Enrollment Reader

Quick Start Guide

V1.0.1

Foreword

General

This manual introduces the functions and operations of the Enrollment Reader (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, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version
V1.0.1
V1.0.0

Privacy Protection Notice

As the Device user or data controller, you might collect the personal data of others such as their face, 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 Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, comply with the guidelines when using it, and keep the manual safe for future reference.

Transportation Requirements

Transport the Device under allowed humidity and temperature conditions.

Storage Requirements

Store the Device under allowed humidity and temperature conditions.

Installation Requirements

 **WARNING**

- Connect the Device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the Device.
- Do not connect the Device to more than one power supply. Otherwise, the Device might become damaged.

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the Device to direct sunlight or heat sources.
- Do not install the Device in humid, dusty or smoky places.
- Install the Device on a solid and flat surface to avoid that it falls off or turns over.
- Do not place the Device on carpet or quilt.
- Do not place any object on the Device.
- Install the Device in a well-ventilated place, and do not block the ventilator of the Device.
- Use the power adapter or case power supply provided by the Device manufacturer.
- The power source should meet limited power source or PS2 requirements according to IEC 60950-1 or IEC 62368-1 and comply with SELV for IEC 60950-1 or comply with ES1 for IEC 62368-1.
- Connect class I electrical appliances to a power socket with protective earthing.

Operation Requirements

- Make sure that the power supply of the Device works properly before use.
- Do not pull out the power cable of the Device while it is powered on.
- Only use the Device within the rated power range.
- Use the Device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the Device. Make sure that there are no objects filled with liquid on top of the Device to avoid liquids flowing into it.
- Do not disassemble the Device.

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.

ISEDC Radiation Exposure Statement:
This equipment complies with ISEDC RF 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.

Cet appareil est
Conforme aux limitesd'exposition de rayonnement RF ISEDC établiespour un environnement non contrôlé. Cetémetteur ne doit pas être co-implanté oufonctionner en onjunction avec toute autreantenne ou transmetteur.
Cet équipement doit être installé et utilisé avec une distance minimale de 20cm entre le radiateur et votre corps.

IC Warning :
This device contains licence -exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence -exempt RSS(s). Operation is subject to the following two conditions:
(1) This device may not cause interference.
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil contient des émetteurs/récepteurs sans licence qui sont conformes aux RSS sans licence d'Innovation, Sciences et Développement économique Canada. L'exploitation est soumise aux deux conditions suivantes:
(1) Cet appareil ne doit pas causer d'interférences.
(2) Cet appareil doit accepter toute interférence, y compris les interférences qui pourraient causer un fonctionnement indésirable de l'appareil.

Contents

Foreword ..... **I**
Important Safeguards and Warnings ..... **III**
1 Introduction **1**
2 Device Operation **2**
Connecting to PC 2
Issuing Cards 2
Assigning Permissions 6
2.3.1 Adding Devices 6
2.3.2 Configuring Permissions 6
Cybersecurity Recommendations **8**

1 Preparation

The Enrollment Reader is a plug-and-play device that connects to the PC through a USB cable. It can issue IC or ID cards. In order to achieve the best working condition of the device, please use the device flat on the table, do not place the device vertically on the desktop.

