

Enrollment Reader

User Manual

Revision 1.0



Enrollment Reader User Manual

Preface

This manual introduces the functions and operations of the enrollment reader. Read carefully before using the device, and keep the manual safe for future reference.

Privacy 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 to: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

Safety Instruction

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.

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 issuer software or try other mainstream issuer 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 Safety Instruction and Warning

Transportation Requirements

Ensure the enrollment reader is transported within the approved humidity and temperature ranges.

Storage Requirements

Store the device in an environment with permissible humidity and temperature levels.

Installation Requirements

- **Power Connection:** Plug the enrollment reader into the designated adapter before switching on the power.
- **Electrical Compliance:** Strictly follow regional electrical safety regulations. Verify that the local voltage is stable and compatible with the device's power specifications.
- **Single Power Source:** Avoid connecting the enrollment reader to multiple power supplies to prevent damage.
- **Safety Precautions:** When working at elevated positions, use all mandated protective gear and follow safety protocols.
- **Environmental Placement:**
 - ◊ Keep the device away from direct sunlight, heat sources, or excessively humid, dusty, or smoky environments.
 - ◊ Position the enrollment reader on a stable, level surface to prevent tipping or falling.
 - ◊ Avoid placing it on soft surfaces (e.g., carpets, quilts) or stacking objects on top.
- **Ventilation:** Install in a well-ventilated area, ensuring no obstructions block the device's cooling vents.
- **Power Supply:** Use only the manufacturer-provided adapter or case power supply.
- **Regulatory Compliance:**
 - ◊ The power source must meet IEC 60950-1 (limited power source/PS2, SELV) or IEC 62368-1 (ES1) standards.
 - ◊ Class I appliances must connect to a grounded power outlet.

Enrollment Reader User Manual

Operation Requirements

- **Power Verification:** Before operation, confirm that the power supply is functioning correctly.
- **Safe Power Handling:** Never disconnect the power cable while the device is active to avoid malfunctions.
- **Power Limitations:** Operate the enrollment reader strictly within its specified power range.
- **Environmental Conditions:** Use the device only within approved humidity and temperature limits.
- **Liquid Protection:**
 - ◇ Avoid exposing the enrollment reader to splashes or spills.
 - ◇ Ensure no liquid-filled objects are placed above it to prevent accidental leakage.
- **Tampering Prohibition:** Do not attempt to disassemble or modify the enrollment reader.

Contents

- Preface* /
- Synopsis* 1
- Device Operation* 2
 - Connecting to Computer*..... 2
 - Issuing Cards*..... 2
 - Issuing a Card*..... 2
 - Issuing Multiple Cards* 4
 - Assigning Permissions* 4
 - Adding Devices* 4
 - Configuring Permissions*..... 5
- Security Recommendation* 6

Enrollment Reader User Manual

Synopsis

The enrollment reader is a plug-and-play device that connects to the computer through a USB cable. It can issue IC or ID cards.

