

VTO3211D-P Guide Start Guide

V1.0.1

Table of Contents

Table of Contents	2
Cybersecurity Statement and Recommendations	4
Cybersecurity Statement	4
Cybersecurity Recommendations	4
1 Product Overview	1
1.1 Product Feature	1
1.2 Networking	1
2 Structure	2
2.1 Front Panel	2
2.2 Rear Panel	3
3 Install and Debug	5
3.1 Device Wiring	5
3.2 Installation	5
3.2.1 Screw Specification	5
3.2.2 Installation Dimension	6
3.2.3 Installation Step	7
3.3 Debugging	9
3.3.1 Before Debugging	9
3.3.2 VTO Setup	9
3.3.3 Indoor Manager	10
4 Operation	13
5 Cell Phone Settings	1
5.1 Set Cell Phone	1
5.2 Check Results	3
6 Electric Lock and Magnetic Door Lock	4
6.1 Electric Door Lock	4
6.2 Magnetic Door Lock	4

Appendix 1 Technical Specifications 5.

Cybersecurity Statement and Recommendations

Cybersecurity Statement

- You are responsible for the risks resulting from connecting your product to the internet, including but not limited to, cyber-attacks, hacking attacks, computer viruses and malware, etc. Please protect your data and personal information by taking necessary actions, such as changing the default password and using a strong combination, changing your password periodically, keeping your firmware up-to-date, etc. Dahua is not responsible for any dysfunction, information leakage or other problems caused by failure to take necessary precautions to secure your devices. We will provide product maintenance services.
- To the extent not prohibited by applicable laws, Dahua and its employees, licensees, and affiliates are not liable for personal injury, or any incidental, special, indirect, or consequential damages whatsoever, including, without limitation, damages for loss of profits, corruption or loss of data, failure to transmit or receive any data, business interruption, or any other commercial damages or losses arising out of or related to the use or inability to use its products or services, however caused, regardless of the theory of liability (contract, tort or otherwise), even if it has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of liability for personal injury, or of incidental or consequential damages, so this limitation may not apply to you.
- In no event shall liability for all damages (other than as may be required by applicable laws in cases involving personal injury) exceed the amount paid for products or services.

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. Dahua recommends changing default passwords immediately and choosing a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security

patches and fixes.

Check the firmware release of your running devices. If the firmware release date is over 18 months old, please contact a Dahua authorized local distributor or Dahua technical support for available update releases.

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for Dahua systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

For latest information about Dahua the cybersecurity statement and recommendations, please visit www.dahuasecurity.com.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others' such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

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 User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's 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 Guide (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.

1 Product Overview

1.1 Product Feature

Metal VTO has simple operation, easy installation with the following functions:

- Mobile phone live preview.
- Call and intercom with VTH.
- Unlock door by card.
- Vandal-proof alarm.

1.2 Networking

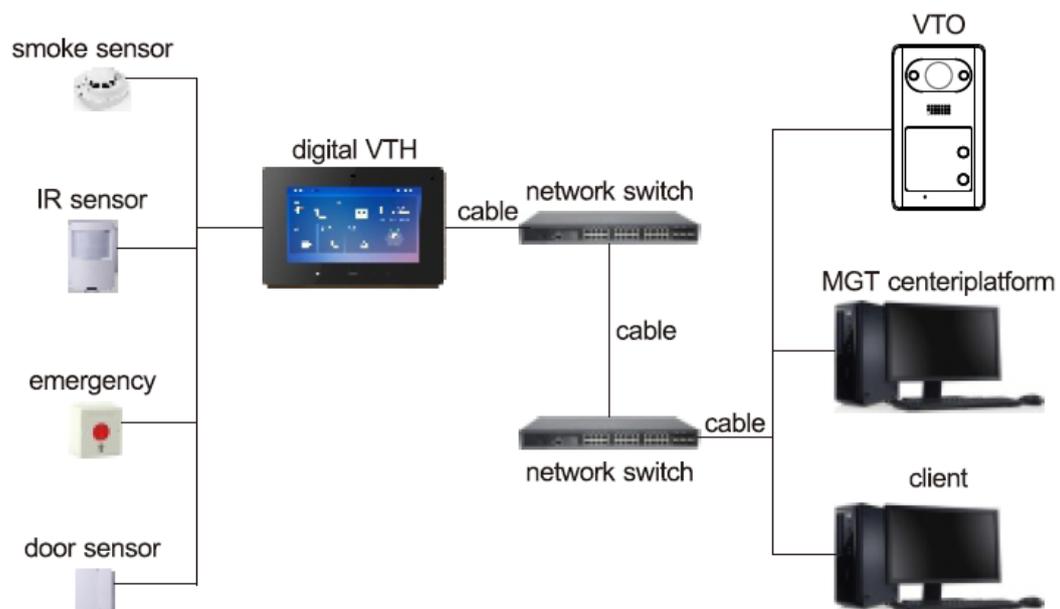


Figure 1-1

2 Structure

2.1 Front Panel

Number of buttons on front panel varies depending on model. For example, VTO3211D-P2 has two buttons; VTO3211D-P4 has four buttons. The following makes VTO3211D-P2 as an example.

