

Digital Face Recognition Outdoor Station

Quick Start Guide

V1.0.1

Foreword

General

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

Model

VTO7541G and VTO7521G



- VTO7541G: With face unlock, fingerprint unlock, and card unlock function.
- VTO7521G: Only support card unlock.

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
 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	July 2019
V1.0.1	Added waterproof operation in installation	November 2019

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 regions. For detailed information, see 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, please refer to our 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 occurred when using the device.
 - If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The following description is the correct application method of the device. Please read the manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual 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.
- Do not 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, in order to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; don't block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- Transport, use and store the device within allowed humidity and temperature range.

Power Requirement

- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- Please 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, please refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Overview	1
1.1 Introduction	1
1.2 Features	1
2 Appearance	2
3 Connecting Cable	4
4 Installation	5
4.1 Installation Requirement	5
4.1.1 Notice	5
4.1.2 Guidance	5
4.2 Installing VTO	6
4.2.1 Installing on the Wall	6
4.2.2 Installing in the Wall	7
5 Configuration	9
5.1 Configuration Process	9
5.2 VDPCConfig	9
5.3 Configuring VTO	9
5.3.1 Initialization	9
5.3.2 Configuring VTO Number	11
5.3.3 Configuring Network Parameters	11
5.3.4 Selecting SIP Servers	12
5.3.5 Adding VTO Devices	15
5.3.6 Adding Room Number	17
6 Operating VTO	20
6.1 Call Function	20
6.1.1 Calling with Room Number	20
6.1.2 Calling with Contact	20
6.2 Project Mode	20
6.2.1 Entering Project Mode	20
6.2.2 Modifying IP Address	20
6.2.3 User Registration	20
Appendix 1 Notes of Face Recording	22
Appendix 2 Cybersecurity Recommendations	24

1 Overview

1.1 Introduction

This Digital Face Recognition Outdoor Station (hereinafter referred to as "VTO") can be connected to the Indoor Monitor (VTH), video intercom master station (VTS), or third party servers to constitute a video intercom system.

The VTO supports fingerprint unlock, face unlock, and card unlock. Other functions like emergency call, information publishing, and history viewing are also supported.

1.2 Features

- Voice/video calls: Make voice/video calls on the VTO with VTS or VTH users.
- Group call: Call multiple VTH users at one VTO simultaneously.
- Video Surveillance: Monitor areas around the VTO from VTH or management center.
- Emergency call: Press the key to call the Center in case of an emergency.
- Auto snapshot: Snapshot pictures automatically during unlock or call, and store them in FTP.
- Alarm: Support various alarms, including tamper alarm, and door contact alarm. Once alarms are triggered, report will be sent to the management center.
- Unlock: card, fingerprint, face and remote unlock.
- Information publishing: Send messages from VTO to multiple VTH devices.
- History viewing: View call history, alarm history, and unlocking history.

2 Appearance

Figure 2-1 Dimensions (mm [inch])

