Digital Door Station

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces basic operations of the digital door station (hereinafter referred to as "VTO").

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 Date
V1.0.0	First release.	August 2021

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.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

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

⚠

- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.
- Please use battery properly to avoid fire, explosion and other dangers.
- Please replace used battery with battery of the same type.
- If you use power plug or appliance coupler as disconnecting device, please maintain the disconnecting device available to be operated all the time.

Installation Requirements

⚠ **WARNING**

- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.

⚠

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.
- The device must be installed on solid and flat surface in order to guarantee safety under load and earthquake. Otherwise, it may cause Device to fall off or turnover.

Table of Contents

1 Structure

1.1 Front Panel

Figure 1-1 Front panel

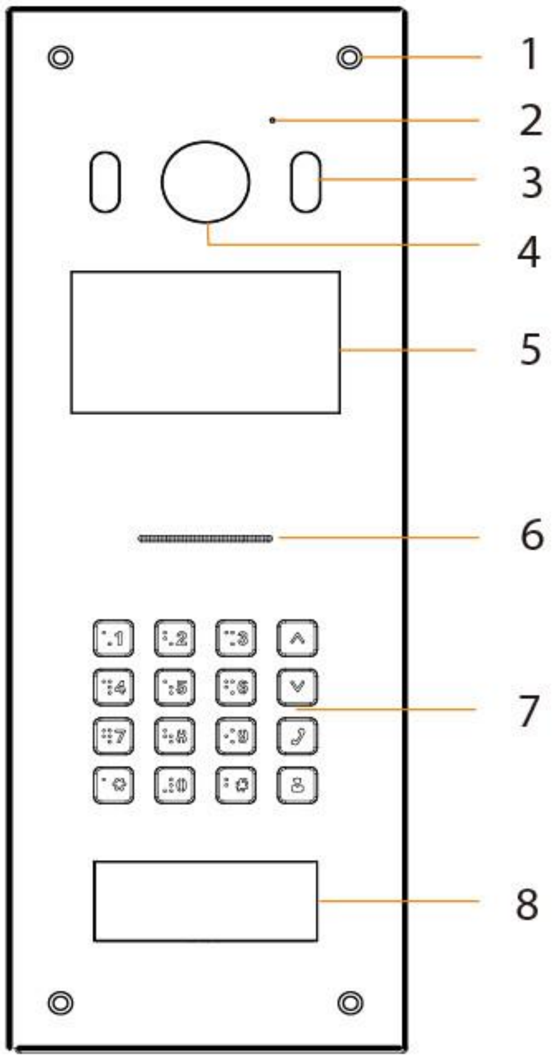


Table 1-1 Components

No.	Description	No.	Description
1	Installation screw	5	Display
2	MIC	6	Loudspeaker
3	White illuminator	7	Keyboard
4	Camera	8	Card swiping area