Appearance



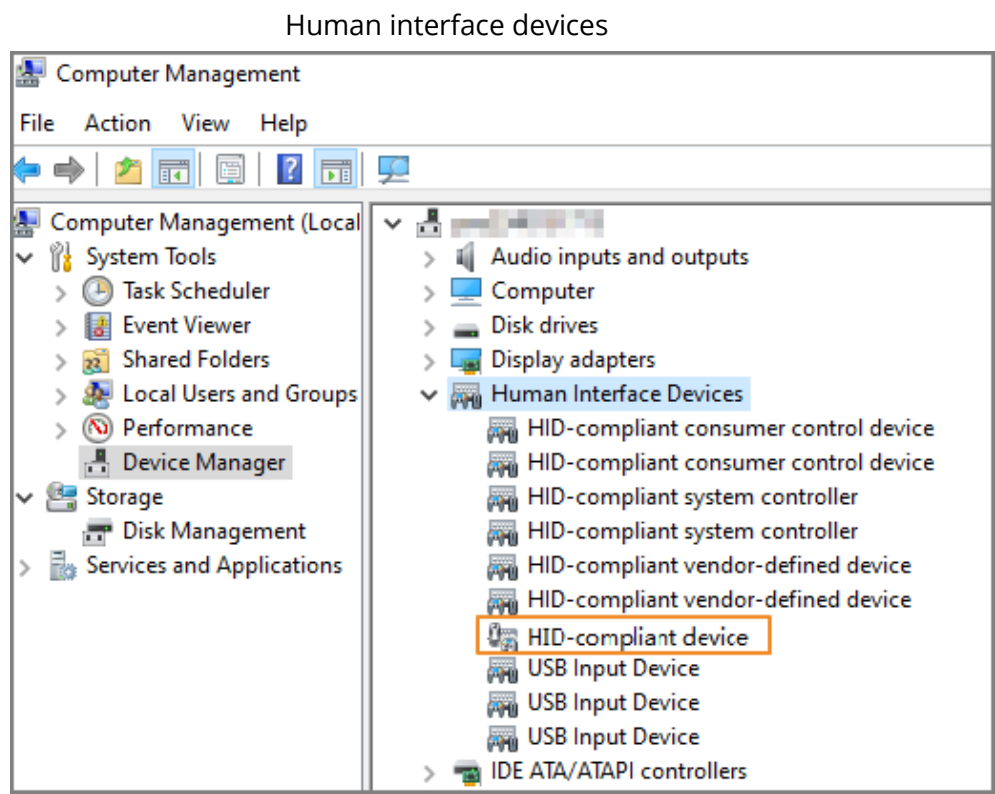
Device Operation

Connecting to Computer

Use a USB cable to connect the enrollment reader to your computer. You do not have to install any drivers. Make sure the enrollment reader is successfully connected to the computer before using it.

Process

1. On the desktop of your computer, right-click the **This PC** icon, and then select **Manage** → **Device Manager**.
2. Under **Human Interface Devices**, check whether there is an HID-compliant device.



Issuing Cards

You need to install QuickView on your computer. Issue cards to users so that they can unlock doors with cards.

Process

1. Use a USB cable to connect the enrollment reader to the computer.



NOTE

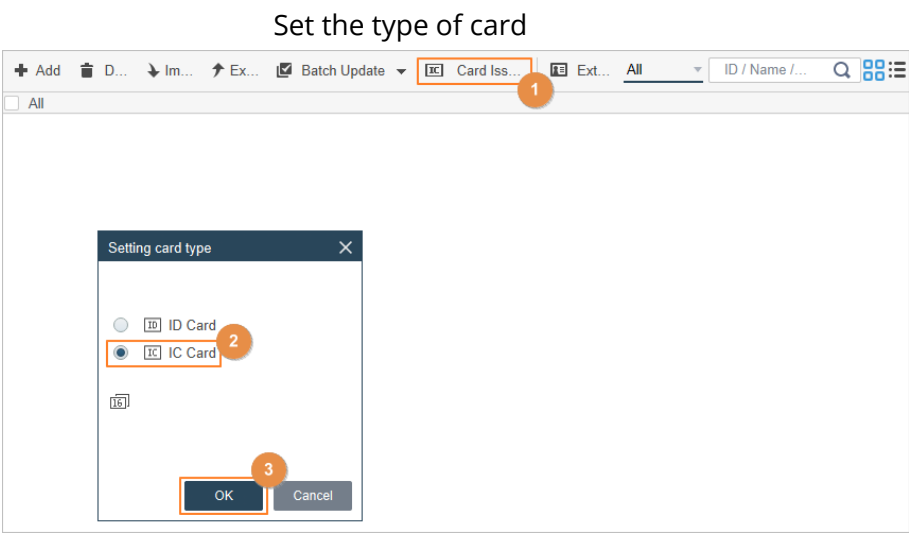
The enrollment reader will buzz once.

2. Open QuickView, and then select **Person and Permission** → **Person Management**.
3. Click **Card Issuing Type**, and then select **IC Card**.



NOTE

Select the card type you want to issue according to the type of the enrollment reader. Here we use IC card as an example.



