Standalone Access Control Device

User Manual

Product Model: ITL-MJ/2MJ-A
Website: www.itlong.com.cn/en
Shenzhen ITLONG Intelligent Technology Co.,Ltd
Service Hotline：+86-755-8667-5996

Chapter 1 Product Overview

1.1 Product Introduction

The device is used for managing the access with the advanced contactless IC card technology and computer network monitoring technology in special area.

1.2 Product Specifications

Chart 1.1 Product Specifications

Power Supply	DC 12V±10%
Working Current	<200mA (do not include the current for electric lock)
Working Environment	－10～60^{o}C; Humidity:20%～93%,no condensation
Storage Environment	－40～60^{o}C; Humidity:20%～96%,no condensation
Signal Input	1chanel magnetic detection; 1chanel exit button
Signal Output	1chanel electric lock control 1chanel backup switch
Open Method	Swipe card, Password, Swipe card+Password
Storage Capacity	IC Card Blacklist: 2000pcs Access Records: 4000pcs
Communication Interface	RS-485, Max transmission distance:1.2km
Response Time	⩽0.3s
Reading	⩾3cm

Range	
Dimension (L*W*H)	120*100*21mm

1.3 Product Picture

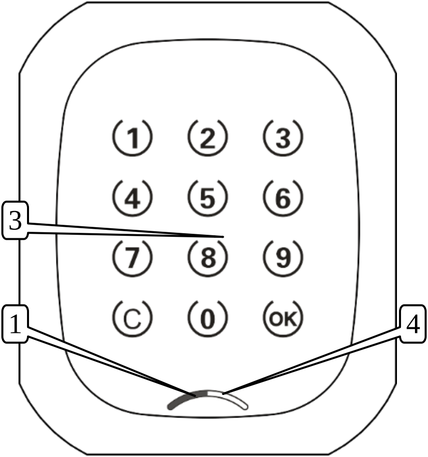


Figure 1.1 Product appearance

1. Status indicator (Red)
2. Card reading indicator (Green)
3. Touch key/ read area

Note: The picture is for reference only.

Chapter 2 System Setup Instructions

2.1 System wiring diagram

According to the actual application, there are two kinds of wiring modes in this system: high-current lock (Figure2.1), low-current lock (Figure2.2).

Instructions:

1.The device connected with the high-current lock:
Cut off PST and GND pin, for JP1: choose NO-COM. The LOCKA and LOCKB are normally open, if swipe the card, they are would be connected for 0.2S, and then cut off.

2. The device connected with the low-current lock:

（1）Power-off unlock: for JP1, choose NO-COM.The LOCKA and LOCKB are normally closed,if swipe the card, they are would be cut-off for 5S (the time can be set by management center), and then connected.

（2）Power-on unlock: for JP1, choose NC-Com The LOCKA and LOCKB are normally open, if swipe the card, they are would be connected for 5S(the time can be set by management center), and then cut off.

3.The device connected with exit button: BUT and GND need to be connected with the exit button. When push the exit button, the device will send the unlocking signal.

4.The power supply for the device provides 2-chanel output for the device and electric lock.

5.If the electric lock start-up current is more than 1A, please use the Figure 2.1 wiring mode; if it is less than 1A, please use the Figure 2.2 wiring mode.

6.For Figure 2.1 wiring mode,the relay may be unnecessary in practical installation.

7.Please follow the instructions to choose interfaces and jumper.

Note: Because of the various electric locks, high voltage pulses generated from the power supply when open or close the electric lock are also different. It is strongly suggested that please use the separated power supply for the electric lock and door access controller!

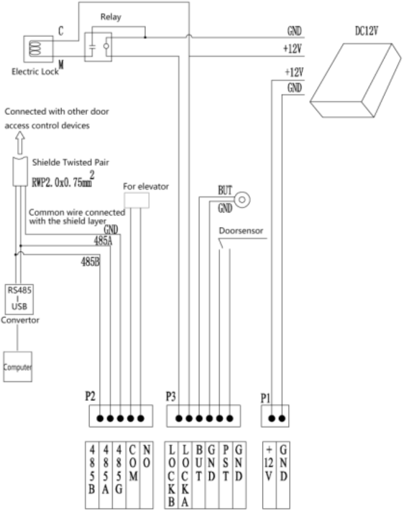


Figure 2.1 high-current lock wiring diagram

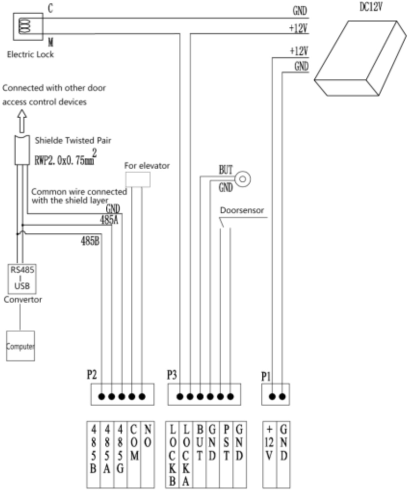


Figure 2.2 low-current lock wiring diagram

2.2 Normally open/closed jumper JP1

It is used for choosing the characteristic of switch signal (open the door signal) outputting

Jumper setting for normally open/closed:
1.Jumper setting for high-current lock as below:

Chart 2.1 Jumper setting for high-current lock

JP1	Open the door signal
NO-COM	Normally open mode
NC-COM	Normally closed mode

Note: Normally open mode should be chosen for high-current lock!