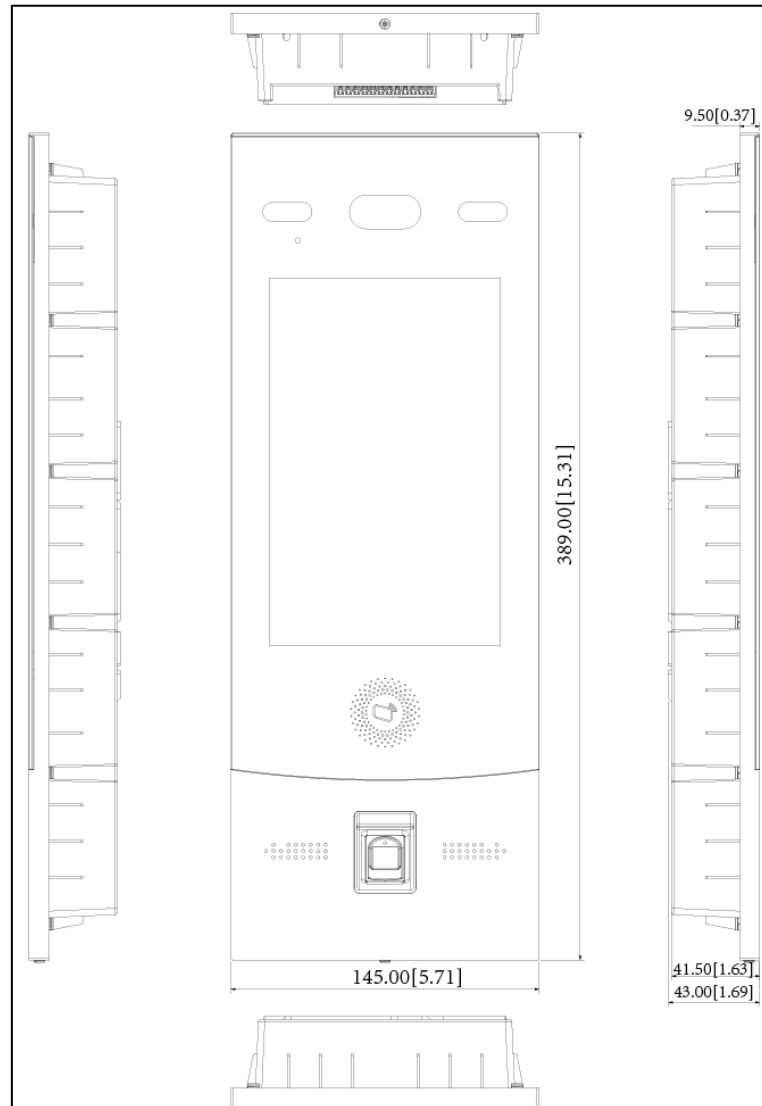


Figure 2-2 Components

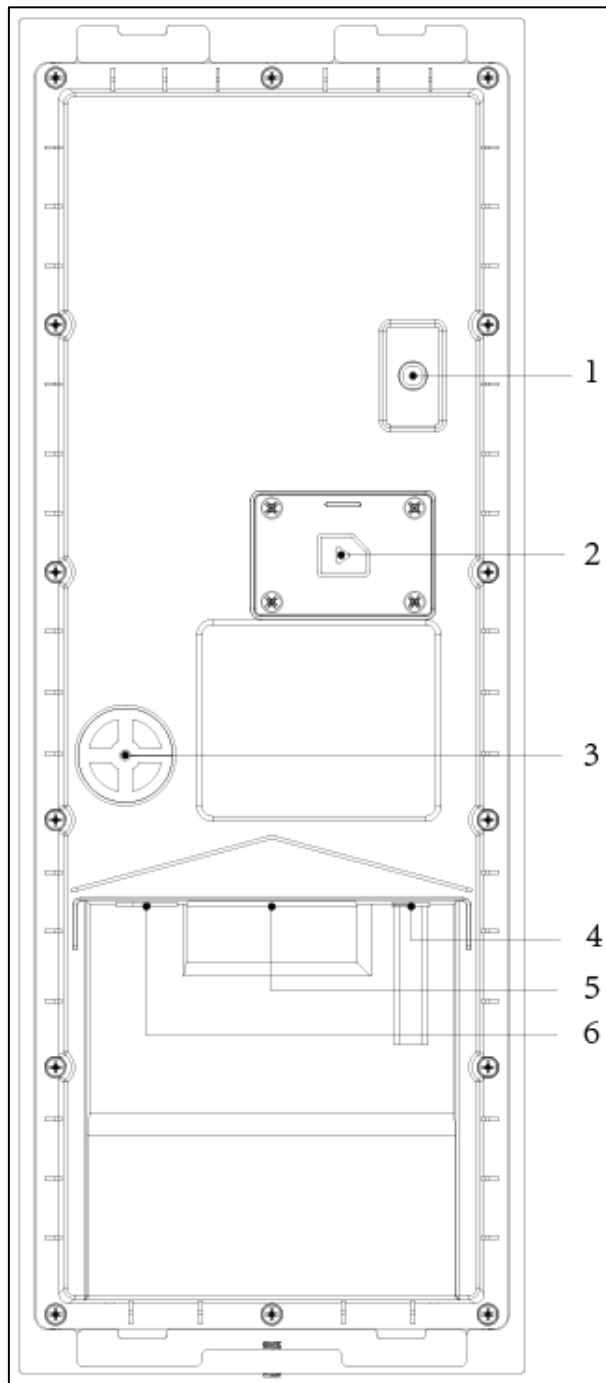


Table 2-1 Component description

No.	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 interface)
6	Ethernet Port

3 Connecting Cable

This port can be used to connect to door locks, and the connection method varies with different locks. For the detailed information, see Figure 3-1, and Figure 3-2.

Figure 3-1 Connecting cables (1)

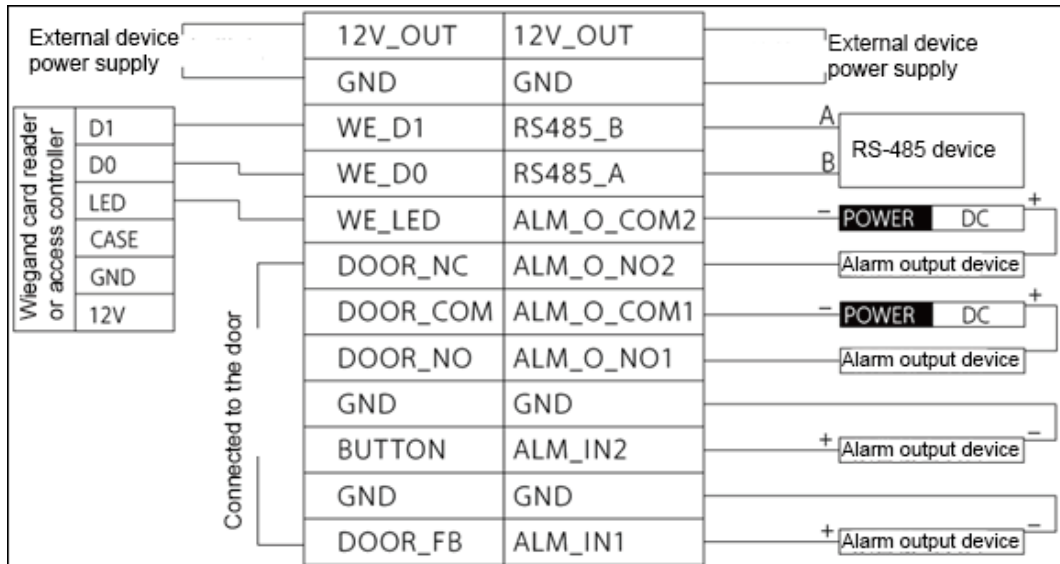
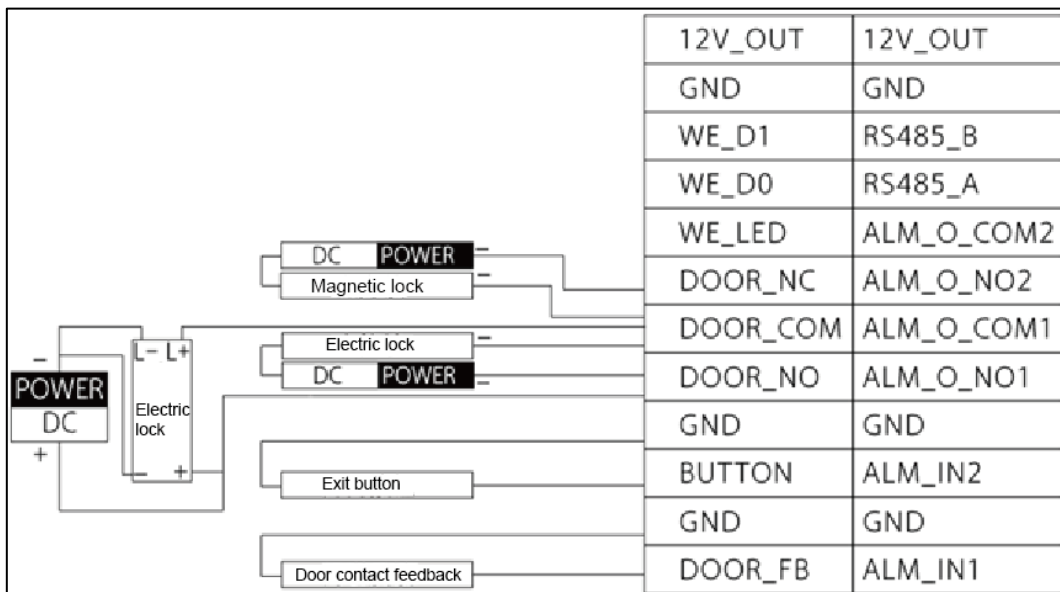


Figure 3-2 Connecting cables (2)



