Digital Door Station (VTO65 Series)

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces basic operations of the digital door station (hereinafter referred to as "VTO"). For details, see the user manual.

Model

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

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	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 it 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.
- Use screened network cables.

Power Requirement

- Use electric wires (power wires) recommended by this area, and 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

Foreword I

Important Safeguards and Warnings III

1 Structure 1

2 Cable Connection 2

3 Installation 3

4 Web Configuration 4

4.1 Procedure 4

4.2 Initialization 4

4.3 Configuring Network Parameters 5

4.4 Configuring VTO Number 6

4.5 Configuring SIP Servers 6

4.6 Adding Room Number 8

5 Engineering Setting 10

5.1 Entering Engineering Setting 10

5.2 Changing IP Address 10

6 User Registration 11

Appendix 1 Notes of Face Recording 12

Appendix 2 Fingerprint Record Instruction 14

Appendix 3 Cybersecurity Recommendations 16

1 Structure

There are six models with different front panels but the same rear panel.

Figure 1-1 Dimensions (mm [inch])

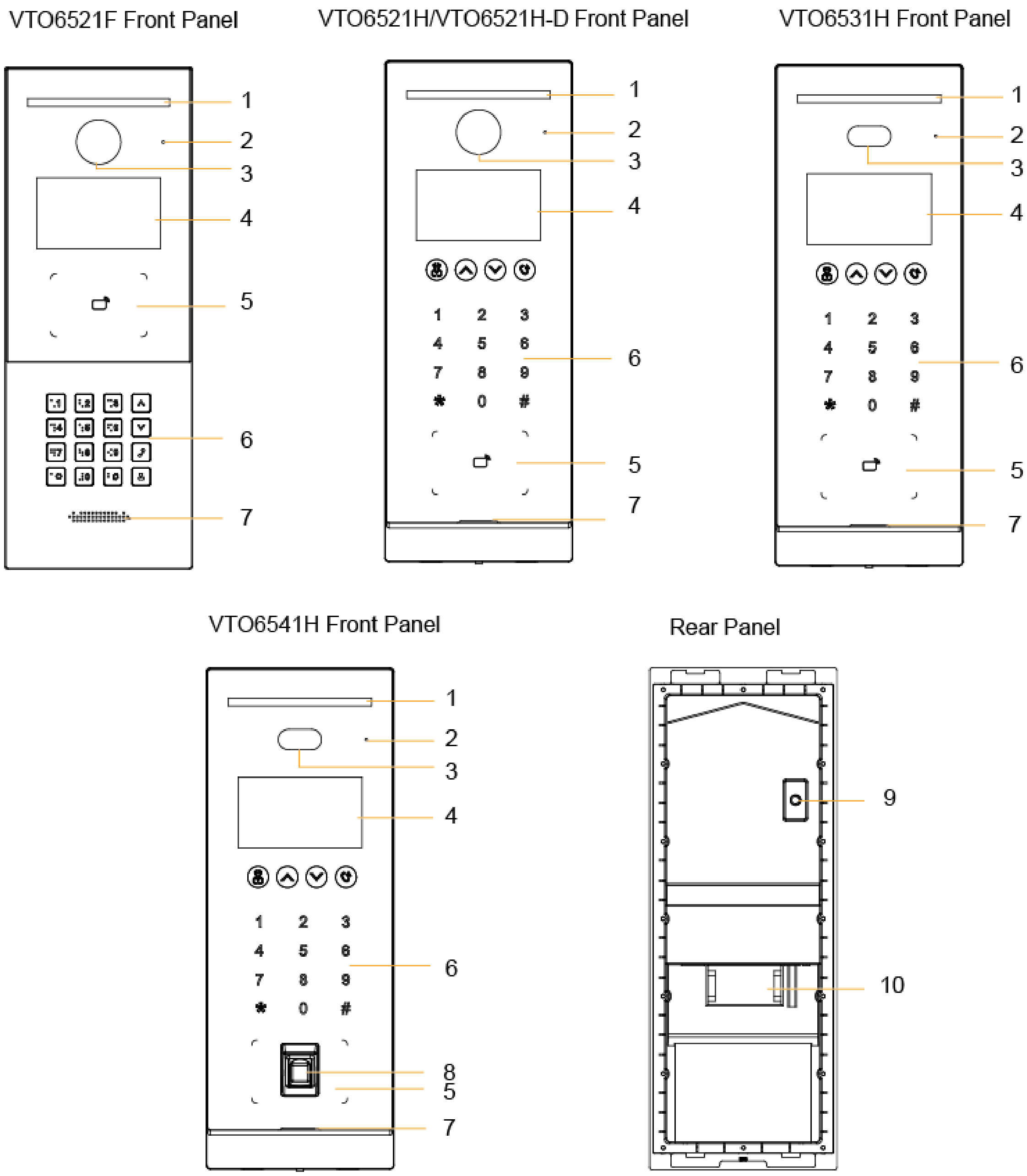
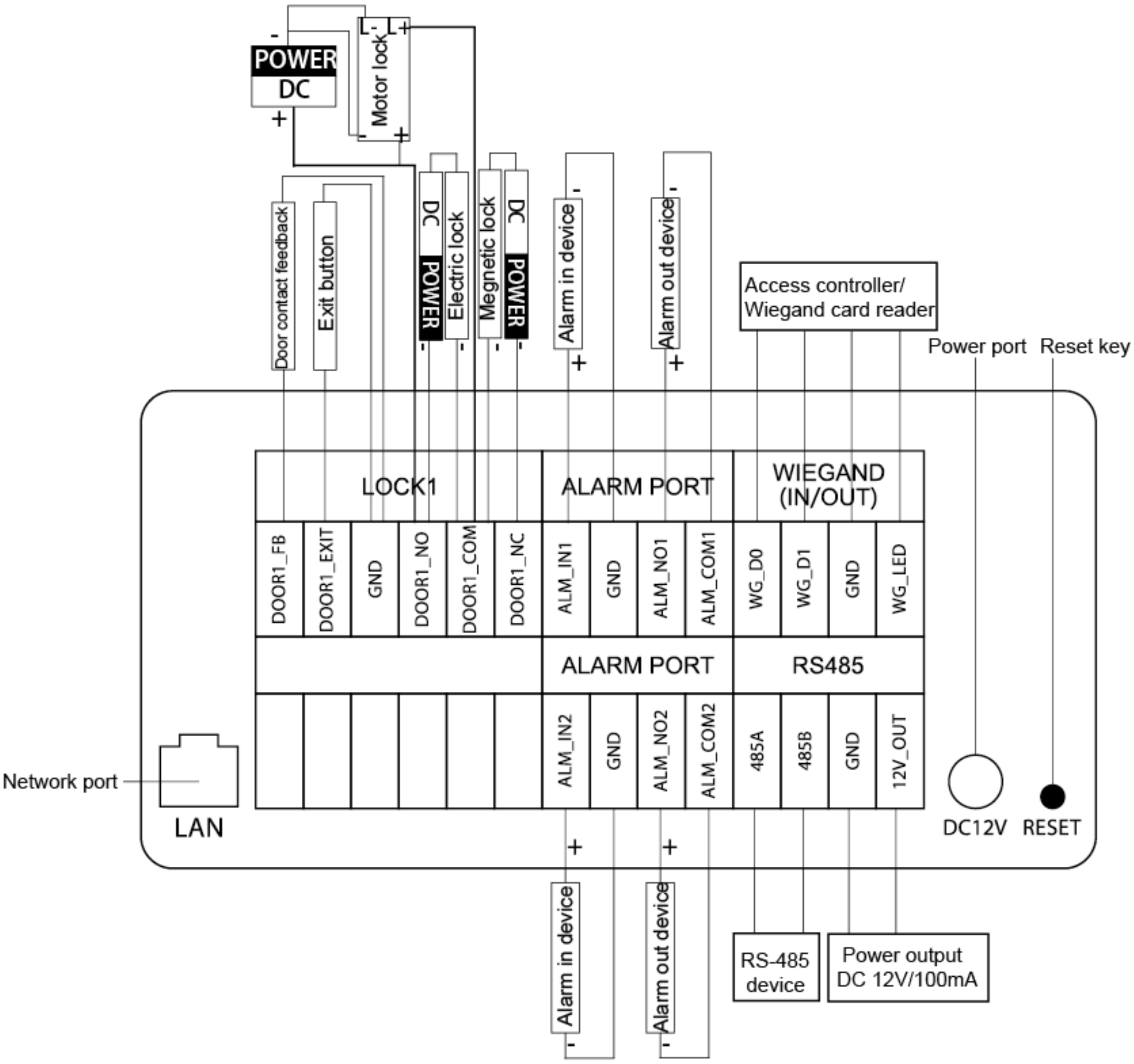