1.2 Rear Panel

Figure 1-2 Rear panel

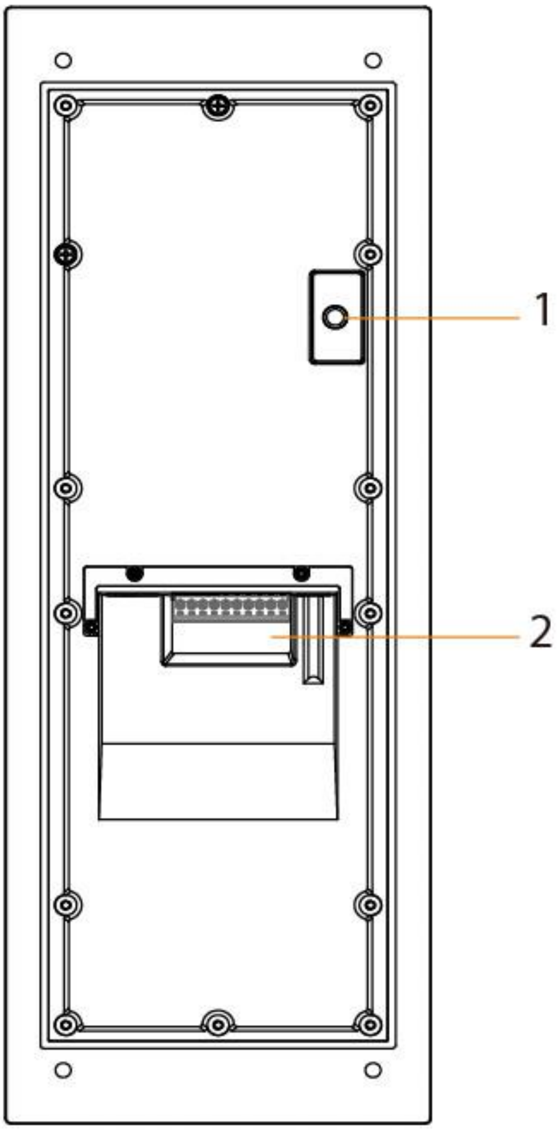
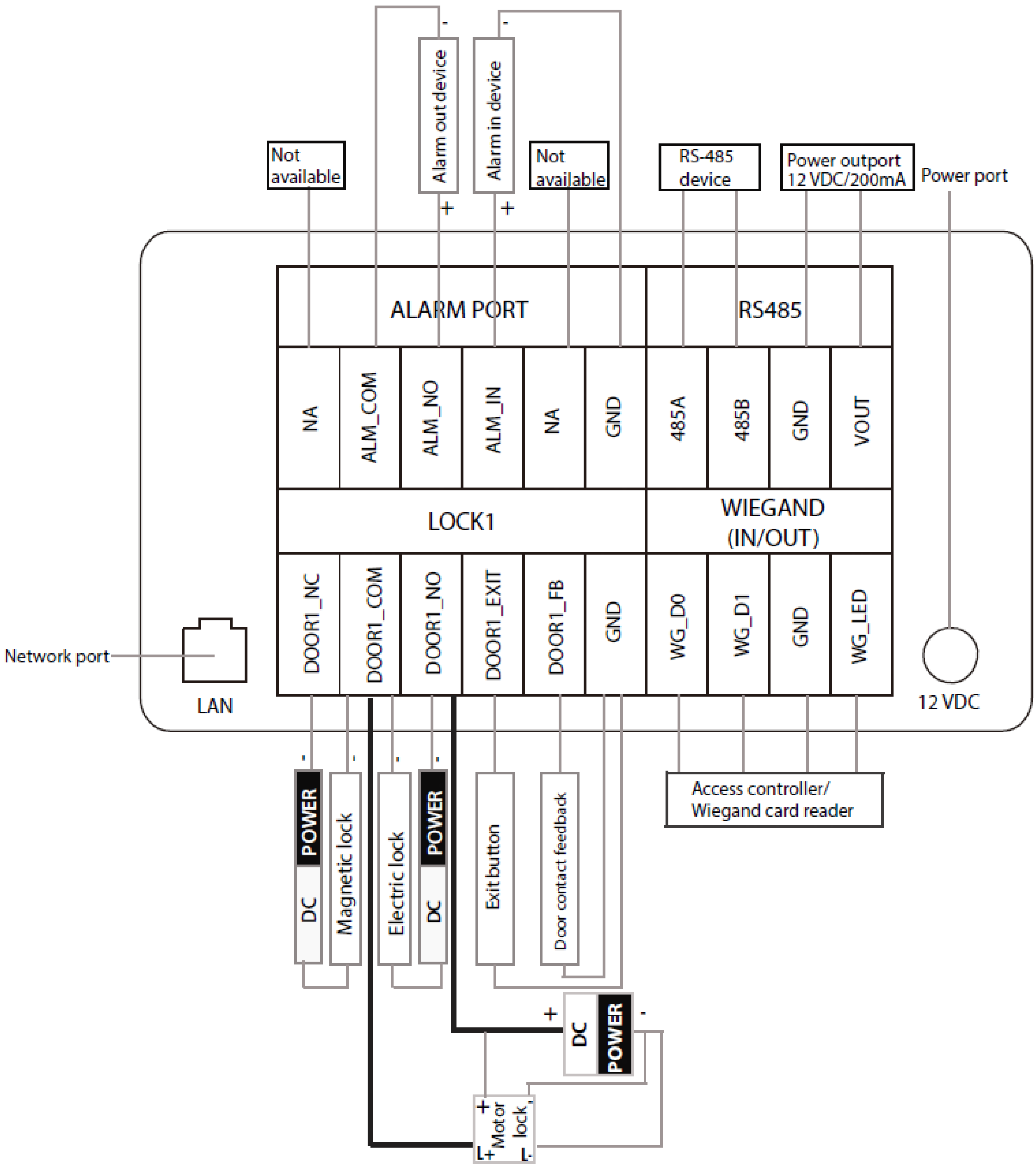


Table 1-2 Components

No.	Description	No.	Description
1	Tamper button	2	Function ports (connected to locks, access controllers, alarm in/out devices)