4. Click **OK**.

Issuing a Card

Process

1. Go to the **Certification** section of a user.
 - If you need to add a new user, select **Person and Permission** → **Person Management**, click **Add**, enter the user ID and name, and then click **Finish**.

Enrollment Reader User Manual

Add a user

- For an existing user, click .

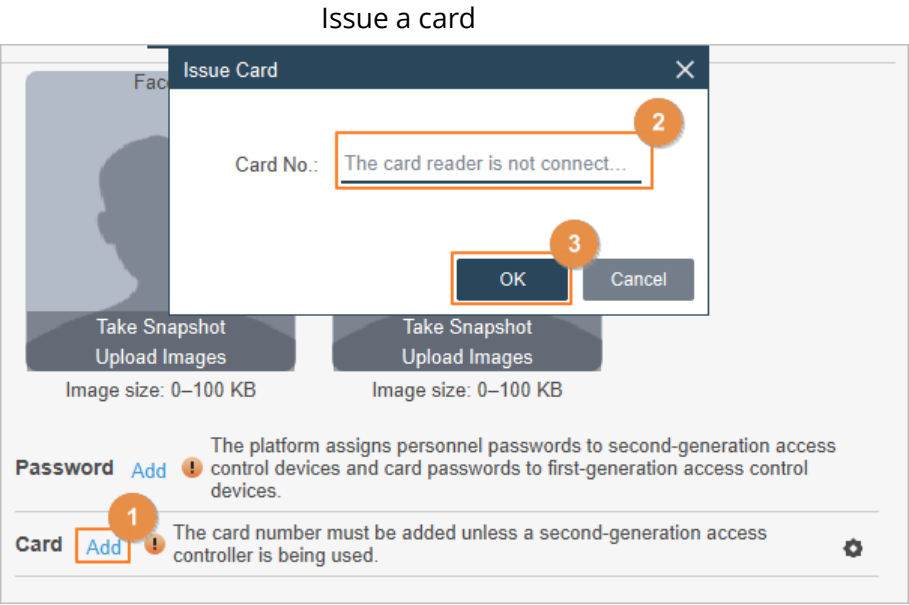
Edit user information

- Click  in the **Card** section.
- Set **Card Reader** to **enrollment reader**, and then click **OK**.

Select a enrollment reader

- Click **Add** in the **Card** section. The enrollment reader buzzes once.
- Swipe a card on the enrollment reader. The card number will be automatically read.
- Click **OK**.
- The indicator of the enrollment reader turns to solid red, indicating it is now in standby mode.

Enrollment Reader User Manual



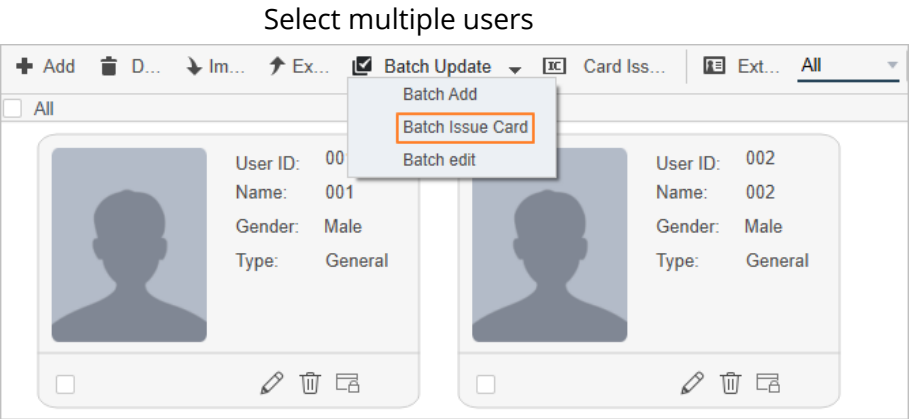
NOTE

- Each user can have up to five cards.
- You can only issue one card at a time. When multiple cards are stacked together, the Enrollment reader will not be able to work properly.