Figure 1-1

Appearance

2 Device Operation

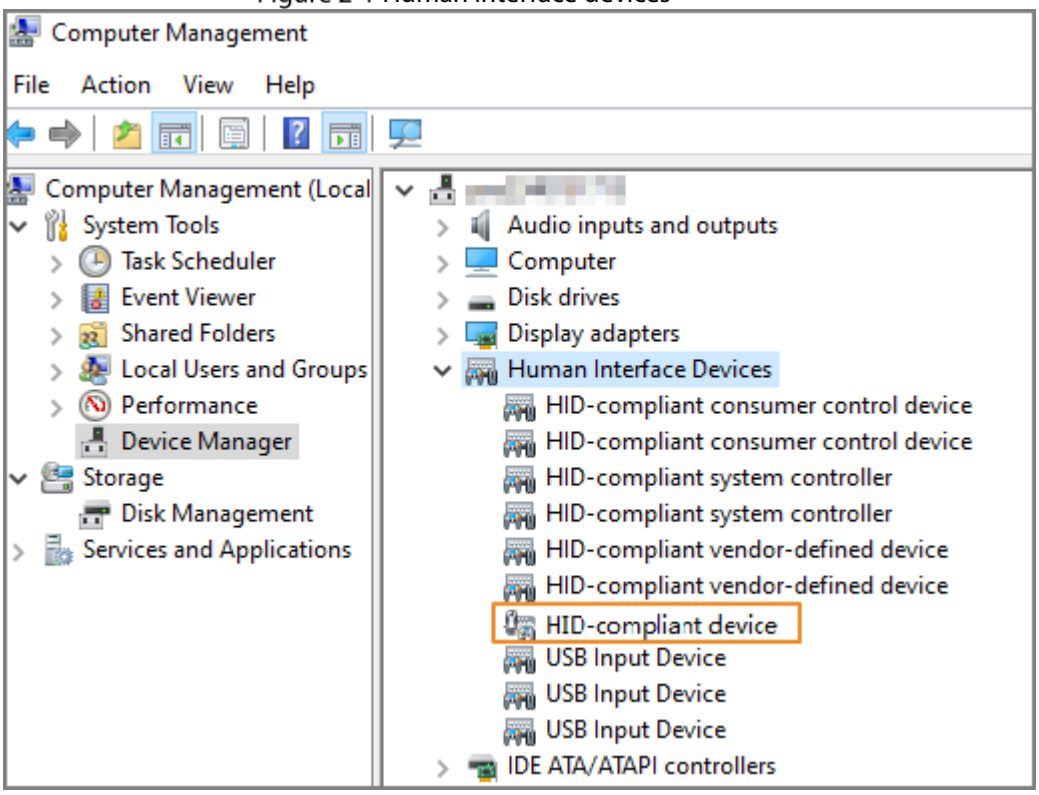
2.1 Connecting to PC

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

Step 1 On the desktop of your PC, right-click the **This PC** icon, and then select **Manage** > **Device Manager**.

Step 2 Under **Human Interface Devices**, check whether there is an HID-compliant device.

Figure 2-1 Human interface devices



2.2 Issuing Cards

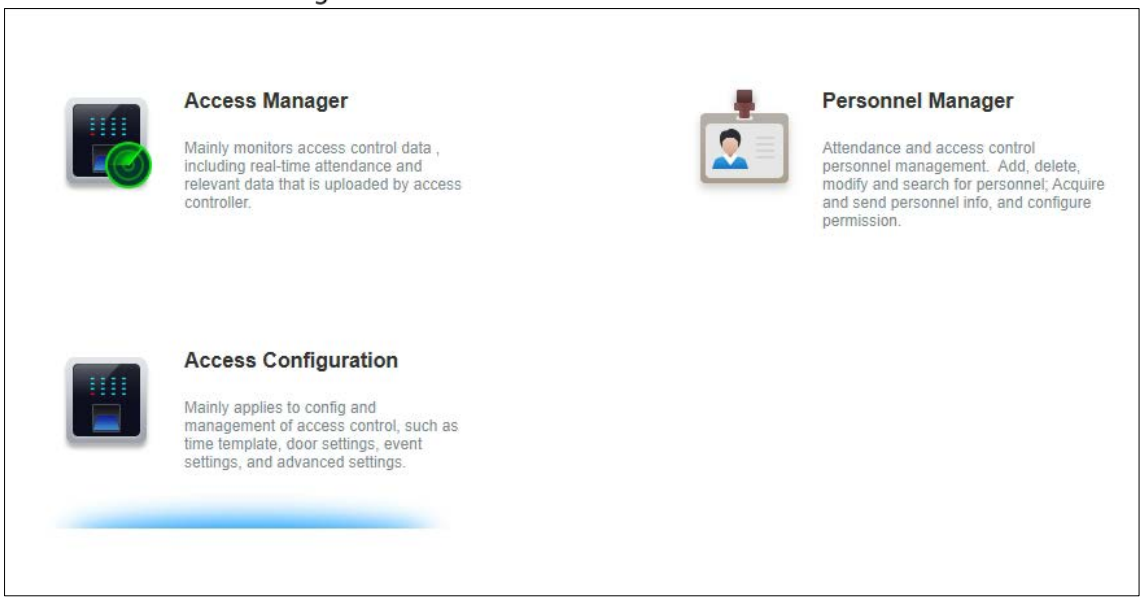
You need to install application on your PC. Issue cards to users so that they can unlock doors with cards.

