



Administrator Guide



VDP-10M

V.1.0

About This Manual

Thank for choosing OMNY VDP-10M door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual provides all the configurations for the functions and features of OMNY door phone.

Introduction of Icons and Symbols



Warning:

- **Always abide by this information in order to prevent the persons from injury.**



Caution:

- **Always abide by this information in order to prevent the damages to the device.**



Note:

- **Informative information and advice from the efficient use of the device.**



Tip:

- **Useful information for the quick and efficient use of the device.**

Related Documentation

You are advised to refer to the related documents for more technical information via the link below:

Table of Contents

1. Product Overview.....	1
2. Change Log.....	2
3. Model Specification.....	3
4. Introduction to Configuration Menu.....	4
5. Access the Device.....	6
5.1. Obtain Device IP Address.....	6
5.2. Access the Device Setting on the Web Interface.....	7
6. Language and Time Setting.....	8
6.1. Language Setting.....	8
6.2. Time Setting.....	8
7. LED Setting.....	10
7.1. Infrared LED Setting.....	10
7.2. LED Setting on Card Reader Area.....	12
7.3. LED Settings on Keypad.....	12
8. Volume and Tone Configuration.....	13
8.1. Volume Configuration.....	13
8.2. Open Door Tone Configuration.....	14
8.3. Upload Tone Files.....	15
8.3.1. Upload Ringback Tone.....	15
8.3.2. Upload Open Door Tone.....	15
9. Network Setting.....	16
9.1. Network Status.....	16
9.2. Device Network Configuration.....	16
9.3. Device Deployment in Network.....	17
9.4. Device Local RTP configuration.....	18
9.5. NAT Setting.....	19
9.6. SNMP Setting.....	20
9.7. VLAN Setting.....	20
9.8. TR069 Setting.....	21
9.9. WEB HTTP Setting.....	22
10. Intercom Call Configuration.....	24
10.1. IP call & IP Call Configuration.....	24
10.2. SIP Call &SIP Call Configuration.....	24
10.3. SIP Account Registration.....	25
10.4. SIP Server Configuration.....	26
10.5. Configure Outbound Proxy Server.....	26
10.6. Configure Data Transmission Type.....	27
10.7. Configure Calling Feature.....	28
10.7.1. DND.....	28
10.7.2. Manager Call.....	30
10.7.3. Web Call.....	30

10.7.4. Auto Answer.....	31
10.7.5. Multicast.....	32
10.7.6. Configure Maximum Call Duration.....	33
10.7.7. Maximum Dial Duration.....	33
10.7.8. Hang Up after Open Door.....	35
11. Audio& Video Codec Configuration for SIP Calls.....	36
11.1. Audio Codec Configuration.....	36
11.2. Video Codec Configuration.....	37
11.3. Configure DTMF Data Transmission.....	38
12. Access White List Configuration.....	39
12.1. Managing Contact Group.....	39
12.2. Managing Contacts.....	40
12.3. Export/Import Contacts.....	41
13. Relay Setting.....	42
13.1. Relay Switch Setting.....	42
13.2. Select Chime Bell Relay.....	43
13.3. Web Relay Setting.....	43
13.4. Configure White List for Door Relay.....	43
14. Door Access Schedule Management.....	47
14.1. Configure Door Access Schedule.....	47
14.1.1. Manage Door Access Schedule.....	47
15. Door Unlock Configuration.....	50
15.1. Configure Access Card Format.....	50
15.2. Configure Access Card for Door Unlock.....	51
15.3. Import and Export Card Data of Access Control.....	52
15.4. Configure Open Relay via HTTP for Door Unlock.....	53
15.5. Configure Exit Button for Door Unlock.....	54
15.6. Configure PIN Code for Door Unlock.....	55
15.7. Configure Public Key for Door Unlock.....	56
16. Security.....	57
16.1. Tamper Alarm Setting.....	57
16.2. Motion Detection.....	57
16.2.1. Configure Motion Detection.....	58
16.3. Security Notification Setting.....	59
16.3.1. Email Notification Setting.....	59
16.3.2. FTP Notification Setting.....	60
16.3.3. SIP Call Notification Setting.....	61
16.3.4. HTTP URL Notification Configuration.....	61
16.4. Security Action Configuration.....	62
16.4.1. Configure Push button Action.....	62
16.4.2. Configure Motion Action.....	63
16.4.3. Configure Input Action.....	63
16.5. Voice Encryption.....	64
16.6. User Agent.....	65
17. Monitor and Image.....	66
17.1. RTSP Stream Monitoring.....	66
17.1.1. RTSP Basic Setting.....	66
17.1.2. RTSP Stream Setting.....	67
17.1.3. RTSP OSD Setting.....	69

17.2. MJPEG Image Capturing.....	70
17.3. ONVIF.....	72
17.4. Live Stream.....	73
18. Logs.....	74
18.1. Call Logs.....	74
18.2. Door Logs.....	75
19. Debug.....	77
19.1. Event Log.....	77
19.2. System Log.....	78
19.3. PCAP.....	79
20. Firmware Upgrade.....	81
21. Backup.....	82
22. Auto-provisioning via Configuration File.....	83
22.1. Provisioning Principle.....	83
22.2. Configuration Files for Auto-provisioning.....	84
22.3. AutoP Schedule.....	85
22.4. PNP Configuration.....	86
22.5. Static Provisioning Configuration.....	86
23. Integration with Third Party Device.....	88
23.1. Integration via Wiegand.....	88
23.2. Integration via HTTP API.....	89
24. Password Modification.....	92
24.1. Modifying Device Web Interface Password.....	92
24.2. Configure Web Interface Automatic Logout.....	92
25. System Reboot&Reset.....	93
25.1. Reboot.....	93
25.2. Reset.....	93
26. Abbreviations.....	94

1. Product Overview

The security that comes with being able to control who comes into your building along with the ability to verbally and visually confirm their identity is immeasurable. VDP-10M is a SIP-compliant, hands-free and video(optional) door phone. It can be connected with indoor monitors for remote access controlling and monitoring. Users can communicate with visitors via audio and video calls, and unlock the door if they need. The door phone enables you to easily monitor an entrance door or gate and gives you the peace of mind knowing that your facility is more secure.

2. Change Log

The change log will be updated here along with the changes in the new software version.

3. Model Specification

Model & Feature	VDP-10M
Button	Physical Numeric Keypad
Housing Material	Aluminum
Camera	2 Mega pixels, automatic lighting
Relay In	2
Relay Out	2
RS485	√
PoE	√
RAM	128MB
ROM	16MB
Card Reader	√
IP Rating	IP65
IK Rating	X
Wall Mounting	√
Flush	√

4. Introduction to Configuration Menu

- **Status:** this sections gives you basic information such as product information, Network Information, and account information etc.
- **Account:** this section concerns SIP account, SIP server, proxy server, transport protocol type, audio&video codec, DTMF, session timer, etc.
- **Network:** this section mainly deals with DHCP&Static IP setting, RTP port setting, and device deployment etc.
- **Intercom:** this section covers Intercom settings, Call Log etc.
- **Surveillance:** this section covers Motion Detection, RTSP, MJPEG, ONVIF, Live stream.
- **Access Control:** this section covers Input control, Relay, Card settings, Face Recognition setting, Private PIN Code, Wiegand connection etc.
- **Device:** this section includes Light settings, tab&button display, LCD settings and Voice settings.
- **Settings:** this section includes Time&language, Action settings, Door settings, Schedule for access control.
- **Upgrade:** this section covers Firmware upgrade, device reset&reboot, configuration file auto-provisioning, fault Diagnosis.
- **Security:** this section is for Password modification.

Mode selection :

1. **Discovery mode:** It is a plug and play configuration mode. Devices will configure themselves automatically when users power on the devices and connect them to network. It is super time-saving mode and it will greatly bring users convenience by reducing manual operations. This mode requires no prior configurations previously by the administrator.
2. **SDMC mode:** SDMC (SIP Device Management Controller) is a simple and comprehensive software for building management.
3. **Omnyvideo mode:** the mode for working with the Omny video service

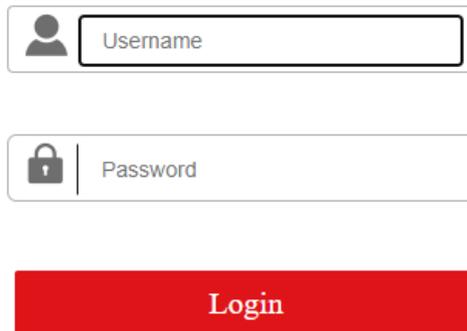
5. Access the Device

5.1. Obtain Device IP Address

By default, the device is in the DHCP mode. To find out the IP address, enter the combination *3258* after switching on. You will hear a voice message about the received IP address. To exit the voice-over mode, click Cancel. If the IP address is not received, you will hear: "IP 0.0.0.0".

5.2. Access the Device Setting on the Web Interface

Enter the device IP address on the web browser in order to log in the device web interface where you can configure and adjust parameter etc. The initial user name and password are all “admin” and please be case-sensitive to the user names and passwords entered.



The login form consists of two input fields and a button. The first field is labeled 'Username' and has a person icon to its left. The second field is labeled 'Password' and has a padlock icon to its left. Below these fields is a red button with the text 'Login' in white.



Tip:

- You can also obtain the device IP address using the IP-scanner to log in the device web interface. Please refer to the URL below for the IP scanner application:



Note:

- Google Chrome browser is strongly recommended.

6. Language and Time Setting

6.1 Language Setting

When you first set up the device, you might need to set the language to your need or you can do it later if needed. And the language can be set up on the device web **Phone > Time/Lang > Web Language** interface according to your preference.

Web Language

Mode English ▼

Parameter Set-up:

- Type: choose a suitable web language. Normally, English is the default web language.

 **Note:**

For VDP-10M, the operation path is Setting > Time/Lang > Web Language

6.2. Time Setting

The set-up on the the device web interface is identical with the setting on the device, it however allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. And when your time zone is selected, the device will automatically notify the NPT server of its time zone in order that the NTP server can synchronize the time zone set-up to your device.

NTP

Time Zone	<input type="text" value="GMT+3:00 Moscow"/>
Preferred Server	<input type="text" value="172.31.72.118"/>
Alternate Server	<input type="text" value="1.pool.ntp.org"/>
Update Interval	<input type="text" value="3600"/> ($\geq 3600s$)
System Time	11:44:02

Parameter Set-up:

- Time Zone: select the specific time zone depending on where the device is used and then press Confirm tab for the confirmation. The default time zone is GMT GMT+0.00.
- Primary/Secondary Server: the time zone server, normally it will automatically obtain the time when connecting to the network. The secondary server will take effect when the primary server is invalid.
- Update Interval: to configure interval between two consecutive NTP requests.

