Digital Door Station (VTO65 Series)

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces basic operations of the digital door station (VTO). For details, see the user manual.

Model

VTO6521H, VTO6521H-D, VTO6531H, VTO6541H
VTO6521F, VTO6531F.

Safety Instructions

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

Signal Words	Meaning
⚠CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
🕮 Note	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release	Feburary, 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. 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 the company names in the manual are the properties of their respective owners.

- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

The following description is the correct application method of the device. Read the Guide carefully before use, in order to prevent danger and property loss. Strictly conform to the Guide during application and keep them properly after reading.

Operating Requirement

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; don’t put on the device anything filled with liquids to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- The device shall be used with screened network cables.

Power Requirement

- Use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.
- Do not cut off power supply during device upgrade. Power supply can be cut off only after the device has completed upgrade and has rebooted.

Table of Contents

1 Structure

The door station (VTO) has six models. Different models have different front panels but the same rear panel.

Figure 1-1 Dimensions (mm [inch])

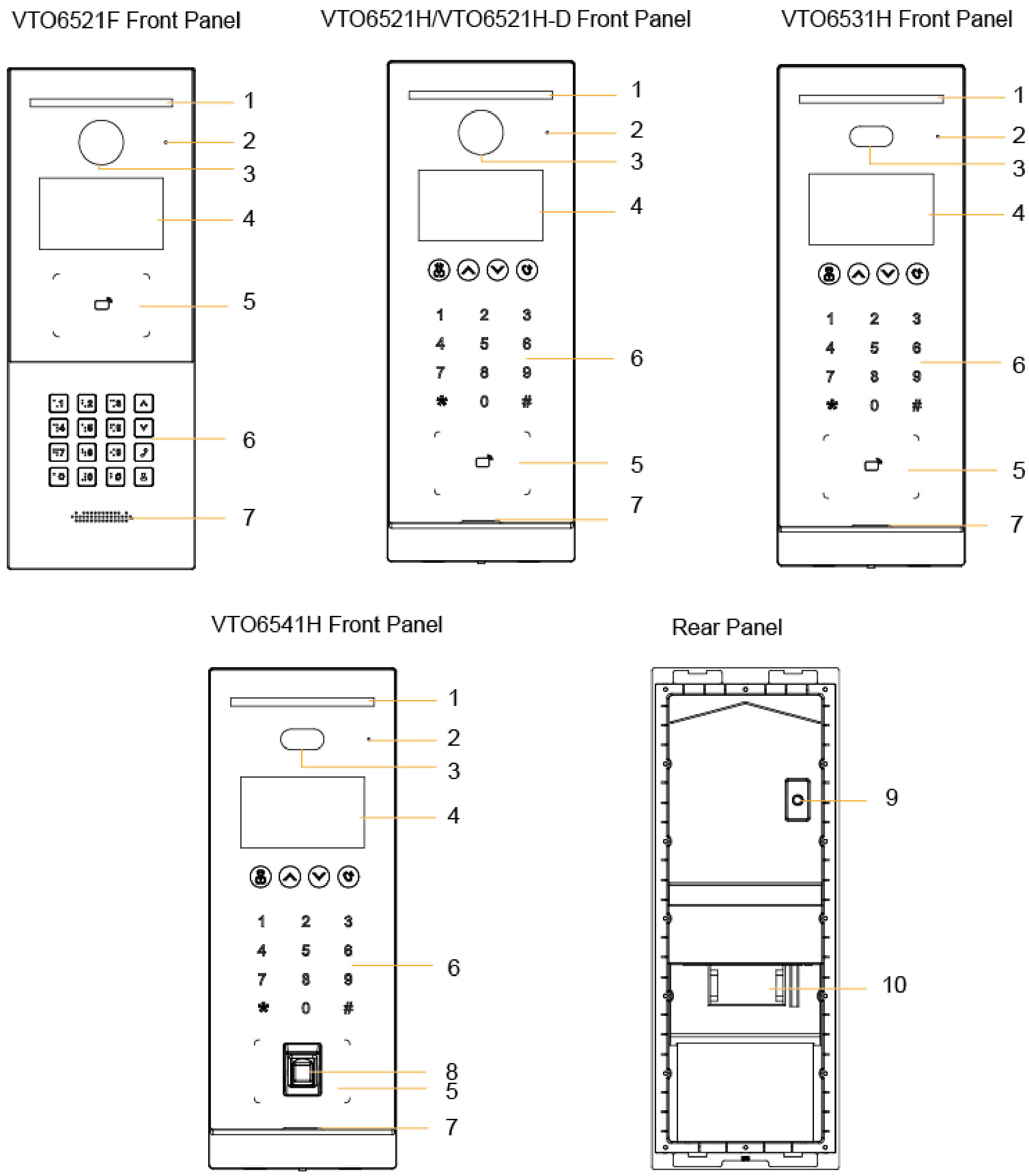
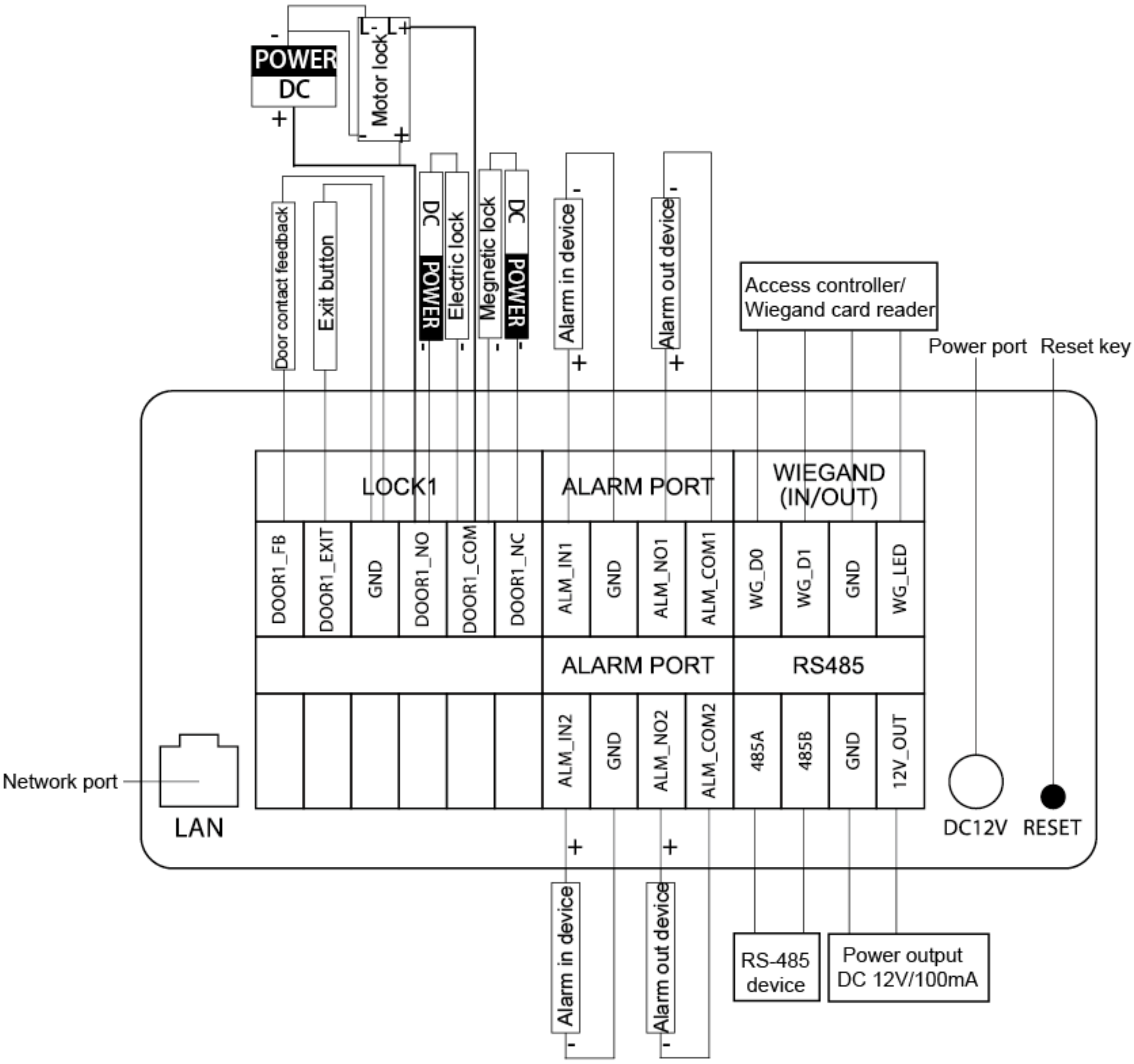