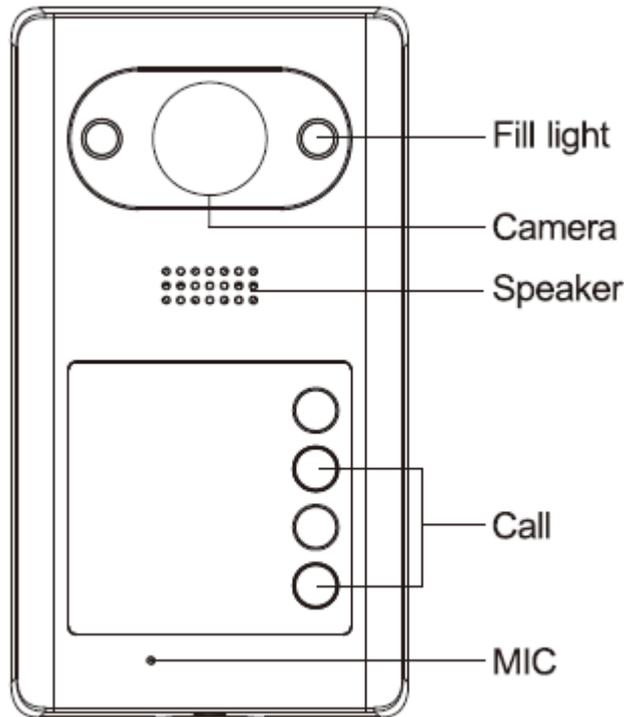


Figure 2-1

Component Name	Description
IR Fill Light	Provide IR light when environment is dark.
Camera	Monitor VTO area.
Speaker	Output sound.
Call Button	Start call. Note: VTO3211D-P4 model has 4 call buttons. Two buttons are not marked, so they are invalid.
MIC	Audio input.

Chart 2-1

2.2 Rear Panel

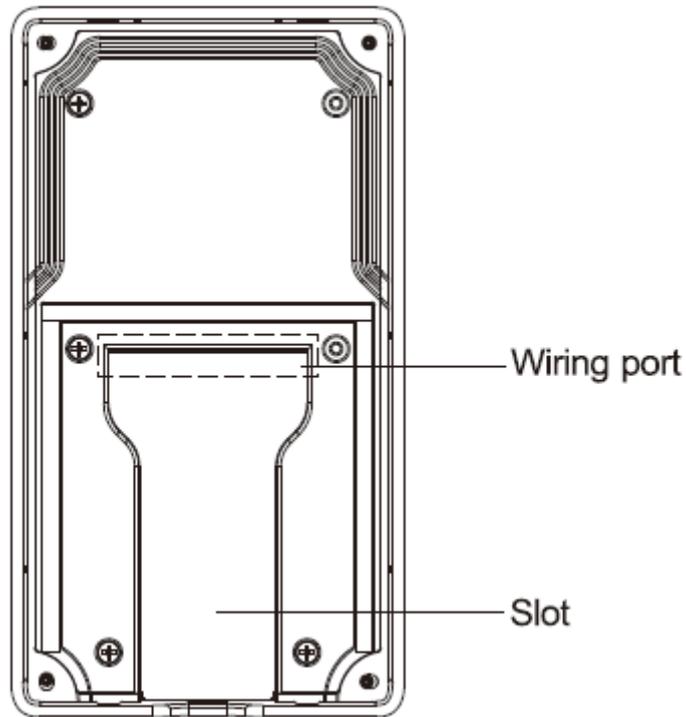


Figure 1- 1

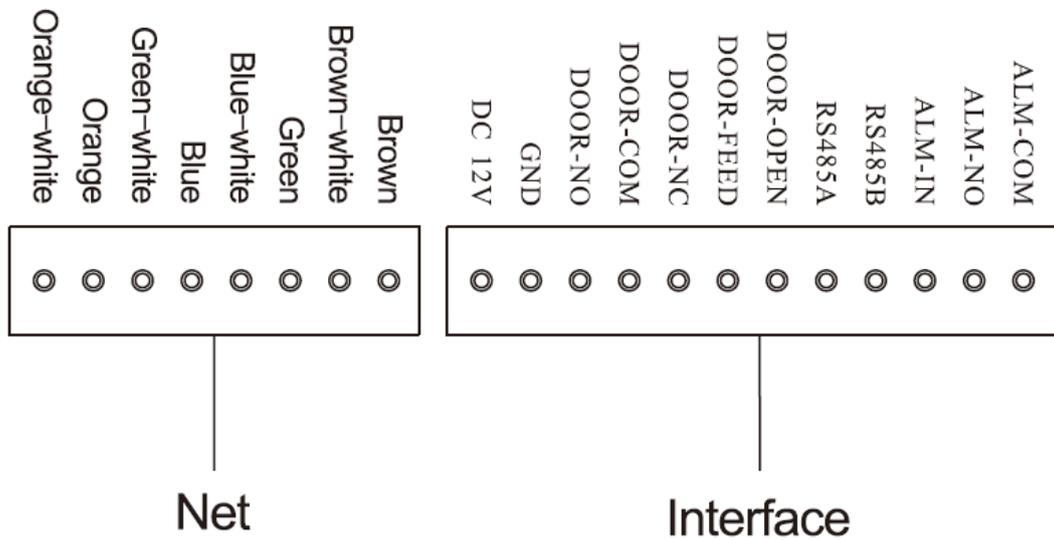


Figure 2-2

Label	Note
DC12V	DC12V power port
GND	Ground
DOOR-NO	Door lock NO port
DOOR-COM	Lock public port