You can also set up time manually, select the Manual checkbox, and input time data.

Type

Manual

Date Year Mon Day

Time Hour Min Sec

Auto

7. LED Setting

7.1 Infrared LED Setting

Infrared LED is applied in the dark environment in which a resident might not be able to see a visitor clearly via the video from the door phone. If the infrared LED is turned off, the door phone will turn to night mode so that you can have a clear view of the visitor. You can setup it on device web **Intercom > Advanced interface**

Parameter Set-up:

- **Photoresistor Setting:** set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the ON-OFF of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off. While the default Minimum and maximum photoresistor value is from "0" minimum to "1000" maximum respectively.
- **Now:** click **Read** to obtain the current environment brightness.

7.2. LED Setting on Card Reader Area

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, If you do not want to have the LED light on the card reader area to stay on, you can also set the timing for the exact time span during which the LED light can be disabled in order to reduce the electrical power consumption.

To do this configuration on the web **Intercom > LED Setting** interface

Card LED Enabled	<input checked="" type="checkbox"/>
Time (H)	<input type="text" value="18"/> - <input type="text" value="06"/> (0~23)

Parameter Set-up:

- Enabled: tick the check box if want to enable the card reader LED lighting and vice versa.
- Start Time- End Time (H): enter the time span for the LED lighting to be valid, e.g. if the time span is set from 8-0 (Sart time- End time) it means LED light will stay on during the time span from 8:00 am to 12:00 pm during one

7.3. LED Settings on Keypad

You can enable or disable the LED lighting of keypad as needed on the web interface. Meanwhile, If you prefer not to have the LED light of keypad stay on, you can also set the timing for the exact time span during which the LED light can be enabled in order to reduce the electrical power consumption etc. To do this configuration on the web **Intercom > LED Setting** interface.

Keypad LED Enabled	<input checked="" type="checkbox"/>
Time (H)	<input type="text" value="00"/> - <input type="text" value="23"/> (0~23)

Parameters Set-up:

- **Keypad LED Enable:** Click to enable or disable the keypad LED lighting
- **Start Time (H):** Enter the time span for the LED lighting to be valid. Eg. If the time span is from 18-22 it means LED light will stay on during the time span from 6:00 pm to 22:00 pm during a day

8. Volume and Tone Configuration

Volume and tone configuration in door phone refers to the microphone volume, speaker volume, temper alarm volume, ringback tone and open door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

8.1. Volume Configuration

To set up the volumes, you can set up on device web **Phone > Voice** interface.

Volume Control

Mic Volume	<input type="text" value="8"/>	(1~15)
Volume Level	<input type="text" value="1"/> ▼	
Speaker Volume	<input type="text" value="15"/>	(1~15)
Keypad Volume	<input type="text" value="8"/>	(1~15)
Tamper Alarm Volume	<input type="text" value="15"/>	(1~15)
Prompt Volume	<input type="text" value="15"/>	(0~15)

Parameters Set-up:

- **Mic Volume:** Adjust the mic volume as needed.
- **Volume Level:** Control the volume of all speakers. The default is 1, the first level of volume, the volume range is roughly 80-95, and 2 is the second level of volume, the volume range is roughly 95-109

- **Speaker Volume:** Adjust the speaker volume as needed.
- **Tamp Alarm Volume:** Adjust the volume for the tamper alarm.
- **Keypad volume:** Adjust the volume for the keypad

8.1.1. Open Door Tone Configuration

You can not only enable or disable the Open Door Tone but also controls the prompt words that accompanies the tone on web **Intercom > Voice** interface.

Open Door Tone Setting

Open Door Inside Tone	<input type="checkbox"/>
Open Door Outside Tone	<input checked="" type="checkbox"/>
Open Door Failed Tone	<input type="checkbox"/>

Parameters Set-up:

- **Open Door Inside tone:** click the field Enabled or Disabled depending on if you want to hear the prompt words that accompanies that Open Door Success tone when use button.
- **Open Door Outside tone:** click the field Enabled or Disabled depending on if you want to hear the prompt words that accompanies that Open Door Success tone when use cardreader.
- **Open Door Failed tone:** click the field Enabled or Disabled depending on if you want to hear the prompt words that accompanies that Open Door Failed tone.

8.2. Upload Tone Files

You can customize all tones if you need. Please follow the prompt about the file size and format.

Tone Upload
File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16

Open Door Succeeded Outside Warning	<input type="text" value="Выберите файл"/> Файл не выбран
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Open Door Succeeded Inside Warning	<input type="text" value="Выберите файл"/> Файл ...ыбран
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Open Door Failed Warning	<input type="text" value="Выберите файл"/> Файл не выбран
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Ringback	<input type="text" value="Выберите файл"/> Файл не выбран
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Trigger Manager Dial Warning	<input type="text" value="Выберите файл"/> Файл ...ыбран
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>

9. Network Setting

9.1. Network Status

To check the network status on the web **Status > Network Information** interface.

Network Information

Port Type	DHCP Auto
Link Status	Connected
IP Address	172.31.170.107
Subnet Mask	255.255.255.0
Gateway	172.31.170.1
Preferred DNS Server	8.8.8.8
Alternate DNS Server	8.8.4.4

9.2. Device Network Configuration

You can check for the door phone's network connection info and configure the default **DHCP mode** (Dynamic Host Configuration Protocol) and static IP connection for the device on the device web **Network > Basic** interface.

LAN Port

<input checked="" type="radio"/> DHCP	<input type="radio"/> Static IP
IP Address	<input type="text" value="192.168.1.100"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
Preferred DNS Server	<input type="text" value="8.8.8.8"/>
Alternate DNS Server	<input type="text"/>

Parameter Set-up:

- **DHCP:** select the DHCP mode by moving the toggle switch to the right. DHCP mode is the default network connection. If the DHCP mode is turned on, then the door phone will be assigned by the DHCP server with IP address, subnet mask, default gateway and DNS server address automatically.
- **Static IP:** select the static IP mode by checking off the DHCP check box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS servers address have to be manually configured according to your actual network environment.
- **IP Address:** set up the IP Address if the static IP mode is selected.
- **Subnet Mask:** set up the subnet Mask according to your actual network environment.
- **Default Gateway:** set up the correct gateway default gateway according to the IP address of the default gateway.
- **LAN DNS1/2:** set up preferred or alternate DNS Server (Domain Name Server) according to your actual network environment. Preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary server address and the door phone will connects to the alternate server when the primary DNS server is unavailable .

9.3. Device Deployment in Network

Door phones should be deployed before they can be properly configured in the network environment in terms of their location, operation mode, address

and extension numbers as opposed to other devices for the device control and the convenience of the management. So you can do it on web **Network > Advanced > Connect Setting** interface.

Connect Setting

Server Mode	<input style="width: 100%;" type="text" value="None"/>
Discovery Mode	<input checked="" type="checkbox"/>
Device Address	<input type="text" value="1"/> . <input type="text" value="1"/> . <input type="text" value="1"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Device Extension	<input type="text" value="1"/>
Device Location	<input type="text" value="Подъезд"/>

Parameter Set-up:

- **Server Type:** it is automatically set up according to the actual device connection with a specific server in the network such as SDMC or Cloud and None. None is the default factory setting indicating the device is not in any server type, therefore you are allowed to choose Cloud, SMDC in discovery mode.
- **Discovery Mode:** click “Enable” to turn on the discovery mode of the device so that it can be discovered by other devices in the network, and click “Disable” if you want to conceal the device so as not to be discovered by other devices.
- **Device Address:** specify the device address by entering device location information from the left to the right :Community, Unit, Stair, Floor, Room in sequence.
- **Device extension:** enter the device extension number for the device you installed.
- **Device Location:** enter the location in which the device is installed and used.

9.4. Device Local RTP configuration

For the device network data transmission purpose, device needs to be set up with a range of RTP port (Real-time Transport Protocol) for establishing an exclusive range of data transmission in the network.

Local RTP

Starting RTP Port	<input type="text" value="11800"/>	(1024~65535)
Max RTP Port	<input type="text" value="12000"/>	(1024~65535)

Parameter Set-up:

- **Starting RTP Port:** enter the Port value in order to establish the start point for the exclusive data transmission range.
- **Max RTP port:** enter the Port value in order to establish the end point for the exclusive data transmission range.

9.5. NAT Setting

NAT (Network Address Translation) allows hosts in an organization's private intranet to transparently connect to hosts in the public domain. There is no need for internal hosts to have registered Internet addresses. It is a way to translate the internal private network IP address into a legal network IP address technology. To do this configuration on web Account > Advance > NAT interface.

NAT

UDP Keep Alive Messages	<input checked="" type="checkbox"/>
UDP Alive Msg Interval	<input type="text" value="30"/> (5~60s)
RPort	<input checked="" type="checkbox"/>
RPort Advanced	<input type="checkbox"/>

Parameter Set-up:

- **UDP Keep Alive Messages:** If enabled, the device will send out the message to the SIP server so that SIP server will recognize if the device is in online status.
- **UDP Alive Msg Interval:** set the message sending time interval from 5-60 seconds, the default is 30 seconds.
- **RPort:** enable the Rport when the SIP server is in WAN (Wide Area Network).

9.6. SNMP Setting

SNMP (Simple Network Management Protocol) is an Internet-standard protocol for managing devices on IP networks. SNMP is widely used in network management system to monitor network-attached devices for conditions that may draw network administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried by managing applications. These variables accessible via SNMP are organized in hierarchies, which are described by Management Information Bases (MIBs). To do the configuration on the web **Network > Advanced > SNMP** Interface.