Table 1-1 Component description

No.	Description	No.	Description
1	White illuminator	6	Keyboard
2	MIC	7	Loudspeaker
3	Camera	8	Fingerprint sensor
4	Display	9	Tamper button
5	Card swiping area	10	Function ports (connected to locks, access controllers, alarm in/out devices)

2 Cable Connection

Figure 2-1 Cable connection



3 Installation

⚠

- Do not install the digital door station in environment with condensation, high temperature, and direct sunshine, and stained, dusty, chemically corrosive places.
- Engineering installation and test shall be done by professionals. Do not dismantle or repair arbitrarily in case of device failure. Contact after-sales service.
- Prepare cross screwdrivers and gloves yourself.
- Recommended distance between the camera and ground is 1.4m–1.6m.

Figure 3-1 Installation height

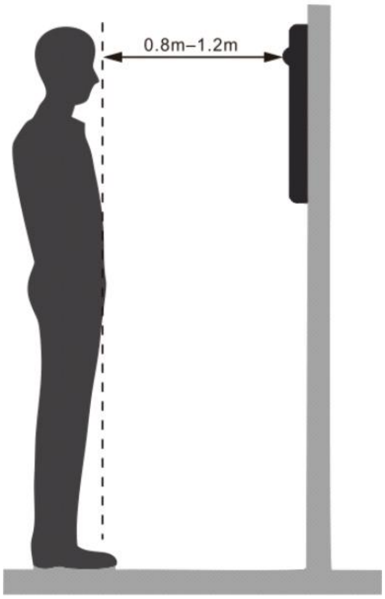


Figure 3-2 Installation

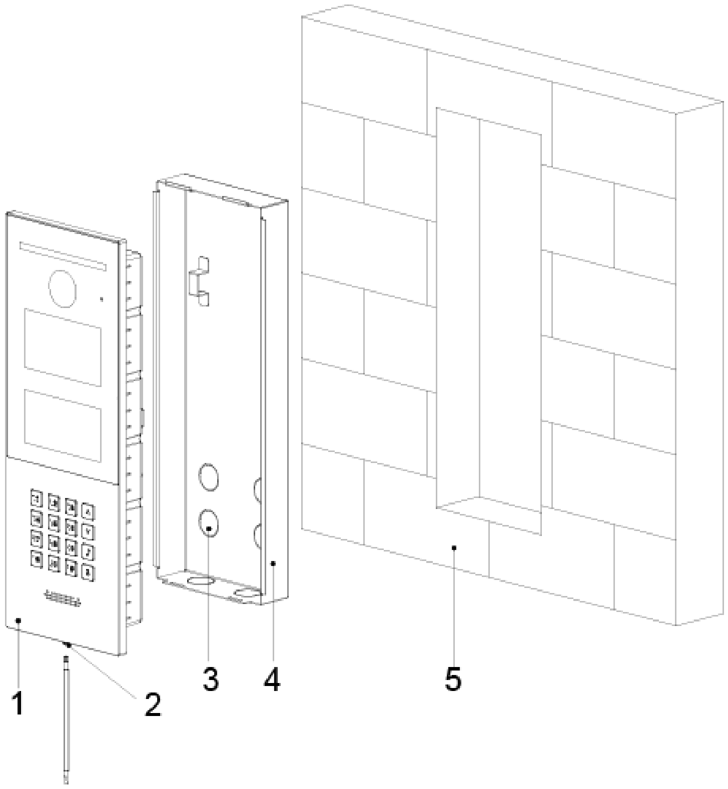


Table 3-1 Component description

No.	Description	No.	Description	No.	Description
1	Door station	3	Cable entry	5	Wall
2	Screw	4	Mounting plate	—	—

Installation Procedure

Step 1 Cut an opening in the wall according to dimensions of the mounting plate.

Step 2 Detach hole covers according to cable entry positions.

Step 3 Put the mounting plate in the opening in the wall.

Step 4 Fix the mounting plate with cement or sealant.

Step 5 Connect cables. Refer to "2 Cable Connection."

Before connecting cables, make sure that the power is disconnected.

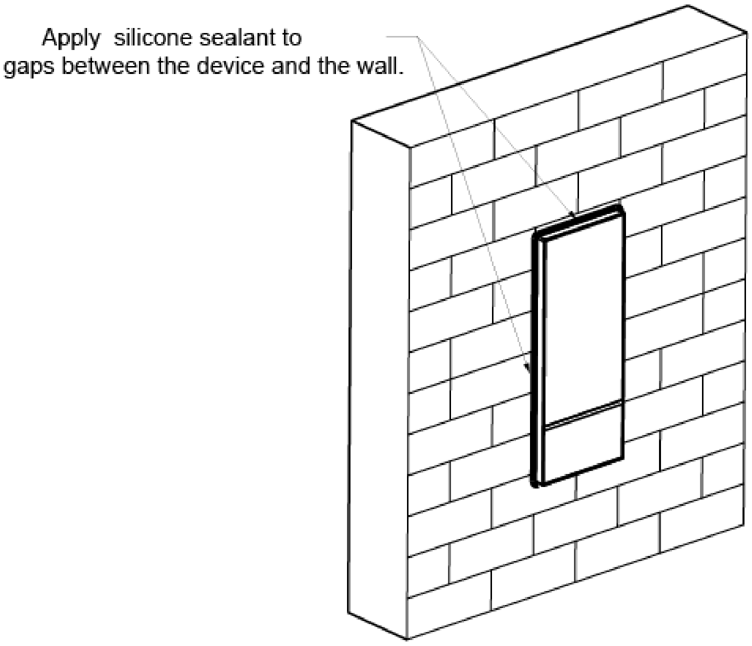
Step 6 Put the door station into the mounting plate, and then place the hook on the back of the door station into the installation slot of the mounting plate.

Step 7 Tighten screws at the bottom of the door station.

Step 8 Apply silicone sealant to gaps between the door station and mounting plate.

The installation is completed.

Figure 3-3 Apply silicone sealant


Apply silicone sealant to
gaps between the device and the wall.

4 Web Configuration

This chapter introduces how to initialize, connect, and configure parameters for the door stations to realize functions like device management, calling, and monitoring. For more details, see the user manual.

4.1 Configuration Process

Step 1 Plan IP address and number for each door station and indoor monitor.

