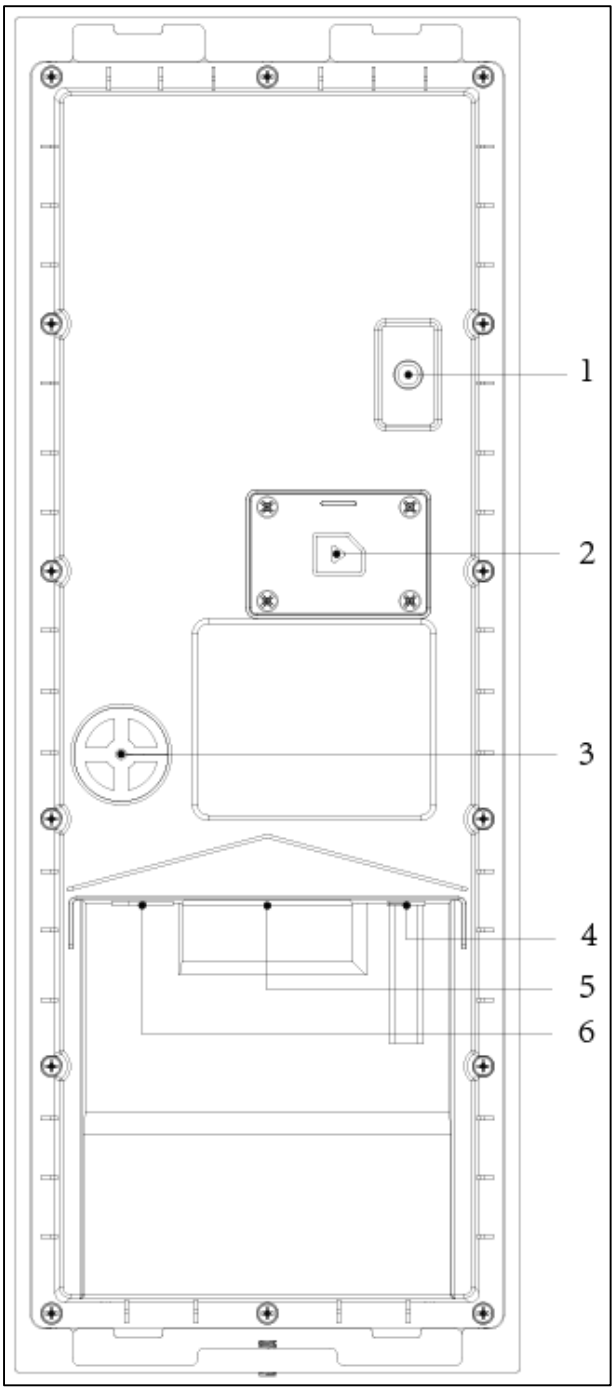


Table 2-1 Component description

No.	Function name
1	Tamper switch
2	SIM card cover
3	4G external antenna port
4	Power port
5	Function ports (such as alarm in/out port, lock port, and wiegand page)
6	Ethernet port

3 Connecting Cable

Connects to door locks, and the connection method varies with different locks. See below for details.

Figure 3-1 Connect cables (1)

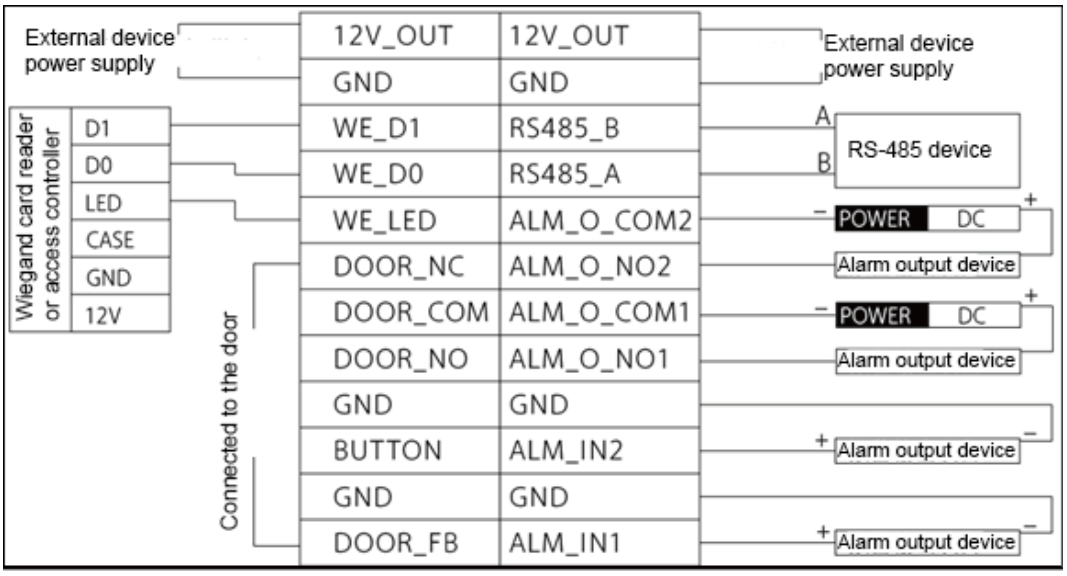
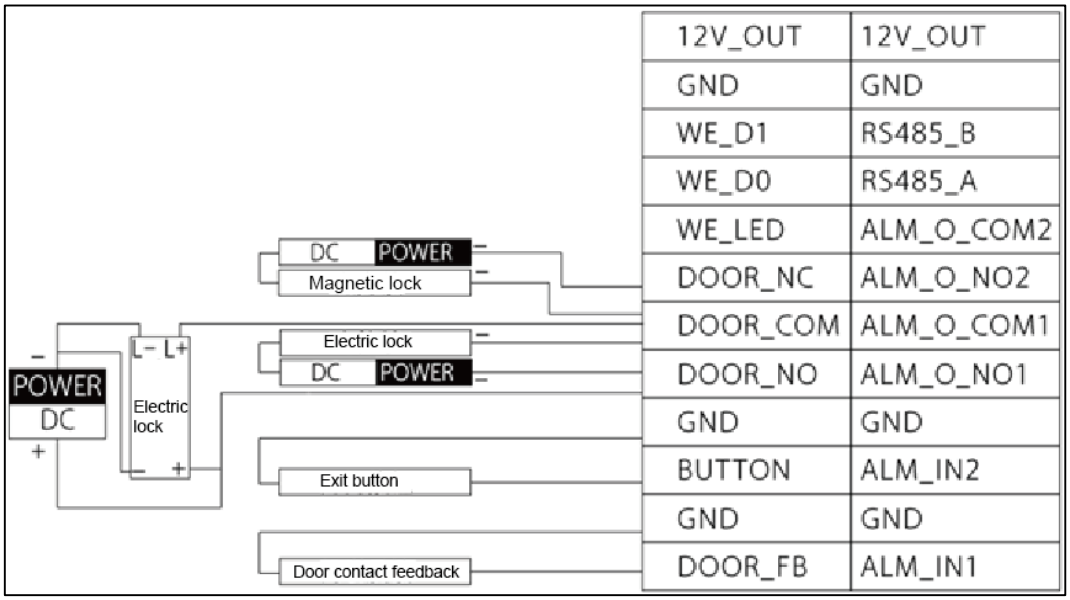


Figure 3-2 Connect cables (2)

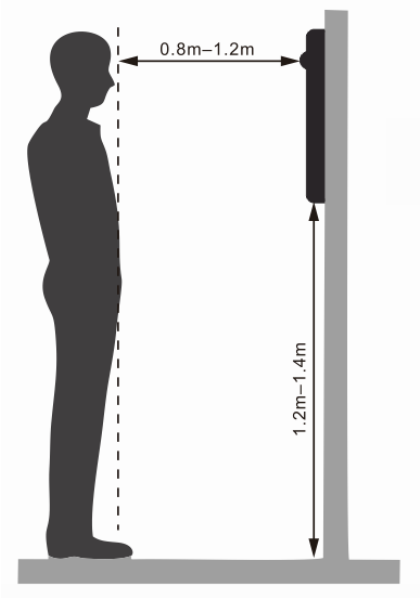


4 Installation

- Do not install the VTO in places with condensation, high temperature, grease or dust, corrosive substance, direct sunlight, or no shelter.
- Installation and configuration should be done by professional teams, and do not dismantle or repair the VTO by yourself. Contact technical support.

See the figure below for the installation position. The human face should face the center of the VTO.

Figure 4-1 Installation position



5 Web Configuration

This chapter provides a step-by-step configuration of the VTO, as well as how to register digital indoor monitors (hereinafter referred to as the "VTH") into the VTO to realize its intercom function. Follow the instructions below to get started.

The snapshots are for reference only and slight differences might be found in the actual web page of the VTO, depending on your model.

5.1 Procedure

Before configuration, check every device and make sure there is no short or open circuit.

Step 1 Plan IP and number (works as a phone number) for each device.

Step 2 Configure the web of the VTO. See "5.3 Configuring VTO".

1) Initialize the VTO. See "5.3.1 Initialization".
2) Configure VTO network parameters. See "5.3.2 Configuring Network Parameters".
3) Configure VTO number. See "5.3.3 Configuring VTO Number".
4) Configure the SIP Server. See "5.3.4 Configuring SIP Servers".
5) Add VTOs to the SIP server. See "5.3.5 Adding VTO".
6) Add room number to the SIP server. See "5.3.6 Adding Room Number".
7) Issue cards for registered users. See "5.3.7Issuing Cards Issuing Cards".

Step 3 Configure the VTH. See the VTH users' manual.