Table 1-1 Component description

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

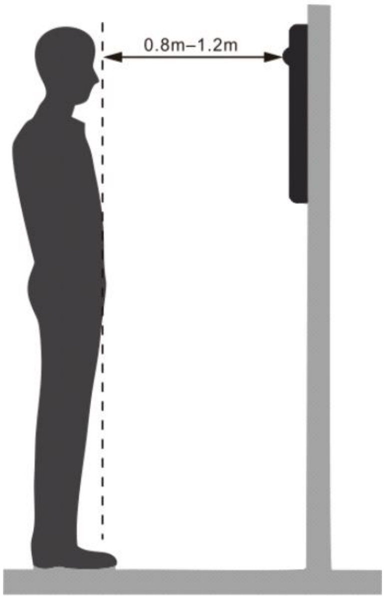


3 Installation

⚠

- Do not install the VTO in environment with condensation, high temperature, and direct sunshine, and stained, dusty, chemically corrosive places.
- Engineering installation and debugging must be done by professionals. Do not dismantle or repair 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 to the VTO and VTH devices. For more details, see the user's manual.

4.1 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 VTO. See 4.2–4.6.

Step 3 Configure the indoor monitor (hereinafter referred as "VTH"). See the VTH or VTO user's manual.

4.2 Initialization

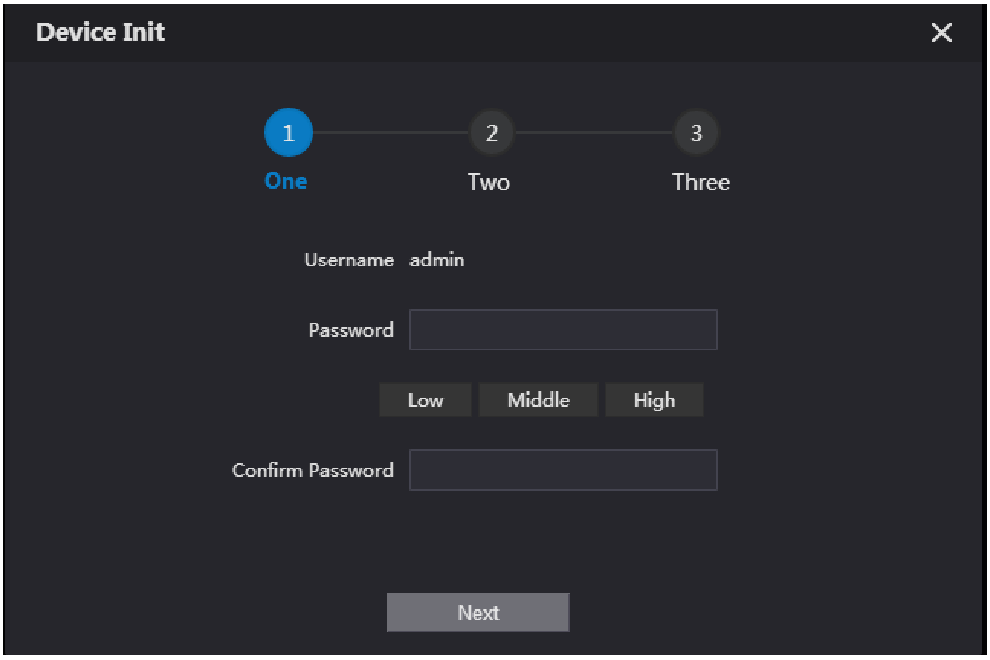
For the first time login, you need to create a password.

Step 1 Power on the VTO.

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

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

Figure 4-1 Device initialization



Username admin

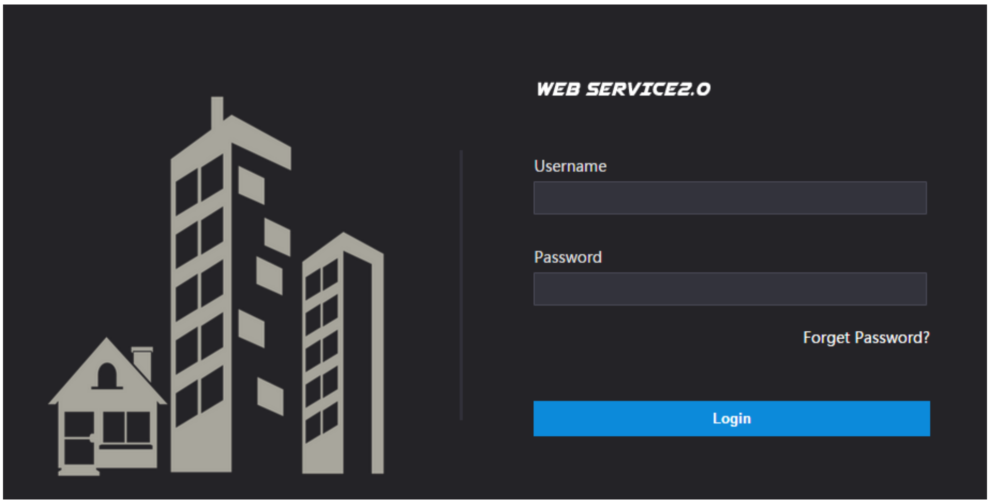
Step 3 Enter and confirm the password, and then click **Next**.

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 **Email** and enter email address for resetting password.

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

Figure 4-2 Login interface



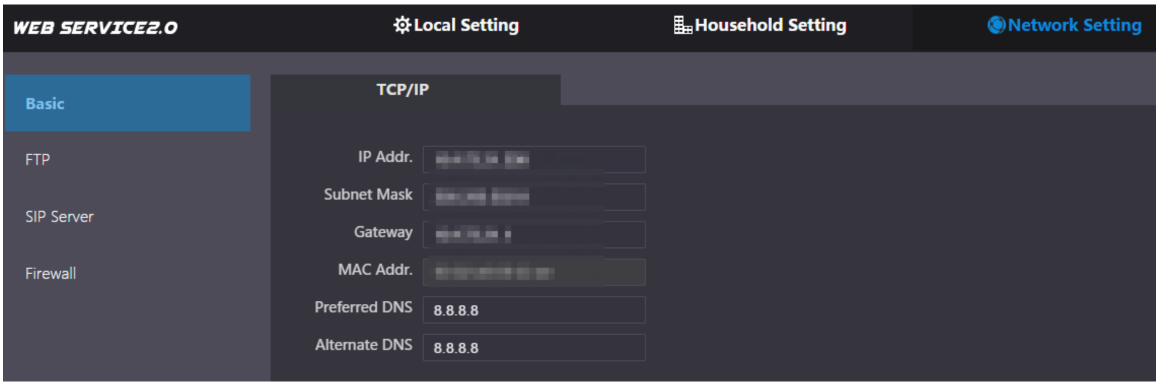
4.3 Configuring Network Parameters

To call other devices, you must make sure the IP address of the VTO is in the same network segment as other devices. To change IP on the VTO, see"5.2 Changing IP Address".

If the default IP address of VTO is in the same network segment as other devices, you do not need to change it.

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 8.8.8.8
Alternate DNS 8.8.8.8

Step 2 Enter the network parameters and click **Save**.