Step 2 Make sure that there is no short circuit or open circuit in the circuits.

Step 3 Configure door station (VTO).

Beside initializing web interface and modifying IP address, configurations will be different depending on SIP server types.

1) When the door station you are operating works as the SIP server, refer to "4.4.1 Door Station (VTO) as SIP Server."
2) When the management platform works as the SIP server, refer to "4.4.2 Platform (DSS Express/DSS Pro) as SIP Server."

Step 4 Configure indoor monitors (VTH). See the indoor monitors (VTH) users' manual or the door station user’s manual.

4.2 Initializing Web Interface

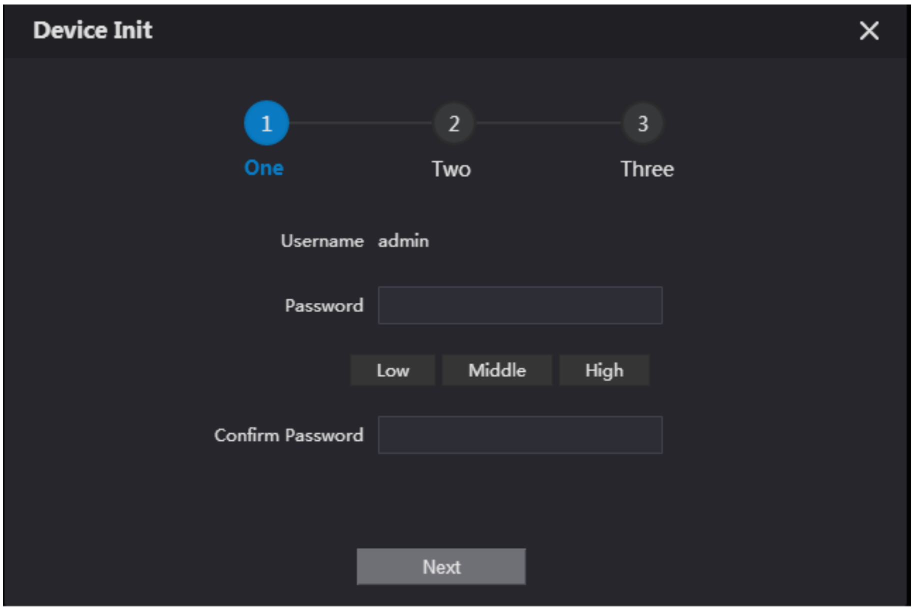
For the first time login, you need to create a password for logging in to the web interface.

The default IP address of door station is 192.168.1.108. Make sure that the PC IP address is in the same network segment as that of the door station.

Step 1 Connect the door station to power source, and then start it.

Step 2 Open the browser on the PC, enter the default IP address of the VTO in the address bar, and then press Enter.

Figure 4-1 Device initialization


Username admin

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

The email setting interface is displayed.

The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

Step 4 Select the **Email** check box, and then enter your email address.

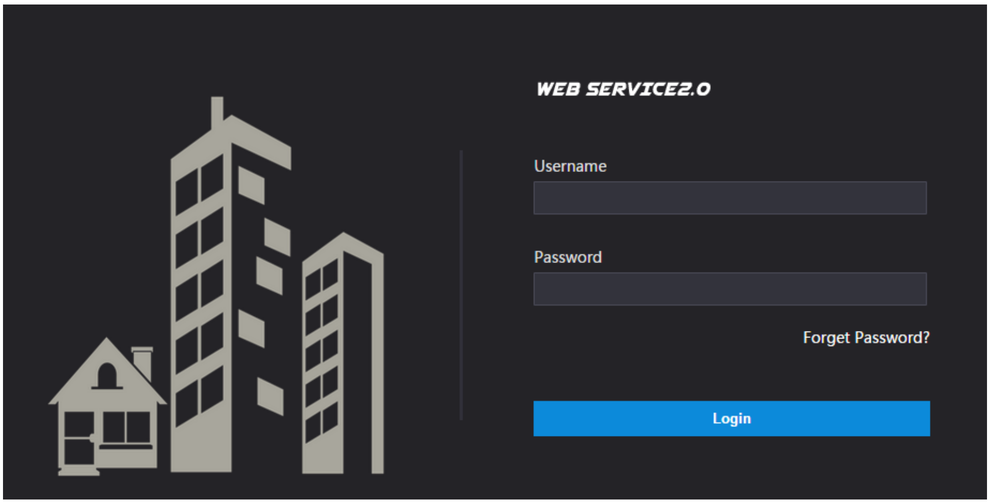
This email address is used to reset the password.

Step 5 Click **Next**.

The initialization succeeded.

Step 6 Click **OK**.

Figure 4-2 Login interface



Step 7 Enter username and password, and then click **Login** to log in to the web interface.

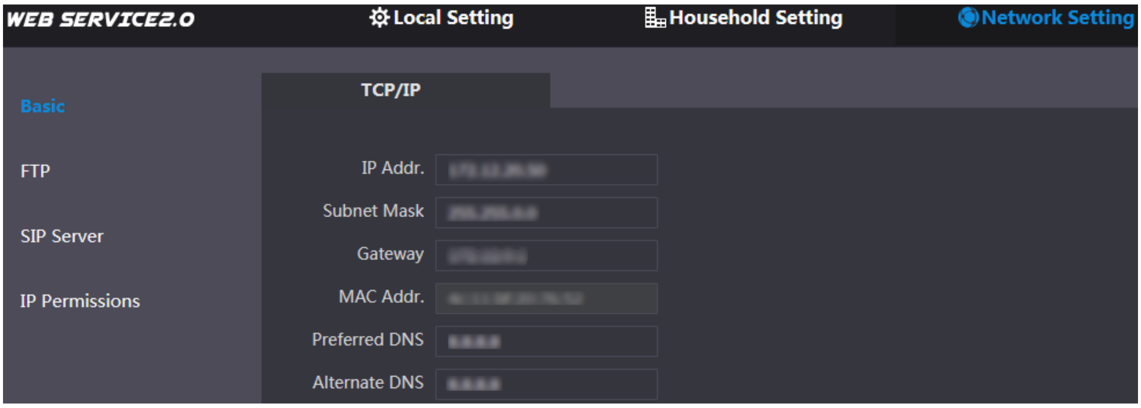
The username is admin by default; the password is the one that you set in Figure 4-1.

4.3 Modifying IP Address

To realize communication among video door phones, you need to modify IP address of the door station. You can modify IP address on the door station or through the web interface. Modifying IP address through the web interface will be demonstrated here. For IP address modification on the door station, see "5.2 Setting IP Address."

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

Figure 4-3 TCP/IP information



IP Addr. [redacted]
Subnet Mask [redacted]
Gateway [redacted]
MAC Addr. [redacted]
Preferred DNS [redacted]
Alternate DNS [redacted]

Step 2 Enter the network parameters that you planned, and then click **Save**.

Make sure that your PC IP address and the door station are in the same network segment.

The VTO will restart.

- Preferred DNS and alternate DNS are both 8.8.8.8 by default.
- If PC IP address is in the planned IP segment, the interface will go to the login interface automatically.
- If PC IP address is not in the planned IP segment, the interface will not go to the login interface. You need to make the PC IP address in the planned IP segment.