Step 4 Commission call functions and user registration. See "6 VTO Operation".

5.2 Configuration Tool

You can download the configuration tool VDPConfig and use it to configure and update multiple devices. For more details, see the corresponding user's manual.

5.3 Configuring VTO

Connect the VTO to your PC with network cable, and configure its web. If you log in for the first time, you need to create a new login password for the web page.

5.3.1 Initialization

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

Step 1 Power on the VTO.

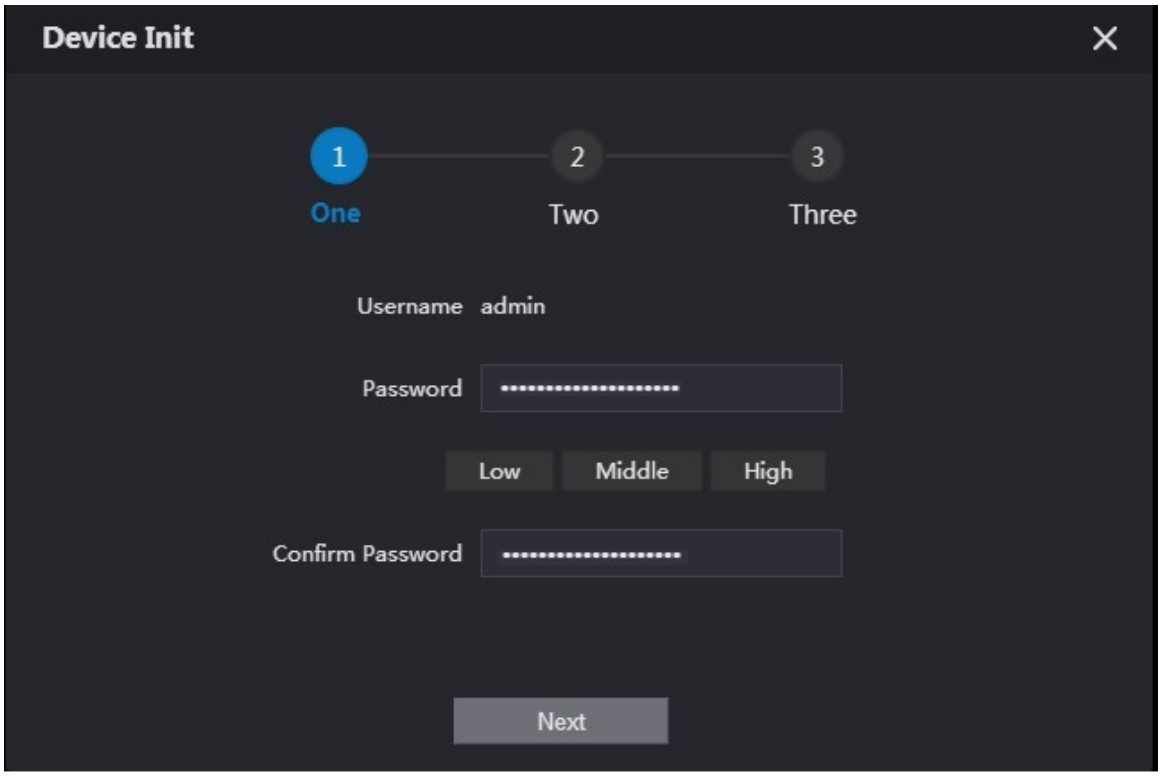
Step 2 Go to the default IP address (192.168.1.108) of the VTO in the browser address bar, and then press the Enter key to go to the web page of the VTO.

- The user name is admin by default.
- Make sure that the IP address of the PC is on the same network segment as the VTO.

Step 3 On the **Device Init** page, enter and confirm the password, and then click **Next**.

The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).

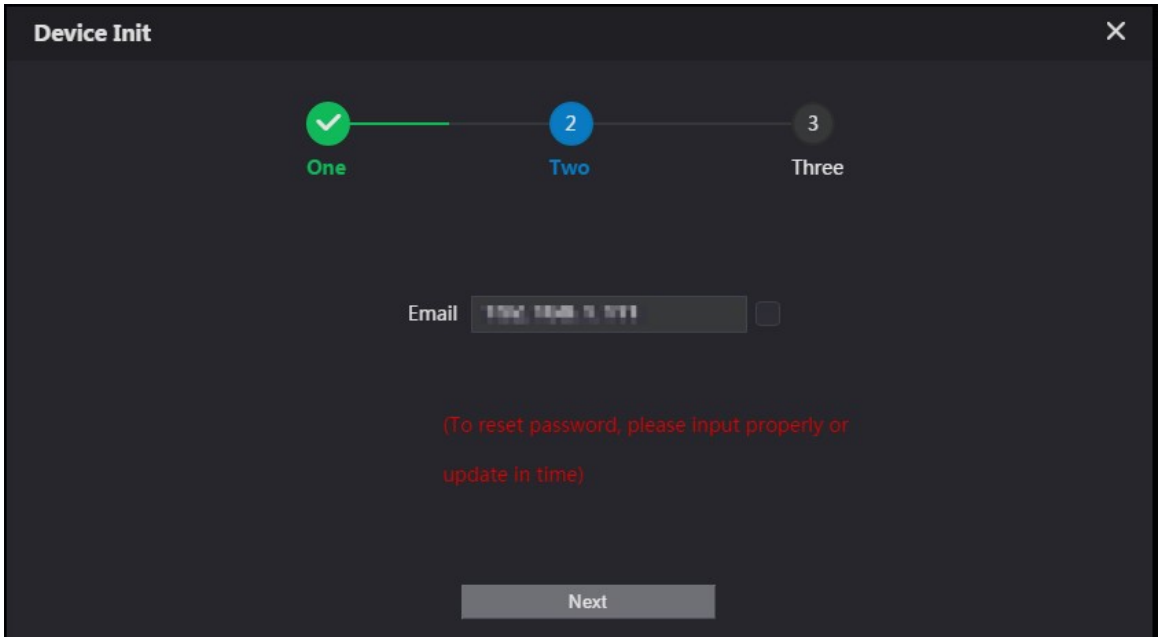
Figure 5-1 Device initialization



Step 4 Select the **Email** checkbox and enter email address.

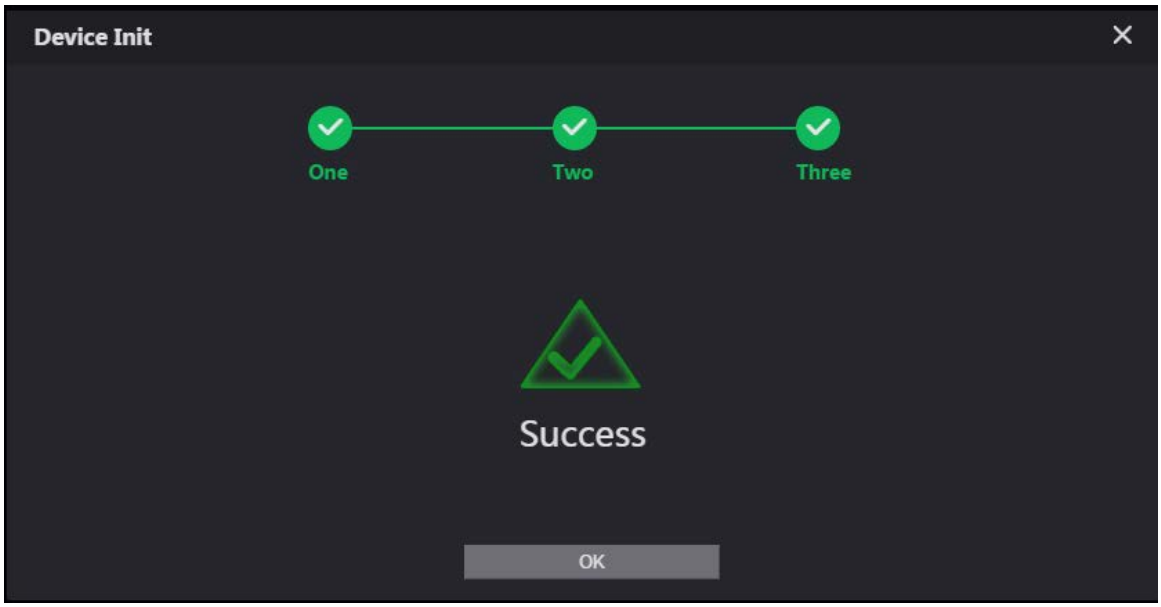
This helps you to reset your password when your password is lost or forgotten.

Figure 5-2 Set an email address



Step 5 Click **Next**.