4 Installation

4.1 Installation Requirement

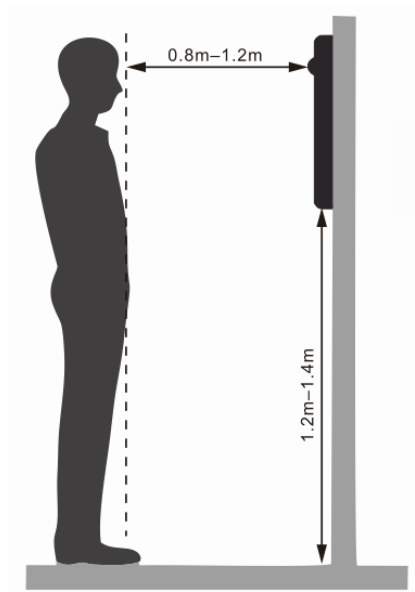
4.1.1 Notice

- Do not install the VTO to places with condensation, high temperature, grease or dust, chemical corrosion, direct sunlight, or zero shelter.
- The installation and adjustment must be finished by professional crew. Do not disassemble the VTO yourself.

4.1.2 Guidance

The VTO horizontal angle of view varies with different models. Try to face the center of the VTO as much as possible. See Figure 4-1 for the installation position.

Figure 4-1 Installation position



4.2 Installing VTO

4.2.1 Installing on the Wall

Figure 4-2 Installing on the wall

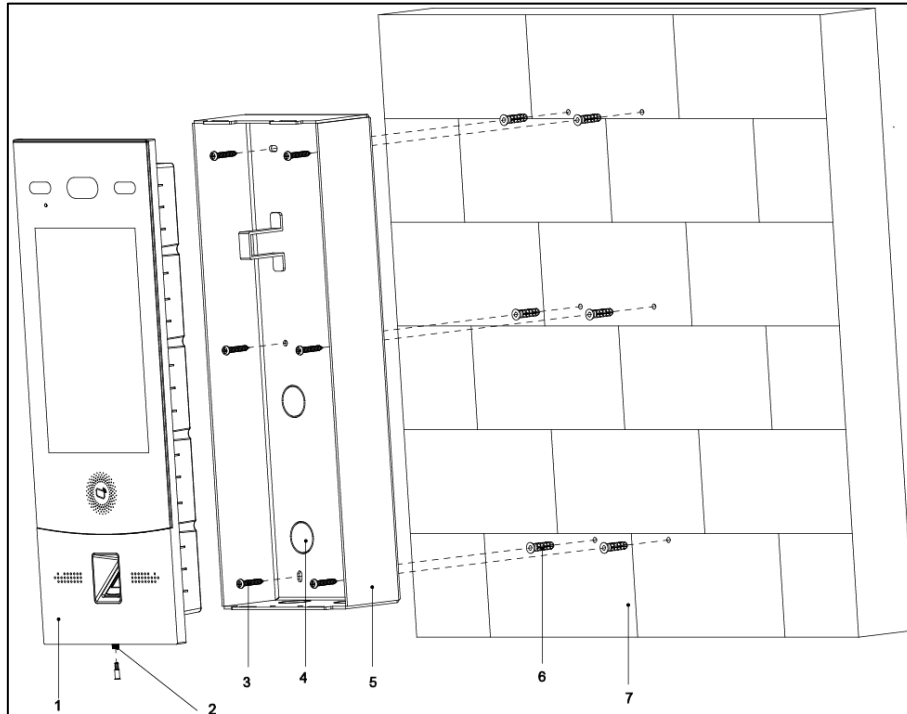


Table 4-1 Item list

No.	Item	No.	Item	No.	Item	No.	Item
1	VTO	2	Locking screw	3	4 × 25 screw	7	Wall
4	Cable entry	5	Mounting box	6	Plastic expansion screw	—	—

Step 1 Drill screw holes on the wall according to screw hole positions on the mounting box, and then put expansion screws in the screw holes.

Step 2 Fix the mounting box on the wall with the ST4.2 × 25 screws.

Step 3 Apply sealant to gaps between the mounting box and wall.

Step 4 Connect cables. See details in "3 Connecting Cable."

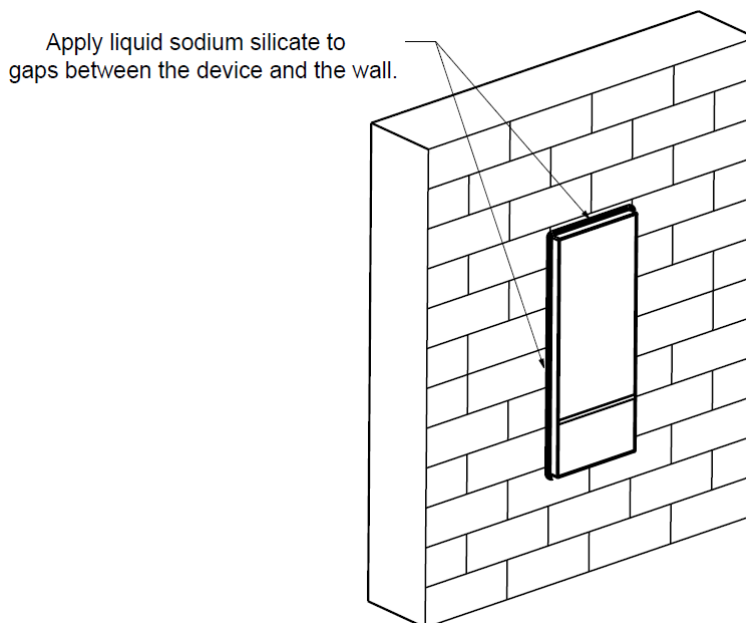
Step 5 Fix the VTO in the mounting box with the M4 × 30 screws.

Step 6 Tighten locking screw at the bottom of the VTO to complete the installation.

Step 7 Apply silica gel to gaps between the device and the wall.

Liquid sodium silicate is recommended.