4.4 Selecting SIP Servers

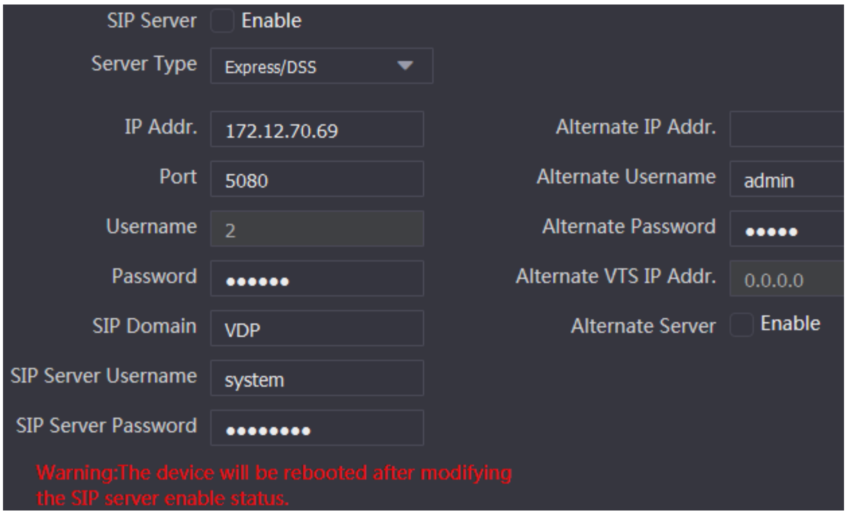
The Session Initiation Protocol (SIP) is used for signaling and controlling multimedia communication sessions in applications of voice and video calls. A SIP server is an application that provides information or direction to a user agent.

- When door stations (VTO) work as SIP server, select **VTO** from the **Server Type** drop-down list. It applies to a scenario where there is only one building.
- When the platform (Express/DSS) works as SIP server, select **Express/DSS** from the **Server Type** drop-down list. It applies to a scenario where there are multiple buildings or multiple units.

Step 1 Log in to the web page.

Step 2 On the homepage, select **Network Setting > SIP Server**.

Figure 4-4 SIP server



SIP Server □ Enable

Server Type: Express/DSS

IP Addr.: 172.12.70.69

Port: 5080

Username: 2

Password: ●●●●●●

SIP Domain: VDP

SIP Server Username: system

SIP Server Password: ●●●●●●●●

Alternate IP Addr.:

Alternate Username: admin

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 Select a SIP server.

4.4.1 Door Station (VTO) as SIP Server

Step 1 Select the **Enable** check box next to **SIP Server**.

Step 2 Select **VTO** from the **Server Type** drop-down list

Step 3 Configure parameters (see Table 4-3 for details).

Step 4 Click **Save**.

The door station (VTO) will restart automatically.

4.4.1.1 Setting Door Station (VTO) No. (1)

Each door station (VTO) has a unique number. The numbers are normally the same as building numbers.

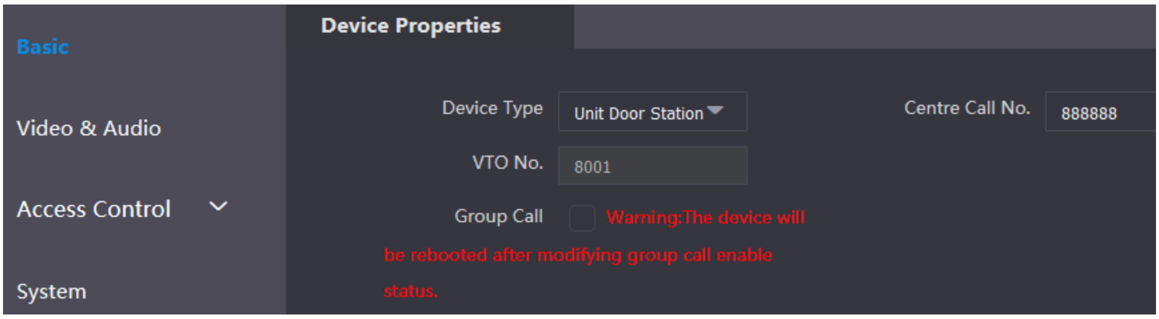
- You can change the number of a door station (VTO) when it does not work as a SIP server.
- Door station (VTO) numbers can contain 5 numbers at most, and it cannot be the same as any room number.

Step 1 Log in to the web interface.

The homepage is displayed.

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

Figure 4-5 Device properties



Device Type: Unit Door Station

VTO No.: 8001

Group Call □ Warning:The device will be rebooted after modifying group call enable status.

Centre Call No.: 888888

Step 3 In the **VTO No.** input box, enter the door station (VTO) number you planned, and then click **Confirm** to save the configuration.

Table 4-1 Device property description

Parameter	Description
Device Type	The door station can be used as unit door station and fence station. Select according to places where door stations are installed.
Centre Call No.	888888 by default. The default value cannot be modified.
VTO No.	VTO No. can only be modified when the door station you are operating does not work as a SIP server.
Group Call	After you have enabled the group call function, you can call the main indoor monitor (VTH) and its extensions at the same time. If the **Group Call** function is enabled, the door station (VTO) will restart automatically, and then this function will be valid.

4.4.1.2 Adding Indoor Monitors (VTH)

When the door station (VTO) you are operating works as the SIP server, you need to add all indoor monitors (VTH) to the door station (VTO); otherwise door stations (VTO) cannot communication with indoor monitors.

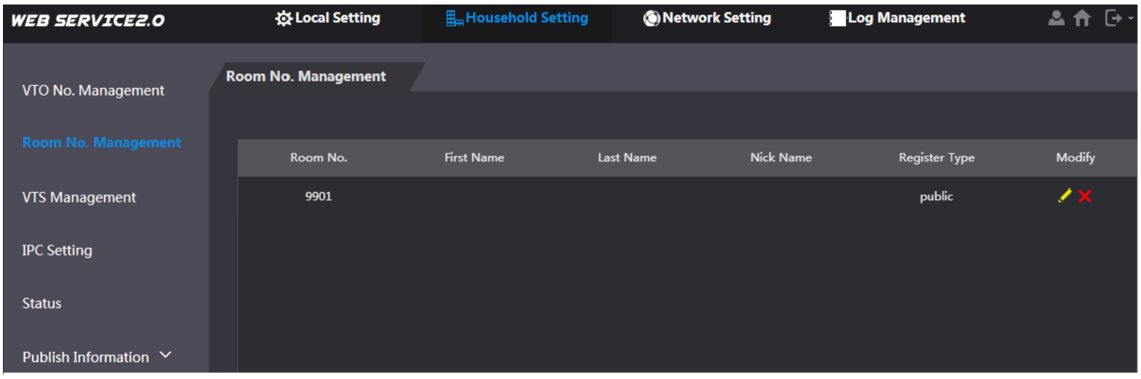
When there are master indoor monitors (VTH) and extensions, first you need to enable the **Group Call** function on the **Basic** Interface, and then add indoor monitors (VTH). To enable the **Group Call** function, refer to "4.4.1.1 Setting Door Station (VTO) No. (1)".

Adding One Indoor Monitor (VTH)

- You need to add indoor monitor (VTH) to the web of the door station (VTO) only when door station (VTO) works as SIP server.
- When there are master indoor monitor (VTH) and extensions, both shall be added to the web of the door station (VTO).

Step 1 Select **Household Setting > Room No. Management**.

