485 Module

User Manual



V1.0.1

Foreword

General

This manual introduces the functions and operations of the 485 module (hereinafter referred to as "the device").

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	Add ground wiring.	February 2025
V1.0.0	First Release.	November 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Turnstile, hazard prevention, and prevention of property damage. Read carefully before using the Turnstile, comply with the guidelines when using it, and keep the manual safe for future reference.

Transportation Requirement



Transport the device under allowed humidity and temperature conditions.

Storage Requirement



Store the device under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the Turnstile while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Turnstile.
- Do not connect the Turnstile to two or more kinds of power supplies, to avoid damage to the Turnstile.



- Install the Turnstile on a stable surface to prevent it from falling.
- Do not place the Turnstile in a place exposed to sunlight or near heat sources.
- Keep the Turnstile away from dampness, dust, and soot.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Turnstile label.
- The Turnstile is a class I electrical appliance. Make sure that the power supply of the Turnstile is connected to a power socket with protective earthing.

Operation Requirements



- Make sure that the power supply is correct before use.
- Do not unplug the power cord on the side of the Turnstile when the adapter is powered on.
- Operate the Turnstile within the rated range of power input and output.

- Transport, use and store the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Turnstile, and make sure that there is no object filled with liquid on the Turnstile to prevent liquid from flowing into it.
- Do not disassemble the Turnstile without professional instruction.

Maintenance Requirements



- After the installation, remove the protective film and clean the Turnstile.
- Regularly perform maintenance on the Turnstile to ensure that it works properly.
- If the Turnstile is installed near places with poor air, such as a swimming pool entrance, within 50 km of the sea or a construction site, then maintenance must be performed more frequently on the stainless cover.
- Do not use paint thinner or any other organic agent during maintenance.
- When using a face recognition component, apply waterproof silicon sealant to the installation position.

Precautions



- Pregnant women, the elderly, and children must be accompanied when passing the Turnstile.
- Children less than the height of 1 m must pass the Turnstile in the arms of or alongside an adult.
- Do not stay or play in the passage.
- Make sure that your suitcase passes in the front or alongside you.
- Only one person can pass through at a time. Do not tailgate a person, linger in the passage or break through the passage.
- Violent impact might damage the machine core and shorten the service life of the Turnstile.
- Make sure that the Turnstile is correctly grounded to prevent personal injury.
- Do not use the Turnstile when thunder occurs.



- When authorizing a person to pass through the Turnstile, there should be no person on the opposite side of the Turnstile, otherwise the barriers will remain unlocked until the person on the opposite side exits.
- Pass through the Turnstile as soon as possible after authorization. If the person does not enter within the specified time, the system will automatically close the barriers.
- When multiple persons are entering, they can pass with continuous authorization when memory mode is enabled. But the interval between continuous authorizations is recommended to be 2 s–5 s.
- Pay attention to the status of the indicator when verifying a person's identity. Red indicates that the identity of the person was not verified. Green indicates that their identity was successfully verified, and that the person can pass through.
- Do not try to forcibly pass through the passage. This Turnstile supports intelligent anti-tailgating and anti-reverse intrusion. If you forcibly break through, the system will automatically lock, closing off the passage. This can result in a person becoming injured.
- The Turnstile will not correctly recognize the authorized card if it is used together with other cards.
- Keep the authorized card well to make sure it works properly.

- Do not pass items through the Turnstile, otherwise the Turnstile will consider the item as unauthorized.

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Packing List 1
2 Product Introduction 2
3 Port Description 3
3.1 485_IO Module Port 3
3.2 485_Relay Module Port 5
3.3 Module Cascade 8
Appendix 1 Security Recommendation 12

1 Packing List

Check the item quantity after unpacking the box.

Table 1-1 Packing list

Item	Quantity
Host	1
Quick Start Guide	1
Manual QR Code	1
485 Connection Cable	2
Screw Spike Package	1

2 Product Introduction

The access control expansion module can be used with the upper-level host and adopts RS-485 bus mode for communication to realize signal output, signal input, and access control expansion services.

It can realize module cascading, support power output and supply power to other modules.