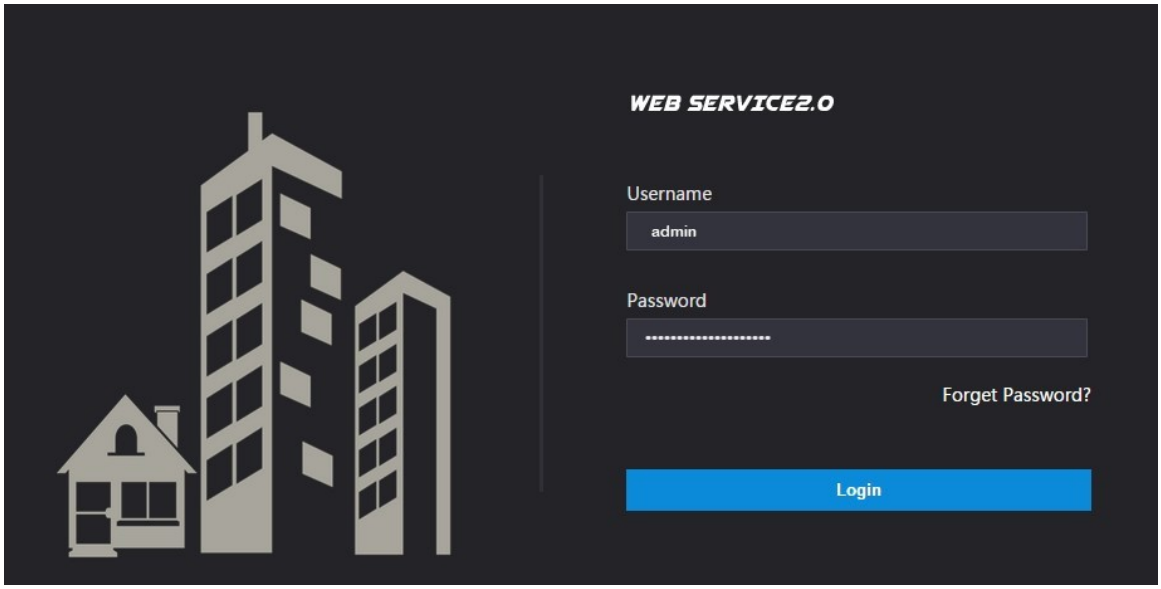
Figure 5-3 Initialization successful



Step 6 Click **OK**.

Enter username (admin by default) and the new password to log in to the web page.

Figure 5-4 Login page

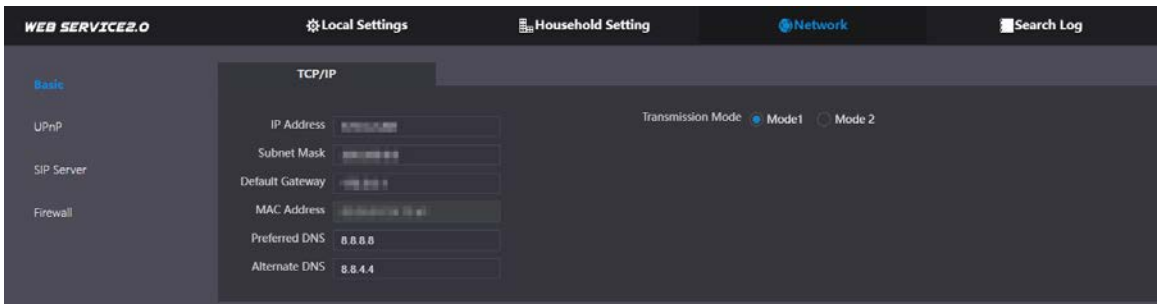


5.3.2 Configuring Network Parameters

You need to configure the TCP/IP information to connect the VTO to the network.

Step 1 Select **Network Setting** > **Basic**.

Figure 5-5 TCP/IP information



Step 2 Enter each parameter and click **Save**.

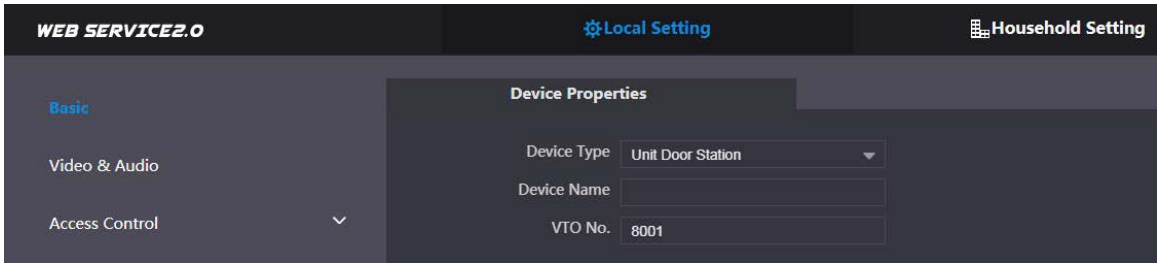
5.3.3 Configuring VTO Number

Numbers can be used to distinguish each VTO, and it is recommended set it according to unit or building number.

Step 1 Log in to the web page of the VTO.

Step 2 Select **Local Setting** > **Basic**.

Figure 5-6 Device properties



Step 3 Enter the number in **VTO No.**, and then click **Save**.

- You can change the number of a VTO when it is not working as the SIP server.
- A VTO number can contain up to 5 numbers, and it cannot be the same as any room number.

5.3.4 Configuring SIP Servers

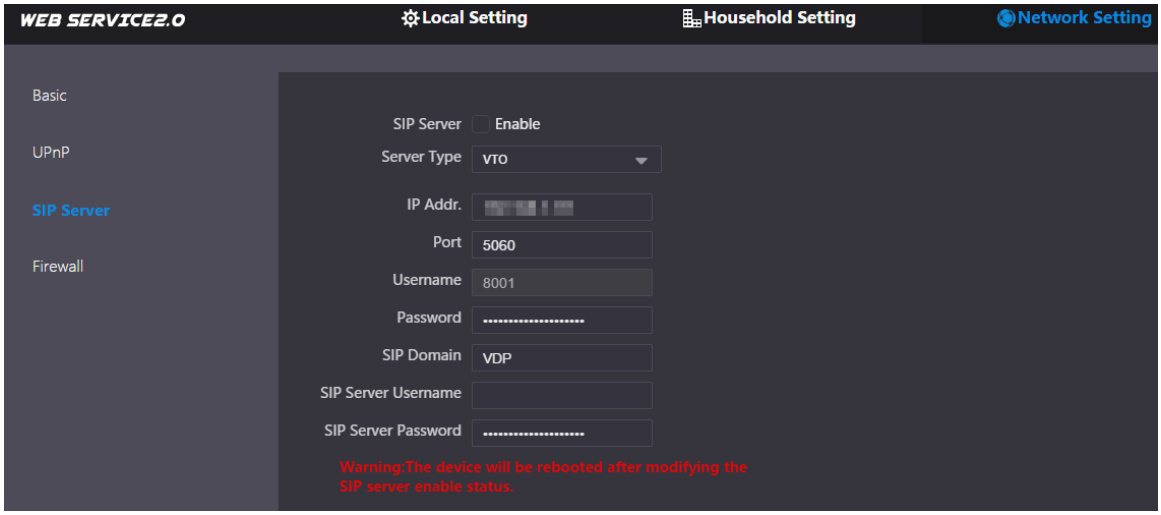
When connected to the same SIP server, all VTOs and VTHs can call each other. You can use a VTO or other servers as the SIP server.

5.3.4.1 VTO as the SIP server (for One Building)

Step 1 Select **Network Setting** > **SIP Server**.

Step 2 Set **Server Type** as **VTO**.

Figure 5-7 VTO as the SIP server



Step 3 Configure the parameters. See Table 5-1.

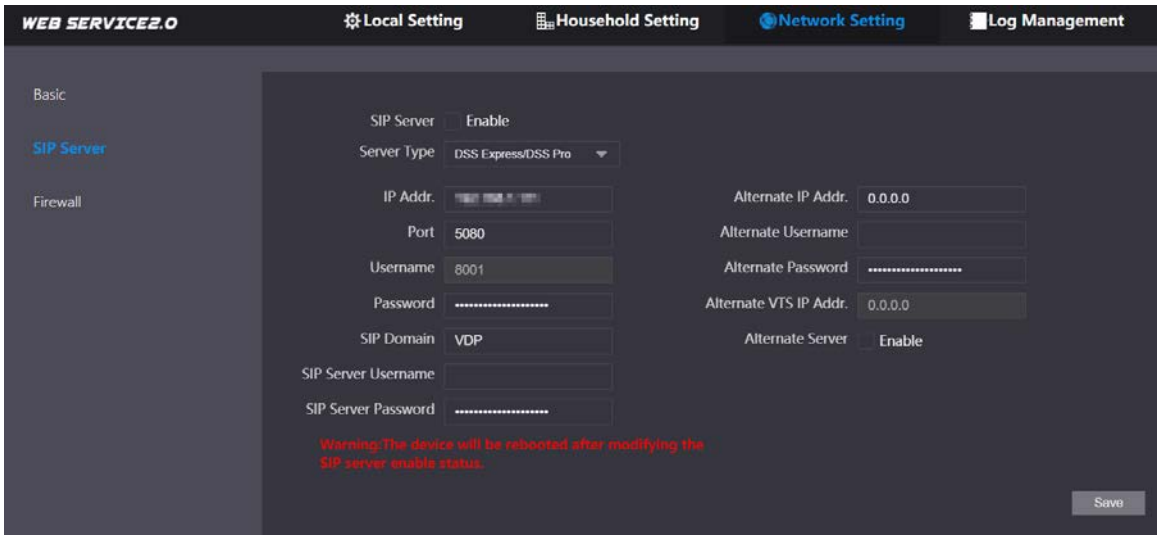
Step 4 Enable **SIP Server**.

Step 5 Click **Save**.

5.3.4.2 Platform (DSS Express/DSS Pro) as the SIP server (for Multiple Buildings or Units)

Step 1 Select **Network Setting** > **SIP Server**.

Figure 5-8 Platform as the SIP server



Step 2 Set **Server Type** as **DSS Express/DSS Pro**.

Step 3 Configure the parameters.

Table 5-1 SIP server parameter description

Parameter	Description
IP Addr.	SIP server IP address.
Port	• 5060 by default when another VTO works as SIP server. • 5080 by default when the platform works as SIP server.
Username/Password	Use default value.
SIP Domain	• It should be VDP when another VTO works as SIP server. • Keep default value VDP or leave it empty when the platform works as the SIP server.
SIP Server Username/ Password	Used to log in to the SIP server.
Alternate IP Addr.	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.
Alternate Username/ Password	Used to log in to the alternate server.
Alternate VTS IP Addr.	IP address of the alternate VTS.