2 Cable Connection

Figure 2-1 Cable connection

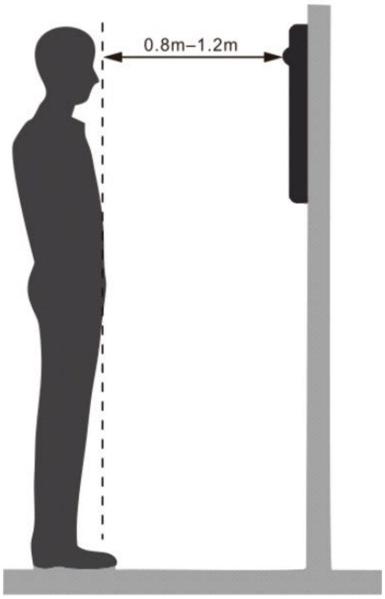


3 Installation

⚠

- Do not expose the VTO to condensation, high temperature, direct sunlight, stain, dust, and chemically corrosive substances.
- Engineering installation and debugging must be done by professionals. Do not dismantle or repair the device by yourself. Contact technical support.
- Prepare cross screwdrivers and gloves yourself.
- Recommended distance between the camera and ground is 1.4 m–1.6 m.

Figure 3-1 Installation height



4 Web Configuration

This chapter introduces the basic configurations of the VTO and the indoor monitor (hereinafter referred to as the "VTH").

4.1 Procedure

Follow these steps to configure the VTO and VTH in the network to realize connection and calling.

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

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

Step 2 Configure the VTO. For details, see "4.2 Initializing VTO", "4.3 Configuring Network Parameters", "4.4 Configuring VTO Number", "4.5 Configuring SIP Servers", and "4.6 Adding Room Number".

Step 3 Configure the VTH. For details, see the VTO user's manual.

4.2 Initializing VTO

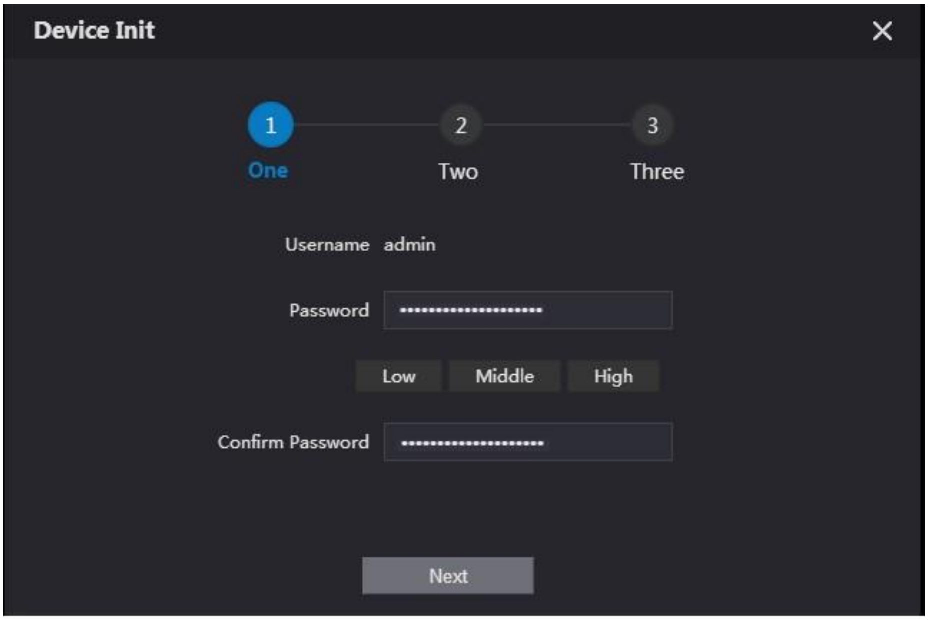
For the first time login, you need to create a password.

Step 1 Power on the VTO.

Step 2 Go to the default IP address (192.168.1.108) of the VTO in the browser.

Make sure that the IP address of the PC is on the same network segment as the VTO.