Step 1 Use a USB cable to connect the Device to the PC.

The Device will buzz once.

Step 2 Open application, and then select **Access Solution** > **Personnel Manager**.

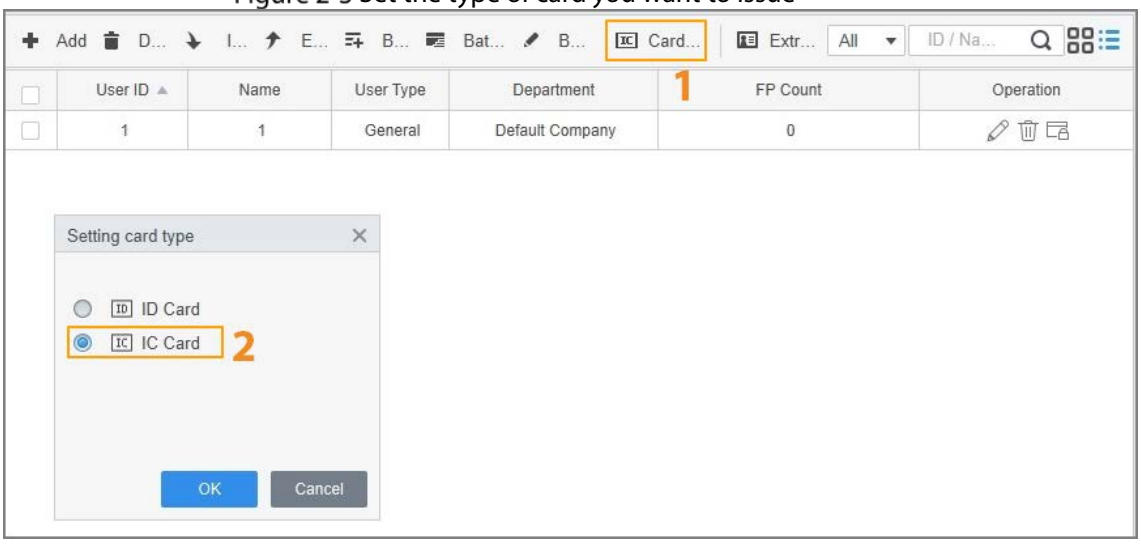
Figure 2-2



Step 3 Click **Card Issuing Type**, and then select **IC Card**.