Step 4 Click **Save**.

When the platform works as the SIP server and you want to configure the building number and building unit number, enable **Support Building** and **Support Unit** first.

5.3.5 Adding VTOs

You can add VTOs to the SIP server and then they can call each other.

Background Information

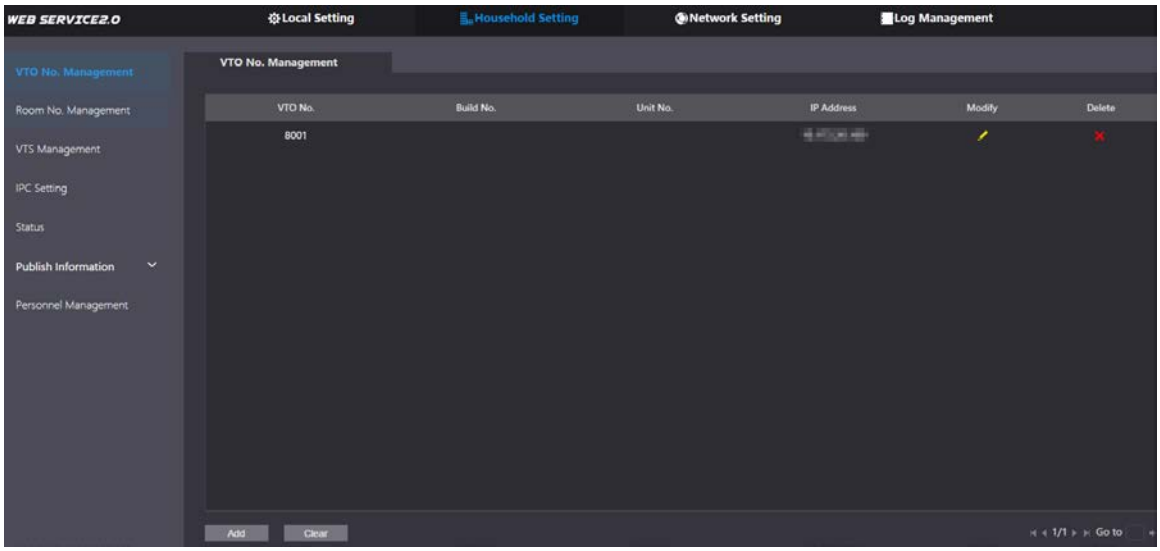
This section applies to the condition in which a VTO works as the SIP server. If you are using other servers as the SIP server, see the corresponding manual for details.

Procedure

Step 1 Log in to the web page of the SIP server.

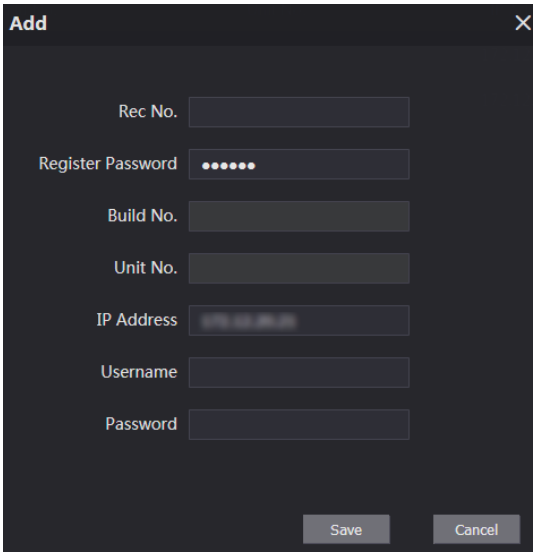
Step 2 Select **Household Setting** > **VTO No. Management**.

Figure 5-9 VTO No. management



Step 3 Click **Add**.

Figure 5-10 Add a VTO



Step 4 Configure the parameters.

Table 5-2 Add a VTO

Parameter	Description
Rec No.	VTO number.
Register Password	Keep the default value.
Build No.	Available only when other servers work as SIP server.
Unit No.	
IP Address	VTO IP address.
Username/Password	Username and password used to log in to the web page of the VTO.

Step 5 Click **Save**.

5.3.6 Adding Room Number

You can add room numbers to the SIP server, and then configure the room number on the VTHs to connect them to the network.

Background Information

This section applies to the condition in which a VTO works as the SIP server. If you are using other servers as the SIP server, see the corresponding manual for details.

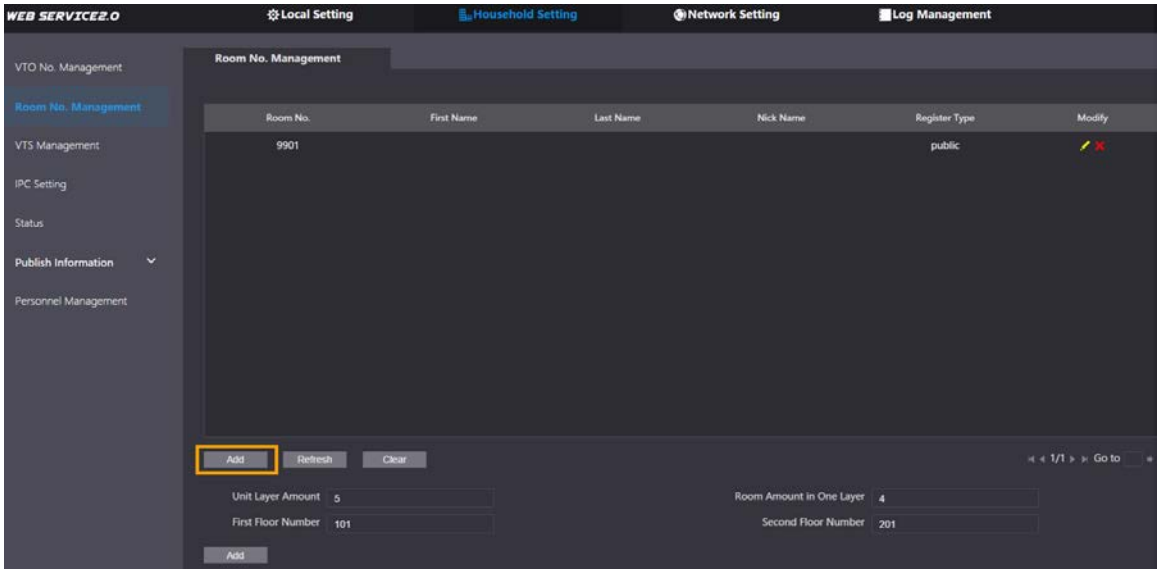
The room number can contain up to 6 digits of numbers, letters or their combination, and it cannot be the same with any VTO number.

Procedure

Step 1 Log in to the web page of the SIP server.

Step 2 Select **Household Setting** > **Room No. Management**.

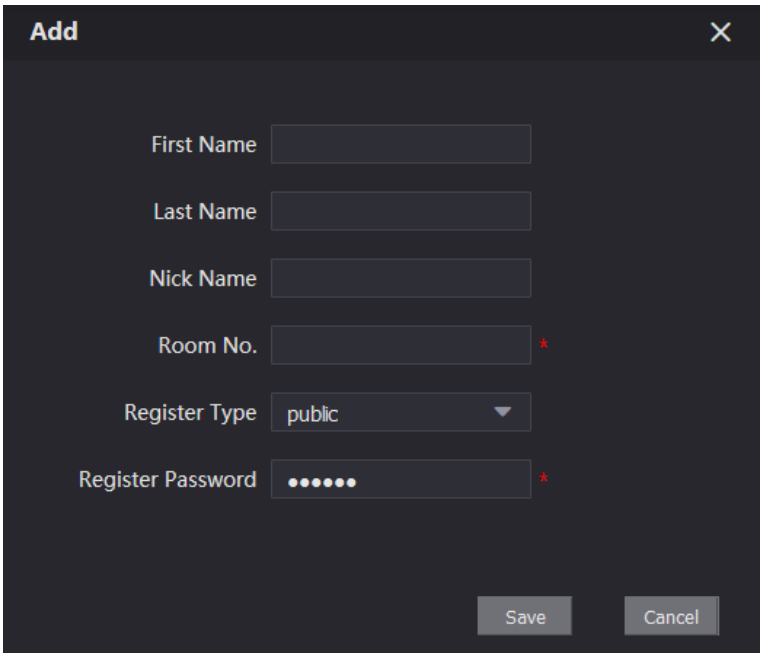
Figure 5-11 Room No. management



5.3.6.2 Adding a Single Room Number

Step 1 On the Room No. Management page, click **Add**.

Figure 5-12 Add a single room number



Step 2 Configure room information.

Table 5-3 Room information

Parameter	Description
First Name	Information used to differentiate each room.
Last Name	
Nick Name	
Room No.	Room number. ● When there are multiple VTHs, the room number for the main VTH should end with #0, and the room numbers for extension VTHs with #1, #2… ● You can have up to 10 extension VTHs for one main VTH.
Register Type	Select **public**.
Register Password	Keep the default value.

Step 3 Click **Save**.

Click to modify room information, and click to delete the room.

