

Remote Controller

User Manual



V1.0.1

Foreword

General

This manual introduces the functions and operations of the remote controller (hereinafter referred to as the "Device"). Read carefully before using the device, and keep the manual safe for future reference.

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.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	• Update the configuration. • Update the wiring.	March 2025
V1.0.0	First release.	December 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 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 (40%–65% (RH)) and temperature (0°C to +40°C) conditions.

Installation Requirements



WARNING

- Do not connect the power adapter to the Turnstile while the adapter is powered on.
- Do not connect the Turnstile to two or more kinds of power supplies, to avoid damage to the Turnstile.
- Please follow the electrical requirements to power the device.
 - ◇ Followings are the requirements for selecting a power adapter.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
 - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
 - ◇ We recommend using the power adapter provided with the device.
 - ◇ When you select the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.



- 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 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.
- When the Turnstile is used with access controller and the lock port connects to the K1 or K2 port of the main control board, configure the unlock duration for the access controller as 0.2 seconds.
- Prepare a separate power adapter when install a face recognition access controller.

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 detection 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.
- If the Turnstile is used with the face recognition access controller, when the lock port on the face recognition access controller is connected to the K1 or K2 port on the main control board on the Turnstile, the unlock duration for the face recognition access controller should be configured as 0.2 seconds.
- If the Turnstile is used with the face recognition access control device, the separate power adapter must be prepared.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Overview.....	1
1.1 Introduction.....	1
1.2 Appearance.....	1
1.3 Functions.....	1
2 Wiring.....	3
2.1 Receiver Ports Description.....	3
2.2 Wiring with the Main Control Board (Supporting NO Port).....	4
2.3 Wiring with the Main Control Board (Not Supporting NO Port).....	5
3 Configuration and Debugging.....	7
3.1 Buttons and Indicator.....	7
3.2 Configuring Pairing Mode.....	8
3.2.1 Starting the Pairing Mode.....	8
3.2.2 Cancelling the Pairing Mode.....	8
3.3 Power Consumption Mode.....	8
3.4 Connecting to Turnstile (1W Model) without NO or Restore.....	9
3.5 Powering on.....	9
4 FAQ.....	10
Appendix 1 Security Recommendation.....	11

1 Overview

1.1 Introduction

The remote controller is used to remotely control turnstiles in such public areas as residential areas, schools, governments agencies, factories and office buildings, which realizes the general dissuasive access control for public channels.

1.2 Appearance

Figure 1-1 Appearance



Table 1-1 Components

Components	Description
Transmitter	Matches codes with the receiver to remotely control the door.
Receiver	Connects to the main control board of the turnstile to remotely control the door.

1.3 Functions

- Reliably performs encryption.
- Remote control.
- Multiple methods to open the door.
- Matches codes through the receiver. One receiver can match codes for up to 32 transmitters.

- Matches codes through the transmitter. One transmitter can match codes for up to 32 receivers.
- Two matching modes.
 - ◇ Press the  button and A button (open for entry) at the same time to start pairing.
 - ◇ Press the  button and B button (open for exit) at the same time to cancel pairing.

2 Wiring

2.1 Receiver Ports Description

Install the receiver under the card swiping board, under the upper cover of the turnstile, or next to the main control board inside the turnstile.