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

Figure 2-3 Set the type of card you want to issue



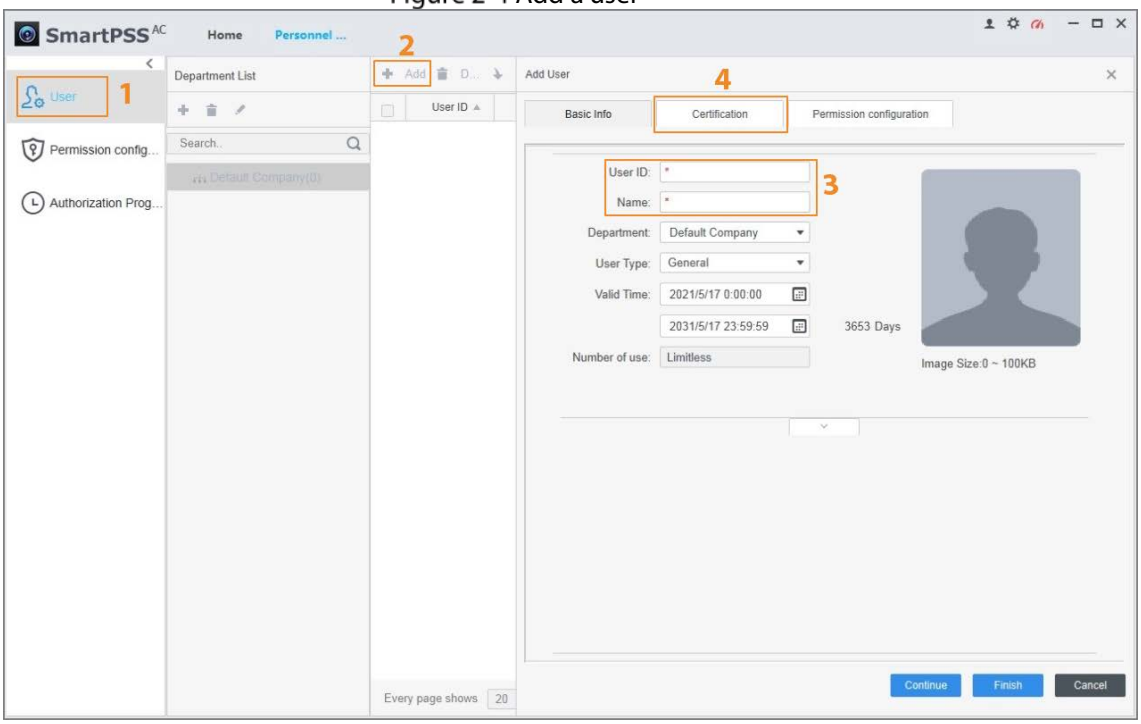
Step 4 Click **OK**.

Issuing a Single Card

Step 1 Go to the **Certification** section of a user.

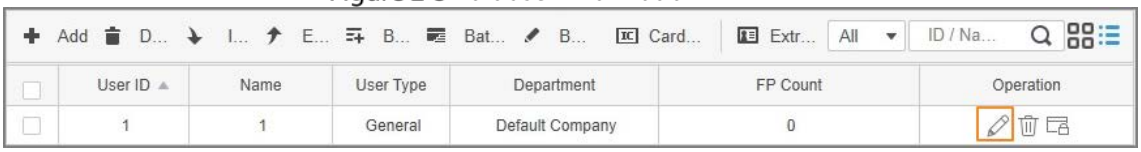
- If you need to add a new user, select **User > Add**, enter the user ID and name, and then click **Certification**.

Figure 2-4 Add a user



- For an existing user, click , and then click **Certification**.

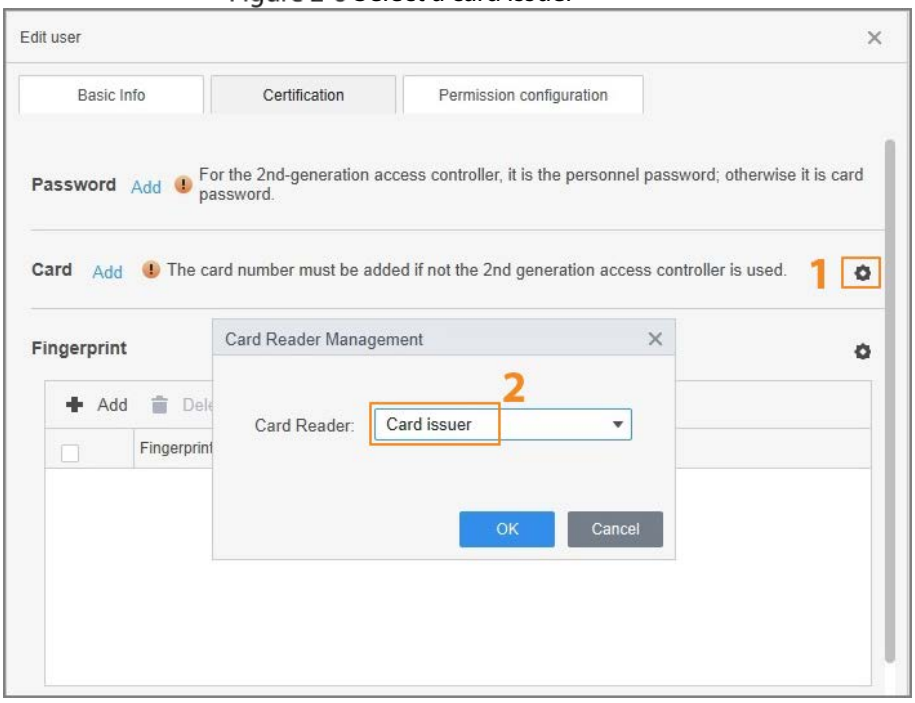
Figure 2-5 Edit user information



Step 2 Click in the **Card** section.