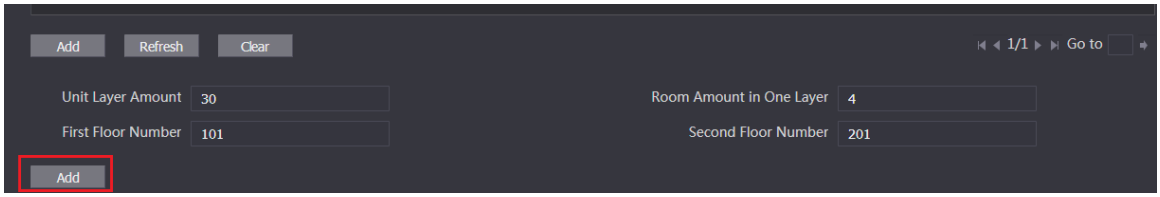
5.3.6.3 Adding Multiple Room Numbers

Step 1 On the **Room No. Management** page, configure the information in **Unit Layer Amount**, **Room Amount in One Layer**, **First Floor Number**, and **Second Floor Number.**

Step 2 Click **Add**.

All the added room numbers are displayed.

Figure 5-13 Add multiple room numbers



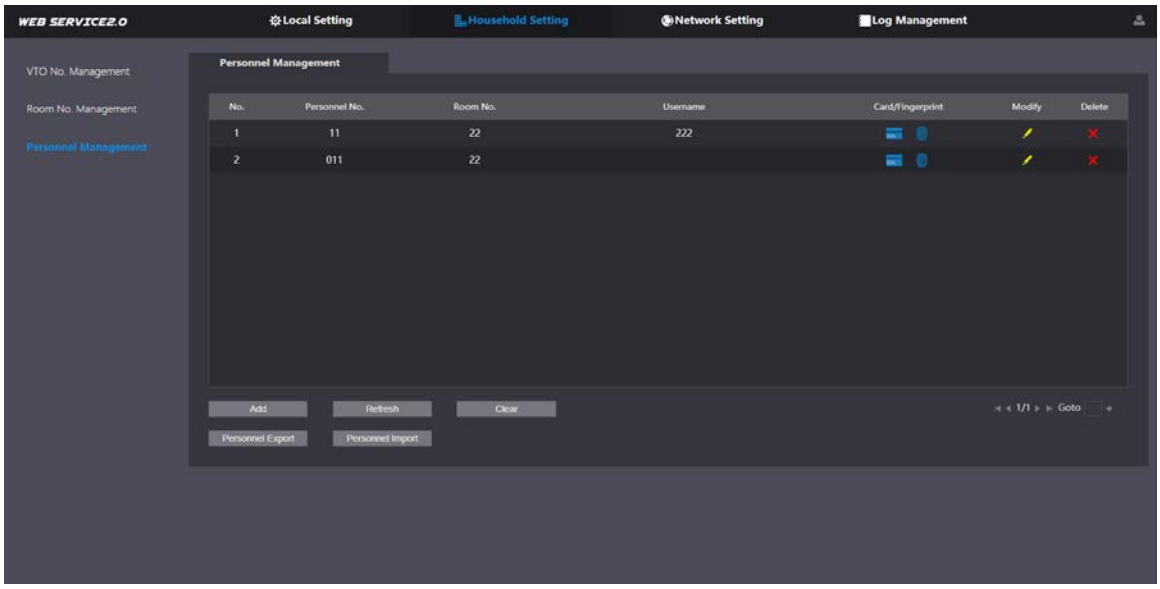
5.3.7 Issuing Cards

Add personnel information to manage registered users, and then you can issue cards.

Step 1 Log in to the web page of the VTO.

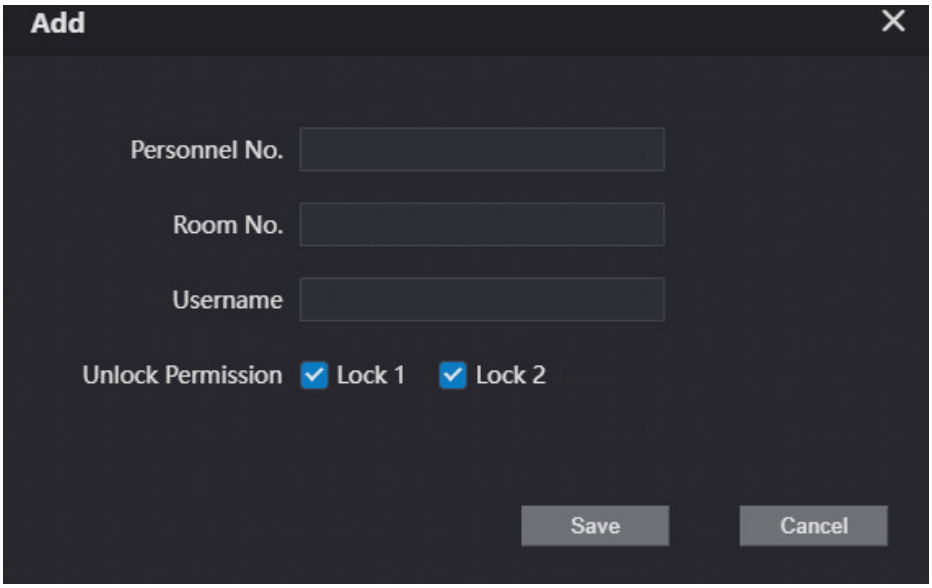
Step 2 Select **Household Setting** > **Personnel Management**.

Figure 5-14 Personnel management



Step 3 Click **Add**.

Figure 5-15 Add Personnel Information



Step 4 Enter the parameters, and then click **Save**.

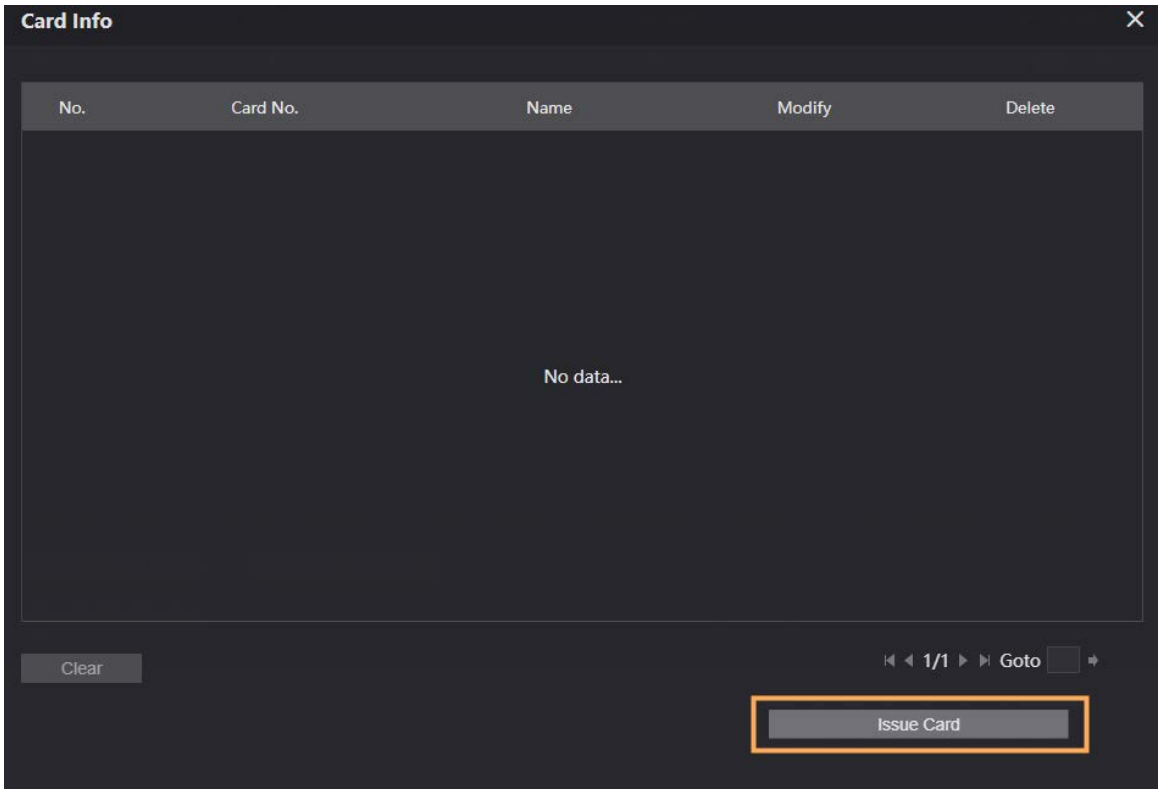
The personnel information displays on the web page.

- Lock 1: local lock.
- Lock 2: RS-485 lock.

Figure 5-16 Operation succeed

Step 5 Select  to go to the card issuing window.