Parameter Set-up:

- **Enabled:** to enable or disable SNMP feature.
- **Port:** to configure SNMP server's port.
- **Trusted IP:** to configure allowed SNMP server address. It could be an IP address or any valid URL domain name

9.7. VLAN Setting

Virtual Local Area Network is a logical grouping of two or more nodes which are not necessarily on the same physical network segment but which share the same logical IP domain. To be specific, the purpose of VLAN is to separate layer 2 broadcast domain. Within trunk links, the tagged packet will only be sent to those ports with same VLAN ID. This is usually achieved by switch or router. User can benefit from deployed VLAN, such as:

- *Security: if without VLAN, all host will be included in unique broadcast domain. Therefore, the consequence of ARP attack will affect all end devices in the organization.
- *Performance: The nature of network broadcast is to flood frames among the network. In certain condition, it is unnecessary to receive broadcast frame. To save bandwidth for high efficiency, it will be better to separate broadcast domain by deploy VLAN. To do the configuration on the web **Network > Advanced > VLAN** interface

VLAN

LAN Port	Enabled	<input type="checkbox"/>
	VID	<input type="text" value="1"/> (1~4094)
	Priority	<input type="text" value="0"/> ▼

Parameter Set-up:

- **Enabled:** to enable or disable VLAN feature for designated port.
- **VID:** To configure VLAN ID for designated port.
- **Priority:** To select VLAN priority for designated po

9.8. TR069 Setting

TR-069 (Technical Report 069) is the document number of the technicalreport, defined by the Broadband Forum, that specifies the “CPE WAN management protocol” or CWMP. It defines an application layer protocol remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between Customer-Premises Equipment (CPE) and Auto-Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. To do the configuration on the web Network > Advanced > TR069 interface.

TR069

	Enabled	<input type="checkbox"/>
	Version	<input type="text" value="1.0"/> ▼
ACS	URL	<input type="text"/>
	UserName	<input type="text"/>
	Password	<input type="text" value="*****"/>
Periodic Inform	Enabled	<input type="checkbox"/>
	Periodic Interval	<input type="text" value="1800"/> (3~24×3600s)
CPE	URL	<input type="text"/>
	UserName	<input type="text"/>
	Password	<input type="text" value="*****"/>

Parameter Set-up:

- **Enabled:** to enable or disable TR069 feature.
- **Version:** to select supported TR069 version (version 1.0 or 1.1).
- **ACS/CPE:** ACS is short for auto configuration servers as server side, and CPE is short for customer-premise equipment as client side devices.
- **URL:** to configure URL address for ACS or CPE
- **User Name:** to configure username for ACS or CPE
- **Password:** to configure password for ACS or CPE
- **Periodic Inform:** to enable periodically inform.
- **Periodic Interval:** to configure interval for periodic info.

 Note:

TR-069 is a technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

9.9. Device WEB HTTP Setting

This function is used to manage whether the device website is allowed to be accessed. The door phone supports two types remote access method HTTP and HTTPS(encryption). To do this configuration on the web **Network > Advanced > Web Server** interface.

Web Server

HTTP Enabled	<input checked="" type="checkbox"/>
HTTPS Enabled	<input checked="" type="checkbox"/>
HTTP Port	<input type="text" value="80"/> (80,1024~65534)
HTTPS Port	<input type="text" value="443"/> (443,1024~65534)

Parameter Set-up:

- **Http Enable:** Set whether HTTP access to the device webpage is allowed, Enabled is allowed, Disabled is not allowed, the default
- **Https Enable:** Set whether HTTPS access to the device webpage is allowed, Enabled is allowed, Disabled is not allowed, the default is Enabled.
- **Http Port:** Setup the port for HTTP access method. 80 is default port. Intercom Call Configuration

Intercom call in the device can be configured to allow you to perform a variety of customized intercom calls such as IP call and SIP call for different application scenarios.

10. Intercom Call Configuration

Intercom call in the device can be configured to allow you to perform a variety of customized intercom calls such as IP call and SIP call for different application scenarios.

10.1. IP call & IP Call Configuration

IP call can be made directly on the intercom device by entering the IP number on the device. And you can also disable the direct IP call if you do not allow IP call to be made on the device. **Phone > Call Feature > Direct IP**

Direct IP	
Enabled	<input checked="" type="checkbox"/>
Auto Answer	<input checked="" type="checkbox"/>
Port	<input type="text" value="5060"/> (1~65535)

Parameters Set-up:

- **Direct IP Call:** click “Enable” or “Disable” to turn the direct IP call on or off. For example if you do not allow direct IP call to be made on the device, you can click “Disable” to terminate the function.
- **Direct IP AutoAnswer:** click “Enable” or “Disable” to turn the direct IP call on or off when the phone automatically answer the incoming call.
- **Direct IP port :** set up the IP direct call port, 5060 is the default port.

10.2. SIP Call & SIP Call Configuration

You can make SIP call (Session Initiation Protocol) in the same way as you do for making the IP calls on the device. However, SIP call parameters related to its account, server, and transport type need to be configured first before you can make calls on the device.

10.3. SIP Account Registration

VDP-10M support two SIP accounts that can all be registered according to your applications. You can for example, switch between them if any one of the account failed and become invalid. The SIP account can be configured on the device and on the device interface. To perform the SIP account setting on the Web Account > Basic > SIP Account Interface.

SIP Account

Status	Registered
Account	Account 1 ▼
Account Enabled	<input checked="" type="checkbox"/>
Display Label	<input type="text"/>
Display Name	<input type="text"/>
Register Name	<input type="text"/>
Username	<input type="text"/>
Password	*****

Parameter Set-up:

- **Status:** check to see if the SIP account is registered or not.
- **Account Active:** click **Enable** or **Disable** to activate or deactivate the registered SIP account.
- **Display Name:** configure the name, for example the device's name to be shown on the device being called to.
- **User Name:** enter the user name obtained from SIP account administrator.
- **Account:** select the exact account (Account 1&2) to be configured.
- **Display Label:** configure the device label to be shown on the device screen.
- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator.
- **Password:** enter the password obtained from the SIP account administrator.

10.4. SIP Server Configuration

SIP servers can be set up for device in order to achieve call session through SIP server between intercom devices. To do this configuration also on web **Account > Basic > SIP Server** interface.

Preferred SIP Server		
Server IP	<input type="text" value="192.168.1.100"/>	Port <input type="text" value="5070"/> (1024~65535)
Registration Period	<input type="text" value="1800"/>	(30~65535s)

Alternate SIP Server		
Server IP	<input type="text"/>	Port <input type="text" value="5060"/> (1024~65535)
Registration Period	<input type="text" value="1800"/>	(30~65535s)

Parameter Set-up:

- **Preferred SIP Server:** enter the primary server IP address number or its URL.
- **Alternate SIP Server:** enter the backup SIP server IP address or its URL.
- **Port:** set up SIP server port for data transmission.
- **Registration Period:** set up SIP account registration time pan. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is “**1800**”, ranging from **30-65535s**.

10.5. Configure Outbound Proxy Server

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish call session via port-based data transmission. To set it up on the device web **Account > Basic > Outbound Proxy Server** Interface.

Outbound Proxy Server

Outbound Enabled	<input type="checkbox"/>			
Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>	(1024~65535)
Backup Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>	(1024~65535)

Parameter Set-up:

- **Outbound Enabled:** click “**Enable**” and “**Disable**” to turn on or turn off the outbound proxy server.
- **Server IP:** enter the SIP address of the primary outbound proxy server.
- **Port:** enter the Port number for establish call session via the primary outbound proxy server
- **Back Server IP:** set up Backup Server IP for the backup outbound proxy server.
- **Port:** enter the port number for establishing call session via the backup outbound proxy server.

10.6. Configure Data Transmission Type

SIP message can be transmitted in three data transmission protocols: **UDP (User Datagram Protocol)**, **TCP(Transmission Control Protocol)**, **TLS (Transport Layer Security)** and **DNS-SRV**. In the meantime, you can also identify the server from which the data come from. To do this configuration on web **Account > Basic > Transport Type** interface.

Transport Type	
Type	<input type="text" value="TCP"/>

Parameter Set-up:

- **UDP:**select “**UDP**” for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP:** select “**TCP**” for Reliable but less-efficient transport layer protocol.
- **TLS:** select “**TLS**” for Secured and Reliable transport layer protocol.
- **DNS-SRV:** select “**DNS-SRV**” to obtain DNS record for specifying the location of servers. And **SRV** not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

10.7. Configure Calling Feature

10.7.1. DND

DND (**Do not disturb**) setting allows you not to be disturbed by any unwanted incoming SIP calls. You can set up DND related parameters properly on the device web **Phone > Call Feature** interface to block SIP calls you do not intend to answer. In the meantime, you can also define the code to be sent to the SIP server when you want to reject the call.

DND

Enabled	<input type="checkbox"/>
Return Code When DND	486(Busy Here) ▼

Parameter Set-up:

- **Account:** select “**Account1**”, “**Account2**” or “**All account**” for the DND application.
- **DND:** enable or disable the DND function. DND function is disabled by default.

- **Return Code When DND:** select what code should be sent to the calling device via SIP server. **404 for “Not found”;** **480 for “Temporary unavailable”** **486 for “busy here”**.
- **DND On Code:** turn on the DND on server using the Code obtained. The DND on Code is **78** by default.
- **DND Off Code:** turn off the DND on server using the code obtained. The DND off Code is **79** by default.
- **Return Code When Refuse:** select code to be sent the caller side via SIP server when you rejected the incoming call.

10.7.2. Manager Call

Manager Dial Call includes two types of calls: Sequence call and group call. It allows quick initiation of pre-configured numbers by pressing the Management key on the door phone. Navigate to the web Intercom > Basic > Manager Dial interface.

Manager Dial

Call Type Group Call ▼

Call Timeout (Sec) 20 ▼

(If the local group is not blank, then only the local numbers will be called.)

Group Call Number (Local)

Group Call Number (Cloud)

Parameters Set-up:

- **Call Type:** select the group call or sequence call (Robin call) for the manager dial call.
- **Sequence Call:** sequence call is used to initiate multiple numbers when your press the manager dial button. If the previous callee does not answer within the sequence call timeout, the call will be transferred to the next one. If the call is answered by one of the callees, the call will not be transferred.
- **When Refused:** if you select End All Calls, the sequence call will be terminated if the call is rejected by the called party. If you select End This Call Only, the sequence call will be continued to the next called party if it is rejected by the first called party.
- **Group Call:** group call is used to initiate calls to multiple numbers at the same when you press the manager dial button.

10.7.3. Web Call

In addition to making IP/SIP call directly on the device, you can also make the call on the device web interface without approaching to device physically for testing purpose etc.

Web Call

Web Call(Ready)

Parameters Set-up:

- **Auto/Account1/Account2:** To choose a suitable SIP account to make a web call. If you call out using IP address, Account selection is no need to chosen.

10.7.4. Auto Answer

You can define how quick the door phone should response in answering the incoming SIP/IP call automatically by setting up the time related parameters. In addition, you can also define the mode in which the calls are to be answered (video mode or audio mode). You can set up the related parameters on web **Phone > Call Feature**.