Step 3 Set **Enrollment Reader** to **Card Issuer**, and then click **OK**.

Figure 2-6 Select a card issuer



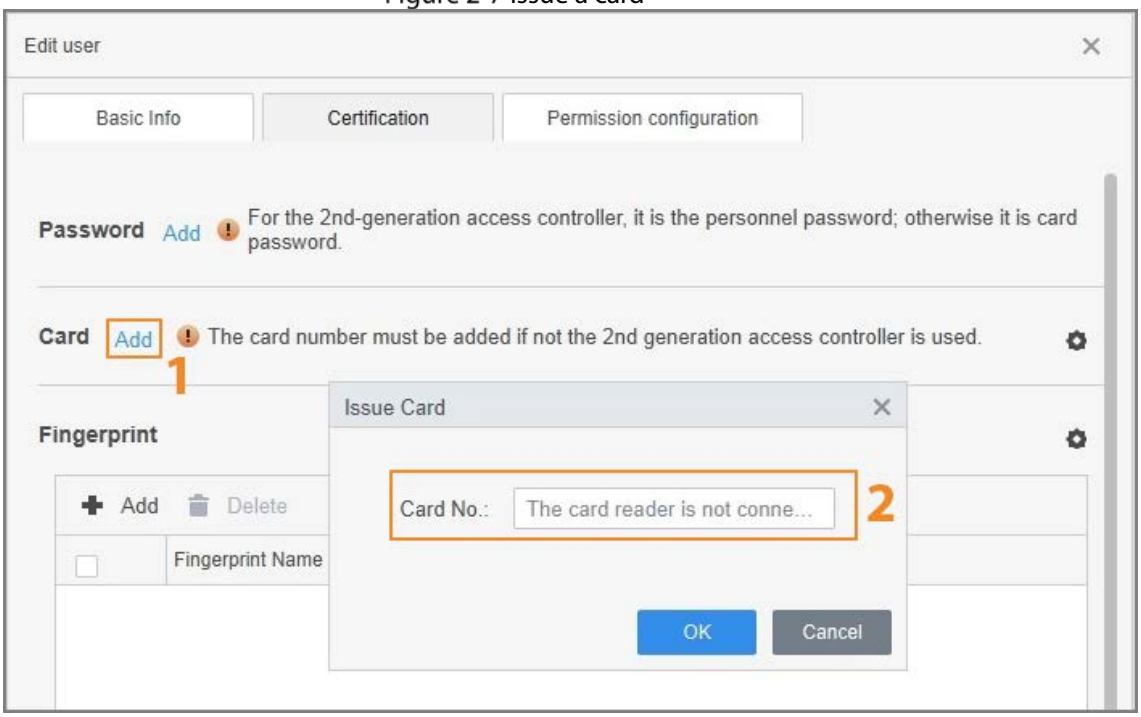
Step 4 Click **Add** in the **Card** section. The Device buzzes once.

Step 5 Swipe a card on the Device. The card number will be automatically read.

Step 6 Click **OK**.

The indicator of the Device turns to solid red, indicating it is now in standby mode.