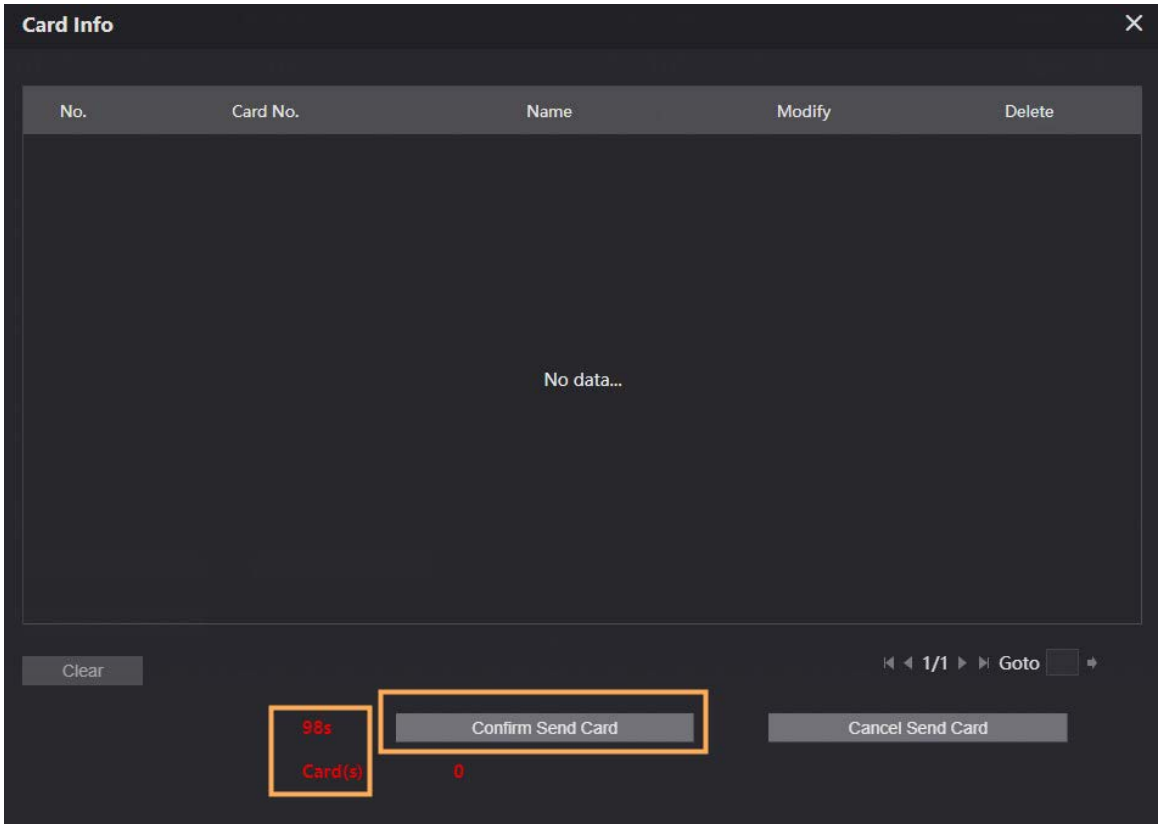
Figure 5-17 Card issuing window



Step 6 Click **Issue Card** to issue cards.

Step 7 The web page displays the countdown prompt (120 s). Once the countdown starts, you need to swipe the card on the card reader of the VTO within this time period. After the swiping, the card number will be automatically recognized by the VTO.

Figure 5-18 Countdown in process



Step 8 Click **Confirm Send Card** after swiping to complete the issuing process.
The information of the newly issued card displays on the window.

Figure 5-19 Information of the newly issued card

Other Operations

- Click  to set it as the main card, and then the icon changes to  . The parent card can be used to issue access cards for this room on the VTO.
- Click  to set it to loss, and then the icon changes to  . The lost card cannot be used to open the door.
- Click  or  to modify the username or delete the card.

6 VTO Operation

The snapshots are for reference only, and slight differences might be found in the operation screen of the VTO, depending on your model.

6.1 Call Function

Figure 6-1 Standby screen overview

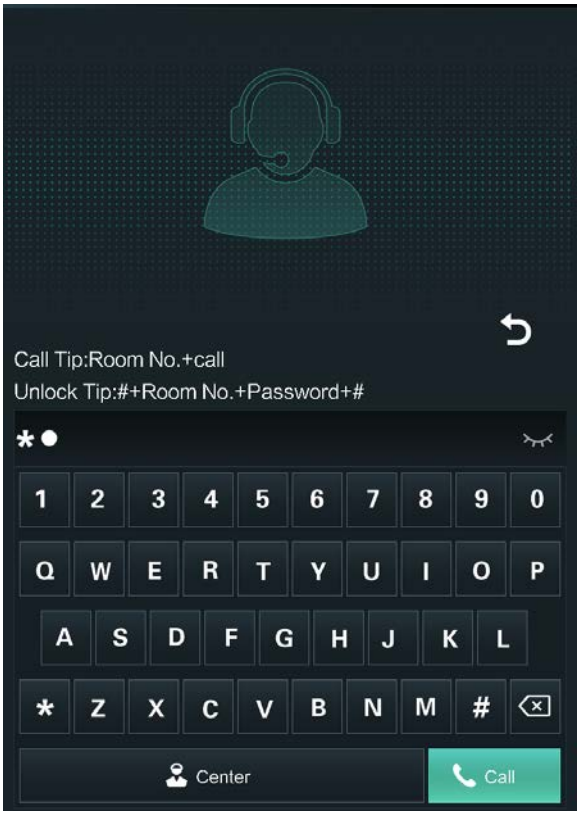
6.1.2 Calling with Room Number

Step 1 On the standby screen Tap .

Step 2 Enter room number, and then tap **Call**.

Step 3 During phone call, tap **Hangup** to end the call.

Figure 6-2 Calling



6.1.3 Calling from Contact

All the room numbers added to the SIP server is displayed in the VTO contact.

Step 1 On the standby screen, tap **PhoneBook**.

Step 2 Select a contact and tap **Call**.

6.2 Project Mode

The project mode is intended for administrators to make advanced configurations to the VTO, including issuing access cards, modifying device IP address, and adding personnel.

6.2.1 Entering Project Mode

On the standby screen, tap **Call** and enter "*+project password+#". You can modify the password on the VTO or its web page.

6.2.2 Modifying IP Address

Step 1 In the project mode, select **IP Settings.**

Step 2 Enter the IP address.

Figure 6-3 IP settings

Step 3 Tap **OK**.

6.3 User Registration

You need to register users to unlock doors. Unlocking method include cards, face recognition and fingerprints. You can add unlocking methods after configuring personnel information.

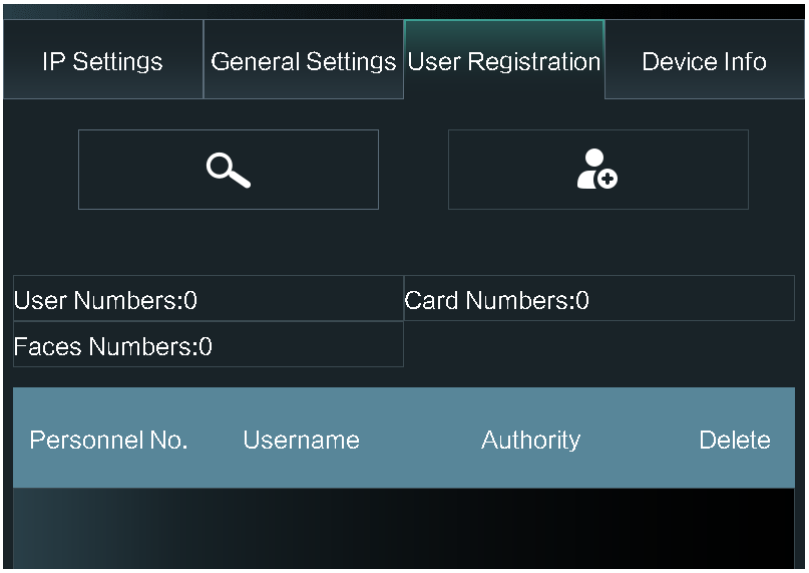
Face recognition or fingerprints are only supported by some models.

6.3.1 Adding Basic information

Basic information includes personnel number, room number and username.

Step 1 On the project mode Screen, tap **User Registration**.

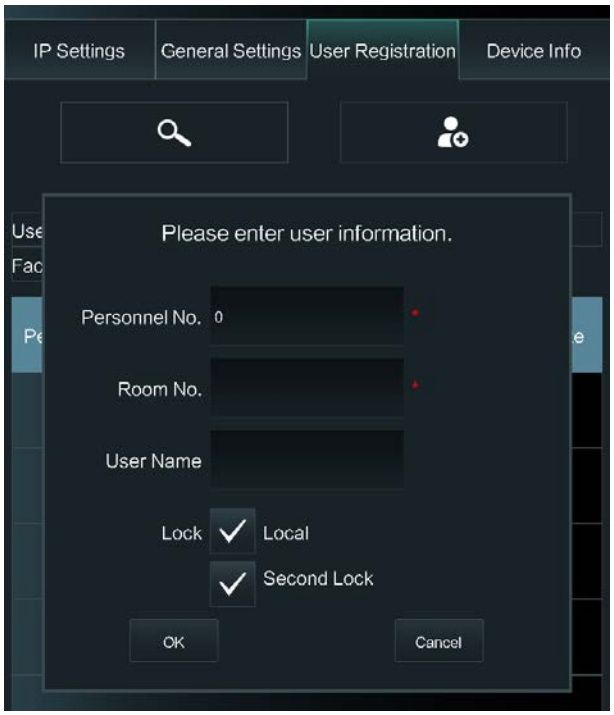
Figure 6-4 User registration



Step 2 Tap .

Step 3 Enter personnel number, room number, and user name.

Figure 6-5 Add personnel



Step 4 Tap **OK** to save the information.