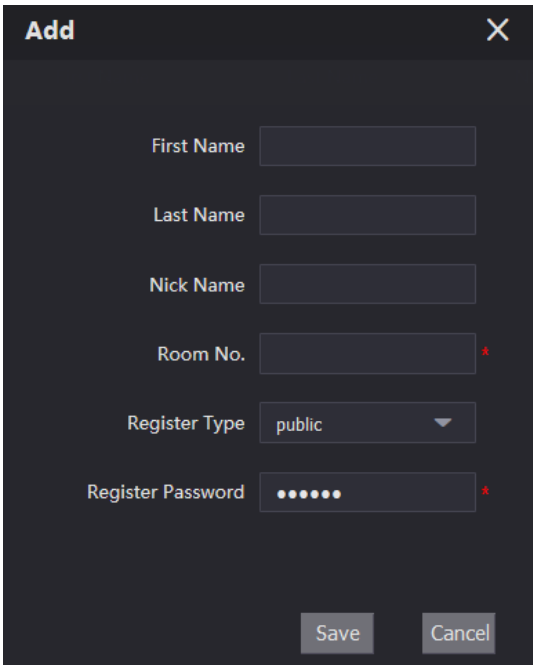
Figure 4-6 Room No. management



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

Step 2 Click **Add**.

Figure 4-7 Add



Add

First Name

Last Name

Nick Name

Room No. *

Register Type: public

Register Password: •••••• *

Step 3 Set indoor monitor (VTH) parameters by reference to Table 4-2.

Table 4-2 Descriptions of adding indoor monitors (VTH)

Parameter	Description
First Name	Set username and nickname for each indoor monitor (VTH).
Last Name	
Nick Name	
Room No.	Set room number at the indoor monitor (VTH). ● Indoor monitor (VTH) short number consists of 1–5 numbers, which includes numbers and "#". It shall be the same as the room number configured at indoor monitor (VTH). ● When there are master indoor monitors (VTH) and extensions, to realize group call function, master indoor monitor (VTH) short No. shall end with "#0", and extension VTH short No. shall end with #1, #2 and #3. For example, if master indoor monitor VTH No. is 101#0, extension numbers will be 101#1, 101#2…
Register Password	Keep the default value to enable signaling interactive in the SIP system.
Register Type	

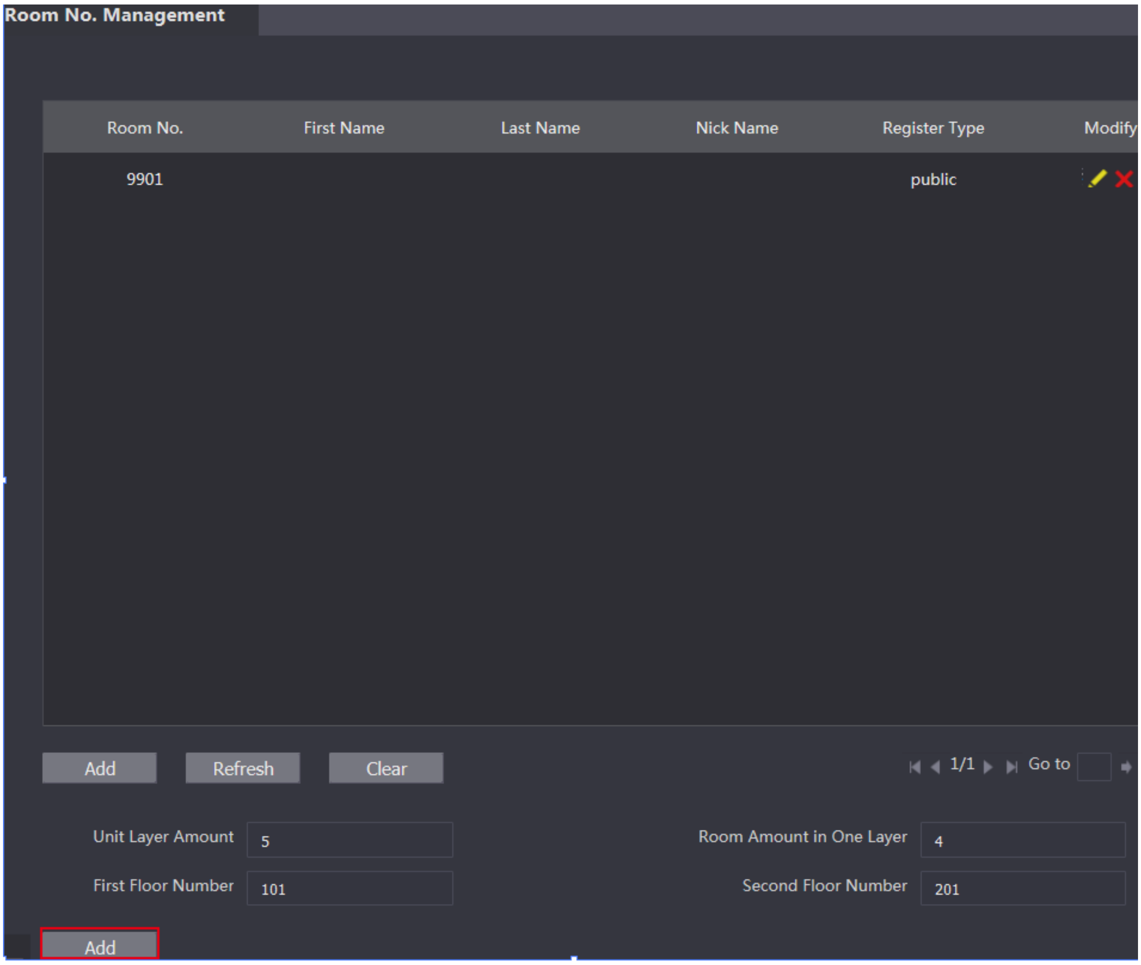
Step 4 Click **Save** to complete adding.

Repeat these steps to add more indoor monitors.

Adding Indoor Monitors (VTH) in Batch

Step 1 Select **Household Setting > Room No. Management**.

Figure 4-8 Adding indoor monitors (VTH) in batch



Room No. Management

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

Unit Layer Amount: 5

Room Amount in One Layer: 4

First Floor Number: 101

Second Floor Number: 201

Step 2 Enter **Unit Layer Amount**, **Room Amount in One Layer**, **First Floor Number**, and **Second Floor Number**.

- The unit layer amount range is 1–99, room amount in one layer range is 1–99, and first floor number range is 1–9999.
- Room numbers of the second floor must be in the same form as those of the first floor. For example, room numbers of the first floor is 100–199, and room numbers of the second floor must be 200–299.

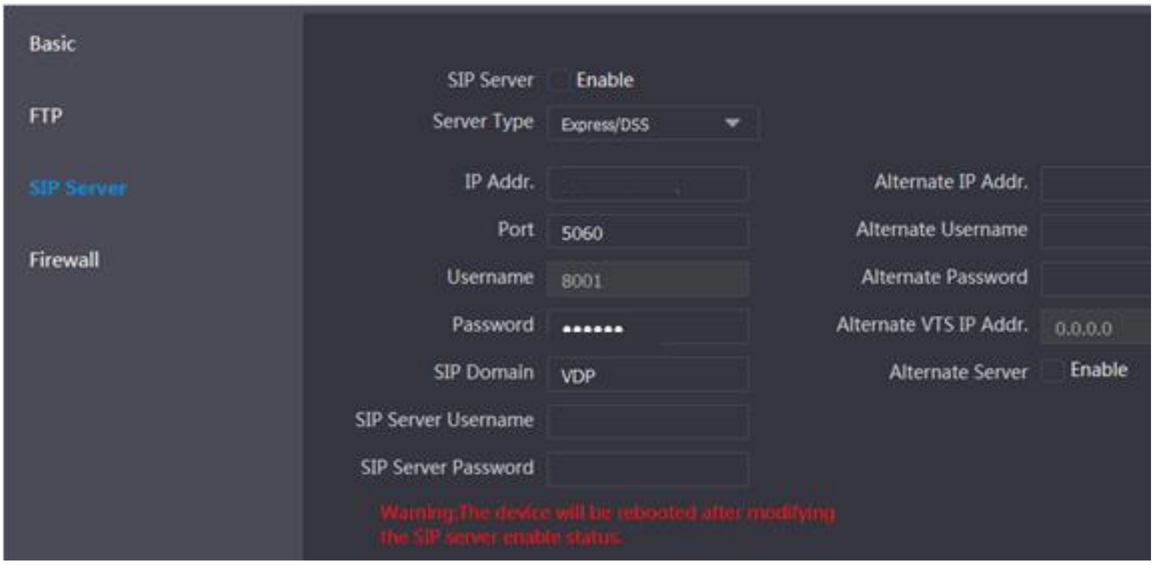
Step 3 Click **Add** to complete the adding.