Figure 2-1 Receiver port

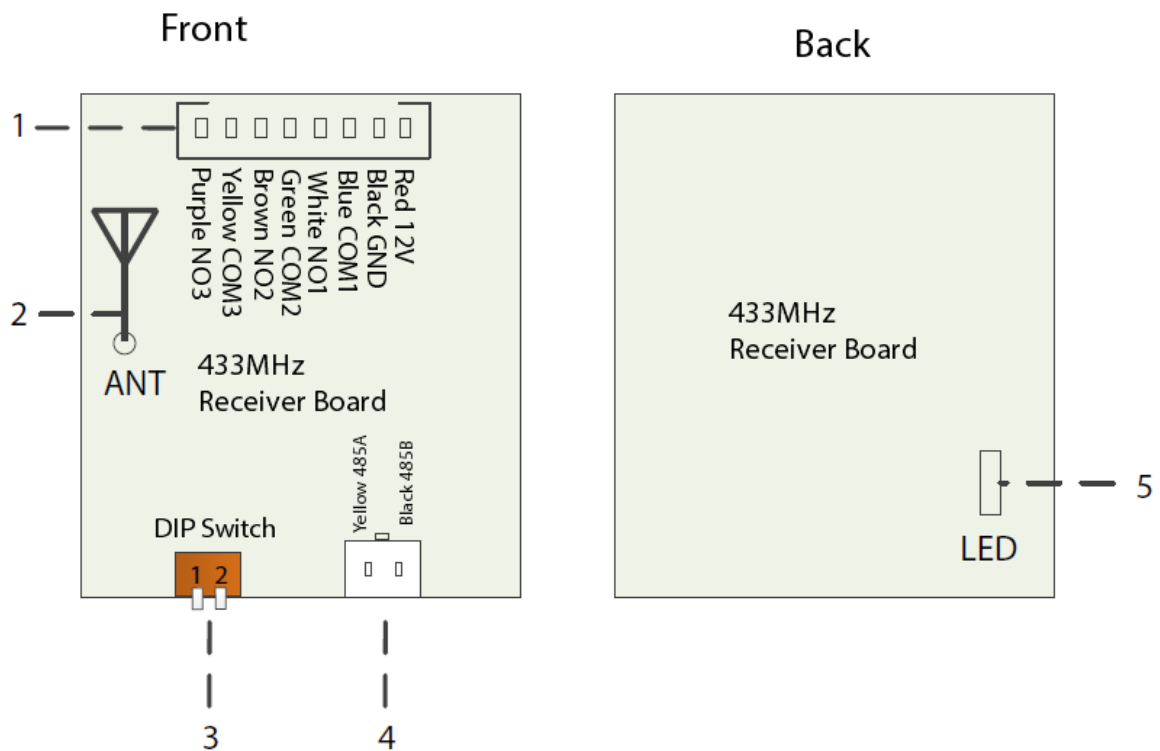


Table 2-1 Receiver port description

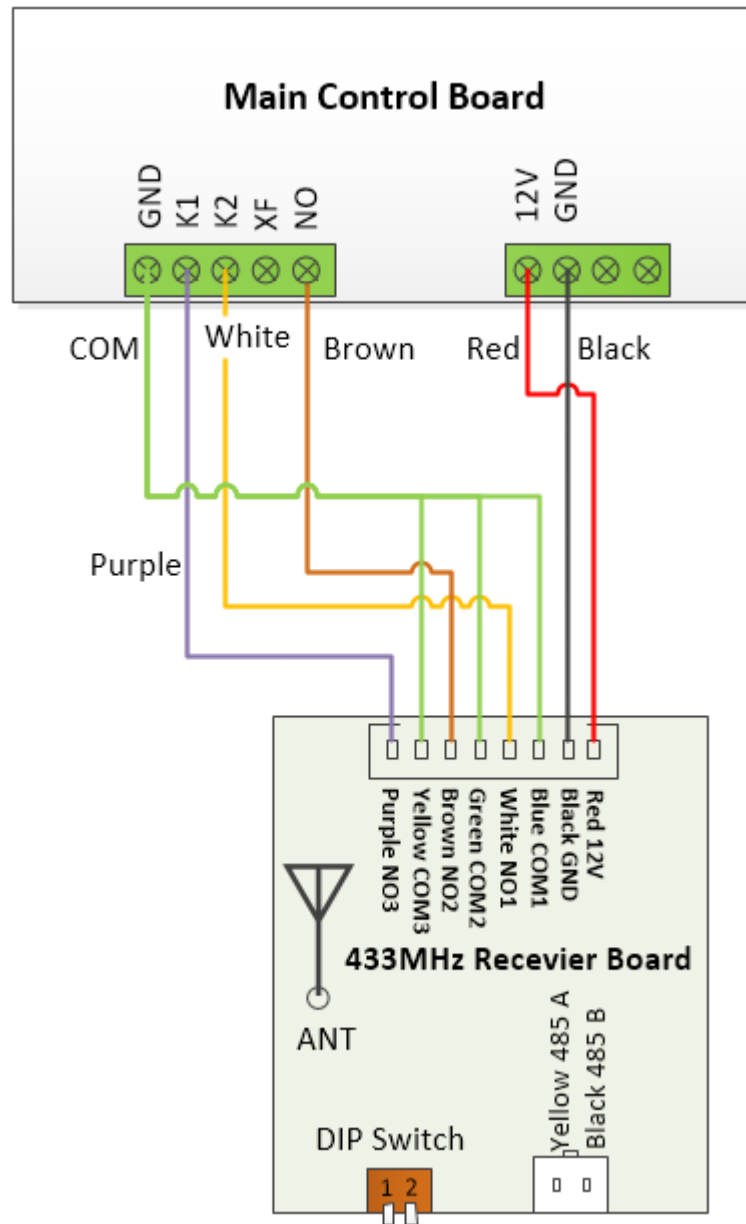
No.	Description
1	Eight pin ports: One channel for 12 V power and three channels for dry contact output. • Red 12 V and black GND: Provides 12 V power. • White NO1: Connects with K2 of main control board of the turnstile. • Brown NO2: Connects with NO of main control board of the turnstile. • Purple NO3: Connects with K1 of main control board of the turnstile. • Blue COM1, green COM2 and yellow COM3: Connects with GND of main control board of the turnstile.
2	Antenna.
3	• Turn on the DIP 1 switch: The receiver starts pairing. • Turn on the DIP 2 switch: The receiver cancels pairing. • Turn on both DIP 1 and DIP 2 switch: Available to turnstile without NO/restore signal (such as W swing barrier).