Label	Note
DOOR-NC	Lock NC port
DOOR-FEED	Lock door sensor feedback
DOOR-OPEN	Door lock unlock button
RS485A	RS485 communication
RS485B	
ALM-IN	Alarm input
ALM-NO	Alarm output
ALM-COM	

Chart 2-2

3 Install and Debug

3.1 Device Wiring

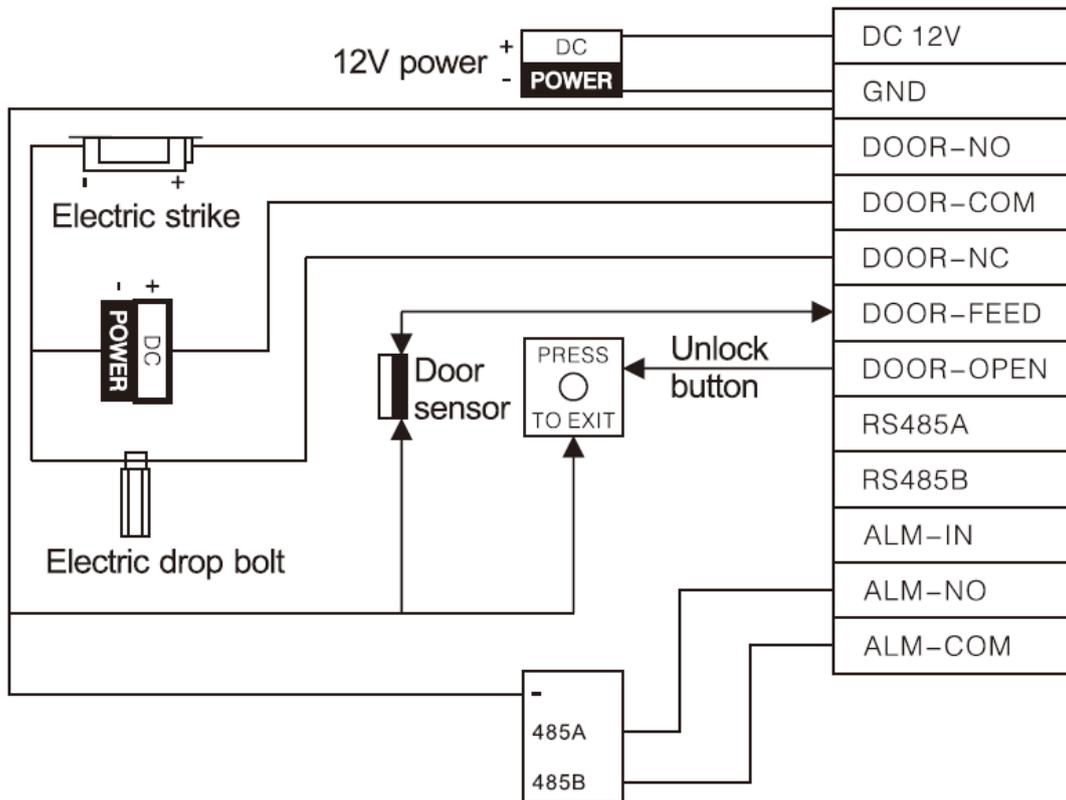


Figure 3-1

3.2 Installation

Warning

- Avoid installation in poor environment, such as condensation, high temperature, oil, dust and etc.
- Installation and debugging of the device must be done by professionals. DO NOT disassemble the device by yourself.

3.2.1 Screw Specification

Component Name	Figure	Quantity
White expansion bolt Φ6×30mm		4
ST3×20 self-tapping screw		4
M3×6 mechanic screw		1