Figure 4-3 Apply silica gel to gaps



4.2.2 Installing in the Wall

Figure 4-4 Installing in the wall

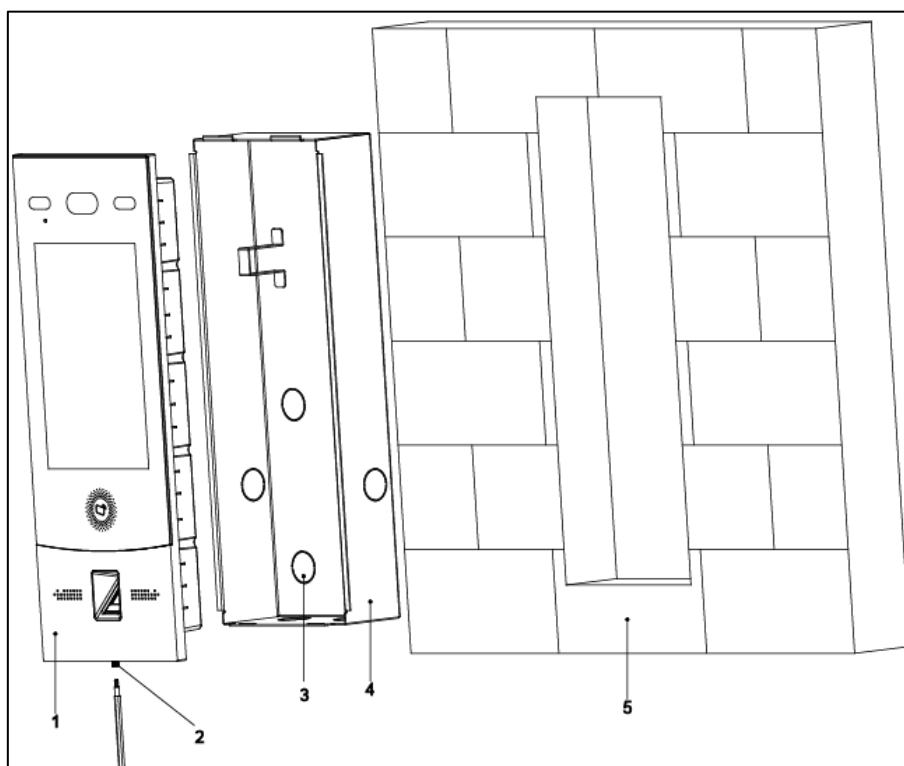


Table 4-2 Item list

No.	Item	No.	Item	No.	Item
1	VTO	2	Locking screw	3	Cable entry
4	Mounting box	5	Wall	-	-

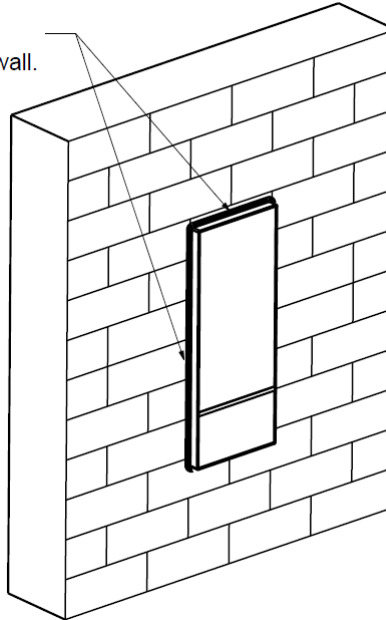
Step 1 Cut an opening with the size of the mounting box on the wall, and then put the mounting box in.

Step 2 Apply sealant to gaps between the mounting box and wall.

- Step 3 Connect cables. See the details in "3 Connecting Cable."
- Step 4 Detach the locking screw at the bottom of the VTO.
- Step 5 Fix the VTO in the mounting box with the M4 x 40 screws.
- Step 6 Tighten locking screw at the bottom of the VTO to complete the installation.
- Step 7 Apply silica gel to gaps between the device and the wall.
Liquid sodium silicate is recommended.

Figure 4-5 Apply silica gel to gaps

Apply liquid sodium silicate to gaps between the device and the wall.



5 Configuration

This chapter introduces how to initialize, connect, and make primary configurations to the VTO and VTH devices to realize basic functions, including device management, calling, and monitoring. For more detailed configuration, see the User's Manual.

5.1 Configuration Process



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

Step 1 Plan IP address for every device, and also plan the unit number and room number you need.

Step 2 Configure VTO. See "5.3 Configuring VTO."

- 1) Initialize VTO. See "5.3.1 Initialization."
- 2) Configure VTO number. See "5.3.2 Configuring VTO Number."
- 3) Configure VTO network parameters. See "5.3.3 Configuring Network Parameters."
- 4) Configure SIP Server. See "5.3.4 Selecting SIP Servers."
- 5) Add VTO devices to the SIP server. See "5.3.5 Adding VTO Devices."
- 6) Add room number to the SIP server. See "5.3.6 Adding Room Number."

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

Step 4 Verify Configuration. See "6 Operating VTO."

5.2 VDPConfig

You can download the "VDPConfig" and do device initialization, IP address modification and system upgrading for multiple devices at the same time. For the detailed information, see the corresponding user's manual.

5.3 Configuring VTO

Connect the VTO to your PC with network cable, and for the first time login, you need to create a new password for the web interface.

5.3.1 Initialization

The default IP address of VTO is 192.168.1.110, and make sure the PC is in the same network segment as the VTO.

Step 1 Connect the VTO to power source, and then boot it up.

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

The **Device Init** interface is displayed. See Figure 5-1.

Figure 5-1 Device initialization

The screenshot shows a dark-themed window titled "Device Init" with a close button in the top right. At the top, there is a progress indicator with three steps: "1 One", "2 Two", and "3 Three". Step 1 is highlighted with a blue circle. Below the progress indicator, the "Username" field is pre-filled with "admin". The "Password" field is empty. Below the password field are three buttons labeled "Low", "Middle", and "High". The "Confirm Password" field is also empty. At the bottom center, there is a "Next" button.

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

The email setting interface is displayed.

Step 4 Select the **email** check box, and then enter your email address. This email address can be used to reset the password.

Step 5 Click **Next**.

The initialization is finished.

Step 6 Click **OK**.

The login interface is displayed. See Figure 5-2.

Figure 5-2 Login interface

The screenshot shows a dark-themed login interface for "WEB SERVICE2.0". At the top, the logo "WEB SERVICE2.0" is displayed in white. Below the logo, there are two input fields: "Username" and "Password". To the right of the "Password" field, there is a link that says "Forget Password?". At the bottom of the interface, there is a large, prominent blue button labeled "Login".