3 Port Description

3.1 485_IO Module Port

485_IO Module

The 485_IO module port has 2 signal modes:

- Input mode: Toggling the 1-bit switch on the right to **0** refers to input mode.
- Output mode: Toggling the 1-bit switch on the right to **1** refers to output mode.

Figure 3-1 Input mode

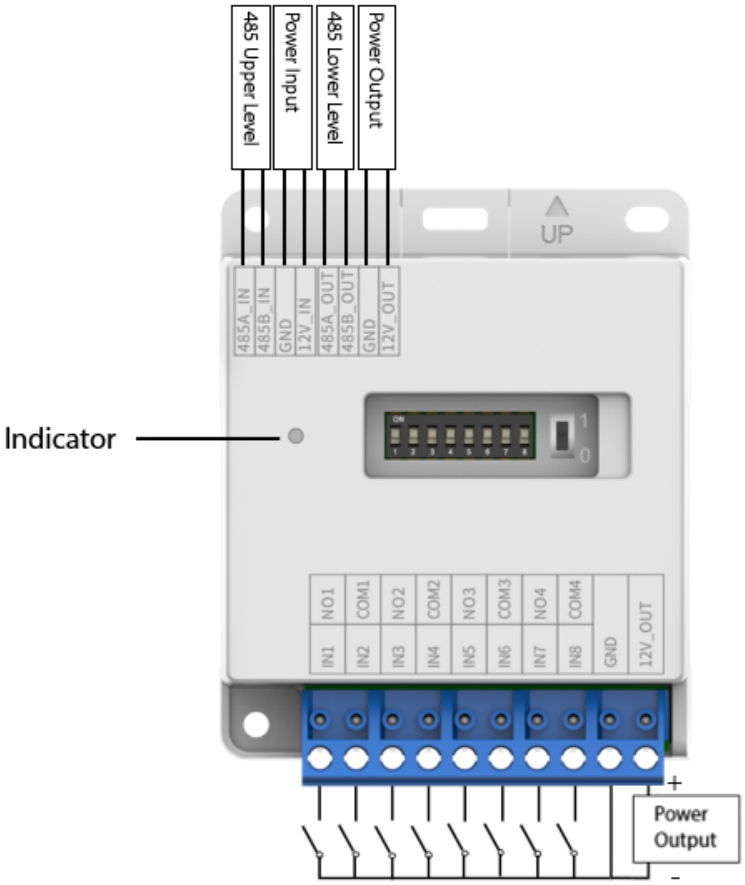
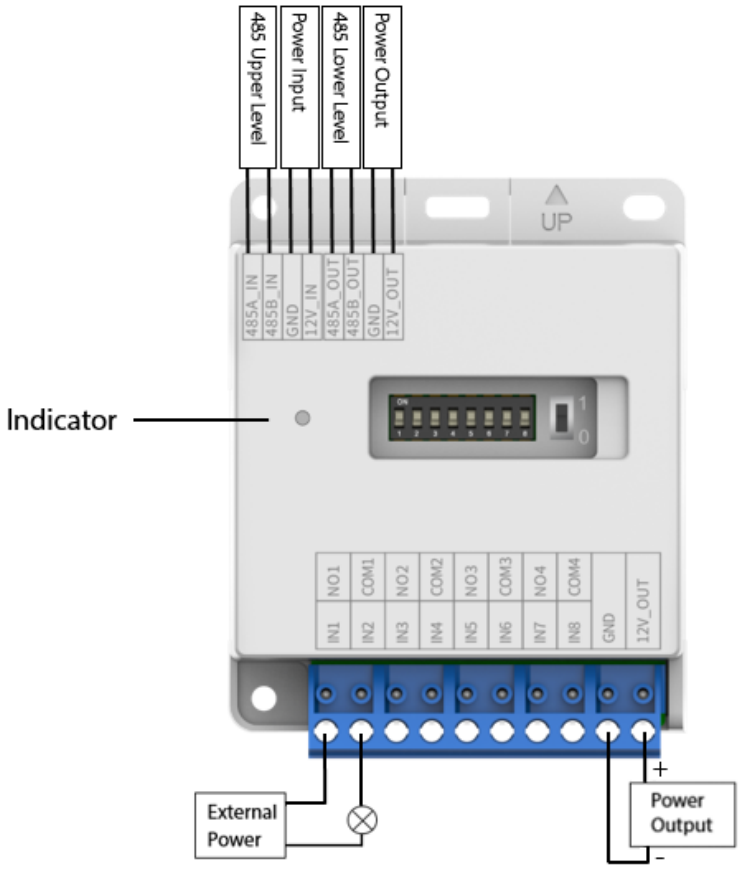