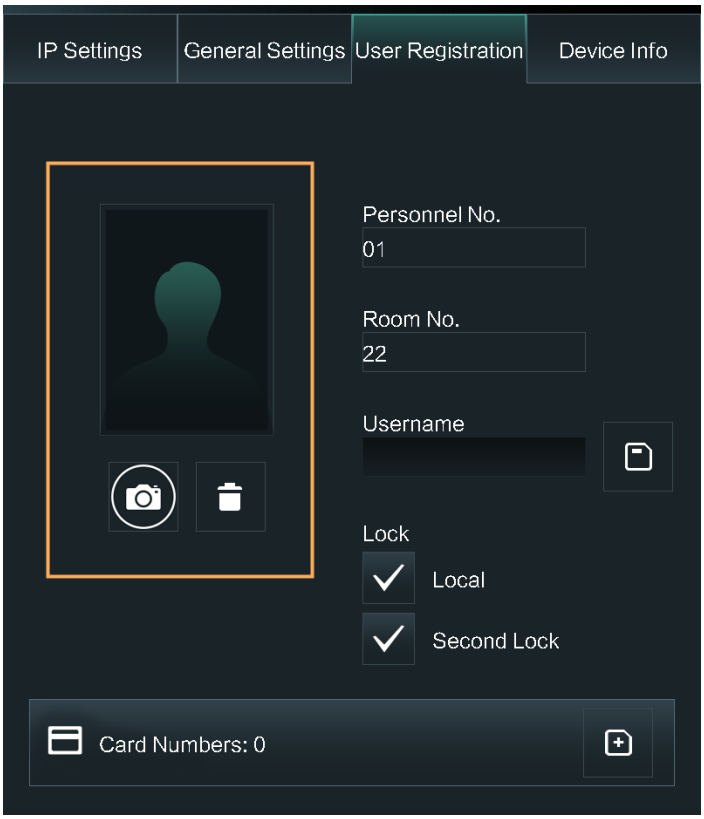
6.3.2 Adding Faces

Add faces of registered users to unlock through face recognition.

Face recognition is only supported by some models.

Step 1 After adding basic information, tap to take a photo.

Figure 6-6 Take a photo



Step 2 Tap **OK** to save the photo.

The current screen goes to the **User Registration** screen again.

Step 3 You can also tap **Cancel** to take a new photo.

6.3.3 Issuing Cards

Step 1 On the **User Registration** screen, tap to issue cards.

You can choose one of the following ways to issue cards.

Figure 6-7 Issue cards

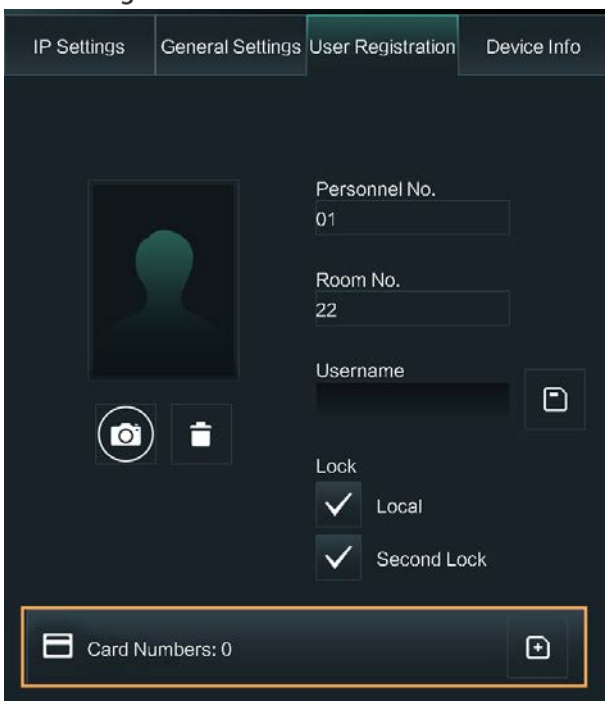
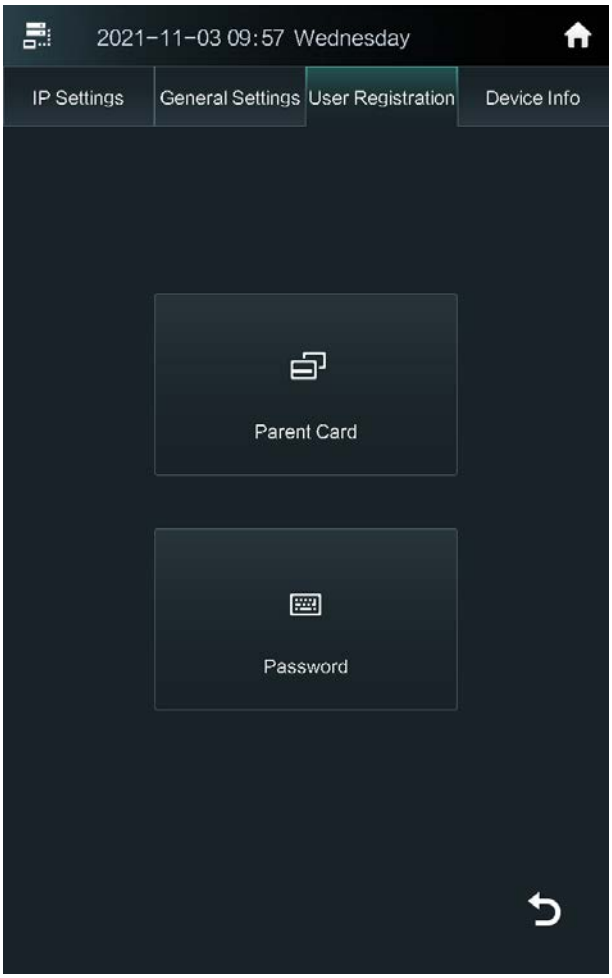


Figure 6-8 Parent card & password

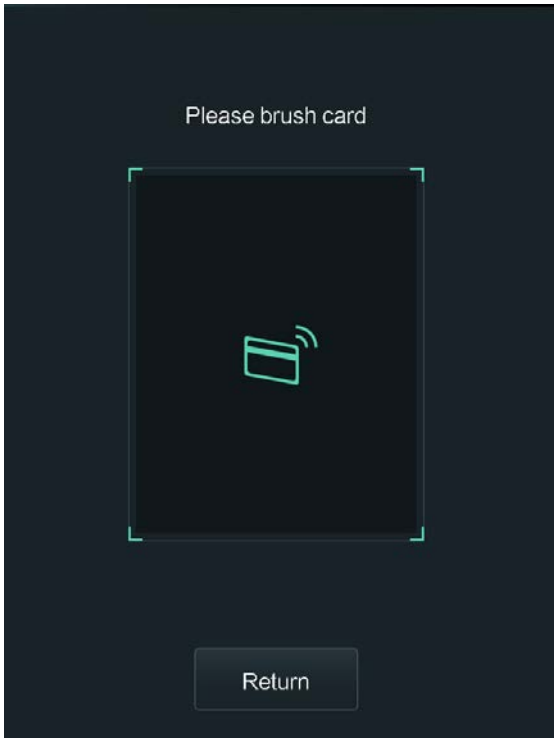


1) Tap **Parent Card** if you want to issue through the main card. And then swipe your main card on the card reader to continue the card issuing process.

If you do not have a main card, issue a card on the VTO through password. Then go to the web page of the VTO, select **Household Setting** > **Personnel Management** , and

click , and then set a card as your main card through clicking .

Figure 6-9 Issuing cards through parent card



2) Tap **Password** if you want to issue cards through the password. Enter the password and tap **OK** to issue cards.

You need to enter your planned password in the **Issue Card password** textbox on the web page of the VTO in **Local Setting** > **Access Control** > **Local**.

Figure 6-10 Issuing cards through password

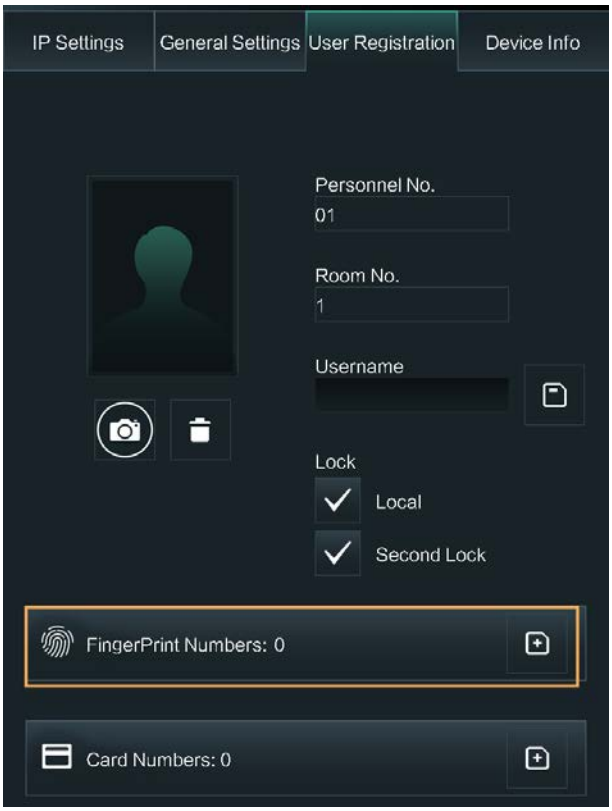
Step 2 Swipe cards on the card reader, and card numbers will be automatically recognized.

6.3.4 Issuing Fingerprints

Fingerprints are only supported by some models.

Step 1 On the **User Registration** screen, tap  to issue fingerprints.