4.4.2 Platform (DSS Express/DSS Pro) as SIP Server

When a management platform works as the SIP server, you need to register indoor monitors (VTH) and door stations (VTO) through the management platform.

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

Figure 4-9 SIP server



SIP Server □ Enable

Server Type Express/DSS

IP Addr.

Port 5060

Username 8001

Password ••••••

SIP Domain VDP

SIP Server Username

SIP Server Password

Alternate IP Addr.

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 2 Select **Express/DSS** from the **Server Type** drop-down list.

Step 3 Set parameters according to Table 4-3.

Table 4-3 SIP server parameter description

Parameter	Description
IP Address	IP address of SIP server.
Port	● It is 5060 by default when other door stations (VTO) rather than the one you are operating works as SIP server. ● It is 5080 by default when management platform works as SIP server.
Username/Password	Use default value.
SIP Domain	● It shall be VDP when other door stations (VTO) rather than the one you are operating works as SIP server. ● It can be null or keep default value when the platform works as SIP server.
Login Username/ Password	Username and password to login SIP server.
Alternate IP Addr.	IP address of the alternate server (the door station (VTO) you are operating). 📖 If DSS Express or DSS Pro works as SIP server and alternate server is enabled, when DSS Express or DSS Pro cannot work normally, the door monitor (VTO) you are operating will be used as SIP server.
Alternate Username	Username and password for logging in to the alternate server.
Alternate Password	
Alternate VTS IP Addr.	IP address of the alternate VTS.
Alternate Server	After entering alternate IP address, username, password, and VTS IP address, you need to select the **Enable** checkbox to enable the alternate server.

Step 4 Click **Save**.

The VTO will restart automatically.

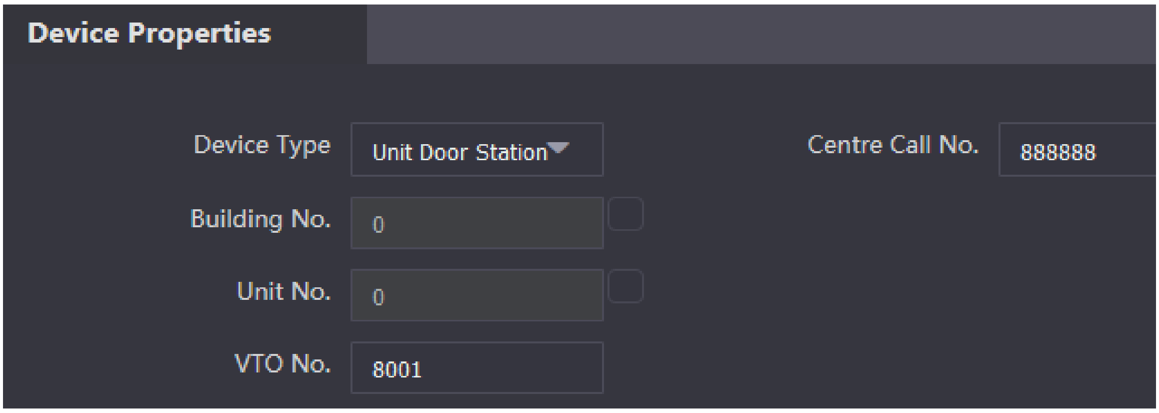
4.4.2.1 Setting Door Station (VTO) Number (2)

After you have selected the **Alternate Server** enable checkbox in Figure 4-9, the door station (VTO) will restart automatically. You need to select device type, building No., unit No., and VTO No. as needed.

Step 1 Log in to the web interface again.

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

Figure 4-10 Device properties



Device Properties

Device Type: Unit Door Station

Centre Call No.: 888888

Building No.: 0 □

Unit No.: 0 □

VTO No.: 8001

Step 3 Click **Confirm**.

Table 4-4 Device properties description

Parameter	**Description**
Device Type	The door station can be used as unit door station and fence station. Select according to places where door stations are installed.
Centre Call No.	888888 by default. The default value cannot be modified.
Building No.	Building No. range is 0-99999. Click □ next to the input box to enable the building No. input function, and then enter the No. of the building where the door station is installed.
Unit No.	Unit No. range is 0-9999. Click □ behind the input box to enable the building No. input function, and then enter the No. of unit where the door station is installed.
VTO No.	VTO No. range is 8001-8099. Enter No. of the door station (VTO) that you are operating. 🕮 ● VTO No. can only be modified when the door station you are operating does not work as a SIP server. ● If there are more than one door stations (VTO) in a unit, the numbers of the door stations (VTO) cannot be the same.

5 Engineering Setting

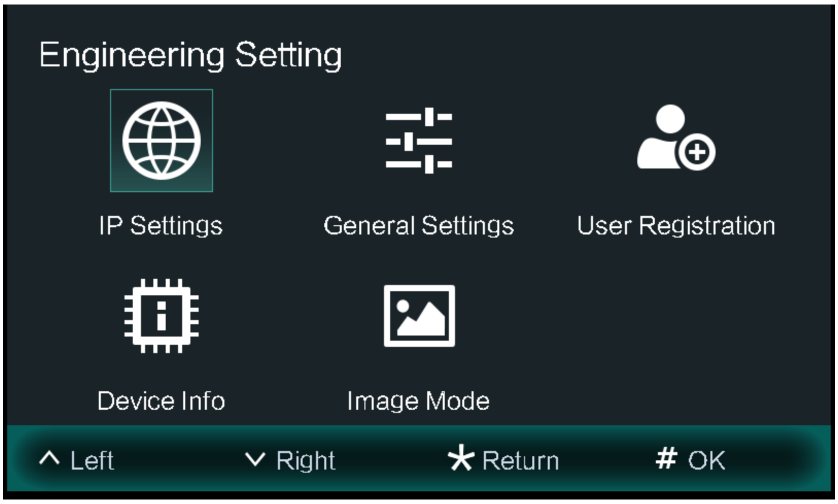
5.1 Entering Engineering Setting

- Project interface is normally for administrators or engineers.
- You need to set the project password by selecting **Local Setting > Access Control > Local** on the web interface.

Step 1 Press "*project password#" on the door station (VTO).

The **Engineering Setting** interface is displayed.