Chart 3-1

3.2.2 Installation Dimension

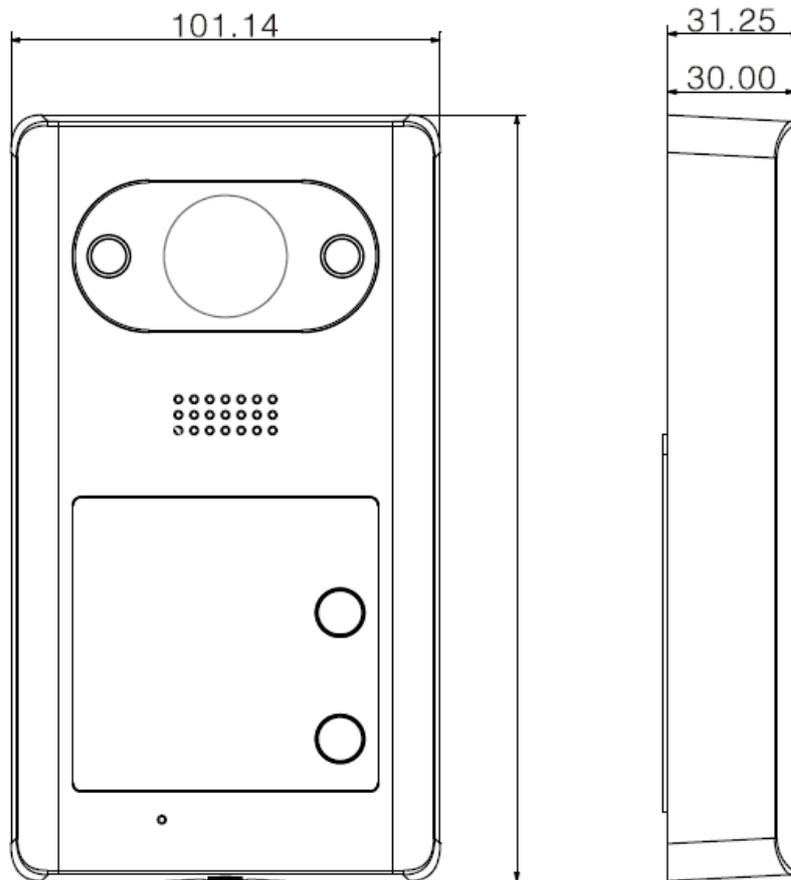


Figure 3-2

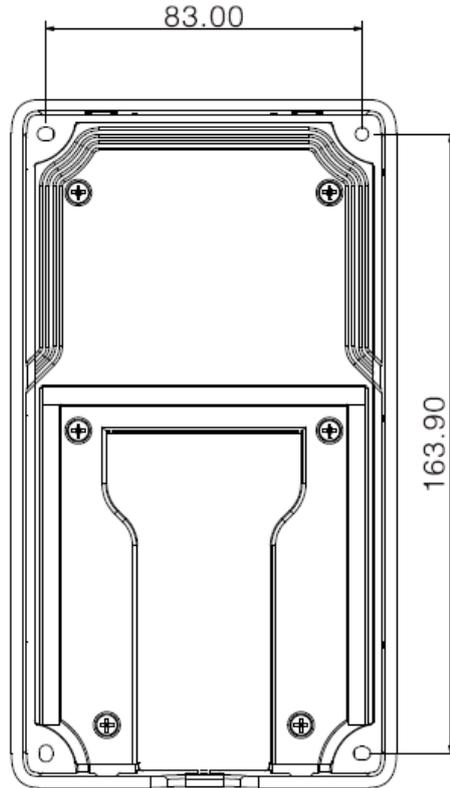


Figure 3-3

3.2.3 Installation Step

Before installation, unfasten the M3*6 mechanic screw at bottom of device, take down metal case, see Figure 3-4.

Step 1. According to the four hole positions on device internal case, dig holes on the installation surface (i.e. wall).

Step 2. Insert expansion bolt into the hole.

Step 3. Fix the 4 self-tapping screws in device internal case at fixed position.

Step 4. Lock the external metal case from top to bottom on internal case.

Step 5. Buckle external metal case to device internal case from bottom.

Step 6. Fasten external metal case and device internal case with M3*6 mechanic screw.

Note:

The recommended distance from device center to ground is 1.4m-1.6m.