5.3.2 Configuring VTO Number

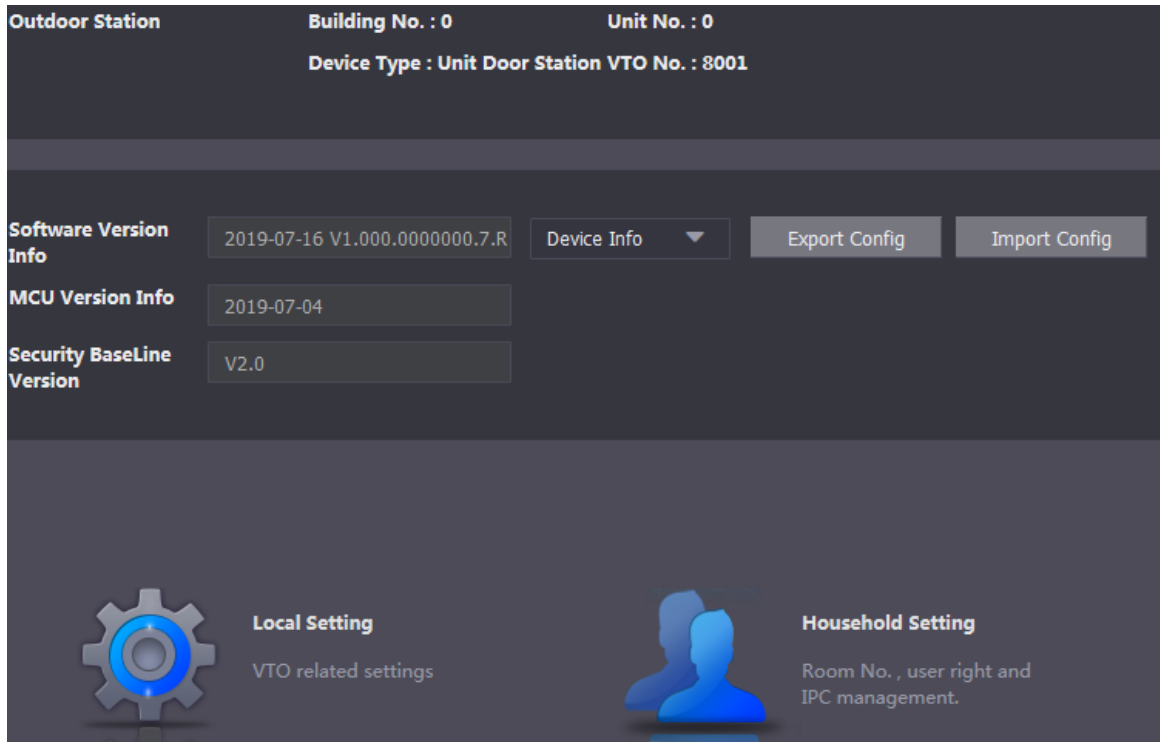
The VTO number can be used to differentiate each VTO, and it is normally configured according to building number.



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

Step 1 Log in to the web interface of the VTO, and then the main interface is displayed. See Figure 5-3.

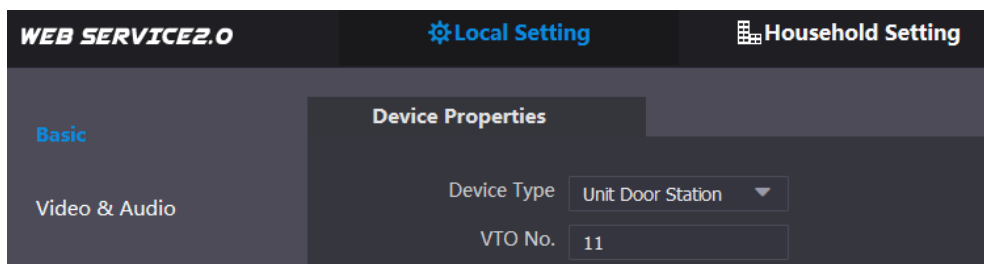
Figure 5-3 Main interface



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

The **Device Properties** interface is displayed. See Figure 5-4.

Figure 5-4 Device properties



Step 3 In the **VTO No.** input box, enter the VTO number you planned for this VTO, and then click **Confirm** to save.

5.3.3 Configuring Network Parameters

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

The TCP/IP information is displayed. See Figure 5-5.

Figure 5-5 TCP/IP information



Step 2 Enter network parameters you planned, and then click **Save**.
The VTO will restart.



Make IP address of your PC and VTO IP are in the same network segment.

5.3.4 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 provides information or direction to a user agent.

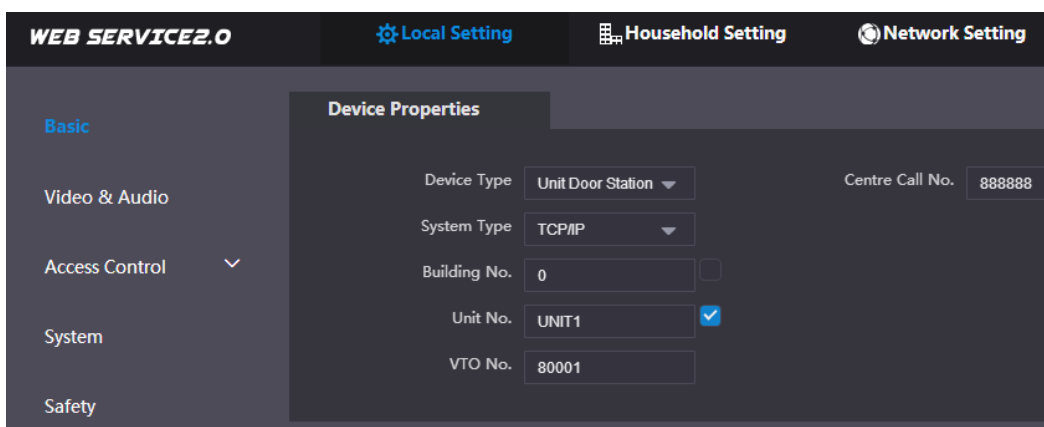
- When this VTO or another VTO works as SIP server, select **VTO** from the **Server Type** drop-down list. It applies to a scenario where there is only one building.
- When the platform (Express/DSS) works as SIP server, select **Express/DSS** from the **Server Type** drop-down list. It applies to a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

Step 1 Log in to the web page.

Step 2 On the homepage, select **Local Setting > Basic**.

The **Device Properties** interface is displayed. See Figure 5-6.

Figure 5-6 Device properties



- 1) Select **TCP/IP** from the **System Type** drop-down list.



Default system type is analogue system and shall be changed to TCP/IP. Otherwise, it will fail to connect VTH.