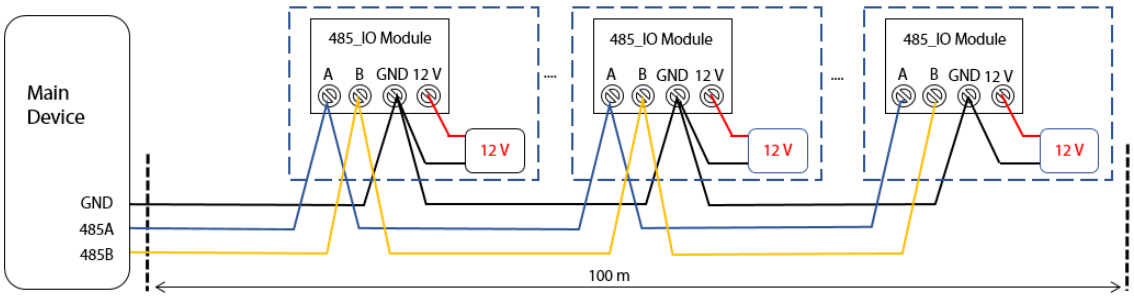
Figure 3-2 Output mode



- Solid green means the device is powered on.
- Solid blue means the device is faulty.
- The light flashing blue means the device is in updating.

When adding an external power adapter to the 485 module which is far away from the main device, connect the ground cables in series to avoid potential difference between the ground cables of the adapters.

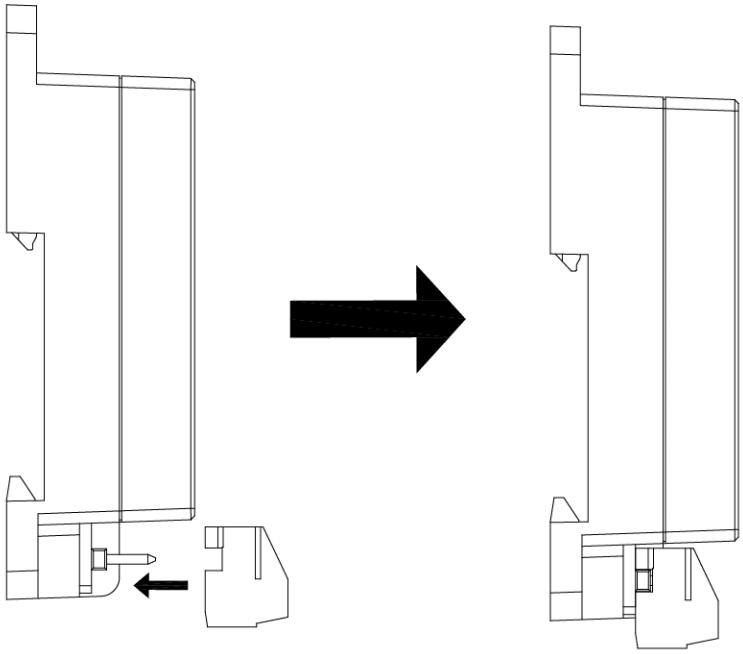
Figure 3-3 Ground wire



Install wiring terminals

Install wiring terminals properly as shown in the following pictures.

Figure 3-4 Install wiring terminals



- Use your palm to fully secure the front of the device, and then detach the terminal block to lest the device cocks.
- When assembling wiring terminals, assemble the terminals together and then assemble them on the 485 module.

3.2 485_Relay Module Port

485_relay module

The 485_relay module port has 2 signal modes:

- 485 mode: Toggling the 1-bit switch on the right to **0** refers to 485 mode.
- Wiegand mode: Toggling the 1-bit switch on the right to **1** refers to wiegand mode.