The VTO will automatically restart. You need to add the IP address of your PC to the same network segment as the VTO to log in again.

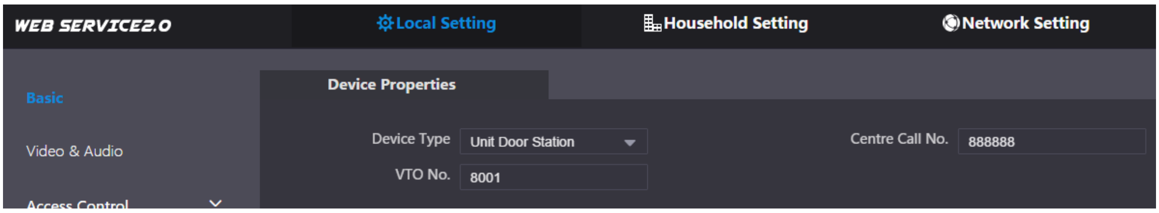
4.4 Configuring VTO Number

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

Step 1 Log in to the web interface.

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

Figure 4-4 Device properties



Device Type: Unit Door Station

VTO No.: 8001

Centre Call No.: 888888

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

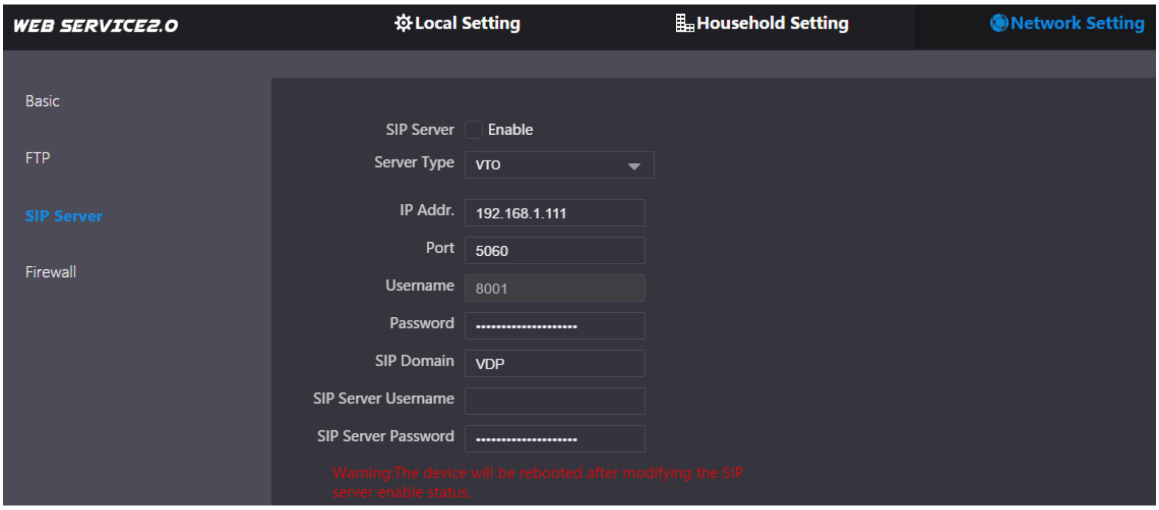
- You can change the number of a VTO when it is not working as the SIP server.
- A VTO number can contain up to 5 numbers, and it cannot be the same as any room number.

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.

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

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 2 Select a SIP server.

VTO as the SIP server (for One Building)

Step 1 Set **Server Type** as **VTO**.

Step 2 Configure the parameters. See Table 4-1.

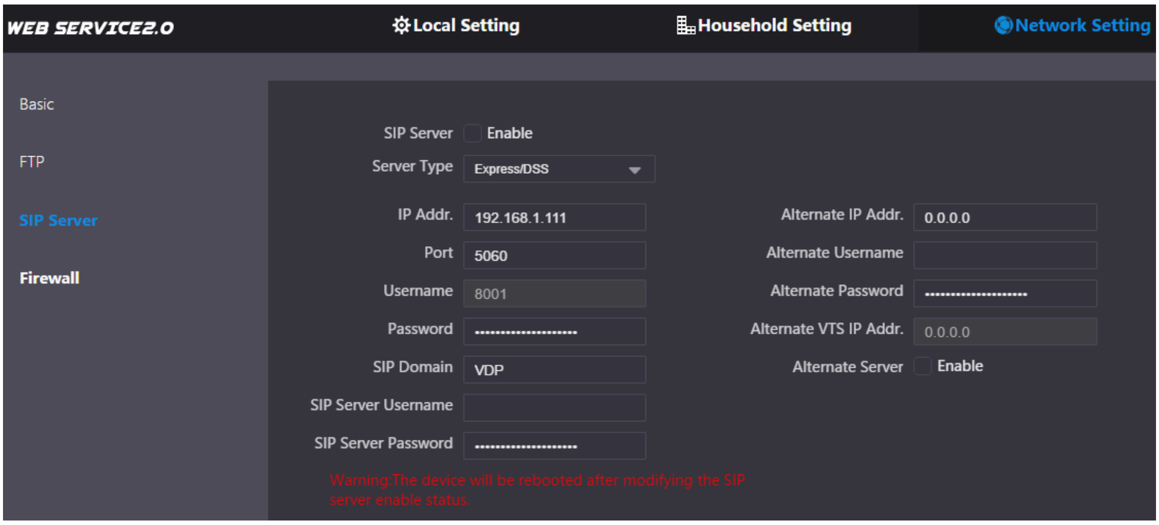
Step 3 Enable **SIP Server**.