2.Jumper setting for low-current lock as below:

Chart 2.2 Jumper setting for low-current lock

JP1	Open the door signal
NO-COM	Suitable for the power-off unlocking lock
NC-COM	Suitable for the power-on unlocking lock

2.3 Communication terminal resistance jumper JP2

The jumper is used for installing RS-485 bus 120Ω terminal resistance. When the device connected with the management computer via RS-485, and at the end of the RS-485 bus, the jumper must be connected to prevent energy reflections in the communication line.

2.4 Dial switch

SW1-Machine number dial switch

The dial is used to set the device machine number.

Binary encoding is adopted in the setting. The address represented by 1 to 10 dial code is shown as below figure:

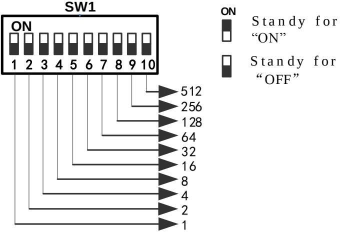
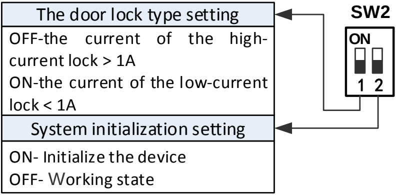


Figure 2.3 The definition diagram of dial switch

Turn to ON stands for "1", turn to OFF stands for "0".
For example: The machine number is 25=1+8+16, the address code is 10011000, so just turn 1,4,5 to ON.
Note: The available machine number range is 1-1023.The dialing codes are not allowed to be set to OFF entirely!

SW2-Function attribute dialing switch
The dial is used to set the door lock type and system initialization.



The door lock type setting

OFF-the current of the high-current lock > 1A

ON-the current of the low-current lock < 1A

System initialization setting

ON- Initialize the device

OFF- Working state

Figure 2.4 The definition diagram of function attribute dialing switch

Turn SW2.1 to "OFF" , the device is deemed to be connected with the high-current lock (pulse electric lock). The description of the corresponding outputting signal as below:

Chart 2.3 The description of high-current lock outputting signal

JP1	Power Off	Power On	Status after reading card successfully
NO-COM	open-circuit signal	open-circuit signal	Recovery after closing 0.2S
NC-COM	closed signal	closed signal	Recovery after opening 0.2S

Note: For the electric lock which unlocked by closure, to prevent burning the lock, it is strongly recommended that do not use NC-COM to short circuit.

Turn SW2.1 to "ON", the device is deemed to be connected with the low-current lock (electric downward mortise lock, Magnetic lock, etc.). The description of the corresponding outputting signal as below:

Chart 2.4 The description of low-current lock outputting signal

JP1	Power Off	Power On	Status after reading card successfully
NO-COM	open-circuit signal	closed signal	Recovery after opening 0.2S
NC-COM	closed signal	open-circuit signal	Recovery after closing 0.2S

Instructions: When the SW2.1= ON, the magnetic signal will be detected when the door access controller is power on (If PST and GND are not closed, LOCKA and LOCKB status would be the same as the status when power off . Only close the PST and GND, the LOCKA and LOCKB output will be contrary to the output when it is power off).
Magnetic signal will also be detected when unlock the door by swiping the authorized card: if the magnetic is not closed, the unlock signal will be output all the time when swiping the authorized card. Only close the magnetic , the lock will be locked. The duration of outputting signal can be adjustable. The duration is 5S by default.

Chapter 3 Installation and Debugging

3.1 Precautions

1. The access control system connects with the network via RS-485 communication mode. In order to guarantee the communication quality, the cables for networking connection should be Shielded Twisted Pair RVVP2*0.75mm^2. The whole construction process is devided into 3 stages: Pipeline laying, installation and wiring, debugging respectively and comprehensively.
2. According to the access control system features, the pipelines of the whole system can be devided into local pipelines and system pipelines. The local pipelines refer to the pipeline laying among the access control device and the power supply, the electronic lock, the exit button, the card reader and other devices. The system pipelines refer to the network pipeline between the access control devices.
3. Please pay attention to the followings on pipelines laying:

(1) The power cord and signal cable (networking cable) should be laying on the different pipe, and the parallel distance of the two pipe should be more than 30cm.