Figure 3-5 485 mode

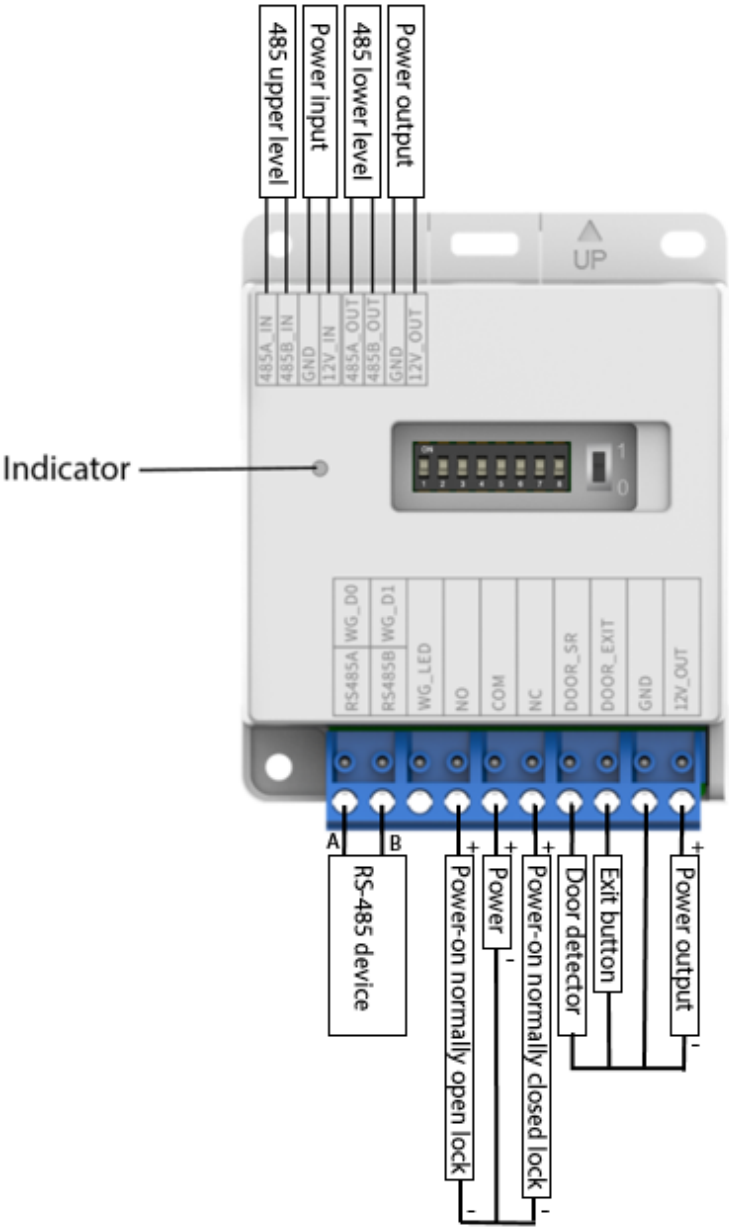
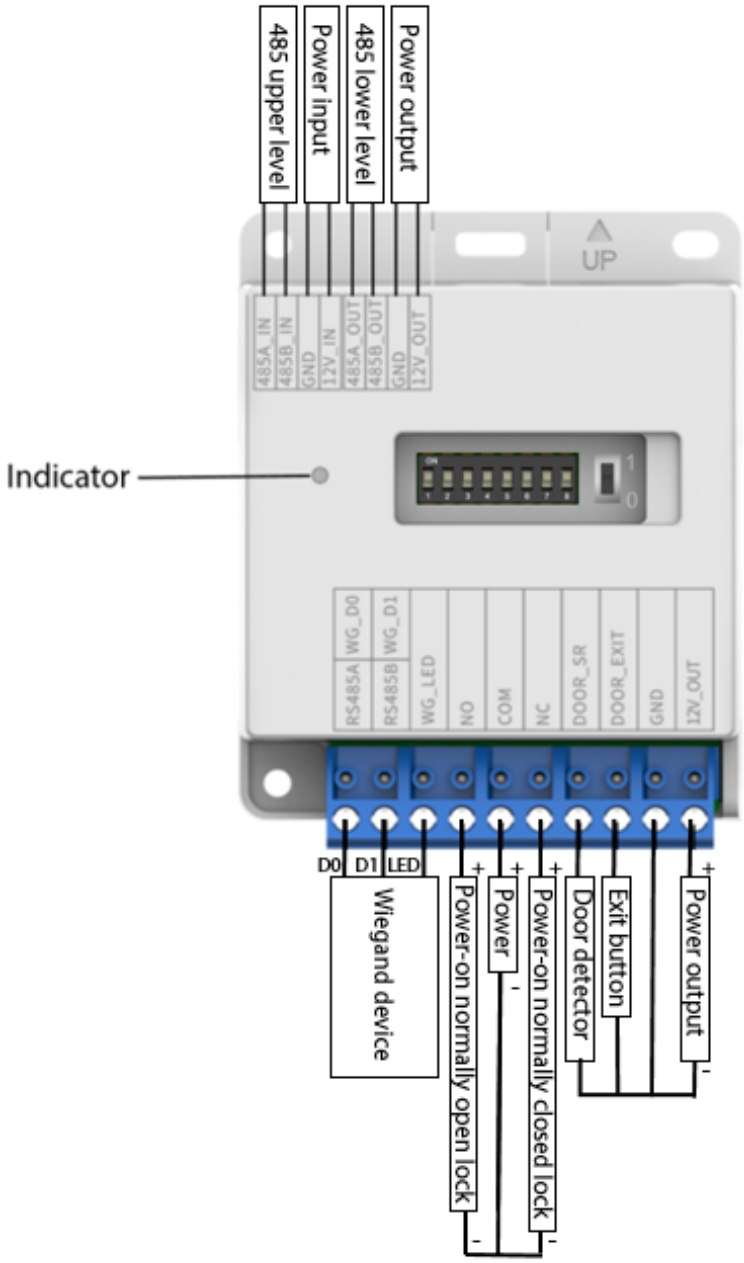