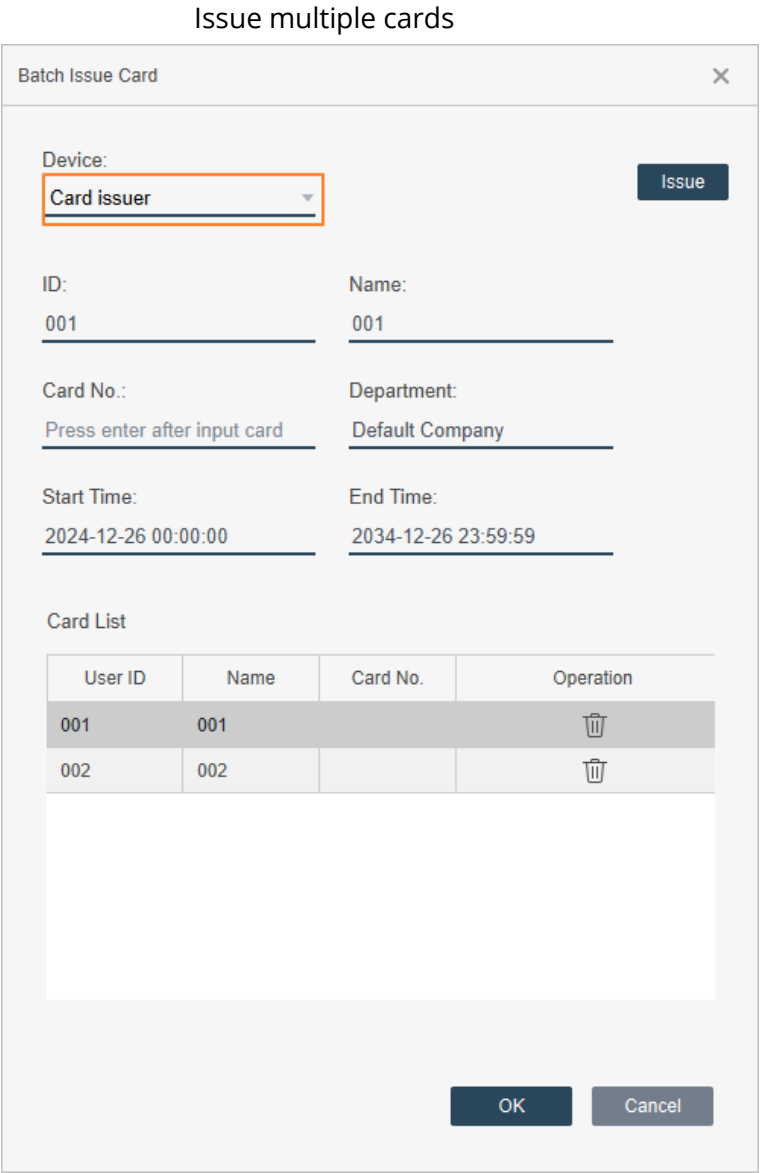
Issuing Multiple Cards

Process

1. Select **Person and Permission** → **Person Management**, select users, and then select **Batch Update** → **Batch Issue Card**.



2. Set **Device** to **enrollment reader**.
3. Click **Issue**, and then swipe the cards one by one on the enrollment reader.