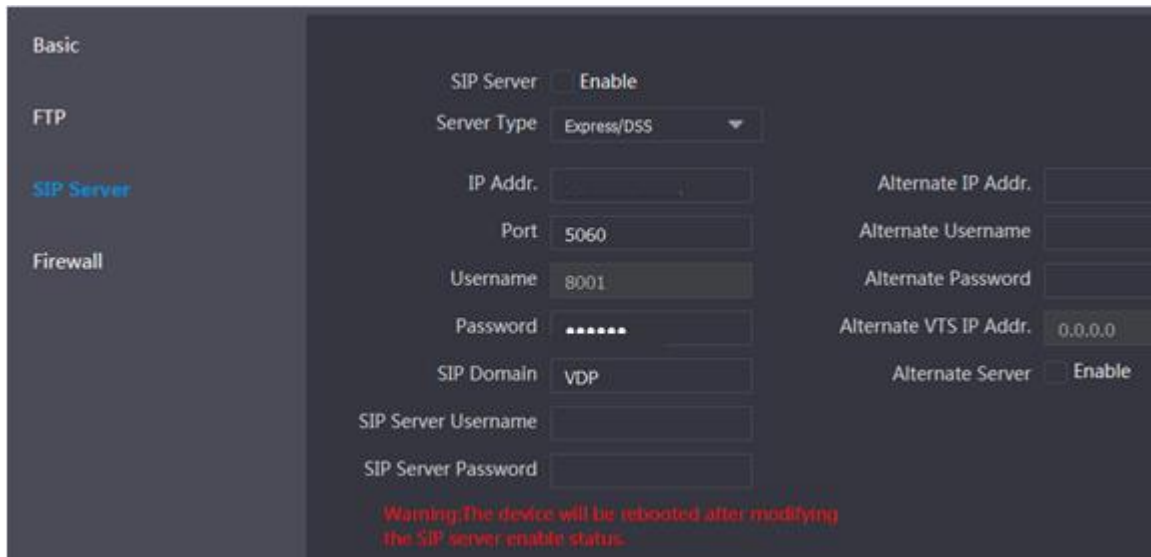
- 2) Click **OK** to save the settings.
- 3) Restart the device manually, or wait for auto restart to make the settings effective.

Step 3 Log in web interface again.

Step 4 Select **Network Setting > SIP Server**.

The **SIP Server** interface is displayed. See Figure 5-7.

Figure 5-7 SIP server (1)



Step 5 Select a SIP server.

VTO as SIP server

- Step 1 Select **Enable** behind **SIP Server**.
- Step 2 Select **VTO** from the **Server Type** drop-down list
- Step 3 Configure parameters (see Table 5-1 for details).
- Step 4 Click **Save**.
The VTO will restart automatically.

Platform (Express/DSS) as a SIP server

- Step 1 Select **Network Setting > SIP Server**.
The **SIP Server** interface is displayed. See Figure 5-8.

Figure 5-8 SIP server (2)

The screenshot displays the configuration page for the SIP server. On the left, a sidebar contains menu items: Basic, FTP, SIP Server (highlighted in blue), and Firewall. The main content area is titled 'SIP Server' and features a toggle switch for 'SIP Server' set to 'Enable'. Below this is a 'Server Type' dropdown menu currently showing 'Express/DSS'. The configuration fields are arranged in two columns:


- IP Addr. (empty text box)
- Port: 5060
- Username: 8001
- Password: masked with seven dots
- SIP Domain: VDP
- SIP Server Username (empty text box)
- SIP Server Password (empty text box)
- Alternate IP Addr. (empty text box)
- Alternate Username (empty text box)
- Alternate Password (empty text box)
- Alternate VTS IP Addr.: 0.0.0.0
- Alternate Server: Enable (checked)

A red warning message at the bottom of the configuration area reads: "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 5-1.

Table 5-1 SIP server parameter description

Parameter	Description
IP Address	IP address of SIP server.
Port	<ul style="list-style-type: none"> It is 5060 by default when another VTO works as SIP server. It is 5080 by default when the platform works as SIP server.
Username/Password	Use default value.
SIP Domain	<ul style="list-style-type: none"> It shall be VDP when another VTO 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.  If alternate server is enabled and Express or DSS works as SIP server, when Express or DSS cannot work normally, the VTO will be used as SIP server.
Alternate Username	Username and password for logging in 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 **OK** to save the configuration.

The VTO will restart automatically.



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

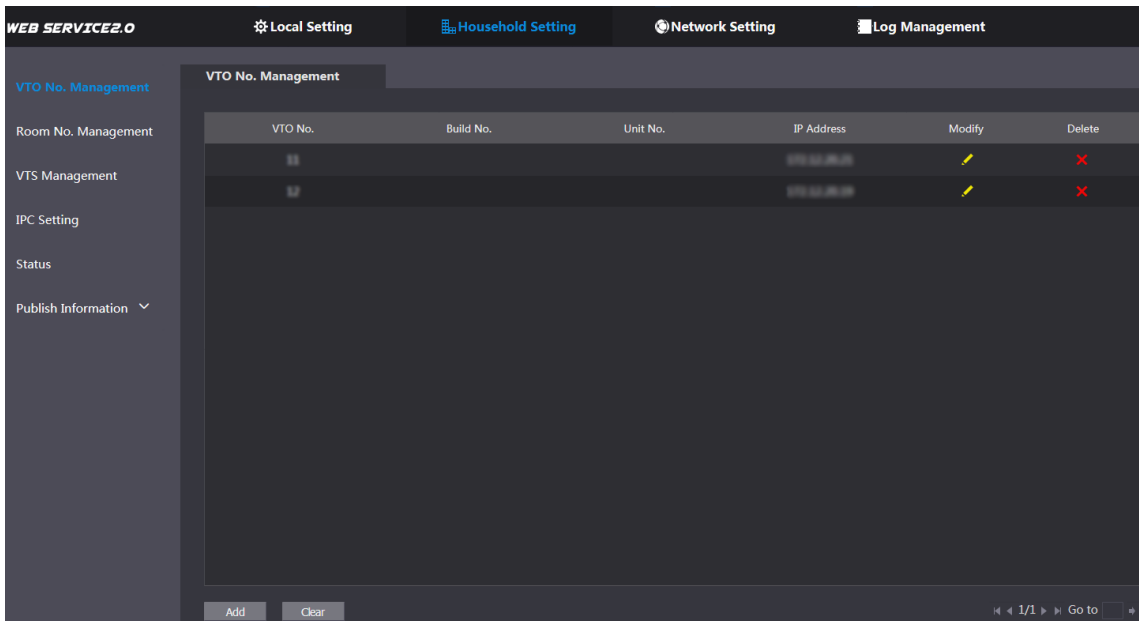
5.3.5 Adding VTO Devices

You need to add VTO to the SIP server, and all intercoms connected to the same SIP server can make video calls among each other. This section applies to the condition in which a VTO works as SIP server, and if you are using other servers as SIP server, see the corresponding manual for the detailed configuration.