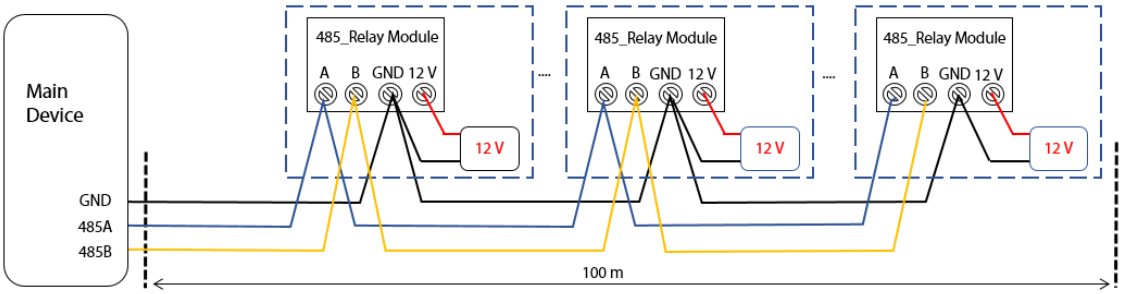
Figure 3-6 Wiegand mode



- Solid green means the device is powered on.
- Solid blue means the device is faulty.
- The light flashing blue means the device is in updating.

When adding an external power adapter to the 485 module which is far away from the main device, connect the ground cables in series to avoid potential difference between the ground cables of the adapters.