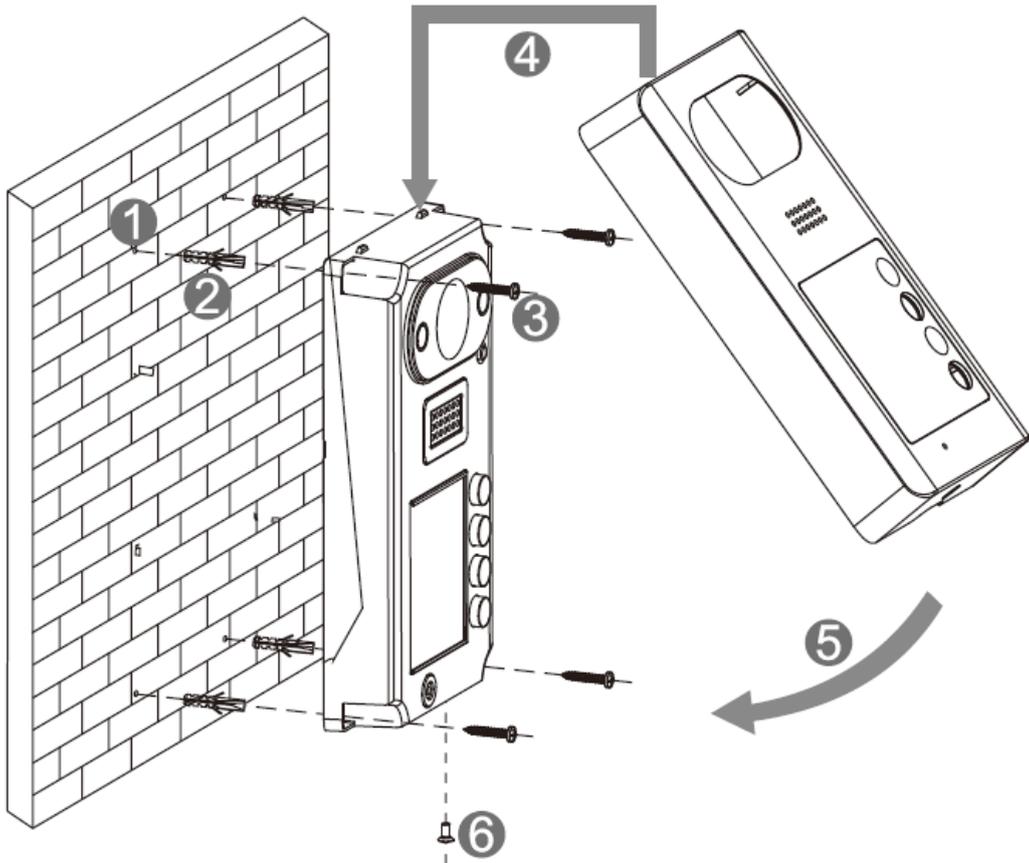


Figure 3-4

After installation, you can see Figure 3-5.

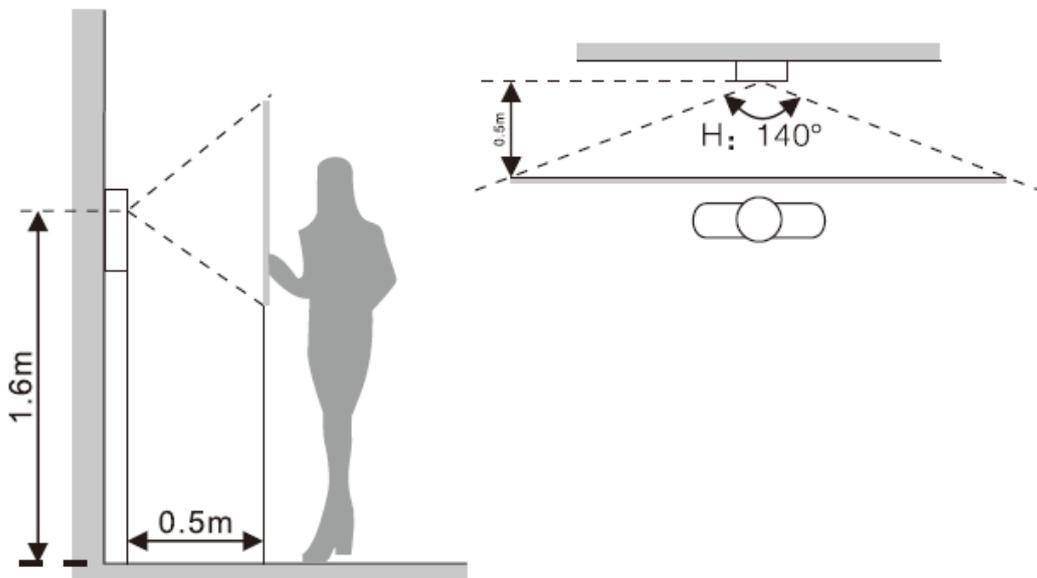


Figure 3-5

3.3 Debugging

3.3.1 Before Debugging

The following makes VTH5221D and 7 inch VTH pairing for debugging.

- Before debugging, the staff shall be familiar with device's installation, wiring and usage.
- Before debugging, check wiring for short or open circuit.
- Ensure VTH can work normally.

3.3.2 VTO Setup

VTO default IP address of 192.168.1.110. Before you use VTO, you must change IP address to a IP address in the same segment with VTH.

Step 1. Plug VTO to power.

Step 2. In the field of address in browser, enter device default IP address (192.168.1.110).

See Figure 3-6.



Figure 3-6

Step 3. Enter username and password, click Login.

Note:

Default username and password are admin and admin. After you log in for the first time, please change password ASAP. Refer to Ch 4.2.6.3.

Step 4. System Config>Network Config>TCP/IP. See Figure 3-7. Modify VTO IP address to be planned IP address. See Ch 4.2.4.1.

After modification is complete, WEB page reboots, and go to new IP address for login.

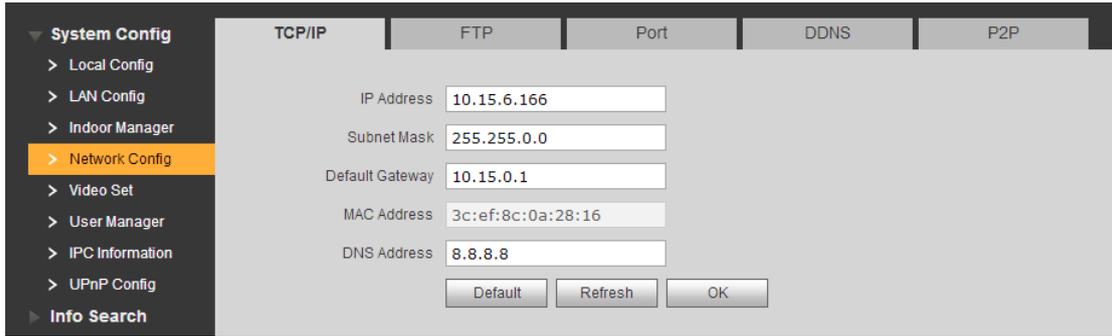


Figure 3-7

Step 5. Select System Config>Indoor Manager>Indoor Manager. See Figure 3-8. Click Add to add VTH info.