(2) Basically AC 220V power supplied from management center to each access control device, Or get power nearby for the access control device but it should be conform to the standard requirement.

(3) Please do remark when threading cable must be put in the joint of terminal box, if ignore this aspect,it may cause some troubles for installation,debugging.

(4) In the one system, all the wires must be the same type.

(5) Please Note that the access control device can not be

installed in the metal surface, because the metal surface and confined environment will interfere with the Bluetooth.

(6) The connection of the controller and electric lock: using 4-core power cord (named as electric lock and magnetic cable). If the electric lock do not have magnetic signal wire, the 2-core power cord could be used, the diameter of it should be equal or more than 0.5mm^2 , RVV2*0.5mm^2. If the electric lock and magnetic cable and the access control device cable in the same pipe, 4-core shielded wire should be used, RVVP4*0.5mm^2 .

(7) The connection of the controller and exit button: using 2-core power cord, the diameter of it should be equal or more than 0.5mm^2 , RVV2*0.5mm^2.

(8) The connection of the controller and exit button: using 2-core power cord, the diameter of it should be equal or more than 0.5mm^2 , RVV2*0.5mm^2.

(8) The connection of the controller and power supply: the diameter of the cord should be equal or more than 0.75mm^2, RVV2*0.75mm^2.

(9) An active relay signal amplifier should be added if the path of the network connection is over 1.2km or when there is a branch on the way.

(10) In order to guarantee the quality of communication, the ground line between the access control devices is required to be connected together by the shielded grid when the system is connected with network.

For (1), (3), (5), (6), (8), (9), (10), (11) , please strictly abide by them when cabling and designing the location for the device. If not, there will be explicit or implicit errors, even inexplicable errors, until then, there will be no way to solve it except rework.

3.2 Device installation location

1. The device installation location: The device is usually installed on the right side of the door, 1.4 meters away from the ground, 3 to 5cm from the door frame, and the two devices should be separated by more than 30cm.
2. Exit button installation location : The button should be installed indoors.The height is depended on the customer requirements.
3. The electric lock location: electric control lock catch and electric clamp lock should be installed on the side of the door frame ; magnetic lock and electric bolt lock should be installed at the top of the door frame ; shear lock should be installed at the bottom of the door frame.
4. Power supply installation location: The device uses specialized power supply,the power supply is generally installed in the indoor ceiling or weak wells.

3.3 Debugging steps

1. Set the device machine number. The machine number is 1 by default. If more than 1 devices are under controlled,by one management center, the machine number should be set(See 2.4 Dial switch). Note:The machine number cannot be repeated.
2. Select the jumper to set the lock driving mode (normally open or normally closed). The jumper depends on the lock power supply mode. (See 2.2 JP1)
3. Set terminal resistance jumper.The setting is applicable.To the case ONLY : If the device were installed at the farthest location from the management center, the jumper should be connected. The device in

the halfway do not need to set the jumper. (See 2.3 JP2).

4. When the power is on, the indicator light (red light) will flash in the frequency of 1Hz.
5. Push the exit button or swipe the card, the buzzer bleep once,and the door will be open. If the buzzer bleep several times, it indicates that the card authorization is wrong.
6. Open the door via exit button, the door would be closed automatically a few moments later. (The duration can be adjustable by management center)
7. Using management software to set the communication port for door control device and computer, and set the number of the device, download time and other operations . (See the management software instructions)
8. Please swipe the management card on the device first, then the user cards can be used to open the door.

3.4 Read card

Management card is the carrier of storing key.When the system is first installed and used,only read the management card first, then the other cards can be read. Put the management card into the induction range of the device , if the buzzer bleep once, it means that the management card is the right one; if the buzzer bleep rapidly , it means that the controller was set by other management card before. In order to use the management card, the controller need to be initialized.

Note: If the system is networking, you can do the settings via management center. If the system is offline, you can do the settings after reading the management card via the device. The details as below:

Read the management card first and enter the following command format through the keyboard:

Chart 3.1 Command Format

Command code (1 bit)	Command parameters	Command code (1 bit)	OK(#)

The 2 command codes should be consistent, codes as below:

0——Set the time of the access control system

1——Set the door open duration time

4——Set the access password

9——Initialize the access control system

After the user enters the command as the above format, please push “OK(#)”. The reader will check the command. If wrong,the buzzer would bleep rapidly. The user should swipe the management card again, and enter the correct command, if correct, the buzzer will bleep once, it means that the command is is successfully executed. If the user found errors when entering the command, please push “C” and then swipe the management card again, and enter the correct command.