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

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

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

Figure 4-6 SIP server (2)



SIP Server □ Enable

Server Type: Express/DSS

IP Addr.: 192.168.1.111

Port: 5060

Username: 8001

Password: ••••••••••••••••••••

SIP Domain: VDP

SIP Server Username:

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

Step 3 Configure the 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	Use default value.
SIP Domain	● It should be VDP when another VTO works as SIP server. ● Keep default value or empty 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 alternate server is enabled, the VTO will be used as SIP server when Express/DSS cannot work properly.
Alternate Username/ Password	Used to log in to alternate server.
Alternate VTS IP Addr.	IP address of the alternate VTS.
Alternate Server	Enable it as needed.

Step 4 Click **OK**.

The VTO will restart automatically.

When the platform works as the SIP server, if it is necessary to set Building No. and Building Unit No., enable **Support Building** and **Support Unit** first.

4.6 Adding Room Number

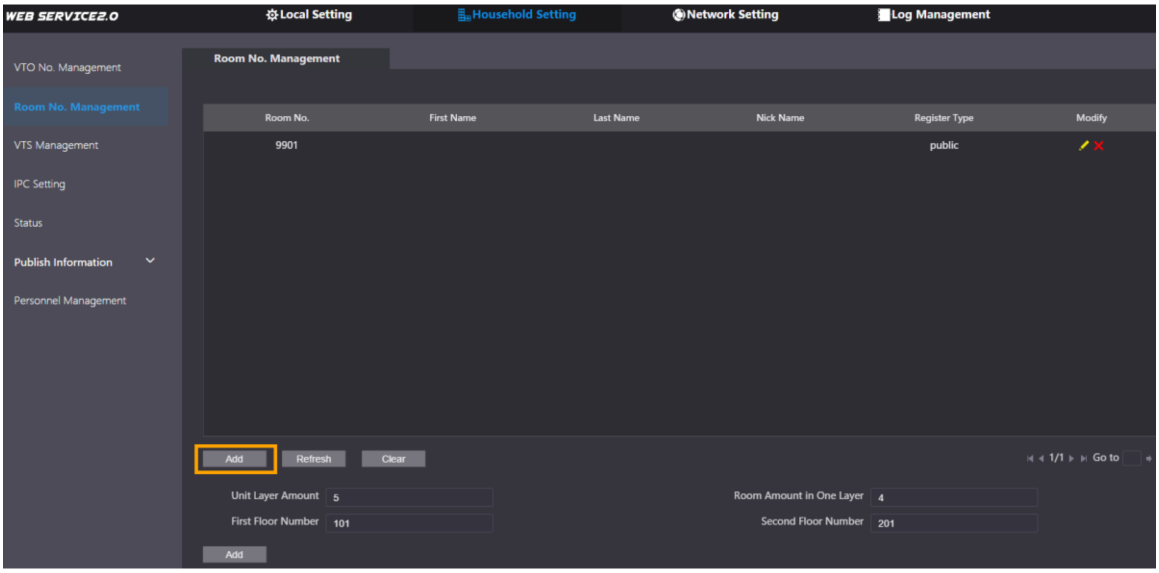
You can add room numbers to the SIP server, and then configure the room number on the VTHs to connect them to the network.

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.

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

Room Amount in One Layer: 4

First Floor Number: 101

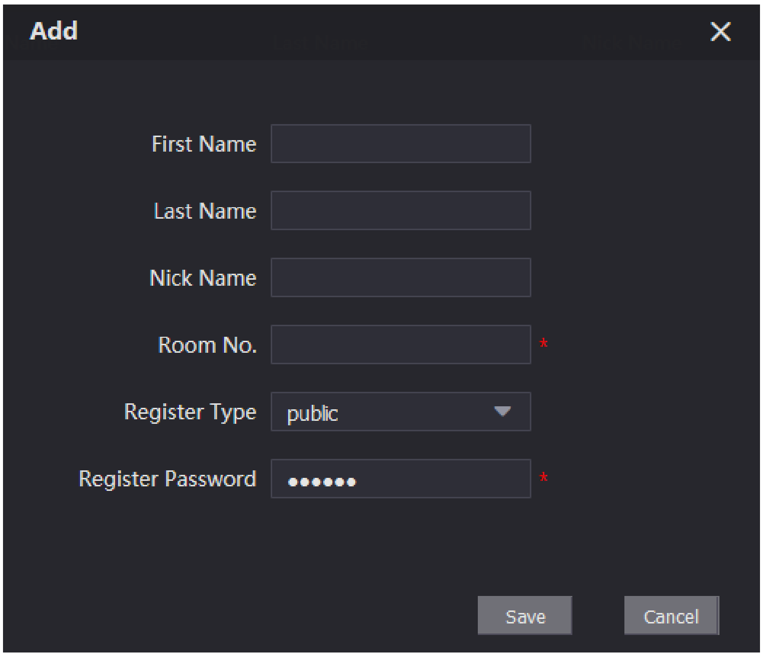
Second Floor Number: 201

Step 2 You can add a single room number or multiple ones.

- Add a single room number.

1) Click **Add**.