4. Click **OK**.

Assigning Permissions

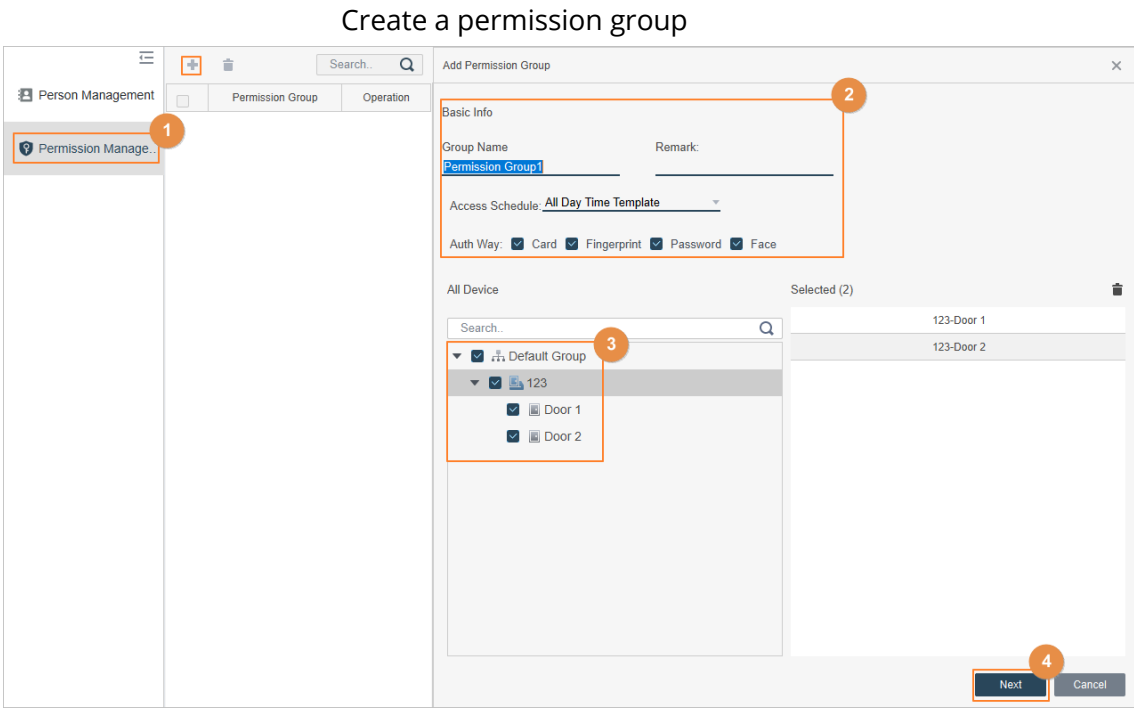
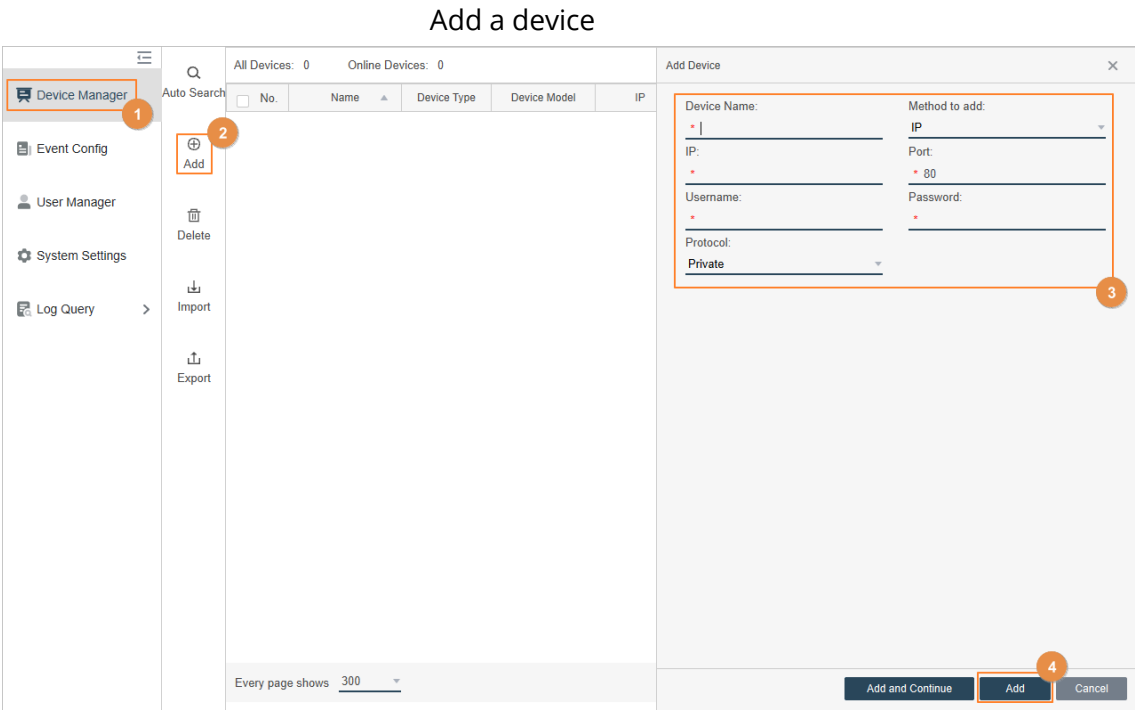
Add devices to a permission group, and then users in the group can unlock corresponding doors.