Figure 3-8

Step 6. Click System Config>Local Config>Facase Layout, click white area on the left, and select VTH room no., see Figure 3-9.



Figure 3-9

3.3.3 Indoor Manager

- Step 1. In VTH homepage, long press Setup for 6 seconds.
- Step 2. Enter password in VTH project setup interface.
- Step 3. Click Network Setup to connect VTH network. See



Figure 3-10

1. Enter Local IP, subnet mask and gateway of VTH.
2. Click OK.

Now you can see  at the upper right corner in the homepage, which means connection is successful.

Note:

You also can enable DHCP to auto get VTH IP, subnet mask and gateway, click OK.

Step 4. Click Local Info to set VTH room no.

See Figure 3-11.

Note:

VTH room no. Must match VTH short no. Set in VTO WEB, refer to Ch 4.2.3.

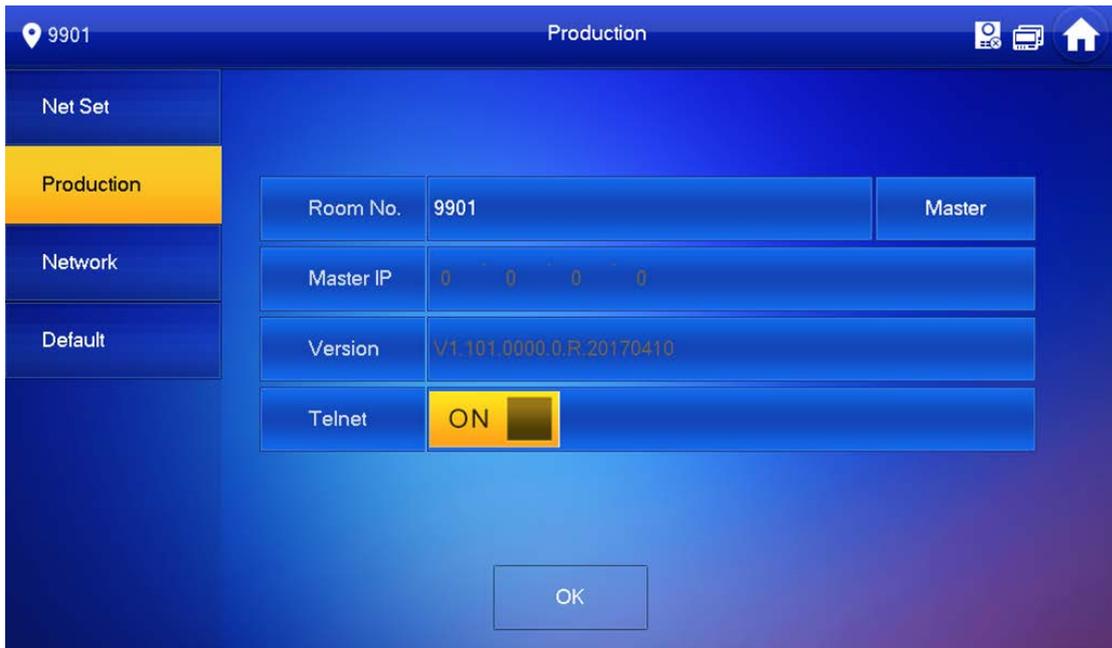


Figure 3-11

- If you set this VTH to be main VTH, select host. Fill in room no., click OK to save. See Figure 3-11.
- If you set this VTH to be extension, select extension. Fill in extension room no., and host IP. Click OK to save.

Step 5. Click Network, to set VTO info. See Figure 3-12.