Figure 4-8 Add a single room number



First Name

Last Name

Nick Name

Room No. *

Register Type: public

Register Password: •••••• *

2) 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… ● You can have up to 10 extension VTHs for one master VTH.
Register Type	Select **public**.
Register Password	Keep the default value.

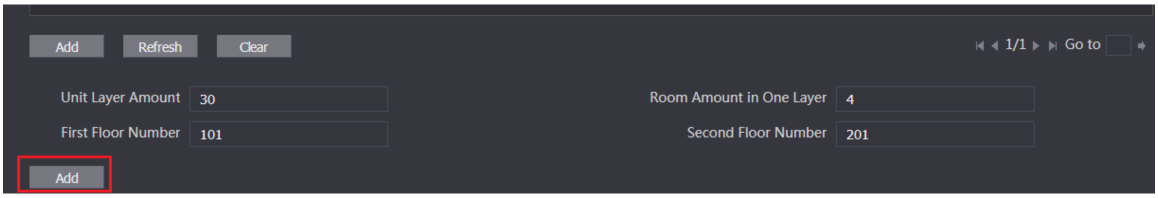
3) Click **Save**.

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

- Adding multiple room numbers.

1) Configure the **Unit Layer Amount**, **Room Amount in One Layer**, **First Floor Number**, and **Second Floor Number** as needed.
2) Click **Add**.
   All the added room numbers are displayed. 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

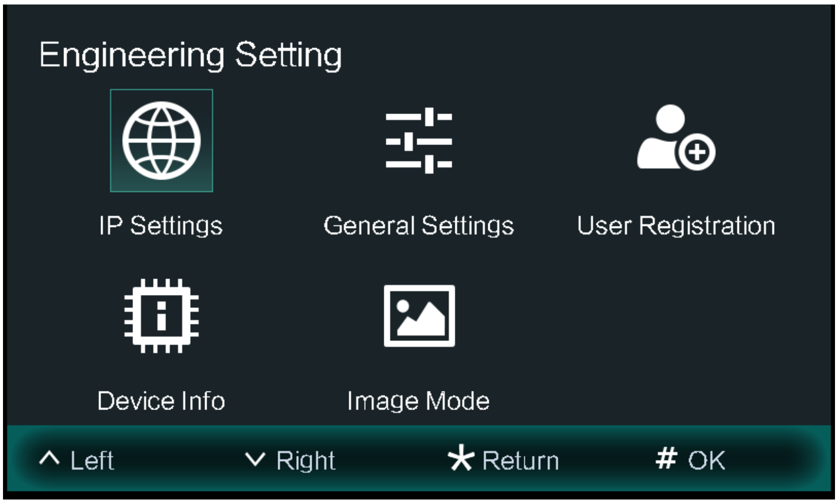
5 Engineering Setting

5.1 Entering Engineering Setting

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

Press "*project password#" on the VTO.

Figure 5-1 Engineering setting



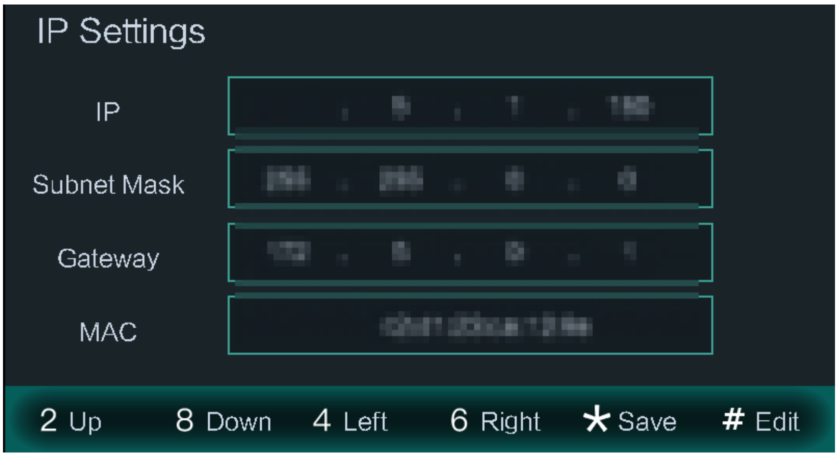
5.2 Changing IP Address

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.

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

Figure 5-2 IP settings



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 VTO to go to the **Engineering Setting** interface.

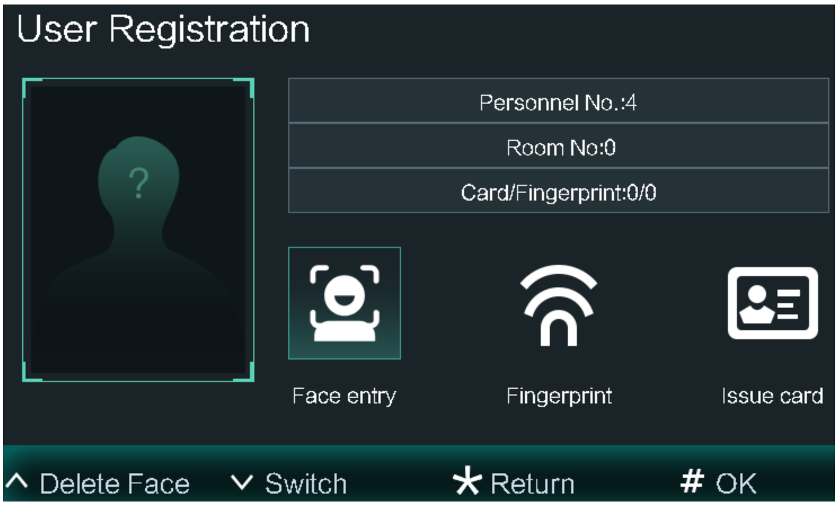
Step 2 On the **Engineering Setting** interface, select **User Registration**.