Figure 4-1 Device initialization



Device Init

Username admin

Password ••••••••••••••••••••

Confirm Password ••••••••••••••••••••

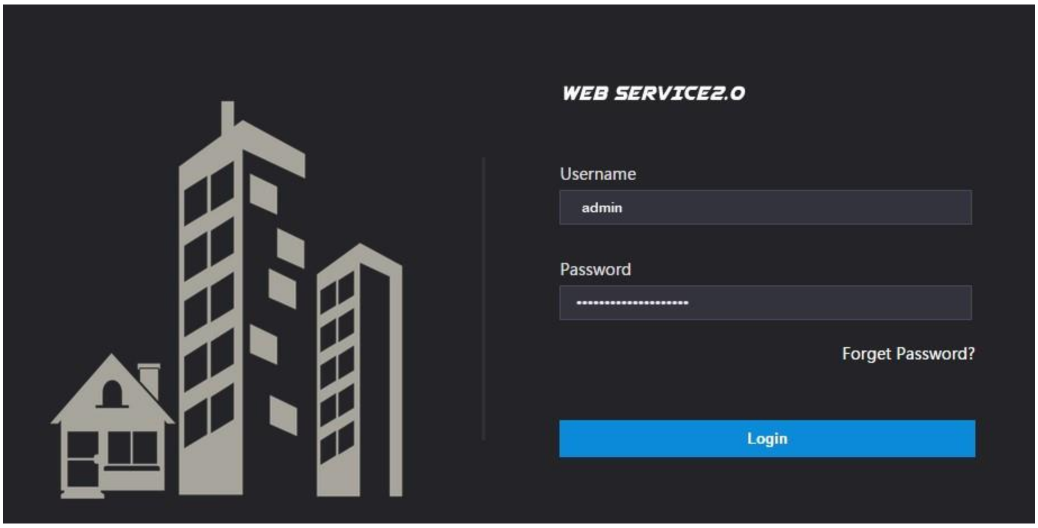
Step 3 Enter and confirm the password, and then click **Next**.

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 ' " ; : &).

Step 4 Select **Email** and enter email address for resetting password.

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

Figure 4-2 Login interface



WEB SERVICE2.0

Username: admin

Password: ••••••••••••••••••••

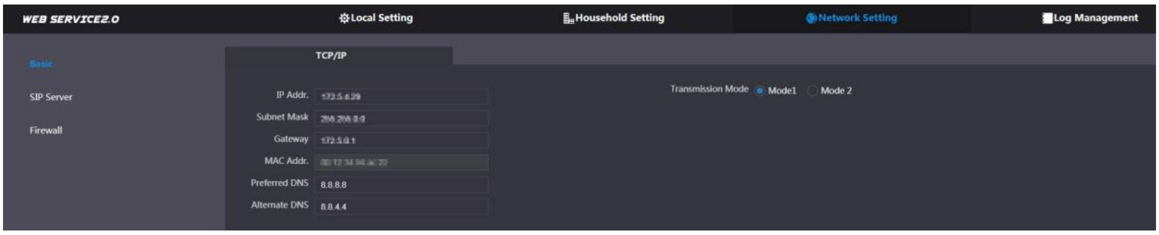
4.3 Configuring Network Parameters

To call other devices, you must make sure that the IP address of the VTO is on the same network segment as other devices. If not, change the IP address of the VTO. For details, see"5.2 Changing IP Address".

Step 1 Log in to the VTO web interface.

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

Figure 4-3 TCP/IP information



IP Addr.: 172.5.4.29

Subnet Mask: 255.255.0.0

Gateway: 172.5.0.1

MAC Addr.: [illegible]

Preferred DNS: 8.8.8.8

Alternate DNS: 8.8.4.4

Transmission Mode: ● Mode1 ○ Mode 2

Step 3 Configure the network parameters, select transmission mode and click **Save**.
You need to change the IP address of your PC to the same network segment as the VTO to log in again.

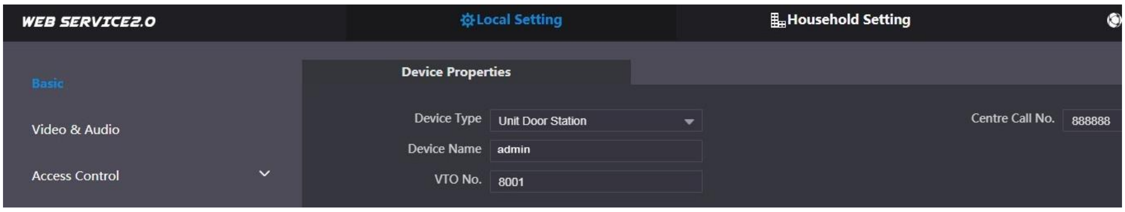
4.4 Configuring VTO Number

Numbers can be used to distinguish each VTO, and we recommend you set it according to unit or building number.

Step 1 Log in to the VTO web interface.

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

Figure 4-4 Device properties



Device Type: Unit Door Station
Device Name: admin
VTO No.: 8001
Centre Call No.: 888888

Step 3 Enter the device name, and 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.