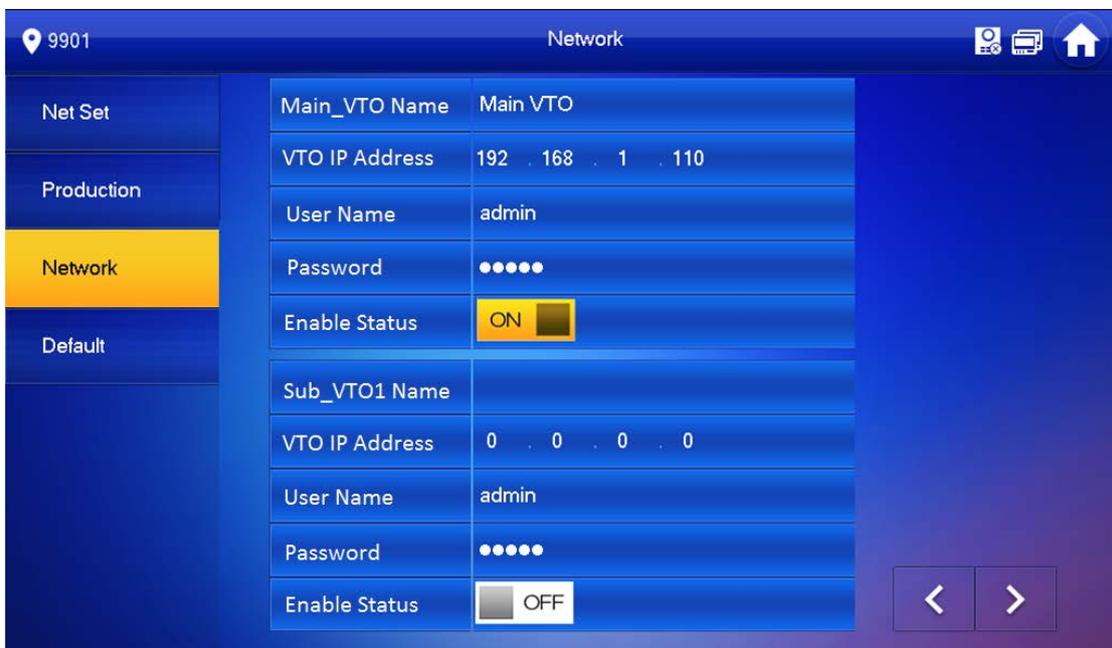


Figure 3-12

1. Enter VTO name and IP address, to set it to host/extension.
2. Set status to ON.

4 Operation

Note:

Please refer to use's manual of this product.

On VTO, click button to bind VTH, call this VTH. VTH pops up monitoring video and button, see Figure 4-1. Now debugging is successful.



Figure 4-1

5 Cell Phone Settings

5.1 Set Cell Phone

- a) Download the APP for your cell phone. Use the cell phone to scan the QR code. See Figure 5-1.



Figure 5-1

On the VTO's web> Indoor Manager, each VTH provides one QR code which allow user to connect to mobile phone client via P2P, and each message can be pushed to the client.

Click , enter username and password (default username and password are both admin), click OK to see VTH QR code and SN. See Figure 5-2, Figure 5-3.



Figure 5-2

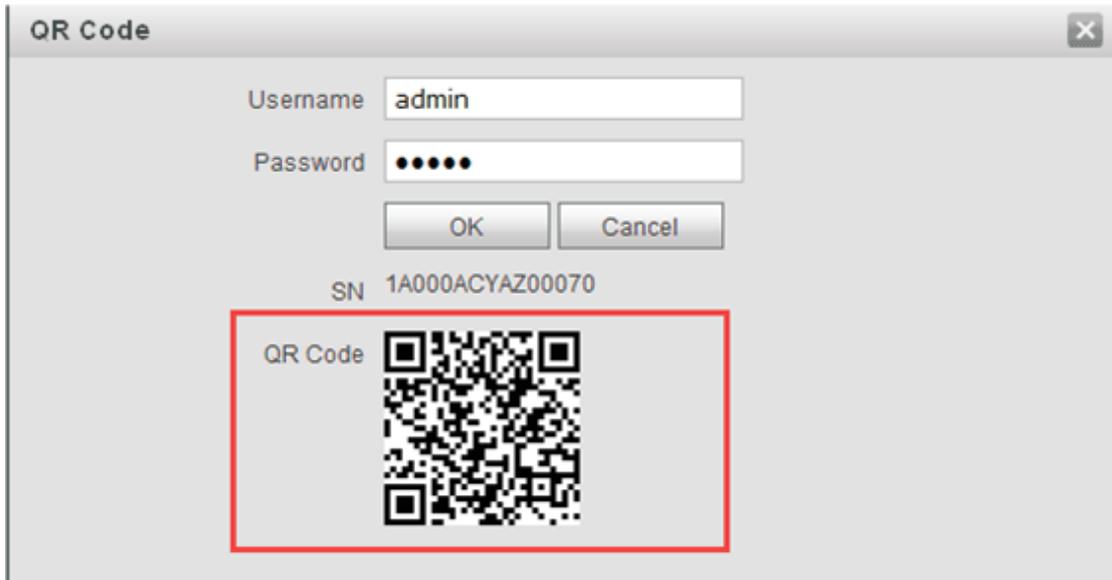


Figure 5-3

b) Use the cell phone to scan the QR code. See Figure 5-4.

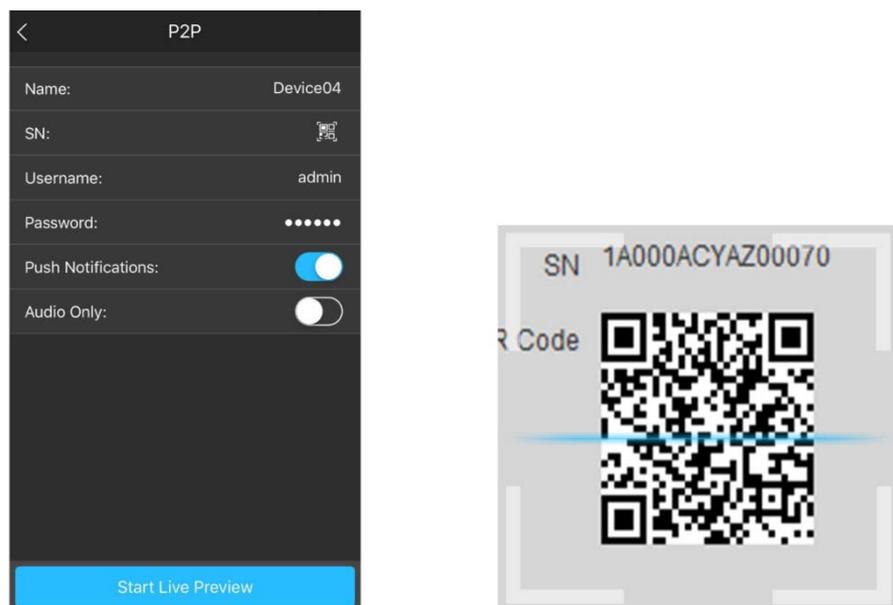


Figure 5-4

c) Give a name to VTO first. Click the detect VTO. You can view the corresponding video from the VTO after it detects the device.