Step 3 Select **Add**.

Step 4 Enter user ID and Room number.

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 VTO through password.
    - On the web interface of the VTO, select **Household Setting > Room No. Management >** ✎, and then you can set a card as an authorized card.
  - ◇ Issue cards through password.

    📖

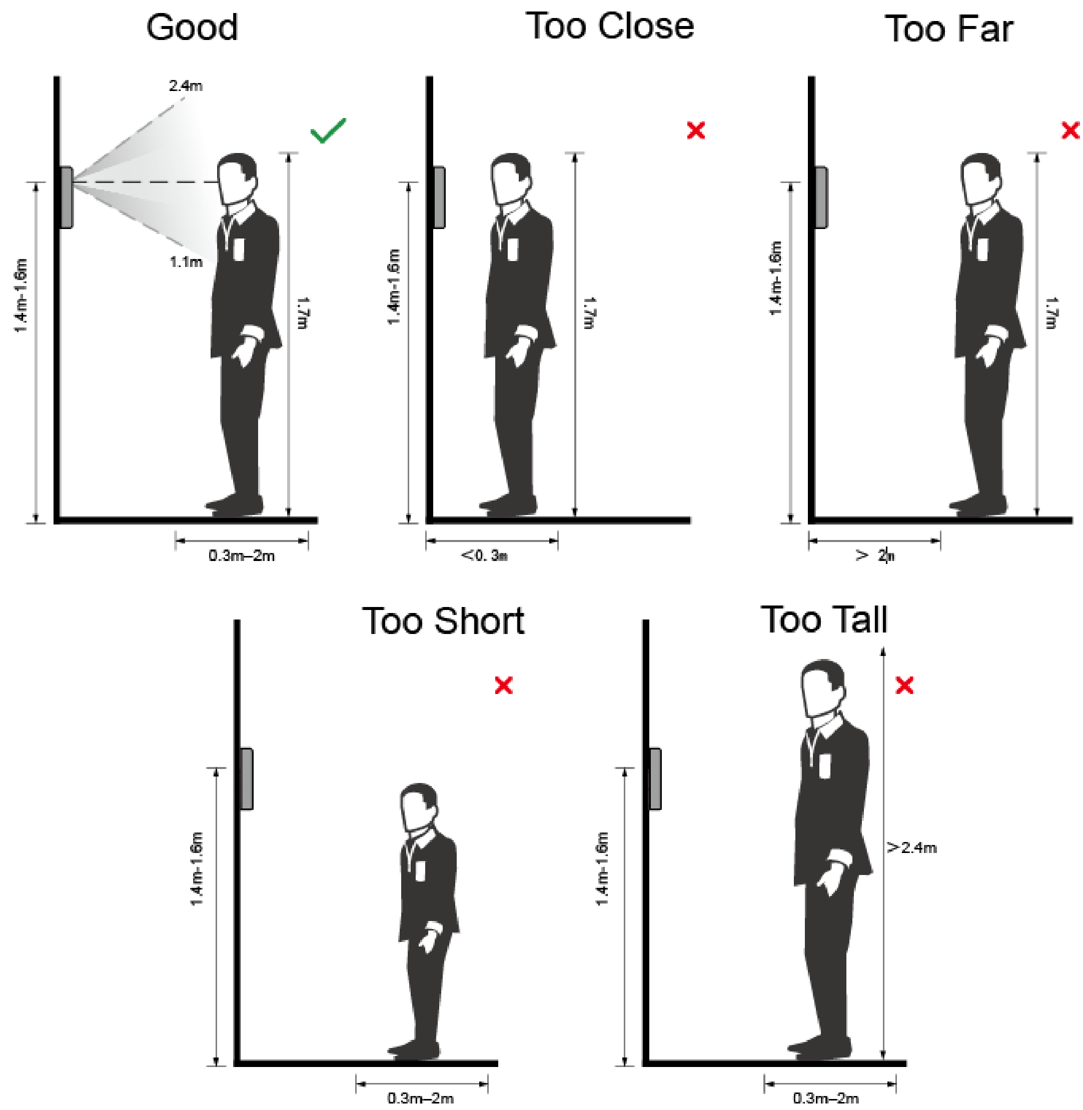
    You need to enter **Issue Card Password** on the web interface of the VTO in **Local Setting > Access Control > Local**.