4.5 Configuring SIP Servers

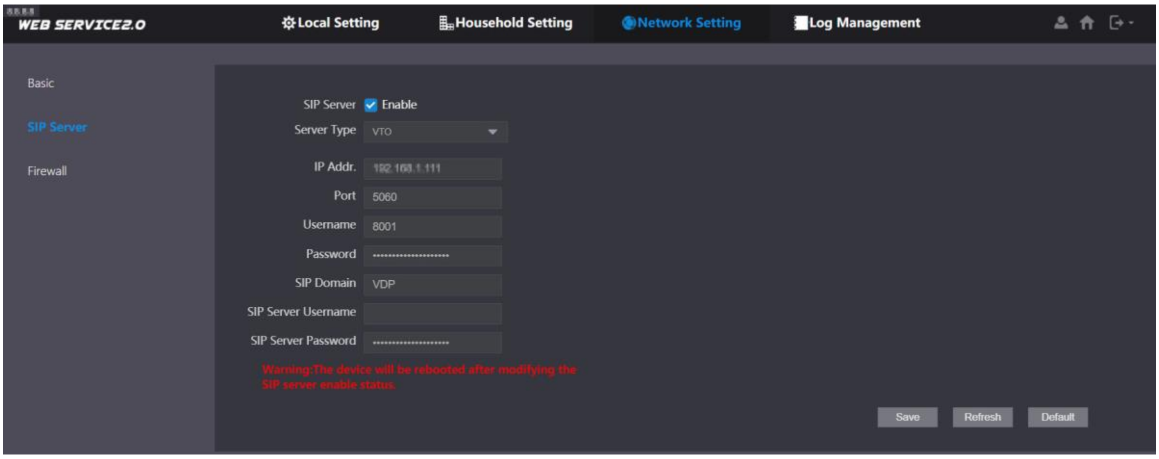
When connected to the same SIP server, all VTOs and VTHs can call each other. You can use a VTO or other servers as the SIP server.

VTO as the SIP Server (for One Building)

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

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

Figure 4-5 SIP server (1)



SIP Server ☑ Enable
Server Type: VTO
IP Addr.: 192.168.1.111
Port: 5060
Username: 8001
Password: ••••••••••••••••••••
SIP Domain: VDP
SIP Server Username:
SIP Server Password: ••••••••••••••••••••

Warning:The device will be rebooted after modifying the SIP server enable status.

Step 3 Configure parameters. For details, see Table 4-1.

Step 4 Enable SIP Server.

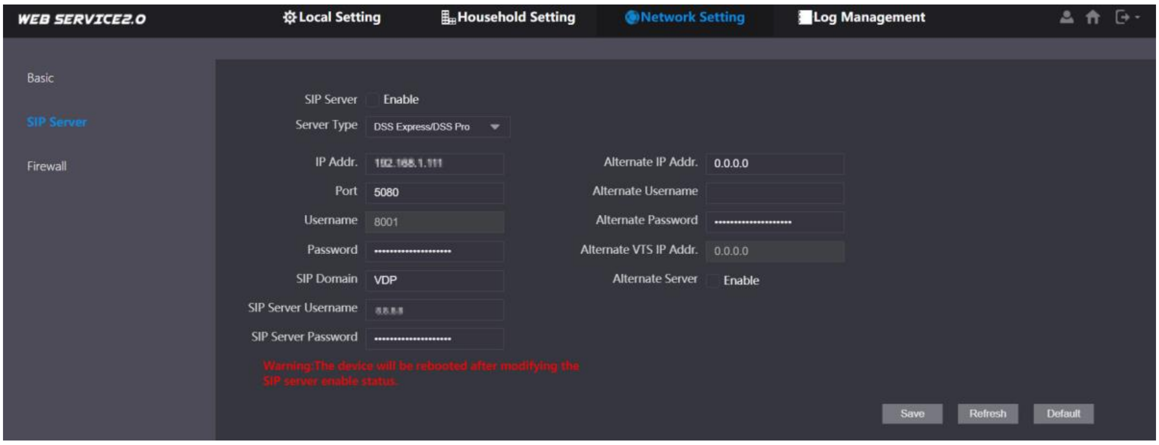
Step 5 Click **Save**. The VTO will restart automatically.

Platform as the SIP Server (for Multiple Buildings or Units)

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

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

Figure 4-6 SIP server (2)



SIP Server □ Enable

Server Type: DSS Express/DSS Pro

IP Addr.: 192.168.1.111

Port: 5080

Username: 8001

Password: ••••••••••••••••••••

SIP Domain: VDP

SIP Server Username: 8888

SIP Server Password: ••••••••••••••••••••

Alternate IP Addr.: 0.0.0.0

Alternate Username:

Alternate Password: ••••••••••••••••••••

Alternate VTS IP Addr.: 0.0.0.0

Alternate Server □ Enable

Warning:The device will be rebooted after modifying the SIP server enable status.