Auto Answer

Auto Answer Delay (0~5 Sec)
Mode

Parameters Set-up:

- **Auto Answer Delay:** Set up the delay time (from 0-5 sec.) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.
- **Auto Answer Mode:** Set up the video or audio mode you preferred for answering the call automatically.

10.7.5. Multicast

Multicast uses one-to-many mode to communicate in a range. Door phone can be a listener and receive the audio from the listened part.

Multicast Setting

Multicast Priority Paging Barge

Paging Priority Enabled

Priority List

IP Address	Listening Address	Label	Priority
1st IP Address	<input type="text"/>	<input type="text"/>	1
2nd IP Address	<input type="text"/>	<input type="text"/>	2
2rd IP Address	<input type="text"/>	<input type="text"/>	3
4th IP Address	<input type="text"/>	<input type="text"/>	4
5th IP Address	<input type="text"/>	<input type="text"/>	5
6th IP Address	<input type="text"/>	<input type="text"/>	6
7th IP Address	<input type="text"/>	<input type="text"/>	7
8th IP Address	<input type="text"/>	<input type="text"/>	8
9th IP Address	<input type="text"/>	<input type="text"/>	9
10th IP Address	<input type="text"/>	<input type="text"/>	10

Parameters Set-up:

- **Paging Barge:** multicast or how many multicast calls are higher priority than SIP call, if you disable Paging Priority Active, SIP call will have high priority.
- **Paging Priority Active:** multicast calls are called in order of priority or not.
- **Listening Address:** Enter the multicast IP address you want to listen. The multicast IP address need to be same as the listened part and the multicast port can not be same for each IP address. Multicast IP address is from 224.0.0.0 to 239.255.255.255
- **Label:** Enter the label for each listening address.

10.7.6. Configure Maximum Call Duration

Door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the intercom device. When the call time duration is reached, the door phone will terminate the calling automatically.

Max Call Time

Max Call Time (2~30 Min)

Parameters Set-up:

- **Max Call Time:** Enter the call time duration according to your need (Ranging from 0-120 min.). The default call time duration is 5 min.

Note:

- Max call time of device is also related with max call time of SIP server. If using SIP account to make a call, please pay attention to the max call time of SIP server. If the max call time of SIP server is shorter than the max call time of device, the shorter one is available.

10.7.7. Maximum Dial Duration

Maximum Dial duration is consisted of Maximum dial in time duration and the maximum dial out time. Maximum dial in time refers to the maximum time duration before the door phone hang up the call if the call is not answered by the door phone. In contrary, Maximum dial out time refers to the maximum time

duration before the door phone hang up itself automatically when the call from the door phone is not answered by the intercom device being called.

Max Dial Time

Dial In Time	<input type="text" value="60"/>	(5~120 Sec)
Dial Out Time	<input type="text" value="60"/>	(5~120 Sec)

Parameters Set-up:

- **Dial in Time:** Enter the dial in time duration for you door phone (ranging from 30-120 sec.) for example, if you set the dial in time duration is 60 second in your door phone, then the door phone will hang up the incoming call automatically if the call is not answered by the door phone in 60 seconds. 60 second is the dial in time duration by default.
- **Dial out Time:** Enter the dial in time duration for your door phone (ranging from 5-120 sec.) for example, if you set the dial out time duration is 60 second in your door phone, then the door phone will hang out the call it dialed out automatically if the call is not answer by the device being called.



Note:

- Max dial time of device is also related with max dial time of SIP server. If using SIP account to make a call, please pay attention to the max dial time of SIP server. If the max dial time of SIP server is shorter than the max dial time of device, the shorter one is available.

10.7.8. Hang Up after Open Door

This feature is used to hang up the call automatically after the door is released during a call. So the caller or callee do not need to click hang up key again. To do this configuration on the web **Intercom > Basic** interface.

Hang Up After Open Door

Type	<input type="text" value="DTMF Or HTTP"/>
Timeout	<input type="text" value="5"/> (0~15 Sec)

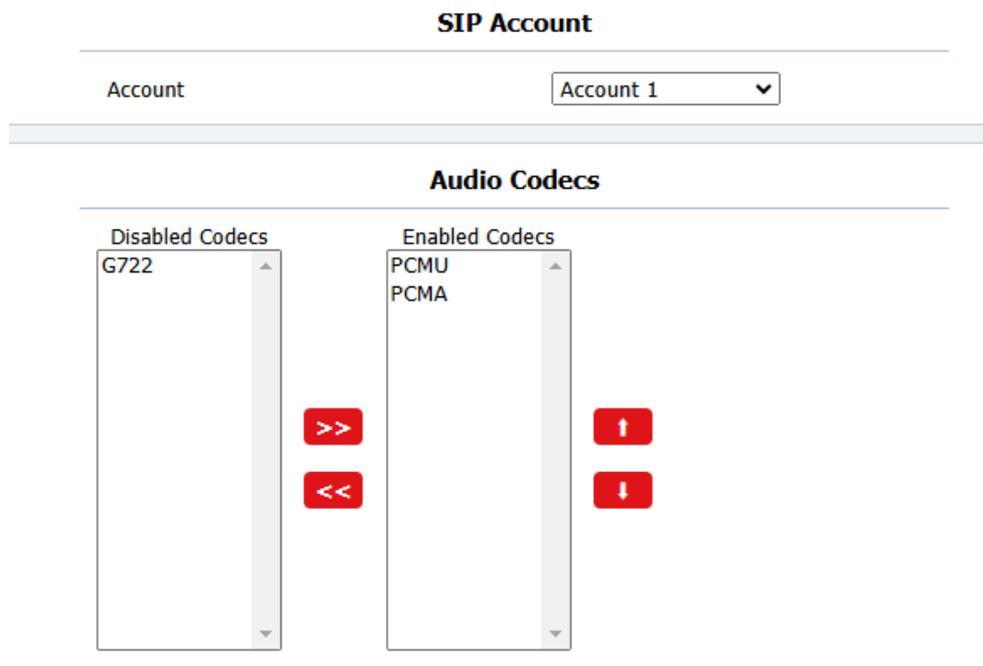
Parameters Set-up:

- **Timeout:** the time out value can be set up from 1 second to 15seconds. 5 seconds is default. The call will be automatically hang up within this valueafter the door is opened.

11. Audio&Video Codec Configuration for SIP Calls

11.1. Audio Codec Configuration

VDP-10M door phone support four types of Codec (PCMU, PCMA, G729, G722) for encoding and decoding the the audio data during the call session. Each type of Codec varies in terms of the sound quality. You can select the specific codec with different bandwidth and sample rate flexibly according to the actual network environment. To do the configuration on device web **Account > Advanced** interface.



Please refers to the bandwidth consumption and sample rate for the four codecs types below:

Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHz
PCMU	64 kbit/s	8kHz
G722	64 kbit/s	16kHz

11.2. Video Codec Configuration

VDP-10M door phone support H264 codec that provides a better video quality at much lower bit rate with different video quality and payload. To set up video codec on web **Account > Advanced** interface.

Video Codec

Name	<input checked="" type="checkbox"/> H264
Resolution	VGA <input type="button" value="v"/>
Bitrate	512 <input type="button" value="v"/>
Payload	104 <input type="button" value="v"/>

Parameter Set-up:

- **Codec Name:** Check to select the H264 video codec format for the door phone video stream. H264 is the video codec by default.
- **Codec Resolution:** select the code resolution for the video quality among four options: “CIF”, “VGA”, “4CIF” and “720P” according to your actual network environment. The default code resolution is 4CIF.
- **Codec Bitrate:** select the video stream bit rate (Ranging from 320-2048). The greater the bitrate, the data transmitted in every second is greater in amount therefore the video will be clearer.. While the default code bitrate is 2048.
- **Codec Payload:** select the payload type (ranging from 90-118) to

configure audio/video configuration file. The default payload is 104.

11.3. Configure DTMF Data Transmission

In order to achieve the door access via DTMF code or some other applications, you are required to properly configure DTMF on web **Account > Advanced > DTMF** in order to establish a DTMF-based data transmission between the door phone and other intercom device for the third party integration.

DTMF	
Type	RFC2833
How To Notify DTMF	Disabled
Payload	101 (96~127)

Parameter Set-up:

- **Type:** select DTMF mode among five options: **“Inband”**, **“RFC2833”**, **“Info+Inband”** and **“Info+RFC2833”** based on the specific DTMF transmission type of the third party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF :** select among four types: **“Disable”** **“DTMF”** **“DTMF-Relay”** **“Telephone-Event”** according to the specific type adopted by the third party device. You are required to set it up only when the third party device to be matched with adopts **“Info”** mode
- **DTMF Payload:** set the payload according the the specific data transmission payload agreed on between the sender and receiver during the data transmission.

12. Contact Configuration

The contacts list is for granting access or calling permission to the indoor monitor or other devices. to set it up on the web **Contacts > Access Allowlist interface.**

12.1. Manage Contact

Enter the group name in the Name column and set up the ring and the description information for the group to add a new group. Check and manage the existing groups in the group list.

Contacts All Contacts ▾

Search Search Reset

Index	Name	Phone Number	Account	Floor	<input type="checkbox"/>
1					<input type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>

Page 1 ▾ Prev Next Delete Delete All

Contact Setting

Name Phone Number

Account Auto ▾ Floor None

Add Edit Cancel

Parameter Set-up:

- **Account:** the registered SIP account to make a call. If using IP direct call, it is not available. he group name.
- **Floor:** Floor: the floor number that the contact is allowed to access. he incoming call ring for the group.

13. Relay Setting

13.1. Relay Switch Setting

You can configure the relay switch(es) and DTMF for the door access on the web **Intercom > Relay** interface.

Relay		
Relay ID	Relay A	Relay B
Type	Default state	Default state
Mode	Monostable	Monostable
Trigger Delay(Sec)	0	0
Hold Delay(Sec)	3	3
DTMF Mode	1 Digit DTMF	
1 Digit DTMF	#	1
2~4 Digits DTMF	010	012
Relay Status	RelayA: Low	RelayB: Low
Relay Name	Pene1	RelayB
Access Method	PIN <input checked="" type="checkbox"/> RF Card <input checked="" type="checkbox"/> NFC <input checked="" type="checkbox"/>	PIN <input checked="" type="checkbox"/> RF Card <input checked="" type="checkbox"/> NFC <input checked="" type="checkbox"/>

Parameter Set-up:

- **Type:** when Default state is selected, the Relay Status shows Low which means the door is closed and the Relay Status shows High which means the door is opened. If Invert State is selected, the Relay Status shows High which means the door is closed and Low means the door is opened.
- **Mode:** there are two modes Monostable and Bistable. If Monostable is selected, the relay status will be automatically reset within the relay delay time after the relay is triggered. If Bistable is selected, relay status will be reset after the relay is triggered again.
- **Trigger Delay (Sec):** the relay trigger delay time ranges from 1-10 seconds. If you set the delay time as 5 seconds, the relay will not be triggered until 5 seconds after you press the unlock tab.