Figure 5-1 Engineering setting



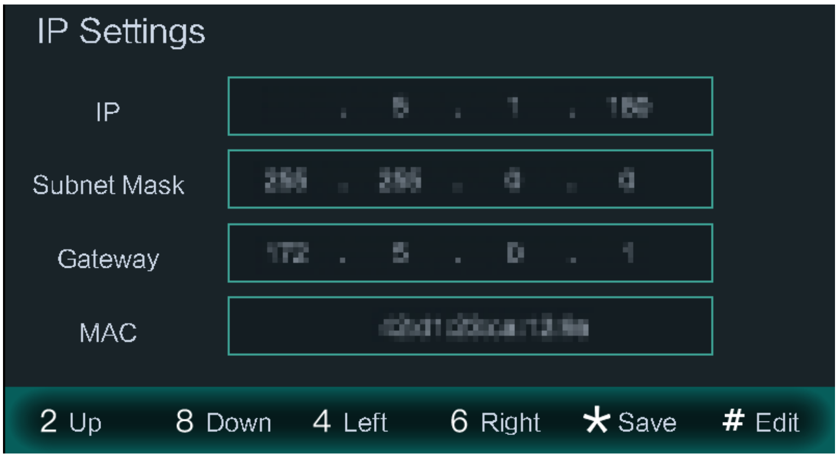
5.2 Setting IP Address

You need to plan an IP address for the door station (VTO) to connect the door station (VTO) to the network.

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

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

Figure 5-2 IP settings


IP Settings

IP [redacted]

Subnet Mask [redacted]

Gateway [redacted]

MAC [redacted]

Step 3 Press * to complete the setting.

6 User Registration

Only users whose information, including username, personnel number, room number, fingerprint, and card number, is registered can unlock doors.

Step 1 Press "*project password#" on the door station (VTO) to go to the **Engineering Setting** interface.

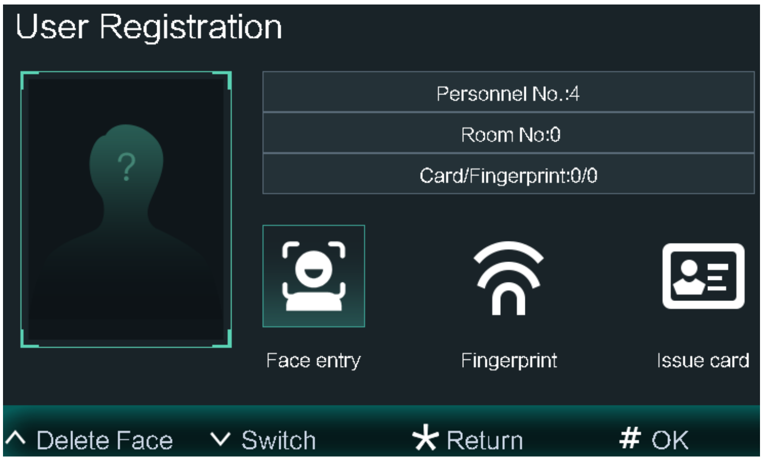
Step 2 On the **Engineering Setting** interface, select **User Registration**.

Step 3 Select **Add**.

Step 4 Enter user ID and Room No.

Step 5 Press # to save the settings.

Figure 6-1 User registration



User Registration

Personnel No.:4

Room No:0

Card/Fingerprint:0/0

Step 6 Record face images and issue cards.

- Face entry: Make sure that your face is in the middle of the frame. User face images will be automatically taken. If you are not satisfied, tap **Cancel** to take a new image.
- (Only for VTO 6541H) Fingerprint: at most three fingerprints of one user can be recorded. Each fingerprint needs to be recorded three times. Operate according to voice prompt.
- Issue card: You can issue at most five cards for each user. Swipe cards on the card issuing interface, card numbers will automatically be recognized.
  - ◇ Issue cards through authorized cards.

    - Before issuing cards, you need to have an authorized card. If there are no authorized cards, you need to issue a card on the door station (VTO) through password.
    - On the web interface of the door station, select **Household Setting > Room No. Management >** ✎, and then you can set a card as an authorized card.
  - ◇ Issue cards through password.

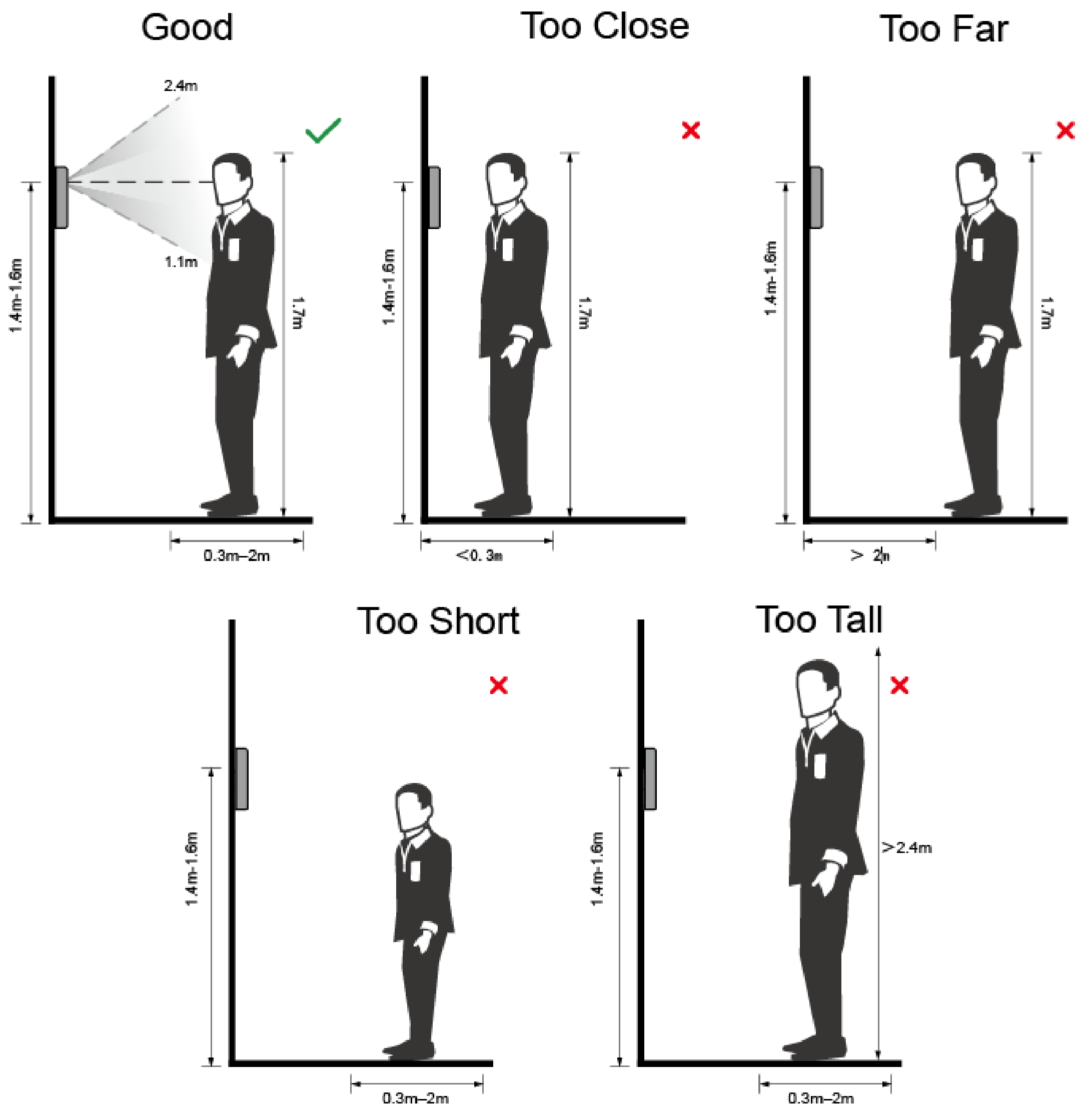
    You need to enter **Issue Card Password** on the web interface of the door station (VTO) in **Local Setting > Access Control > Local**.