Step 3 Configure parameters.

Table 4-1 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	Leave it as default.
SIP Domain	● It should be VDP when another VTO works as the SIP server. ● Leave it as default or blank when the platform works as SIP server.
SIP Server Username/ Password	Used to log in to SIP server.
Alternate IP Addr.	Alternate server IP address. If Express/DSS works as SIP server and the alternate server is enabled, the alternate server will be used as SIP server when Express/DSS stops responding.
Alternate Username/ Password	Used to log in to the alternate server.
Alternate VTS IP Addr.	IP address of the alternate VTS.
Alternate Server	Enable it as needed.

Step 4 Click **Save**. The VTO will restart automatically.

When the platform works as the SIP server, if it is necessary to set building number and building unit number, enable **Support Building** and **Support Unit** first.

4.6 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.

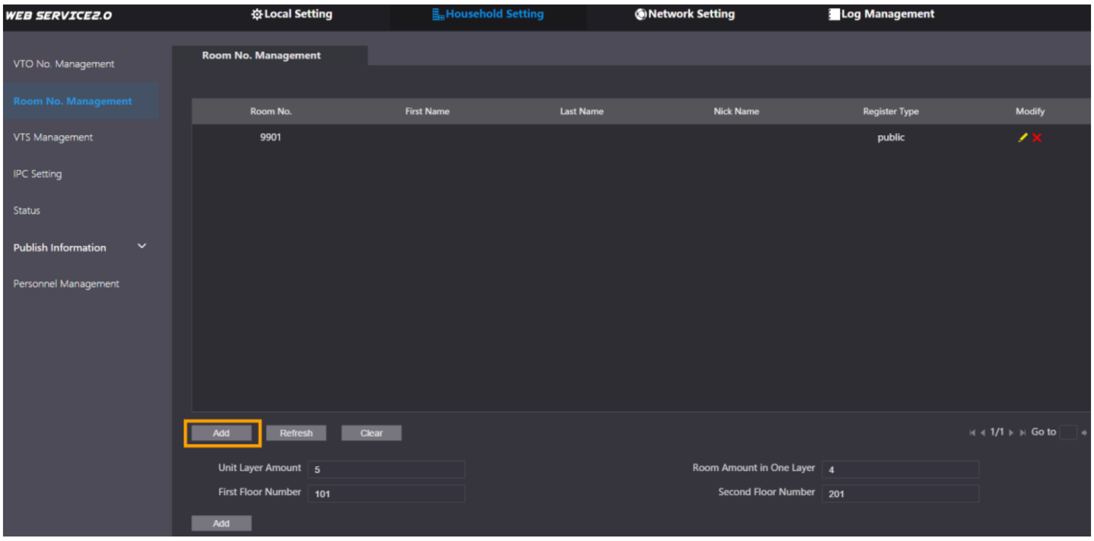
This section applies to the condition in which a VTO works as the SIP server. If you are using other servers as the SIP server, see the corresponding manual for details.

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.

Adding a Single Room Number

Step 1 Log in to the web interface of the SIP server, and then select **Household Setting** > **Room No. Management**.

Figure 4-7 Room No. management



Room No.	First Name	Last Name	Nick Name	Register Type	Modify
9901				public	✎ ✗

Unit Layer Amount: 5

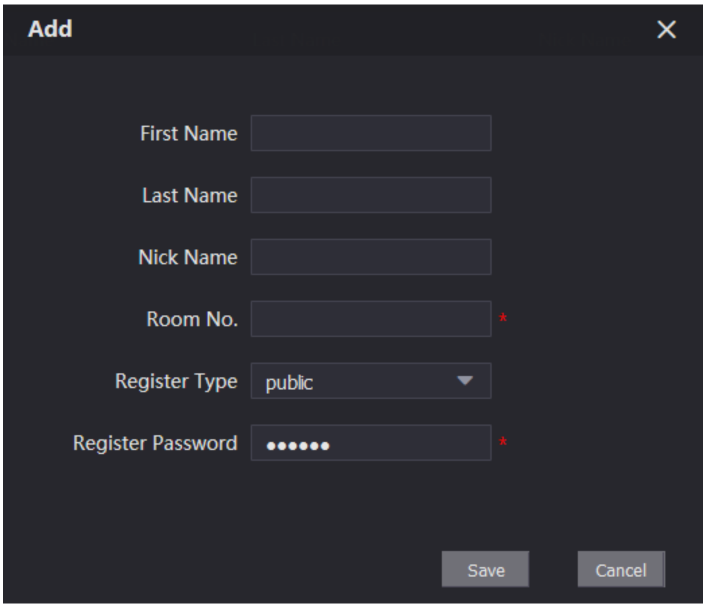
First Floor Number: 101

Room Amount in One Layer: 4

Second Floor Number: 201

Step 2 Click **Add**.