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

The **VTO No. Management** interface is displayed. See Figure 5-9.

Figure 5-9 VTO No. management



Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 5-10.

Figure 5-10 Add VTO

Step 3 Configure the parameters, and be sure to add the SIP server itself too. See Table 5-2.

Table 5-2 Add VTO configuration

Parameter	Description
Rec No.	The VTO number you configured for the target VTO. See the details in "5.3.2 Configuring VTO Number."
Register Password	Keep default value.
Build No.	Available only when other servers work as SIP server.
Unit No.	
IP Address	IP address of the target VTO.
Username	The user name and password for the web interface of the target VTO.
Password	

Step 4 Click **Save**.

5.3.6 Adding Room Number

You can add the planned room number to the SIP server, and then configure the room number on VTH devices to connect them to the network. VTO works as SIP server will be taken as an example, and if you use other servers as SIP server, see the corresponding manual for the details.

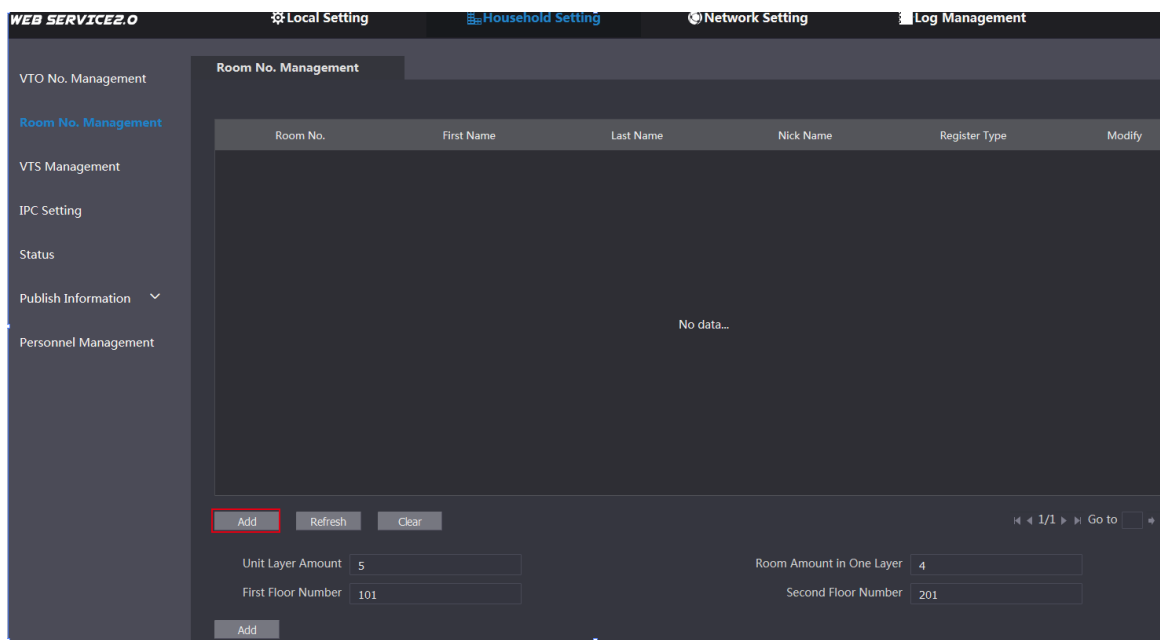


The room number contains 6 digits of numbers or letters or their combination at most, and it cannot be the same as any other VTO numbers.

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

The **Room No. Management** interface is displayed. See Figure 5-11.

Figure 5-11 Room No. management




Step 2 You can add single room number or do it in batch.

- Add single room number
- 1) Click **Add**. See Figure 5-11.
The **Add** interface is displayed. See Figure 5-12.

Figure 5-12 Add single room number

2) Configure room information. See Table 5-3.

Table 5-3 Room information

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	
Nick Name	
Room No.	<p>The room number you planned.</p>  <ul style="list-style-type: none"> If you use multiple VTH devices, the room number of the master VTH should be "room number#0", and the room number of the extension VTH should be "room number#1", "room number#2", and so on. You can have 10 extension VTH devices at most for one master VTH.
Register Type	Select public , and local is reserved for future use.
Register Password	Keep the default value.

3) Click **Save**.

The added room number is displayed. Click  to modify room information, and click

 to delete a room.

- Add room number in batch
- Configure the Unit Layer Amount, Room Amount in One Layer, First Floor Number, and Second Floor Number according to the actual condition.
 - Click **Add** at the bottom left of the interface. See Figure 5-13.

Figure 5-13 Add in batch


The screenshot shows a dark-themed web interface for batch adding room numbers. At the top, there are three buttons: 'Add', 'Refresh', and 'Clear'. To the right, there is a pagination control showing '1/1' and a 'Go to' field. Below these are four input fields arranged in a 2x2 grid: 'Unit Layer Amount' with the value '30', 'Room Amount in One Layer' with the value '4', 'First Floor Number' with the value '101', and 'Second Floor Number' with the value '201'. At the bottom left, there is an 'Add' button highlighted with a red rectangular box.

All the added room numbers are displayed. Click **Refresh** to view the latest status, and click **Clear** to delete all the room numbers.

6 Operating VTO

6.1 Call Function

6.1.1 Calling with Room Number

- Step 1 On standby mode, Tap .
The call interface is displayed.
- Step 2 Enter room number, and then tap **Call**.
You will hear the voice message "Calling now, please wait a moment."
- Step 3 During phone call, tap **Hangup** to end the call.

6.1.2 Calling with Contact

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

- Step 1 On standby mode, tap **PhoneBook** to view contact.
- Step 2 Select a contact you need to call, and then tap **Call**.

6.2 Project Mode

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

6.2.1 Entering Project Mode

On the standby interface, tap **Call** and then enter "*+project password+#", and then you can go to the project mode. The default project password is 888888, and you can modify it on the VTO or in the VTO web interface.


6.2.2 Modifying IP Address

- Step 1 In the project mode, select **IP Config**.
- Step 2 Enter the planned IP address.
- Step 3 Tap **OK** to save the new IP, or tap **Cancel** to cancel the modification.