Appendix 1 **Notes of Face Recording**

Face Position

If your face is not at the appropriate position, face recognition effect might be influenced.

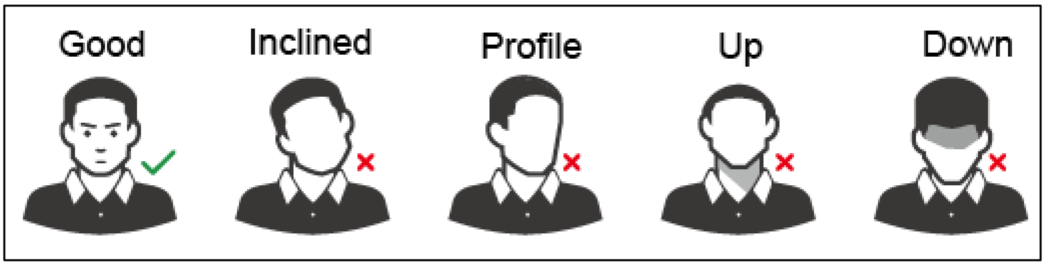
Appendix Figure 1-1 Appropriate face position



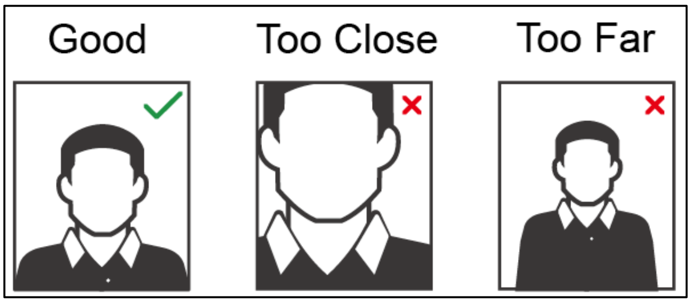
Requirements of Faces

- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face is toward the center of camera.
- When recording your face or during face recognition, do not keep your face 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 image pixels are more than 500 × 500; image size is less than 100 KB; image format is JPG; image background color is pure color (white is the best); and that image name and person ID are the same.

Appendix 2 Fingerprint Record Instruction

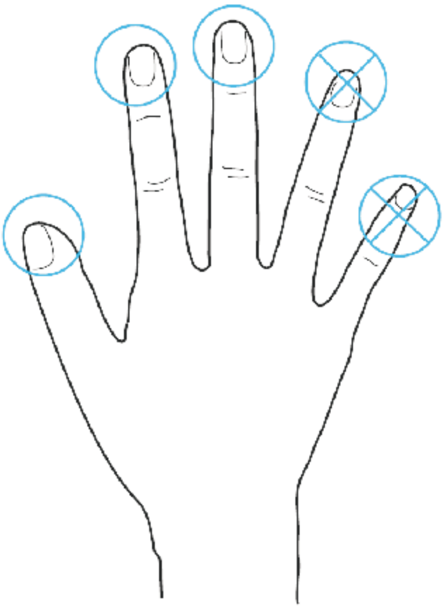
Notice

- Make sure that your fingers are clean and dry before recording your fingerprints.
- Press your finger to the fingerprint recording area, and make your fingerprint is centered on the recording area.
- Do not put the fingerprint sensor at places with intense light, high temperature, and high humidity.
- For the ones whose fingerprints are worn or are unclear, try other unlock methods.

Fingers Recommended

Thumbs, forefingers, and middle fingers are recommended because other fingers cannot be put at the recording center easily.

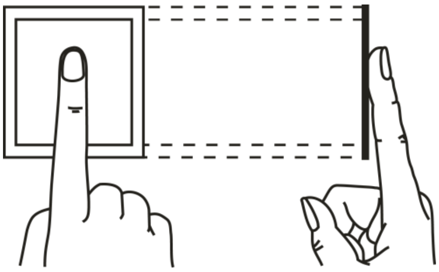
Appendix Figure 2-1 Recommended fingers



Finger Pressing Method

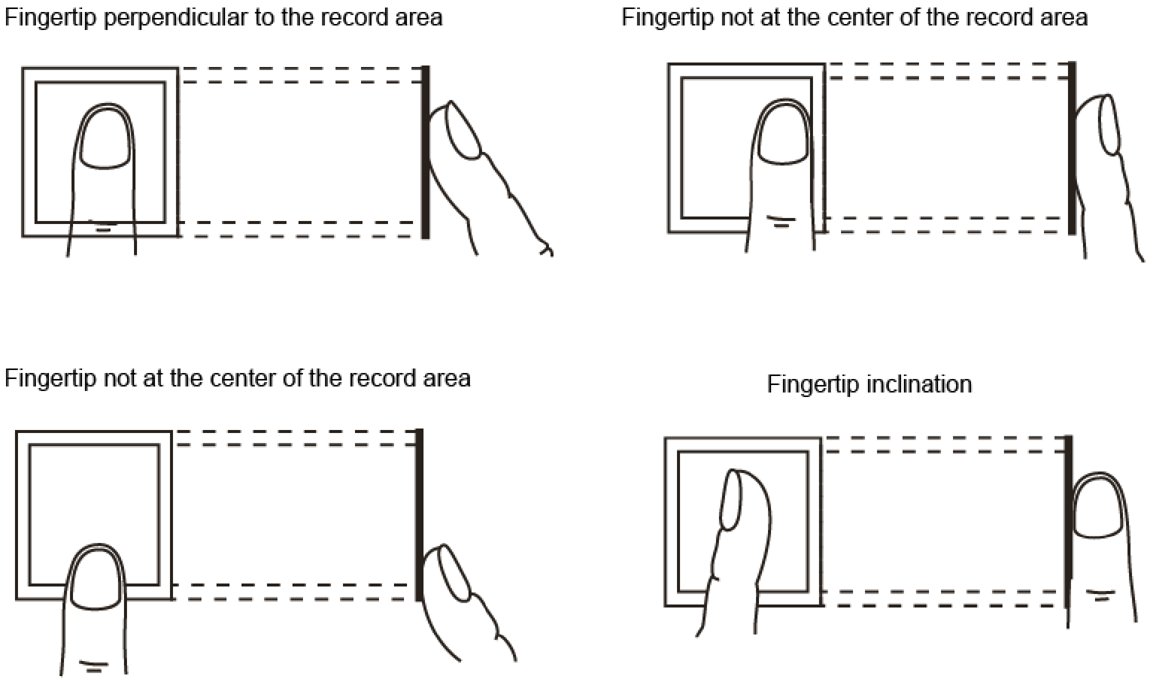
- Correct method

Appendix Figure 2-2 Correct finger pressing



- Incorrect method

Appendix Figure 2-3 Wrong finger pressing



Fingertip perpendicular to the record area

Fingertip not at the center of the record area

Fingertip not at the center of the record area

Fingertip inclination

Appendix 3 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it’s something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer’s IP address and the accompanying equipment’s IP address to the whitelist.

8. **MAC Address Binding**

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

9. **Assign Accounts and Privileges Reasonably**

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

10. **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.

11. **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.

12. **Secure Auditing**

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

13. **Network Log**

    Due to the limited storage capacity of the equipment, 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.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment 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.