Figure 4-8 Add a single room number



First Name:

Last Name:

Nick Name:

Room No.: *

Register Type: public

Register Password: •••••• *

Step 3 Configure room information.

Table 4-2 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 master VTH should end with #0, and the room numbers for extension VTHs with #1, #2…
Register Type	Select **public**.
Register Password	Leave it as default.

Step 4 Click **Save**.

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

Adding Multiple Room Numbers

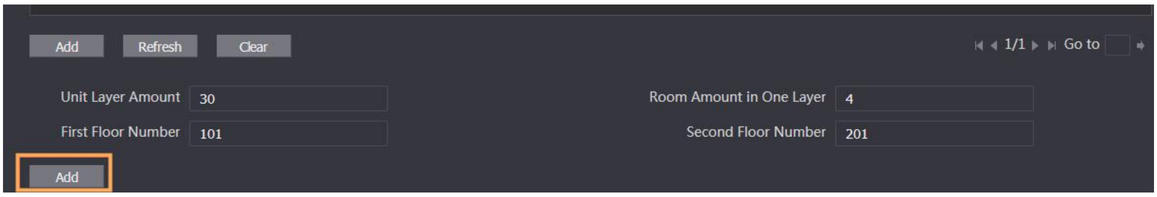
Step 1 Configure the **Unit Layer Amount, Room Amount in One Layer**, **First Floor Number**, and **Second Floor Number**.

Step 2 Click **Add**.

All the added room numbers are displayed.

Step 3 Click **Refresh** to view the latest status, and click **Clear** to delete all the room numbers.

Figure 4-9 Add multiple room numbers



Unit Layer Amount 30

Room Amount in One Layer 4

First Floor Number 101

Second Floor Number 201

5 Engineering Setting

5.1 Entering Engineering Setting

Engineering setting is intended for administrators or engineers.

Tap "*project password#" on the VTO.

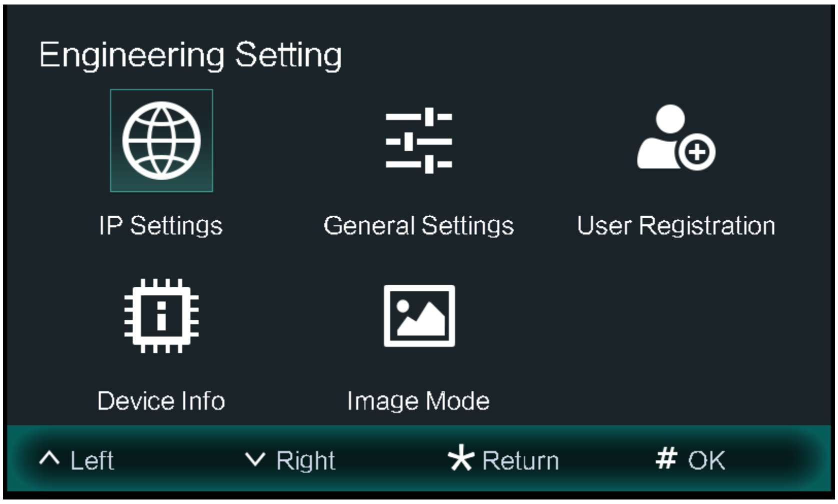
- You need to set the project password by selecting **Local Setting** > **Access Control** > **Local** on the web interface.

5.2 Changing IP Address

You need to plan an IP address for the VTO to connect it to the network.