Parameter Set-up:

- Hold Delay (Sec): the relay hold delay time ranges from 1-10 seconds. If you set the hold delay time as 5 seconds, the relay will resume the initial state after maintaining the triggered state for 5s.
- DTMF Mode: the number of DTMF digits for the door access control (Ranging from 1-4 digits).
- 1 Digit DTMF: select the code from *0-9 and ,# if the DTMF Option is set as 1 digit.
- 2~4 Digits DTMF: set the DTMF code according to the DMTP Option setting. For example, you are required to set the 3-digits DTMF code if DTMP Option is set as 3-digits.
- Relay Status: relay status is low by default which means normally closed(NC). If the relay status is high, then it is in normally open status(NO).
- Relay Name: name the relay switch to distinguish it from others. You can name the relay switch according to where it is located for convenience.

13.3. Web Relay Setting

In additional to the relay that is connected to the door phone, you can also control the door access using the network-based web relay on the device and on the device web interface.

Web relay needs to be set up on the web **Phone > WebRelay** interface where you are required to fill in such information as relay IP address, password, web relay action etc before you can achieve the door access via web relay.

Web Relay

Type Disabled

IP Address

Username

Password *****

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
01	<input type="text"/>	<input type="text"/>	<input type="text"/>
02	<input type="text"/>	<input type="text"/>	<input type="text"/>
03	<input type="text"/>	<input type="text"/>	<input type="text"/>
04	<input type="text"/>	<input type="text"/>	<input type="text"/>
05	<input type="text"/>	<input type="text"/>	<input type="text"/>
06	<input type="text"/>	<input type="text"/>	<input type="text"/>
07	<input type="text"/>	<input type="text"/>	<input type="text"/>
08	<input type="text"/>	<input type="text"/>	<input type="text"/>
09	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>

Parameter Set-up:

- **Type:** select among three options “**Disabled**” “**WebRelay**” and “**Both**”. Select “**Webrelay**” to enable the web relay. Select “**Disable**” to disable the web relay. Select “**Both**” to enable both local relay and web relay.
- **IP Address:** enter the we relay IP address provided by the web relay manufacturer.
- **User Name:** enter the User name provided by the web relay manufacturer.
- **Password:** enter the password provided by the web relay manufacturer. The passwords is authenticated via HTTP and you can define the passwords using “**http get**” in Action.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay. Without

adding ip, username, pwd, you can fill in the HTTP command in the web relay action, so you can configure multiple webrelays

- **Web Relay Key:** it can be null or enter the configured DTMF code, when the door is unlock via DTMF code, the action command will be sent to the web relay automatically.
- **Web Relay Extension:** it can be null or enter the relay extension information, which can be a SIP Account user name of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device, while this setting is optional. And please refer to the example below:

<http://admin:admin@192.168.1.2/state.xml?relayState=2>.

13.4. Configure White List for Door Relay

For security, VDP-10M door phone give a permission for who can unlock the door by DTMF code. To do this configuration on the web **Intercom > Relay > Open Relay Via DTMF** interface.

Open Relay Via DTMF

Assigned The Authority For

Only Contacts List ▼

Parameter Set-up:

- Access Phone Numbers: there are three options - Disabled, WhiteList Number and All Number. If Disabled is selected, the DTMF code for unlock can not available during the call. If WhiteList is selected, VDP-10M door phone can only be unlocked by the contacts existed in the phone book. If All Number is selected, all callees can open the door phone during the call by using DTMF code .

14. Door Access Schedule Management

You are required to configure and make schedule for the user-based door access via RF card, Private PIN and Facial recognition.

14.1. Configure Door Access Schedule

You can create door access schedules so that they can be later conveniently applied to the door access control intended for individual user or a group of users created. More over, you can edit your door access schedule if needed.

14.1.1. Manage Door Access Schedule

You can create the door access schedule on a daily or monthly basis and you can also create a schedule that allows you to plan for a longer period of time in addition to running the door access schedule on a daily or monthly basis. To do this configuration on web **Intercom > Schedules** interface.

Schedule Setting

Schedule Type:

Schedule Name:

Date Range: -

Day of Week: Mon Tue Wed Thur
 Fri Sat Sun Check All

Date Time: : - :

Add

Reset

Schedules Management

Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	<input type="checkbox"/>
1	1002	Local	Daily	Never	-	-	-	<input type="checkbox"/>
2	1001	Local	Daily	Always	-	-	00:00:00-23:59:59	<input type="checkbox"/>

Parameters Set-up:

- **Schedule Type:** set the type of time period. There are three types to choose from: Daily, Weekly, and Normal. The default is Daily.
- **Schedule Name:** set the name of the time period.
- **Date Time:** set the corresponding time period.
- **Day of Week:** select the corresponding day of the week. This field will only be displayed when the Week and Normal types are selected.
- **Date Range:** set the corresponding date. This field will only be displayed when the Normal type is selected.



Note:

- For VDP-10M, the operation path is **Setting > Schedule**.

15. Door Unlock Configuration

VDP-10M door phone offer you many types of door access. You can configure them on the device and web interface. More over, you can import or exporting the configured files to maximize your RF card configuration efficiency.

15.1. Configure Access Card Format

If you want to integrate with the third party intercom system in terms of RF card door access, you can change the RF card code format to be identical with that applied in the third party system. You can do this configuration on web **Intercom > Card Setting** interface.

RFID	
IC Card Display Mode	8HN
ID Card Order	Normal
ID Card Display Mode	8HN
ID Card Reading Bytes	3 Bytes

Parameters Set-up:

- **RFID Display Mode:** Select the card code format for the IC card for the door access among five format options: 8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR. The card code format is 8HN by default in the door phone.
- **ICCARD Display Mode:** Select the card code format for the **IC card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR.** The card code format is 8HN by default in the door phone.
- **IDCard Display Mode:** Select the card format for the **ID Card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR.** The card code format is 8HN by default in the door phone.
- **WIEGAND Display Mode :** Select the card format for the **WIEGAND Card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR.** The card code format is 8HN by default in the door phone.

15.2. Configure Access Card for Door Unlock

You can manage the card number and corresponding parameters on web **Intercom > Card Setting** interface.

Card Type Support

IC Support Enabled

ID Support Enabled

Access Setting

Relay

Relay A Relay B

Security Relay A

Web Relay

0

Floor No.

None

All Schedules

1001:Always
1002:Never

Enabled Schedules

1001:Always



Parameters Set-up:

- **IC/ID Enable:** to active the IC or ID card type.
- **Card Status:** select “**Car Issuing**” in the field before adding the RFID card and change the status back to “**Normal**” after the card is added.
- **IC key DoorNum:** select the relay switch available for the RIFD card door access.

- **IC Key Tags:** select the frequency of the validity the RFID card for the door access among three options: “**Allow**” “**Schedule**” and “**Forbidden**” For example, if you select “**Allowed**” then the card is always valid for unlimited door access according to your setting. If you select “**Schedule**” you are required to set up the specific time of the RFID card access validity. If you select “**Forbidden**” then the RFID card will never be valid for the door access.
- **Frequency:** if select the Tags as “**schedule**”, you also need to set up the using frequency which means the number of times the card can be used in a special time period.
- **IC key Code:** find the RFID card code in the field.
- **Schedule Management:** select an available time for the card from All Schedule to Enable Schedule.



Note:

- RF card with 13.56 MHz 125 Khz can be applicable to the door phone for the door access.

15.3. Import and Export CardData of Access

Control

VDP-10M door phone support card data of access control to shared among Omny door phones through import and export while you can also export the card data out of the door phone and then import to a third party device on web **Intercom > User** interface.

Import/Export User

User Data (.tgz)	<input type="button" value="Выберите файл"/>	Файл...бран	<input type="button" value="Import"/>	<input type="button" value="Export"/>
AES Key For Import	<input type="text" value="*****"/>			

15.4. Configure Open Relay via HTTP for Door

Unlock.

You can unlock the door remotely without approaching the device physically for the door access by typing in the created the HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for the door access. To do this configuration on web Intercom > Relay

Open Relay Via HTTP

Enabled	<input checked="" type="checkbox"/>
Session Check	<input type="checkbox"/>
UserName	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>

Parameter set-up:

- **Enabled:** enable the HTTP command unlock function by clicking on Enable field.
- **Session Check:** this feature is for some network security limitation, if you enable it , the door may not be unlocked by this w
- **User Name:** enter the user name of the device web interface, for example “admin”.
- **Password:** enter the password for the HTTP command. For example : “12345”

Example:

http://192.168.1.100/fcgi/do?action=OpenDoor&UserName=admin&Password=admin&DoorNum=1

For High Security Mode

Example_1:

http://admin:admin@192.168.1.100/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

Example_2:

http://192.168.1.100/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

15.5. Configure Exit Button for Door Unlock

When you need to open the door from inside using the Exit button installed by the door, you can configure the door phone Input to trigger the relay for the door access on web **Intercom > Input** interface.

Input A

Enabled	<input type="checkbox"/>
Trigger Electrical Level	<input type="text" value="Low"/>
Action To Execute	FTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP <input type="checkbox"/> SIP Call <input type="checkbox"/>
HTTP URL	<input style="width: 100%;" type="text"/>
Action Delay	<input style="width: 100%;" type="text" value="0"/> (0~300 Sec)
Action Delay Mode	<input type="text" value="Unconditiona"/>
Execute Relay	<input type="text" value="None"/>
Door Status	A: High

Parameter set-up:

- **Enabled:** Select “ **Enable** “ to be able to use the Input function.
- **Trigger Option:** Select the trigger options according the actual operation on the exit button.
- **Action To Execute:** select the method to carry out the action among four options: FTP, Email, HTTP, TFTP.
- **Http URL:** enter the URL if you select the HTTP to carry out the action.
- **Action Delay:** set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds., then the corresponding actions will be carried out 5 seconds after your press the button.
- **Execute Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of input signal.