6.2.3 User Registration

Only registered users can unlock doors, so you need to register users.

- Step 1 On the Project Mode interface, select **User Registration**.
The **User Registration** interface is displayed.

Step 2 Tap .

The enter user information interface is displayed

Step 3 Enter Personnel No. Room No., and User Name.

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

Step 5 Tap  to take a photo of the user.

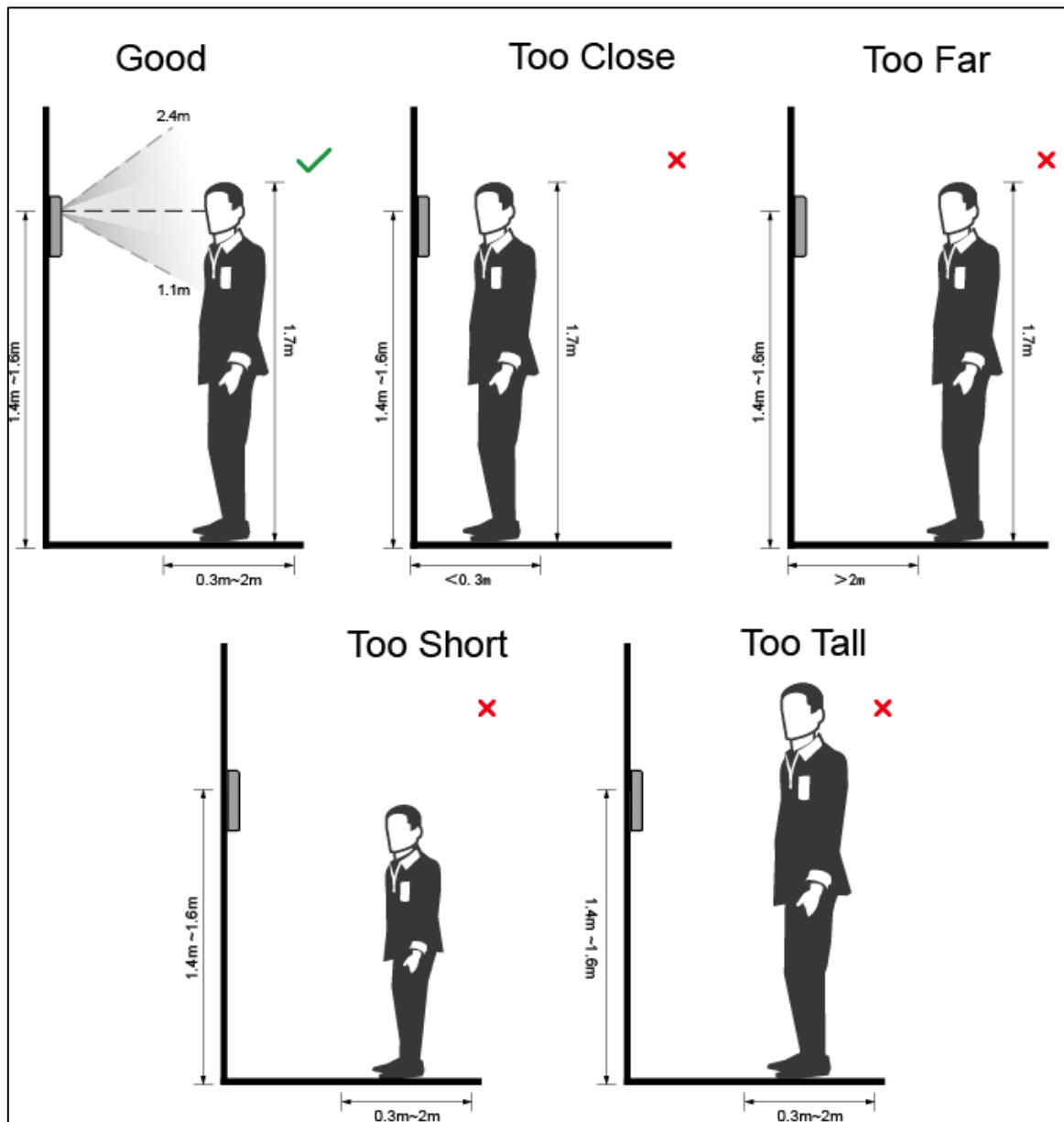
Step 6 Tap **OK** to save the photo, and the interface goes to the **User Registration** interface; or tap **Cancel** to take a new photo.

Appendix 1 Notes of Face Recording

Face Position

If faces are not at the appropriate position, face recognition effect might be influenced.

Appendix figure 1-1 Appropriate face position



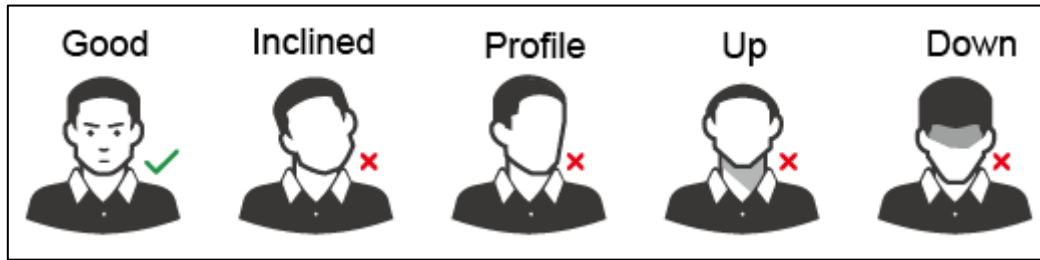
Requirements of Faces

- 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

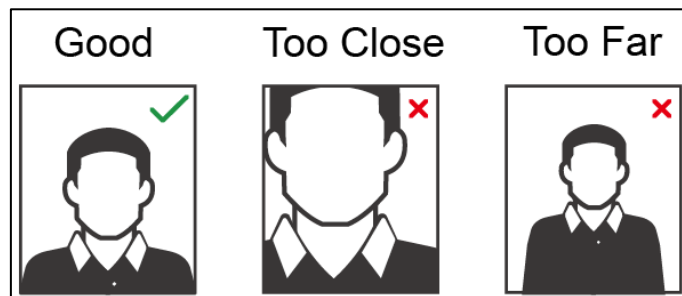
camera.

- 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 resolution is within the range 150×300–600×1200; image pixel is more than 500×500; image size is less than 100KB, and image name and person ID are the same.
- Make sure that face does not take 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

Appendix 2 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.