Appendix 1 Notes of Face Recording

Face Position

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

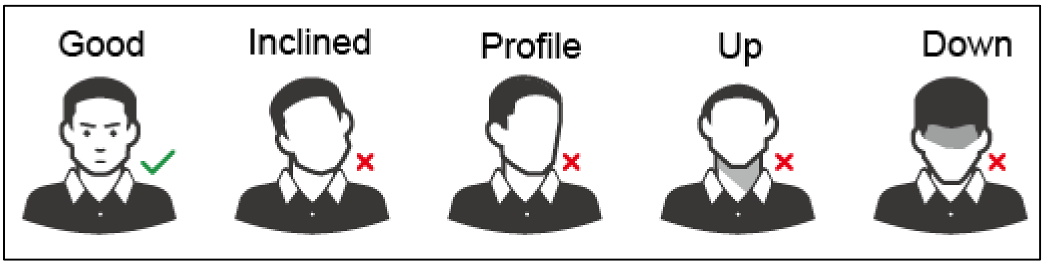
Appendix Figure 1-1 Appropriate face position



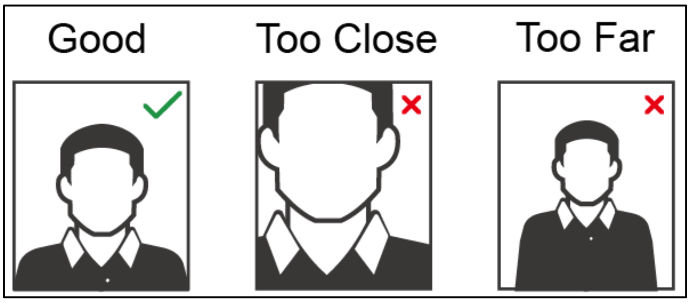
Requirements of Faces

- 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

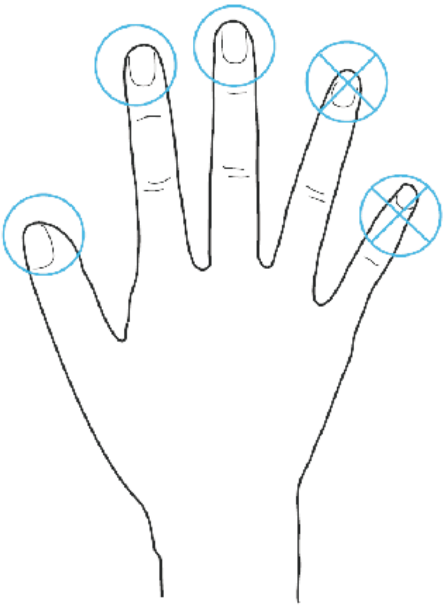
Notice

- 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.

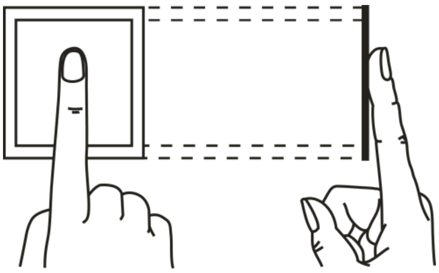
Appendix Figure 1-4 Recommended fingers



Finger Pressing Method

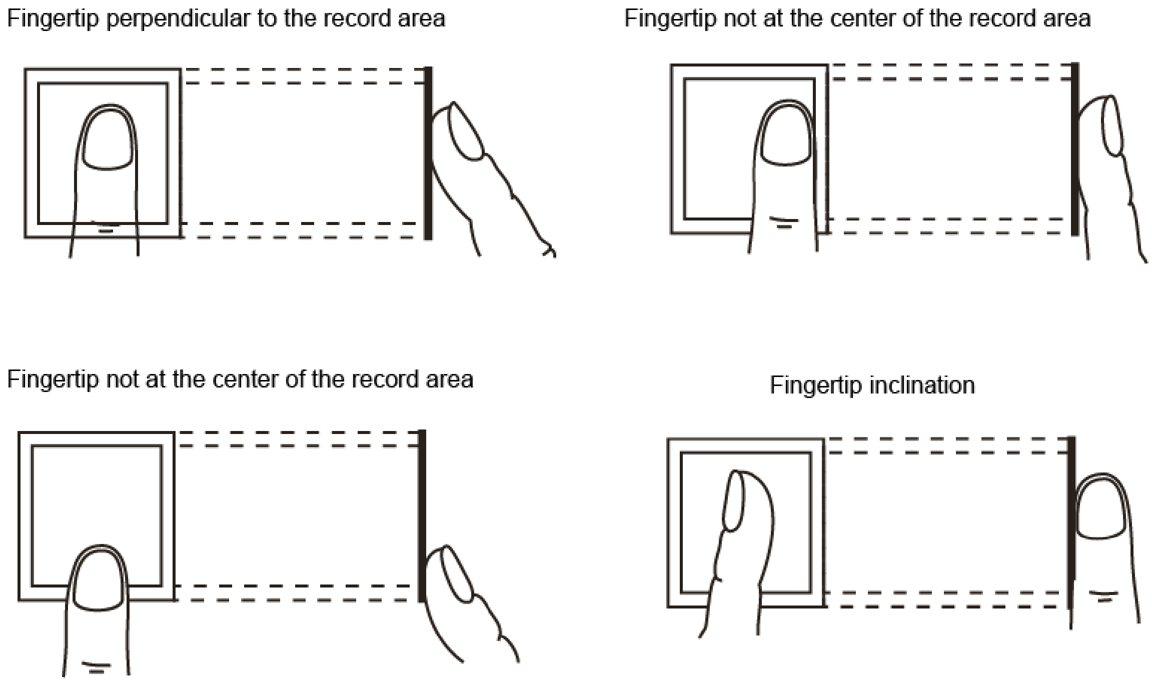
- Correct method

Appendix Figure 1-5 Correct finger pressing



- Incorrect method

Appendix Figure 1-6 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 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.