15.6. Configure PIN Code for Door Unlock

On the web interface, you can create the PIN code and customize additional settings, such as defining the door access schedule to determine when the code is valid and specifying which relay to open.

To enable the private PIN code on the web Intercom > PIN Setting > Private PIN interface

Private PIN

Enabled

To configure it on the web Intercom > User interface. Click Add.

User Basic

User ID	<input type="text" value="20"/>
Name	<input type="text" value="10"/>
Role	<input type="text" value="general user"/> ▼

Private PIN

Code	<input type="text"/>
------	----------------------

15.7. Configure Public Key for Door Unlock

Public PIN code is configured and used by the property in the same building or in the same community. To do this configuration on the web Intercom >PIN Settingc

(3~8 digits, press #PIN Code# to unlock)

Enabled	<input checked="" type="checkbox"/>
PIN Code	<input type="text" value="*****"/> (3~8 digits, press #PIN Code# to unlock)
Admin Code	<input type="text" value="*****"/> (Press *Admin Code # to modify the public PIN)

Parameter set-up:

- **Pin code:** customize 3-8 digit numbers for public key value.

16. Security

16.1. Tamper Alarm Setting

Tamper alarm function serves as a protection against any unauthorized removal of the devices by triggering off the temper alarm while sending out calls to the designated location. Tamper alarm will be triggered off when the door phone changes its gravity value as opposed to its original gravity value set up when the device is installed.

Tamper Alarm

Enabled	<input type="checkbox"/>
Gravity Sensor Threshold	<input type="text" value="32"/> (0~127)
Trigger Options	<input type="text" value="Only Alarm"/> ▼

Parameter Set-up:

- **Enabled:** click to select “ON “ in the Tamper Alarm field in order to enable the anti-theft alarm function.
- **Gravity Sensor Threshold:** set the threshold for the gravity sensory sensitivity. The lower the value is, the more sensitive the gravity sensor. The gravity sensor value is 32 by default.

16.2. Motion Detection

Motion Detection is often used for unattended surveillance video and automatic alarm. The images collected by the camera at different frame rates will be calculated and compared by the CPU according to a certain algorithm. When the picture changes, if someone walks by, the lens is moved, the number obtained by the calculation and comparison result will exceed the threshold and indicate that the system can the corresponding processing is made automatically.

16.2.1. Configure Motion Detection

You can turn on the motion detection and set up the motion detection interval on the device.

Motion Detection Options

Suspicious Moving Object Detection	<input style="width: 100%;" type="text" value="Disabled"/>
Timing Interval	<input style="width: 100%;" type="text" value="10"/> (0~120 Sec)

Motion Detect Time Setting

Day	<input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thur <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun <input type="checkbox"/> Check All
Start Time - End Time	<input style="width: 30px;" type="text" value="00"/> : <input style="width: 30px;" type="text" value="00"/> - <input style="width: 30px;" type="text" value="23"/> : <input style="width: 30px;" type="text" value="59"/>

Parameter Set-up:

- **Suspicious Moving Object Detection:** To enable or disable Motion Detection.

- **Timing Interval:** set the time interval for the motion detection. If you set the default time interval as “**10**” Sec, then the motion detection time span will be 10 seconds. Assuming that we set the time interval as “**10**” then, and the first movement captured can be seen as start point of the motion detection, and if the movement continues through 7 seconds of the 10 second interval, then the alarm will be triggered at 7 seconds (the first trigger point) and motion detection action can be triggered (sending out notification) any where between **7-10** seconds once the movement is detected. “10” Sec interval is a complete cycle of the motion detection before it starts another cycle of the same time interval. To be more specific, the first trigger point can be calculated as the “ **Time interval minus three**”

16.3. Security Notification Setting

16.3.1 Email Notification Setting

If you want to receive the security notification via email, you can configure the Email notification on the web **Intercom > Action > Email Notification** interface properly. The email notification will show as the captures.

Email Notification

Sender's Email Address	<input type="text"/>
Receiver's Email Address	<input type="text"/>
SMTP Server Address	<input type="text"/>
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password" value="*****"/>
Email Subject	<input type="text"/>
Email Content	<input type="text"/>
Email Test	<input type="button" value="Email Test"/>

Parameter set-up:

- **Sender's email address:** enter the sender's email address from which the email notification will be sent out.
- **Receiver's Email Address:** enter the receiver's email address.
- **SMTP Server Address:** enter the SMTP server address of the sender.
- **SMTP User Name:** enter the SMTP user name, which is usually the same with sender's email address.
- **SMTP Password:** configure the password of SMTP service, which is same with sender's email address.
- **Email Subject:** enter the subject of the email.

- **Email Content:** compile the emails contents according to your need

 **Note:**

- For VDP-10M, the operation path is **Setting > Action > Email Notification**

16.3.2. FTP Notification Setting

If you want to receive the security notification via FTP, you can configure the FTP notification on the web **Intercom > Action > FTP Notification** properly.

FTP Notification

FTP Server	<input type="text"/>
FTP User Name	<input type="text"/>
FTP Password	<input type="password" value="*****"/>
FTP Test	<input type="button" value="FTP Test"/>

Parameter set-up:

- **FTP Server:** enter the address (URL) of the FTP server for the FTP notification.
- **FTP User Name:** enter the FTP server user name.
- **FTP Password:** enter the FTP server password.

16.3.3. SIP Call Notification Setting

In addition to FTP and Email notification, the door phone can also make a SIP call when some feature action is triggered. To configure a SIP call notification on web **Intercom > Action > SIP Call Notification** interface.

SIP Call Notification

SIP Call Number	<input type="text"/>
SIP Caller Name	<input type="text"/>

Parameter Set-up:

- **SIP Call Number:** To configure SIP call number.
- **SIP Call Name:** To configure display name of door phone.

 **Note:**

- For VDP-10M, the operation path is **Setting > Action > SIP Call Notification**

Parameter Set-up:

- **Http URL:** tick the check box to enable HTTP URL notification.
- **HTTP URL:** If you choose HTTP mode, enter the URL format: [http://http_server IP address/any information](http://http_server_IP_address/any_information).

16.4. Security Action Configuration

16.4.1. Configure Push button Action

When pressing the push button, the door phone will trigger the pre-configured action type, the notification can be sent out by the Email, FTP notification or a SIP call. To do this configuration on web **Intercom > Basic** interface

Trigger Relay By Speed Dial or Manager Dial

Relay ID Relay A Relay B

Parameter Set-up:

- **Action to execute:** To choose which action to be executed after triggering.

16.4.2. Configure Motion Action

When the Motion Detection feature is working , you can make it trigger an action. To do this configuration on web **Intercom > Motion** interface.

Action To Execute

Action To Execute FTP Email SIP Call HTTP
HTTP URL

Parameter Set-up:

- **Action to execute:** To choose which action to be executed after triggering.

 **Note:**

- For VDP-10M, the operation path is **Surveillance > Motion**

16.4.3. Configure Input Action

When Input interface is working , it can also trigger an action. You can do this configuration on web **Intercom > Input** interface.

Input A

Enabled

Trigger Electrical Level

Action To Execute FTP Email HTTP SIP Call

HTTP URL

Action Delay (0~300 Sec)

Action Delay Mode

Execute Relay

Parameter Set-up:

- **Action to execute:** To choose which action to execute after triggering.

 **Note:**

- For VDP-10M, the operation path is **Access Control> Input**

16.5. Voice Encryption

SRTP(Secure Real-time Transport Protocol) is a protocol defined on the basis of Real-time Transport Protocol. The data of the transmission protocol provides encryption, message authentication, integrity assurance and replay protection. To configure this feature on web **Account > Advanced > Encryption** interface.

Encryption

Voice Encryption(SRTP)

Parameter Set-up:

- **Voice Encryption(SRTP):** choose **Disabled**, **Optional** or **Compulsory** for SRTP. If it is **Optional** or **Compulsory**, the voice during the call is encrypted, and you can grab the RTP packet to view

16.6. User Agent

You can customize user agent field in the SIP message. if user agent is set to specific value, users can see the information from PCAP. If user agent is blank, by default, users can see the company name “Mycompany”, model number and firmware version from PCAP.

User Agent

User Agent

Parameter Set-up:

- **User Agent:** support to enter another specific value, Mycompany is by default.

17. Monitor and Image

17.1. RTSP Stream Monitoring

OMNY door phones support RTSP stream that allows intercom devices such as indoor monitor or the monitoring unit from the third party to monitor or obtaining the the real time audio/ video (RTSP stream) from the door phone using the correct URL.

17.1.1. RTSP Basic Setting

You are required to set up RTSP function on device web **Intercom > RTSP > RTSP Basic** interface in terms of RTSP Authorization, authentication and password etc before you are able to use the function.

RTSP Basic	
Enabled	<input checked="" type="checkbox"/>
RTSP Authorization Enabled	<input type="checkbox"/>
MJPEG Authorization Enabled	<input checked="" type="checkbox"/>
Authentication Mode	<input type="text" value="Digest"/>
Username	<input type="text" value="admin"/>
Password	<input type="text" value="*****"/>

Parameter Set-up:

- **Enable:** click on Enable and Disable in **RTSP Enable** field to turn on or turn off the RTSP function.
- **RTSP Authorization:** click on Enable and Disable in RTSP Authorization field to enable or disable the RTSP authorization. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP Username, RTSP Password on the intercom device such as indoor monitor for authorization.

- **Username:** enter the name used for RTSP authorization.
- **Password:** enter the password for RTSP authorization.
- **Authentication Mode:** select RTSP authentication type between “ **Basic**” and “ **Digest**”. “ **Basic** ” is the default authentication type.



Note:

- For VDP-10M, the operation path is **Intercom > RTSP**.

17.1.2. RTSP Stream Setting

You can select the video codec format for the RTSP stream for the monitoring and configure video resolution and bit-rate etc based on your actual network environment on the web **Intercom > RTSP > RTSP stream** interface.

RTSP Stream	
Audio Enabled	<input checked="" type="checkbox"/>
Video Enabled	<input type="checkbox"/>
2nd Video Enabled	<input checked="" type="checkbox"/>
Audio Codec	PCMU ▼
Video Codec	H.264 ▼
2nd Video Codec	H.264 ▼

Parameter Set-up :

- **Audio Enabled** : tick to enable RTSP audio which means , the door phone can also send audio information to the monitor by RTSP.
- **Video Enabled** : the door phone can send the video information to the monitor. After enabling RTSP feature, the video RTSP is enabled by default and can not be modified.