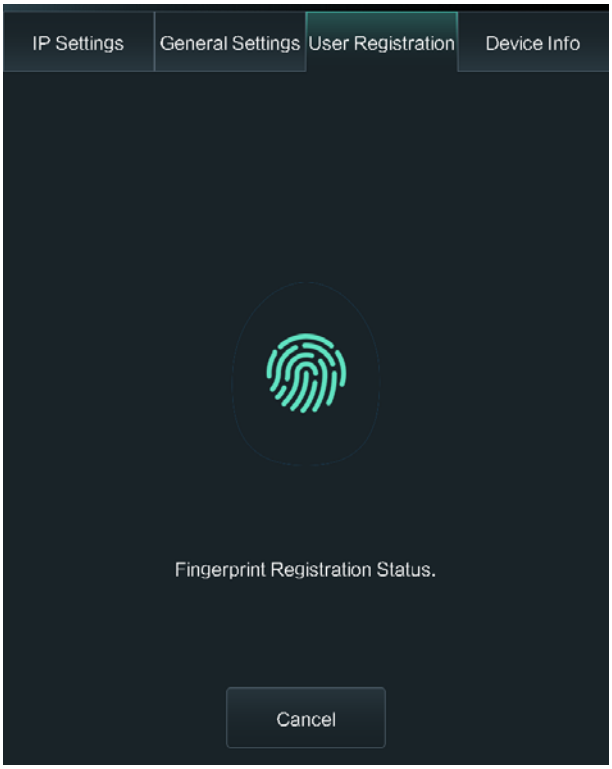
Figure 6-11 Issue fingerprints



Step 2 Put your fingerprint on the finger recording area on the VTO.

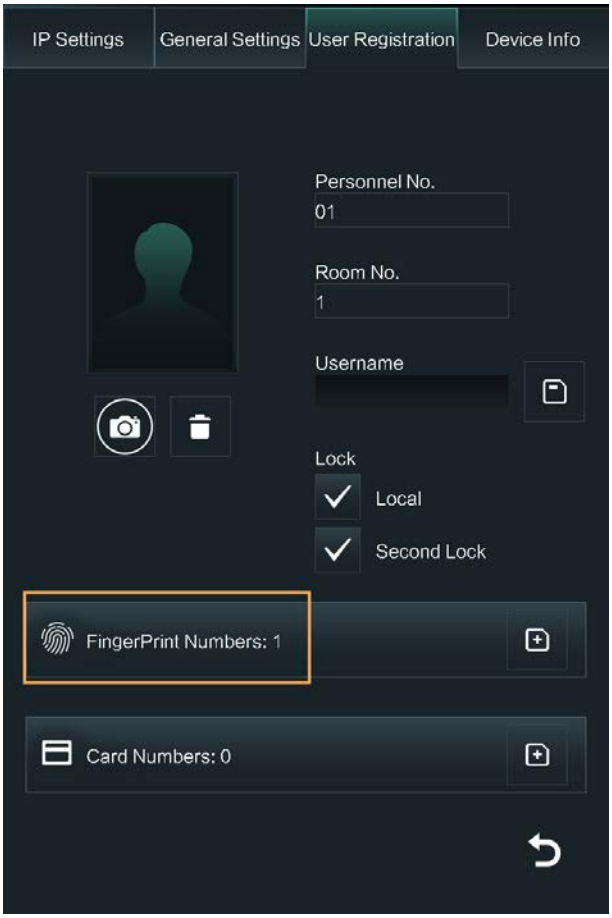
You need to record your fingerprint for three times until the fingerprint is successfully collected.

Figure 6-12 Register fingerprints



Step 3 Go back to the **Registration User** screen and check whether your fingerprint is collected.

Figure 6-13 Fingerprint collected

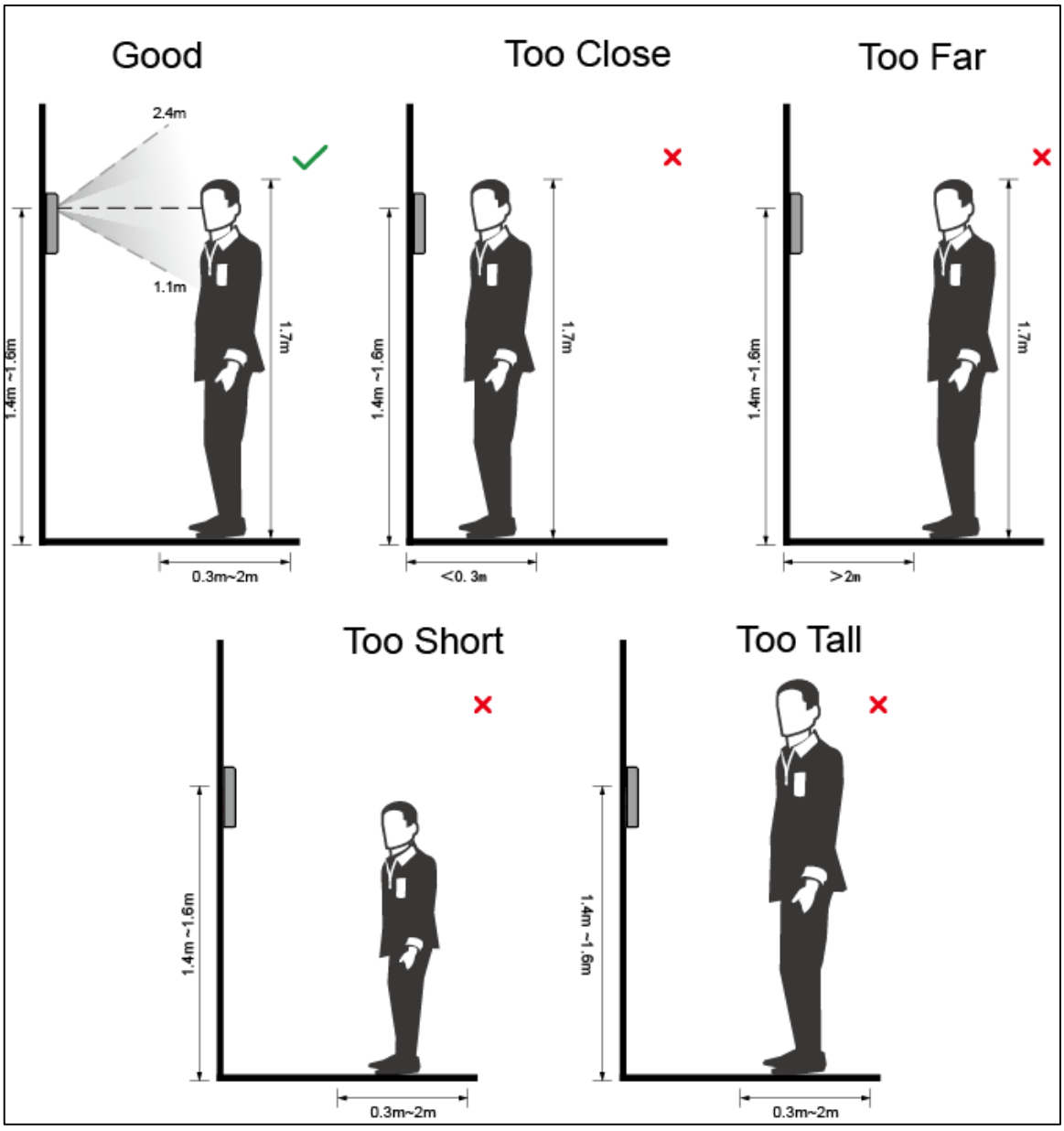


Appendix 1 Notes of Face Recording

Face Position

Inappropriate face position may influence the recognition effect.

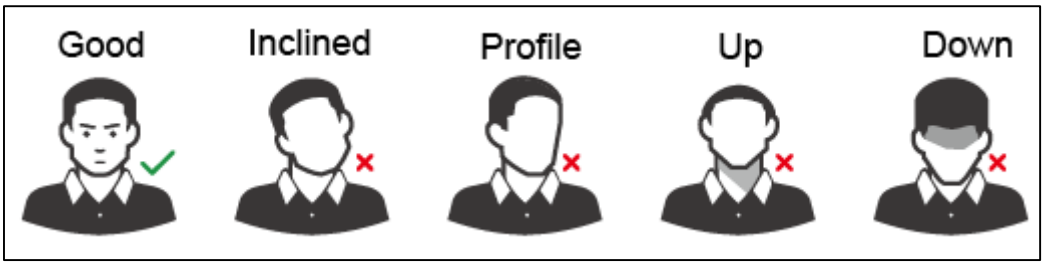
Appendix Figure 1-1 Appropriate face position



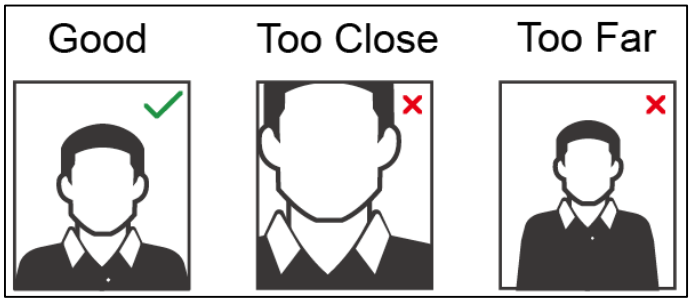
Face Requirements

- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, thick beards, or other face ornaments that influence face recording.
- Open your eyes, make no expressions, and face the center of the camera.
- When recording your face or during face recognition, do not stand too close to or too far from the camera.

Appendix Figure 1-2 Head position



Appendix Figure 1-3 Face distance



- When importing face images through the management platform, make sure that the image resolution is between 150×300–600×1200; image pixel is more than 500×500; image size is less than 100KB; image name and person ID are the same.
- Make sure that the face does not take up 2/3 of the image, and the aspect ratio does not exceed 1:2.

Appendix 2 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

2. **Update Firmware and Client Software in Time**

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

3. **Set and Update Passwords Reset Information Timely**

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

4. **Enable Account Lock**

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

5. **Change Default HTTP and Other Service Ports**

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

minimum set of permissions to them.

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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