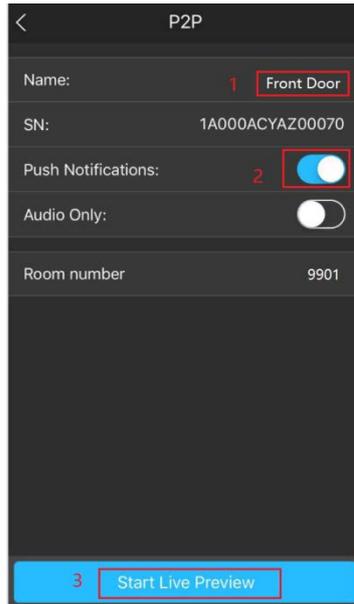


Figure 5-5

5.2 Check Results

When the VTO is calling the VTH, you can see a push message on your cell phone. Open the message; you can see the video from the VTO.

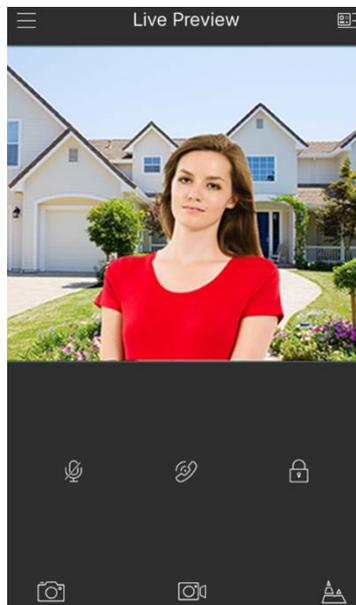


Figure 5-6

6 Electric Lock and Magnetic Door Lock

6.1 Electric Door Lock

When connect the VTO to the electric door lock, connect the positive end of the electric door lock to the NO of the VTO, connect the negative end of the electric door lock to the public end.

When connect to the on-off button, connect one end of the on-off button to the one end of the on-off button of the VTO, and then connect the other end of the on-off button to the GND of VTO. See Figure 6-1.

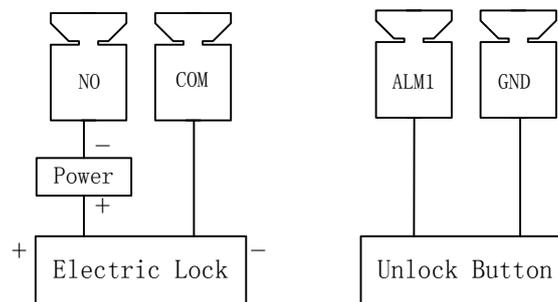


Figure 6-1

6.2 Magnetic Door Lock

When connect the VTO to the magnetic door lock, connect the positive end of the magnetic door lock to the NC of the VTO, connect the negative end of the magnetic door lock to the public end.

When connect to the magnetic door lock feedback, connect one end of the feedback to the one end of the feedback of the VTO, and then connect the other end of the feedback to the GND of VTO. See Figure 6-2.

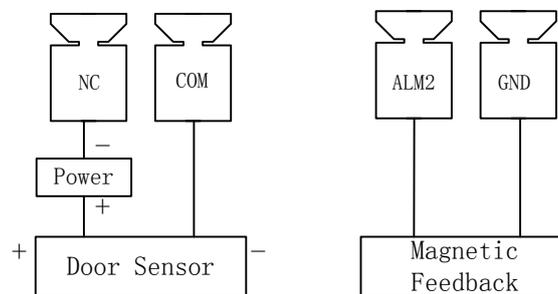


Figure 6-2

Appendix 1 Technical Specifications

Model		VTO3211D-P	VTO3211D
System	Main Process	Embedded micro controller	
	OS	Embedded Linux os	
Video	Video Compression Standard	H.264	
Audio	Audio Standard	G.711	
	Input	Omnidirectional Mic	
	Output	Built-in speaker	
	Talk	Support bidirectional talk	
Operation Mode	Input	Mechanical key	
Alarm	Input	1-ch unlock button, 1-ch door sensor feedback	
	Output	1-ch relay output	
	Front Camera	2.0 MP	
Network	Ethernet	10M/100Mbps self-fit	
Other	485 BUS	1-ch	
	External TF Card	Max 64G	
General	Power	DC 12V or standard PoE	DC 12V
	Protection	IK08	
	Waterproof	IP65	
	Consumption	Standby $\leq 1W$; working $\leq 7W$	
	Dimension (LxWxH)	182mm*101mm*30mm	

Note:

- **This manual is for reference only. Slight difference may be found in user interface.**
- **All the designs and software here are subject to change without prior written notice.**
- **All trademarks and registered trademarks are the properties of their respective owners.**
- **If there is any uncertainty or controversy, please refer to the final explanation of us.**
- **Please visit our website or contact your local service engineer for more information.**