- **2nd Video Enabled** : VDP-10M door phones support 2 RTSP streams, you can enable the second one.
- **Audio Codec** : choose a suitable audio codec for RTSP audio.
- **Video Codec** : choose a suitable video codec for RTSP video.

H.264 And H.265 Video Parameters

Video Resolution	4CIF ▼
Video Framerate	30 fps ▼
Video Bitrate	2048 kbps ▼
2nd Video Resolution	VGA ▼
2nd Video Framerate	30 fps ▼
2nd Video Bitrate	512 kbps ▼

Parameter Set-up:

- **Video Resolution:** select video resolutions among seven options: **,"CIF",,"VGA",,"4CIF",,"720P", 1080P"** . The default video resolution is **"4CIF"**. and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than **"4CIF"**.
- **Video Framerate:** **"30fps"** is the video frame rate by default.
- **Video Bitrate:** select video bit-rate among six options: **"128 kbps", "256kbps", "512 kbps", "1024 kbps", "2048 kbps", "4096 kpbs"** according to your network environment. The default video bit-rate is **" 2048 kpbs"**.
- **2nd Video Resolution:** select video resolution for the second video stream channel. While the default video solution is **"VGA"**.
- **2nd Video Framerate:** select the video framerate for the second video stream channel. **"25fps"** is the video frame rate by default for the second video stream channel.
- **2nd Video Bitrate:** select video bit-rate among the six options for the second video stream channel. While the second video stream channel is **"512 kpbs"** by default.

17.1.3. RTSP OSD Setting

This feature is used to add watermark to the RTSP video or picture. To protect the owner of the video or image. To do this configuration on the web Intercom > RTSP > RTSP OSD Setting interface.

RTSP OSD Setting

RTSP OSD Enabled	<input type="checkbox"/>
RTSP OSD Color	<input type="text" value="White"/>
RTSP OSD Text	<input type="text"/>

Parameter Set-up:

- **RTSP OSD Color:** there are five color options - White, Black, Red, Green,Blue for RTSP watermark text.
- **RTSP OSD Text:** enter the customized text you want to show for the watermark.

17.2. MJPEG Image Capturing

OMNY door phones allow you to capture the Mjpeg format monitoring image if needed. You can enable the Mjpeg function on **Intercom > RTSP > RTSP Basic** and set the image quality on the web **Intercom > RTSP > MJPEG Video Parameters** interface.

RTSP Basic

Enabled	<input checked="" type="checkbox"/>
RTSP Authorization Enabled	<input type="checkbox"/>
MJPEG Authorization Enabled	<input checked="" type="checkbox"/>
Authentication Mode	<input type="text" value="Digest"/>
Username	<input type="text" value="admin"/>
Password	<input type="text" value="*****"/>

MJPEG Video Parameters

Enabled	<input checked="" type="checkbox"/>
Video Resolution	<input type="text" value="VGA"/>
Video Framerate	<input type="text" value="30 fps"/>
Video Quality	<input type="text" value="90"/>

Parameter Set-up:

- **MJPEG Authorization:** tick it to access device video or real-time screenshots through a browser, http address such as:
http://device_IP:8080/video.cgi - (dynamic video),
http://device_IP:8080/picture.jpg - (static screenshot)
- **Video Resolution:** select video resolutions among seven options: "CIF", "VGA", "4CIF", "720P", "1080P". The default video resolution is "4CIF". and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than "4CIF".
- **Video Framerate:** "30fps" is the video frame rate by default.
- **Video Quality:** the video bitrate, from 50 to 90.



Note:

- For VDP-10M, the operation path is **Intercom > RTSP > MJPEG Video Parameters**

17.3. ONVIF

Real-time video from the door phone camera can be searched and obtained by the OMNY indoor monitor or by the third party devices such as NVR (**Network Video Recorder**) you can configure the ONVIF function on the web **Intercom > ONVIF** interface so that other device will be able to see the video from the door phone.

Basic Setting

Discoverable	<input checked="" type="checkbox"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>

Parameter Set-up:

- **Discoverable:** tick the check box to enable the Discoverable ONVIF mode. If you select “ **Discoverable**” then the video from the door phone camera can be searched by other devices.
- **Username:** enter the user name. The user name is “ **admin**” by default.
- **Password:** enter the password. The password is “ **admin**” by default.

After the setting is complete, you can enter the ONVIF URL on the third party device to view the video stream.

For example: http://IP address:80/onvif/device_service



Note:

Fill in the specific IP address of the door phone in the URL.

17.4. Live Stream

If you want to check the real-time video from the door phone, you can go to the the device web **Intercom > Live Stream** interface to obtain the real-time video or you can also enter the correct URL on the we browser to obtain it directly.

To check the real time video using URL, you can Enter the correct URL (**http://IP_address:8080/video.cgi**) on the web browser if you want to obtain the real-time video directly instead of going to the web interface.



Note:

- For VDP-10M, the operation path is **Surveillance > Live Stream**

18. Logs

18.1. Call Logs

If you want to check on the calls inclusive of the dial-out calls , received calls and missed calls in a certain period of time, you can check and search the call log on the device web **Phone > Call Log** interface.

The screenshot shows the 'Call Log' interface. At the top, there is a 'Save Call Log Enabled' checkbox which is checked. Below it is a 'Call History' dropdown menu set to 'All' and a red 'Hang Up' button. There are two date pickers for 'Time' with the format 'DD.MM.YYYY'. Below that is a 'Name/Number' search field with a 'Search' button and an 'Export' button. The main part of the interface is a table with the following data:

Index	Type	Date	Time	Local Identity	Name	Number
1	Dialed	2025-03-14	16:21:54	172.31.170.1 24@172.31.17 0.124	172.31.170.18	172.31.170.1 8@172.31.170 .18
2	Dialed	2025-03-14	16:21:00	172.31.170.1 24@172.31.17 0.124	172.31.170.18	172.31.170.1 8@172.31.170 .18

Parameter Set-up:

- **Call History:** select call history among four options: “All”, “Dialed” “ Received” “ Missed” for the specific type of call log to be displayed.
- **Hangup:** to hangup the call from web.
- **Index:** the order of the call logs.
- **Date:** the date for the call log.
- **Time:**the time for the call log.
- **Name/Number:** the name and number for the contact.

 **Note:**

- For VDP-10M, the operation path is **Intercom > Call Log**.

18.2. Door Logs

If you want to search and check and import/export on the various types of door access history, you can search and check the door logs on the device web **Phone > Door Log** interface.

Door Log

Save Door Log Enabled

Status All

Time ДД.ММ.ГГГГ - ДД.ММ.ГГГГ

Name/Code Search Export

Index	Name	Code	Type	Date	Time	Status	<input type="checkbox"/>
1	Visitor	F00000000000000000	Card	2025-02-12	14:50:47	Failed	<input type="checkbox"/>
2	Visitor	F00000000000000000	Card	2025-02-12	14:50:46	Failed	<input type="checkbox"/>
3	Visitor	F00000000000000000	Card	2025-02-12	14:50:41	Failed	<input type="checkbox"/>
4	Visitor	F00000000000000000	Card	2025-02-12	14:50:39	Failed	<input type="checkbox"/>
5	Visitor	F00000000000000000	Card	2025-02-	14:50:38	Failed	<input type="checkbox"/>

Parameter Set-up:

- **Index** : **the order of** the call logs.
- **Name** : If it is a locally added key or card, the corresponding added name will be displayed. If it is an unknown key or card, it will display Unknown.
- **Code** : If opening the door via PIN code, the corresponding PIN code will be displayed. If opening the door via RF cards, the corresponding card number will be displayed, and if the door is opened by HTTP command, it will be empty.
- **Type** : If opening the door via PIN code, **Password** will be displayed. If opening the door via RF cards, **Card** will be displayed, and if the door is opened by HTTP command, **Http** will be displayed.
- **Date** : The date for opening the door.
- **Time** : the time for opening the door.
- **Status** : the door opening result **Success** or **Failed**.

 **Note:**

- For VDP-10M, the operation path is **Access Control > Door Log**.

19. Debug

19.1.Event Log

It is used to export device-specific logs (calling, card issue, door opening, download application configuration files for upgrading, network configuration, hacker incidents, etc.) to the remote server. To configure it on web **Upgrade > Advanced > System Log** interface.

System Log

Log Level	3 ▾
Export Log	Export
Remote System Log Enabled	<input type="checkbox"/>
Remote System Server	<input type="text"/>
Remote System Port	<input type="text"/>

Parameter Set-up:

- **Log Level:** select log levels from 1 to 7 levels. You will be instructed by OMNY technical staff about the specific log level to be entered for debugging purpose. The default log level is “5”. the higher the level is, the more complete the log is.
- **Remote System Log Enabled:** select “Enable” or “Disable” if you want to enable or disable the remote system log.
- **Remote System Server:** enter the remote server address to receive the the device **log**. And the remote server address will be provided by OMNY technical support.
- **Remote System Port:** the port of remote server.

the device **log**. And the remote server address will be provided by OMNY technical support.



Note:

- For VDP-10M, the operation path is **Upgrade > Diagnose > System Log**.

19.3. PCAP

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purpose. You can set up the PCAP on the device web **Upgrade > Advanced > PCAP** interface properly before using it.

PCAP

Specific Port	<input style="width: 100%;" type="text"/> (1~65535)
PCAP	Start Stop Export
PCAP Auto Refresh	<input type="checkbox"/>
New PCAP	Start

Parameter set-up:

- **Specific Port:** select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** click **Start** tab and **Stop** tab to capture the a certain range of data packets before clicking **Export** tab to export the data packets to you Local PC.
- **PCAP Auto Refresh:** select “**Enable**” or “**Disable**” to turn on or turn off the PCAP auto fresh function. If you set it as “**Enable**” then the PCAP will continue to capture data packet even after the data packets reached its
- **New PCAP:** click Start to capture bigger data package.

1M maximum in capacity. If you set it as “ **Disable**” the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.



Note:

- For VDP-10M, the operation path is **Upgrade > Advanced > PCAP**.

20. Firmware Upgrade

Firmwares of different versions for door phone can be upgraded on the device web **Upgrade > Basic** interface.

Firmware Version	320.143.10.212
Hardware Version	320.0
Upgrade	<input type="text" value="Выберите файл"/> Файл не выбран Reset: <input type="checkbox"/> Upgrade Cancel
Reset To Factory Setting	Reset
Reboot	Reboot

Parameter Set-up:

- **Upgrade:** Choose .rom firmware from your PC, then click **Submit** to update.