No.	Description
4	RS-485 port. Communicates with the main control board of the turnstile.
5	Indicator. ● Blue: Working. ● Green: Pairing. ● Red: Canceling pairing. ● Yellow: Available to turnstile without normally or restore signal (such as W swing barrier).

2.2 Wiring with the Main Control Board (Supporting NO Port)

The controlling signal of the receiver connects to the K1, K2, and NO signals of the main control board.

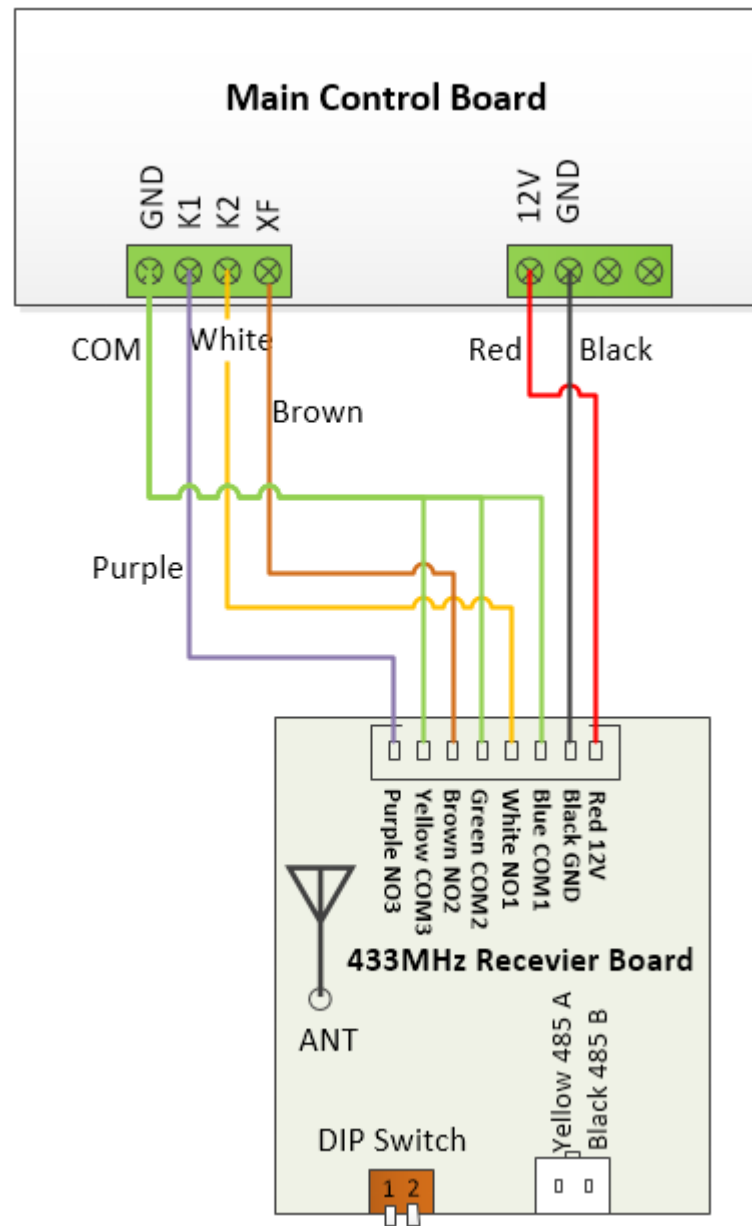
Figure 2-2 Wiring



2.3 Wiring with the Main Control Board (Not Supporting NO Port)

The receiver connects to the main control board. The controlling signal can be controlled through K1 and K2 signals.