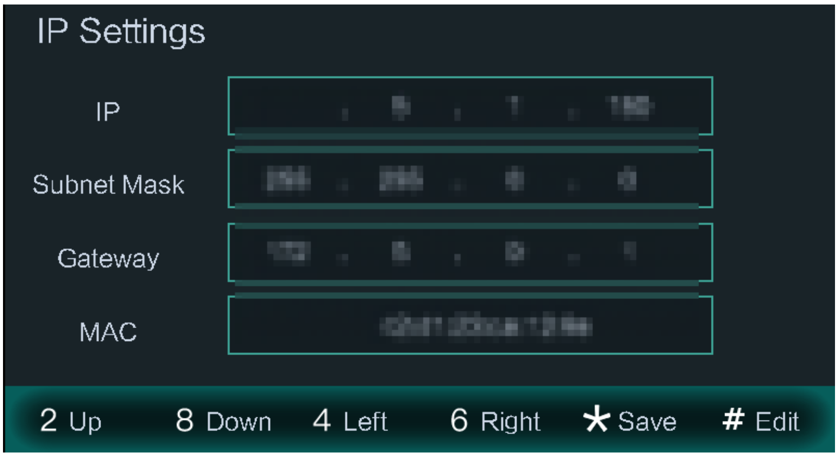
Step 1 Select IP Settings on the **Engineering Setting** interface.

Figure 5-1 Engineering setting



Step 2 Enter IP address, subnet mask, and gateway.

Figure 5-2 IP settings



Step 3 Tap **Save** to complete the setting.

6 User Registration

Only registered users can unlock doors.

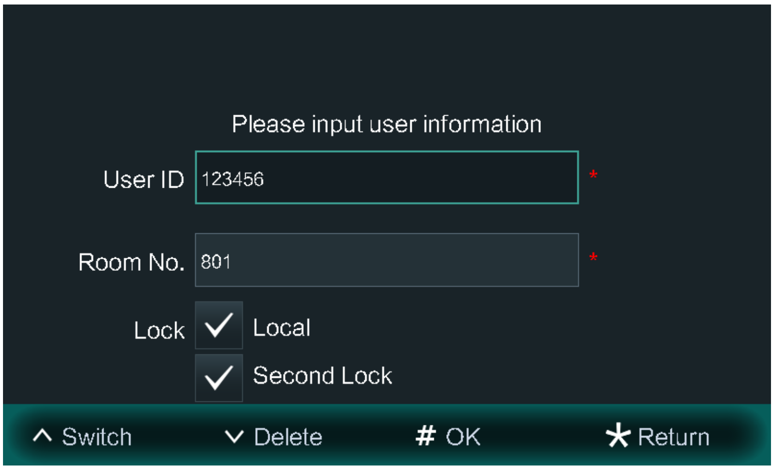
Step 1 Tap "*project password#" on the VTO to go to the **Engineering Setting** interface.

Step 2 On the Engineering Setting interface, select **User Registration**.

Step 3 Select **Add**.

Step 4 Enter user ID and room number.

Figure 6-1 User registration



Please input user information

User ID 123456 *

Room No. 801 *

Lock ☑ Local

☑ Second Lock

Step 5 Tap **OK** to complete the settings.

Step 6 Issue cards. You can issue five cards at most for each user.

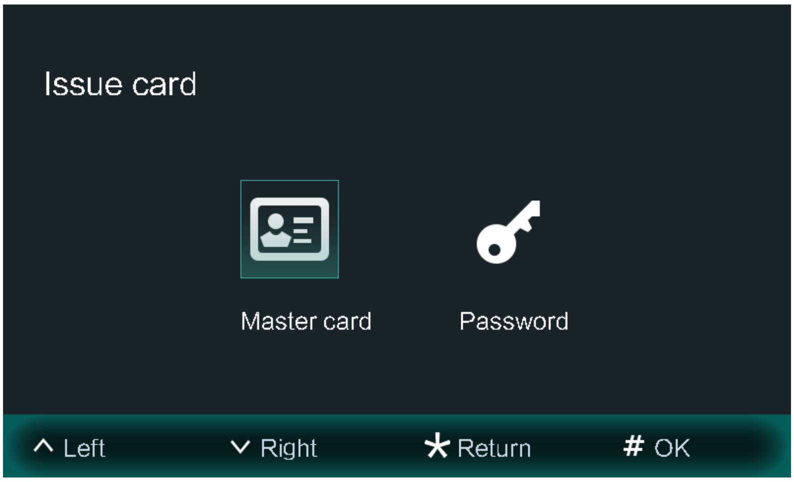
a. Issue cards through password. Tap **Issue card** > **Add** > **Password**.

Enter the password to complete the setting.

b. Issue cards through master card. Tap **Issue card** > **Add** > **Master card**.

You need a master card before you start issuing. If you do not have one, issue a card on the VTO through password. Then go to the web interface of the VTO, select **Household Setting** > **Personnel Management** > **Card** > **Main card**, set a card as your master card.

Figure 6-2 Master card



Step 7 Swipe cards on the card issuing interface, and card numbers will be automatically recognized.

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

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

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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