21. Backup

Configuration files can be imported to or exported out of the device to your local PC on the device web **Upgrade > Advanced > Others** interface if needed.

Others

Config File(.tgz/.conf/.cfg) Выберите файл Файл не выбран

Export (Encrypted)

Import **Cancel**

Parameter Set-up:

- **Export Config File:** to export current config file.
- **Export/Import:** to export current config file (Encrypted) or import new config file.



Note:

- For VDP-10M, the operation path is **Upgrade > Advanced > Others**.

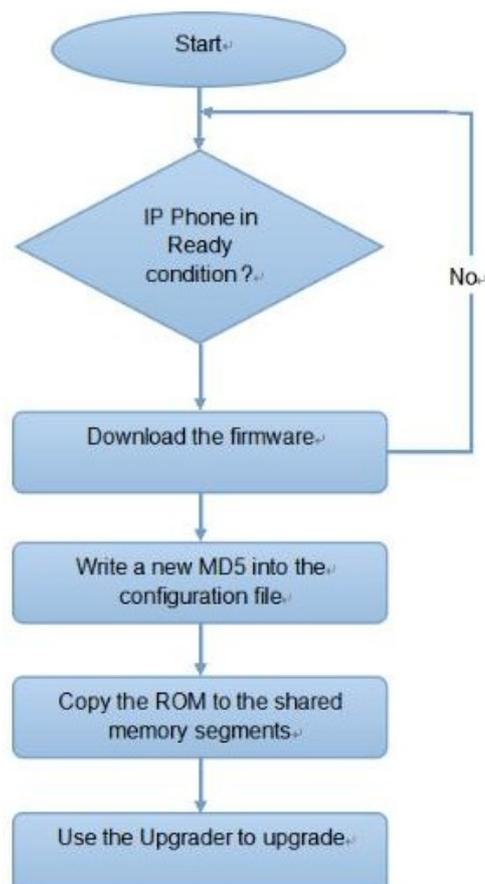
22. Auto-provisioning via Configuration

File

Configurations and upgrading on OMNY door phone can be done on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configuration needed one by one manually on the door phone.

22.1. Provisioning Principle

Auto-provisioning is a feature used to configure or upgrade the devices in batch via third party servers. **DHCP, PNP, TFTP, FTP, HTTPS** are the protocols used by the OMNY intercom devices to access the URL of the address of the third party server which stores configuration files and firmwares, which will then be used to update the firmware and the corresponding parameters on the door phone.



22.2. Configuration Files for Auto-provisioning

Configuration files have two formats for the auto-provisioning. one is the general configuration files used for the general provisioning and other one is the MAC-based configuration provisioning.

The difference between the two types of configuration files is shown as below:

- **General configuration provisioning:** a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices. For example : r000000000010m.cfg.
- **MAC-based configuration provisioning:** MAC-based configuration files is used for the auto-provisioning on a specific device as distinguished by its unique MAC number. And the configuration files named with device MAC number will be matched automatically with the device MAC number before being downloaded for the provisioning on the specific device.

To get the Autop configuration file template on **Upgrade > Advanced > Automatic Autop** interface.

Automatic Autop

Mode	<input type="text" value="Power On"/>
Schedule	<input type="text" value="Sunday"/>
	<input type="text" value="22"/> (0~23 hour)
	<input type="text" value="0"/> (0~59 min)
Clear MD5	<input type="button" value="Clear"/>
Export Autop Template	<input type="button" value="Export"/>



Note:

- If a server has these two types of configuration files, then IP devices will first access the general configuration files before accessing the MAC-based configuration files.

22.3.AutoP Schedule

We provides you with different Autop methods that enable the door phone to perform provisioning for itself in a specific time according to your schedule.

Automatic Autop

Mode	<input type="text" value="Power On"/>
Schedule	<input type="text" value="Sunday"/>
	<input type="text" value="22"/> (0~23 hour)
	<input type="text" value="0"/> (0~59 min)

Parameter Set-up:

- **Mode:** select “**Power on**”, “ **Repeatedly**”, “**Power On + Repeatedly**”, “**Hourly Repeat**” as your Autop schedule.
 Select “**Power on**”, if you want the device to perform Autop every time it boots up.
 Select “ **Repeatedly**”, if you want the device to perform Autop according to the schedule you set up.
 Select “**Power On + Repeatedly**”, if you want to combine **Power On** Mode and **Repeatedly** mode that will enable the device to perform Autop every time it boots up or according to the schedule you set up.
 Select “**Hourly Repeat**”, if you want the device to perform Autop every hour.

22.4.PNP Configuration

Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user. To do this configuration on web **Upgrade > Advanced > PNP Option** interface.

PNP Option

PNP Config Enabled



22.5.Static Provisioning Configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an autop schedule is set up, the door phone will perform the auto provisioning on a specific timing according to Autop schedule you set up. In addition,TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration.

Manual Autop

URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>
Common AES Key	<input type="password" value="*****"/>
AES Key(MAC)	<input type="password" value="*****"/>

AutoP Immediately

Parameter set-up:

- **URL:** set up tftp , http , https , ftp server address for the provisioning
- **User Name:** set up a user name if the server needs an user name to be accessed to otherwise leave it blank.
- **Password:** set up a password if the server needs a password to be accessed to otherwise leave it blank.

- **Common AES Key:** set up AES code for the intercom to decipher general Auto Provisioning configuration file.
- **AES Key (MAC):** set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

 **Note:**

- AES is one type of encryption, it should be configured only when the config file is encrypted with AES, otherwise leave the field blank.

 **Note:**

Server Address format:

- TFTP: tftp://192.168.0.19/
- FTP: ftp://192.168.0.19/ (allows anonymous login)
- ftp://username:password@192.168.0.19/(requires a user name and password)
- HTTP: <http://192.168.0.19/> (use the default port 80)
- http://192.168.0.19:8080/ (use other ports, such as 8080)
- HTTPS: https://192.168.0.19/ (use the default port 443)

 **Tip:**

- Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

23. Integration with Third Party Device

23.1. Integration via Wiegand

If you want to integrate OMNY door phone with the third party devices via Wiegand, you can configure the Wiegand on the web interface.

Wiegand Card Reader Mode	Wiegand-26 ▼
Wiegand Transfer Mode	Input ▼

Parameter set-up:

- **Wiegand Type:** set the wiegand data transmission format among three options: **Wiegand 26**, **Wiegand 34**, **Wiegand 58**. The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand Mode:** set the Transfer mode between **Input** or **Output** if the door phone is used as a receiver then set it as “Input” for the door phone and vice versa.

23.2. Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third party device with the OMNY intercom device. You can configure the HTTP API function on the web **Intercom > HTTP API** interface for the integration.

HTTP API

Enabled	<input checked="" type="checkbox"/>
Authorization Mode	Digest
Username	admin
Password	*****
1st IP	
2nd IP	
2rd IP	
4th IP	
5th IP	

Parameter Set-up:

- **HTTP API:** select “**Enable**” or “**Disable**” to enable or disable the HTTP API function for the third party integration. For example, if the function is disabled any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Auth Mode:** select among four options: “**None**” “**WhiteList**” “**Basic**”, “**Digest**” for authorization type, which will be explained in detail in the following chart.
- **User Name:** enter the user name when “**Basic**” and “**Digest**” authorization mode is selected. The default user name is “Admin”.
- **Password:** enter the password when “**Basic**” and “**Digest**” authorization

mode is selected. The default user name is “Admin”.

- **IP01-IP05:** enter the IP address of the third party devices when the “WhiteList” authorization is select for the integration.

Please refer to the following description for the Authentication mode

NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by OMNY only.
3	WhiteList	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The whitelist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the User name and the password for the authentication. In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.
5	Digest	Password encryption method, only supports MD5. MD5(Message-Digest Algorithm) In Authorization field of Http request header: WWW-Authenticate:Digest realm="HTTPAPI",qop="auth,auth-int",nonce=" xx", opaque="xx".

6	Token	This mode is used by OMNY only.
----------	--------------	---------------------------------

24. Password Modification

24.1. Modifying Device Web Interface Password

To change the default web password on web **Security > Basic** interface. Select "**admin**" for the administrator account and "**User**" for the User Account. Click the **Change Password** tab to change the password.

Web Password Modify

Username

24.2. Configure Web Interface Automatic Logout

It is a protection design. When there is no operation on the website and when the Session Time Out Value time is reached, the website will automatically log out.

Session Time Out

Session Time Out Value (60~14400 Sec)

Parameters Set-up:

- **Session Time Out Value:** The range from 60 to 14400 sec. If there is no operation over the time, you need to log in the website again.

25. System Reboot&Reset

25.1.Reboot

If you want to restart the device system, you can operate it on the device **Upgrade > Basic** web interface as well.

Reboot

Reboot

25.2.Reset

If you want to reset the device system to the factory setting, you can it on the web **Upgrade > Basic** interface.

Reset To Factory Setting

Reset

26. Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatical Provisioning

AES: Advanced Encryption Standard

BLF: Busy Lamp Field

COM: Common

CPE: Customer Premise Equipment

CWMP: CPE WAN Management Protocol

DTMF: Dual Tone Multi-Frequency

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DND: Do Not Disturb

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure Socket Layer

IP: Internet Protocol

ID: Identification **IR:** Infrared

LCD: Liquid Crystal Display

LED: Light Emitting Diode

MAX: Maximum

POE: Power Over Ethernet

PCMA: Pulse Code Modulation A-Law
PCMU: Pulse Code Modulation μ -Law
PCAP: Packet Capture
PNP: Plug and Play
RFID: Radio Frequency Identification
RTP: Real-time Transport Protocol
RTSP: Real Time Streaming Protocol
MPEG: Moving Picture Experts Group
MWI: Message Waiting Indicator
NO: Normal Opened
NC: Normal Connected
NTP: Network Time Protocol
NAT: Network Address Translation
NVR: Network Video Recorder
ONVIF: Open Network Video Interface Forum
SIP: Session Initiation Protocol
SNMP: Simple Network Management Protocol
STUN: Session Traversal Utilities for NAT
SMTP: Simple Mail Transfer Protocol
SDMC: SIP Devices Management Center
TR069: Technical Report069
TCP: Transmission Control Protocol
TLS: Transport Layer Security
TFTP: Trivial File Transfer Protocol
UDP: User Datagram Protocol
URL: Uniform Resource Locator
VLAN: Virtual Local Area Network
WG: Wiegand