Figure 2-3 Wiring



3 Configuration and Debugging

3.1 Buttons and Indicator

Figure 3-1 Buttons and indicator

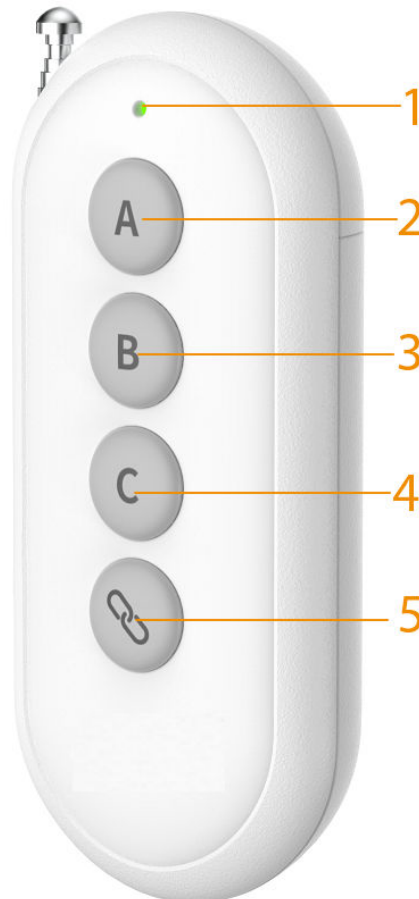


Table 3-1 Description of buttons and indicator

No.	Name	Description
1	Indicator	Indicates the status and the running mode of the remote controller. ● Green flashes once: Successful transmission. ● Red flashes once: Failed transmission. ● Green and red flash once respectively: Low power but successful transmission.
2	A (open for entry)	Press the button to open the door in the entry direction.
3	B (open for exit)	Press the button to open the door in the exit direction.

No.	Name	Description
4	C (one-key for normal open/restore)	Press the button to keep the turnstile open, and then press it again to close the door. You can change the power consumption mode when used with the  button. For details, see "3.3 Power Consumption Mode".
5	Pair	Press the button and A button or B button at the same time to configure the pairing mode. For details, see "3.2 Configuring Pairing Mode".

3.2 Configuring Pairing Mode

3.2.1 Starting the Pairing Mode

Procedure

- Step 1 Turn on the DIP 1 switch of the receiver, and then the indicator flashes green.
- Step 2 Press the  button and A button at the same time to start pairing.
- The indicator flashes green: The receiver starts pairing.
 - The indicator flashes green for 3 seconds, and then turns off after a short solid green: Successful pairing.
 - The indicator flashes green for 10 seconds, and then turns off: Failed pairing.
- Step 3 After pairing is complete, turn off the DIP 1 switch.

3.2.2 Cancelling the Pairing Mode

Procedure

- Step 1 Turn on the DIP 2 switch of the receiver.
- Step 2 Press the  button and B button at the same time to cancel pairing.
- The indicator flashes red: The receiver starts canceling the pairing mode.
 - The indicator flashes red for 3 seconds, and then turns off after a short solid red: Successful canceling.
 - The indicator flashes red for 10 seconds, and then turns off: Failed pairing.
- Step 3 After canceling, turn off the DIP 2 switch.

3.3 Power Consumption Mode

There are 2 power consumption modes. Press the  button and C button at the same time to change the mode.

- High power consumption mode: The remote control distance reaches 15 meters (the indicator light is yellow).
- Low power consumption mode: The remote control distance cannot reach 15 meters (the indicator light is green).



The device is in low power consumption mode by default.

3.4 Connecting to Turnstile (1W Model) without NO or Restore

To connect the Device to the Turnstile without NO or restore functions such as 1W model, turn on the DIP switch as needed.

Procedure

- Step 1 Pair the receiver and transmitter. For details, see "3.2 Configuring Pairing Mode".
- Step 2 Turn on the DIP 1 and DIP 2 of the receiver.

3.5 Powering on

Procedure

- Step 1 Check the components.



The device is fully inspected before it leaves the factory. Transportation and installation might affect it.

- Step 2 Check if the connection is stable and normal.

- Step 3 Power on the remote controller.

If the indicator of the receiver turns solid blue, the receiver is working normally.

- Step 4 Match codes between the receiver and the transmitter.

Press the 3 buttons to check that if the turnstile opens in the same direction as the button direction. If the turnstile opens in the wrong direction, follow the wiring instructions to change the connection.

4 FAQ

- The indicator does not turn on when the receiver is powered on.
Check the power cable of the receiver.
- The turnstile does not open when the A button is pressed.
 - ◇ Check if the device was correctly wired.
 - ◇ Check the power of the transmitter.
- The turnstile opens in the exit direction when the A button is pressed.
Check if the device was correctly wired.

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 logout function

The account logout 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;
- Establish 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).