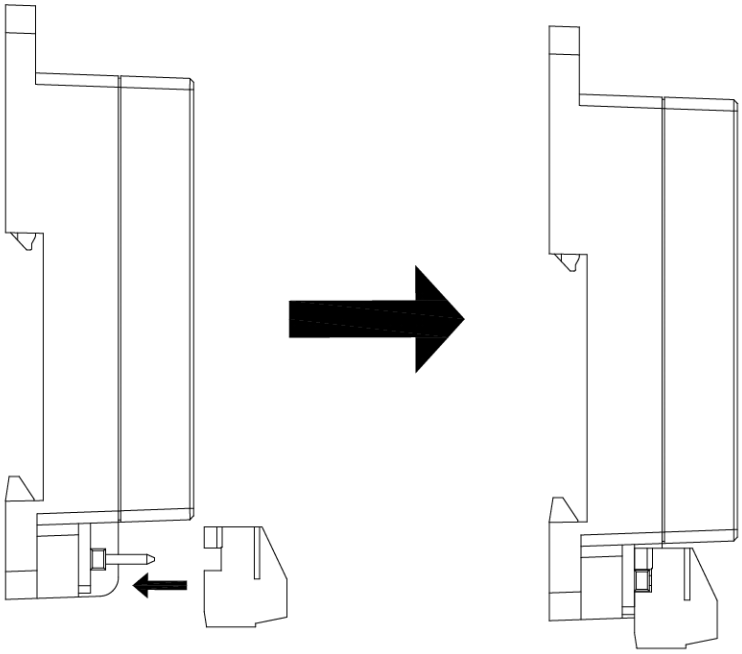
Figure 3-7 Ground wire



Install wiring terminals

Install wiring terminals properly as shown in the following pictures.

Figure 3-8 Install wiring terminals



- Use your palm to fully secure the front of the device, and then detach the terminal block to lest the device cocks.
- When assembling wiring terminals, assemble the terminals together and then assemble them on the 485 module.

3.3 Module Cascade

485_IO module and 485_relay module can be cascaded. You can set the module address by DIP switch.

The first switch to the sixth switch are used to set the module address.

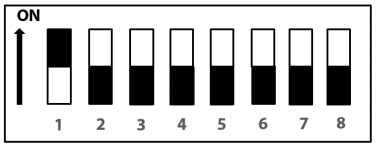
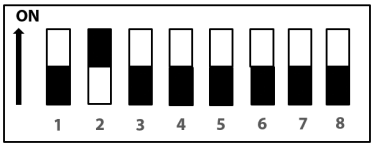
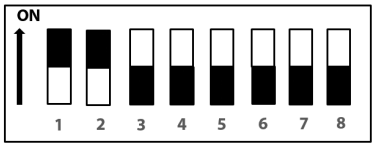
Table 3-1 Relation between address and DIP switch

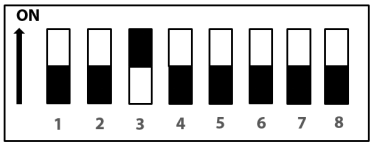
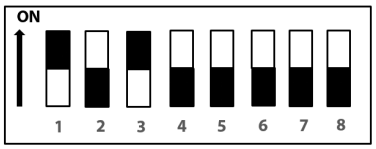
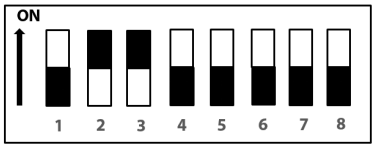
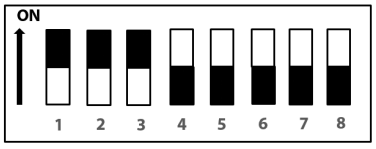
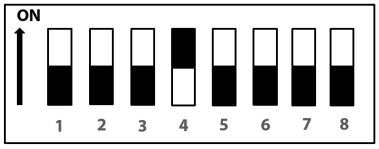
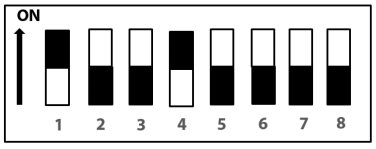
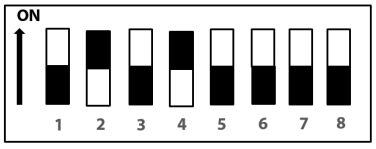
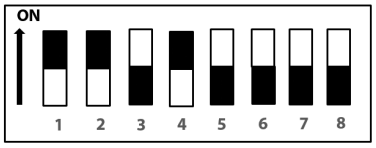
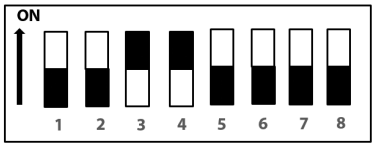
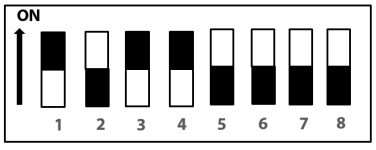
Address	DIP Switch	Address	DIP Switch	Address	DIP Switch	Address	DIP Switch
1	1	17	1, 5	33	1, 6	49	1, 5, 6
2	2	18	2, 5	34	2, 6	50	2, 5, 6
3	1, 2	19	1, 2, 5	35	1, 2, 6	51	1, 2, 5, 6
4	3	20	3, 5	36	3, 6	52	3, 5, 6
5	1, 3	21	1, 3, 5	37	1, 3, 6	53	1, 3, 5, 6
6	2, 3	22	2, 3, 5	38	2, 3, 6	54	2, 3, 5, 6
7	1, 2, 3	23	1, 2, 3, 5	39	1, 2, 3, 6	55	1, 2, 3, 5, 6
8	4	24	4, 5	40	4, 6	56	4, 5, 6
9	1, 4	25	1, 4, 5	41	1, 4, 6	57	1, 4, 5, 6
10	2, 4	26	2, 4, 5	42	2, 4, 6	58	2, 4, 5, 6
11	1, 2, 4	27	1, 2, 4, 5	43	1, 2, 4, 6	59	1, 2, 4, 5, 6
12	3, 4	28	3, 4, 5	44	3, 4, 6	60	3, 4, 5, 6
13	1, 3, 4	29	1, 3, 4, 5	45	1, 3, 4, 6	61	1, 3, 4, 5, 6
14	2, 3, 4	30	2, 3, 4, 5	46	2, 3, 4, 6	62	2, 3, 4, 5, 6
15	1, 2, 3, 4	31	1, 2, 3, 4, 5	47	1, 2, 3, 4, 6	63	1, 2, 3, 4, 5, 6
16	5	32	6	48	5, 6		