1. Set the time of the access control system

After reading the management card, please enter the command as below to set and correct the time:

Chart 3.2 The command format of setting time

Command code	Year		Month		Date		Hour		Minute		Second		Year		Month		Date		Hour		Minute		Second		Command code
0																									0

The 2 times should be consistent. Each “x” stands for one keypad bit, the command includes 26 bits totally.

Each field must follow the actual time requirements:

For year range, it is 00～99, 20 will be filled in by the reader.

For month range, it is 01～12.

For date range, it is 01～31.

For hour range, it is 01～23.

For minute and second range,both of them are 00～59.

For example: 2016,January,1th,12:00 O'clock, the command code is 0 16 01 01 12 00 00 16 01 01 12 00 00 0, then push "OK".

2. Set the door open duration time

The opening duration can be set within 1-255 seconds. After reading the management card, please enter the command as below to set the door open duration time:

Chart 3.3 The command format of setting the delay time

Command code	Time domain	Time domain	Command code
1			1

The 2 time domains should be consistent,and the reader will check them. 1-3 keypad bits for time domain.

3. Set the password

The device supports password to open the door. If the user forget bringing the card, the users can enter the password.The password can be set via management center or the reader. After reading the management card, please enter the command as below to set the password:

Chart 3.4 The command format of setting the password

Comm	Group	Pass-	Group	Pass-	Comm-

-and code	No.	word	No.	word	and code
4	x	xxxx xxxx	x	xxxx xxxx	4

The above 2 Group No. and the password should be consistent, and the device will check them.1 keypad bit for the Group.No, the range is 0~9. It means the maximum password that users can set for the reader is 10. Every password has 8 keypad bits, the range is 00000000-99999999. The users can open the door by using the password after finishing set.

Note: The Group 9 password is set for sending signal. If the users is coerced to open the door, please use the Group9 password, the device unlock the door and send record to the management center at the same time.

Chart 3.5 The command format of deleting the password

Command code	Group No.	Group No.	Command code
4			4

The 2 Group No.should be consistent, and the device will check them. 1 keypad bit for the Group.No, the range is 0~9. The user can not open the door by using the deleted password.

4. Initialize the access control system

Initialization will clear some parameter, such as black list, holiday schedule, opening time, please carefully use it.

Chart 3.6 The command format of initializing

Comm -and code	Command parameters	Comm -and code

9	0	1	2	3	4	5	6	7	9

3.5 Read the user card

1. Read card

The buzzer bleep once, the door will be open.If the buzzer will bleep rapidly, it indicates that the authorization is wrong, and the door will not be open.

2. Password+ Read card (set via management center)

Swipe the card first, buzzer bleep once, then enter the password (6 bits) and push "OK". If the password is wrong, the buzzer would bleep rapidly.

Note: If open the door by this way, the password should be set when issue the user card via management center.

Chapter 4 Common troubleshooting

Here are some common faults and simple ways to check them. Please cut off the power while conducting operation on hardware device.

Symptom 1: After finishing the installation, the software can not communicate with the computer

Diagnosis:

1. The wiring connected the device and the communication Converter is wrong.
2. The abnormity of the computer serial port (damaged or occupied).
3. The communication port or the serial port setting in the management software is wrong.

Symptom 2: The system online communication is unstable.

Diagnosis:

1. Check the welding or quality of the communication cables.
2. Check the system networking whether has too much branched or over 1.2km, without adding the relay amplifier.
3. Check the terminal resistance of the farthest access device whether is connected.

Symptom 3: When the device is power on, and indicator light is normal .but the device has no response after swiping a card.

Diagnosis:

1. Unauthorized card.
2. The master key in management card is lost.

Symptom 4: Swipe the card, the buzzer bleep once, but the door is not open.

Diagnosis:

1. Check the wiring.
2. Check the signal outputting of the switch
3. Check the door magnetic signal cables of the device. It may be short-circuited or connected with the electric magnetic signal.

Symptom 5: Swipe the card, the buzzer bleep 4 times rapidly, and the door can not be open.

Diagnosis:

Unauthorized card.

Symptom 6: The card reading distance is close.

Diagnosis:

1. There is serious signal interference in the surrounding

(such as strong electromagnetic interference or metal absorption) . If so, please add ferrite to avoid.

2. Check the card and the device whether is provided by the same supplier.

Symptom 7: The device always works well, but the authorized card can not open the door suddenly, the card turn into invalid card.

Diagnosis:

The device is initialized by the operator or some reasons cause the device executes the initialization command.

Symptom 8: Swipe the card, the door can be open, but the the indicator light is off or the buzzer always bleep.

Diagnosis:

1. The device and the electric lock share one power supply, when the lock works on , the reverse potential interfere the device causing the resetting.
2. The power supply is not enough, the device can not work well.

Chapter 5 Regulatory

Note:This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits aredesigned to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Warning: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and(2) this device must accept any interference received, including interference that may cause undesired operation.