Adding Devices

Process

1. On the homepage of QuickView, go to **Device Manager** → **Add**.
2. Enter the information of the device, and then click **Add**.

Enrollment Reader User Manual



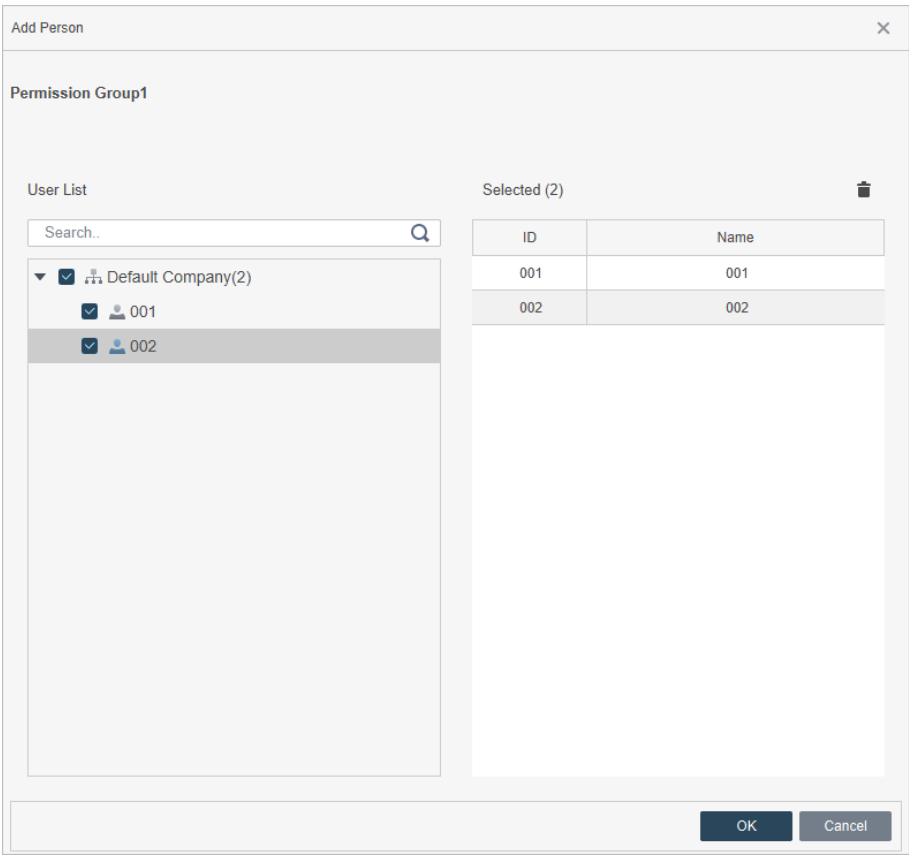
Configuring Permissions

Process

1. Go to **Person and Permission** → **Permission Management**.
2. Click **+**.
3. Enter the group name, remarks (optional), and select a time template.
4. Select the devices.
5. Click **Next**.

6. Select the users that you want to add to the permission group.
7. Click **OK**.
Users in the permission group can now swipe their cards, or use other unlock methods to unlock the door.

Add users to a permission group



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 Allowlist

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

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.

Enrollment Reader User Manual

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).

1. 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.

(2) This device must accept any interference received, including interference that may cause undesired operation.

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

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 are designed 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

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.