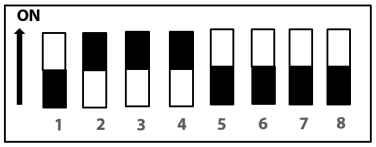
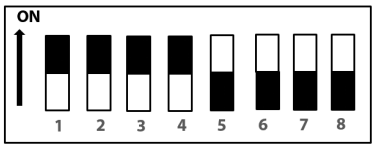
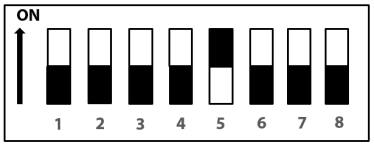
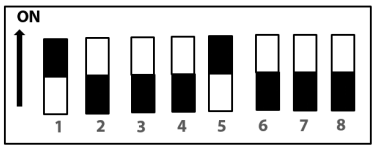
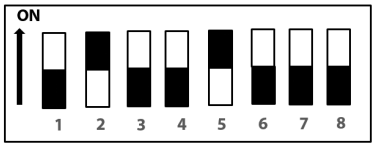
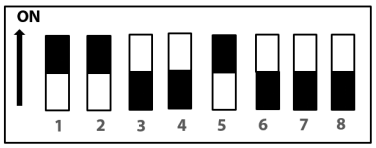
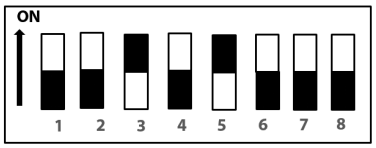
1–6 indicates the DIP switch is toggled to **ON**. Other digits do not toggle the DIP switch.

The DIP switch combination of 1–20 is shown as follows.

Table 3-2 1–20 DIP switch combination

Device ID	DIP Switch Combination	Coding Rule
1		DIP 1
2		DIP 2
3		DIP 1+ DIP 2

Device ID	DIP Switch Combination	Coding Rule
4		DIP 3
5		DIP 1+ DIP 3
6		DIP 2+ DIP 3
7		DIP 1+ DIP 2+ DIP 3
8		DIP 4
9		DIP 1+ DIP 4
10		DIP 2+ DIP 4
11		DIP 1+ DIP 2+ DIP 4
12		DIP 3+ DIP 4
13		DIP 1+ DIP 3+ DIP 4

Device ID	DIP Switch Combination	Coding Rule
14		DIP 2+ DIP 3+ DIP 4
15		DIP 1+ DIP 2+ DIP 3+ DIP 4
16		DIP 5
17		DIP 1+ DIP 5
18		DIP 2+ DIP 5
19		DIP 1+ DIP 2+ DIP 5
20		DIP 3+ DIP 5

Appendix 1 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.

2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.

2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.

4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).