Figure 2-7 Issue a card

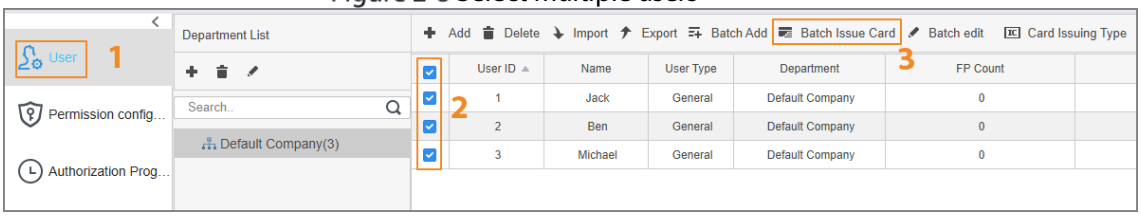


- Each user can have up to five cards.
- You can only issue one card at a time. When multiple cards are stacked together, the Device will not be able to work properly.

Issuing Multiple Cards

Step 1 Click **User**, select users, and then click **Batch Issue Card**.

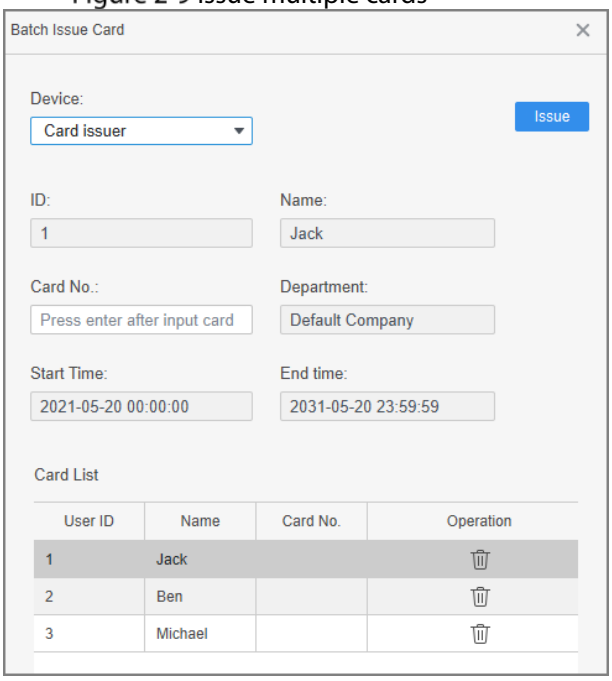
Figure 2-8 Select multiple users



Step 2 Set **Device** to **Card Issuer**.

Step 3 Click **Issue**, and then swipe the cards one by one on the Device.

Figure 2-9 Issue multiple cards



Step 4 Click **OK**.

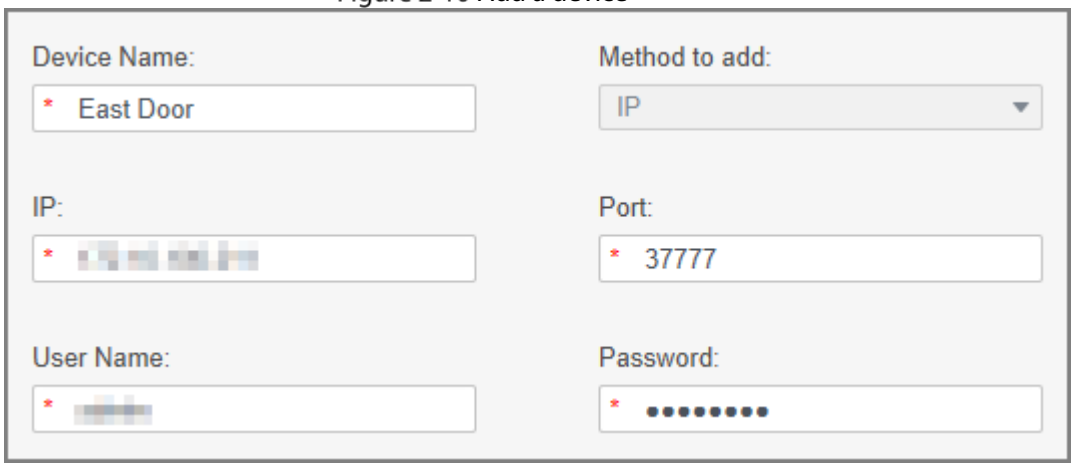
2.3 Assigning Permissions

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

2.3.1 Adding Devices

Step 1 On the homepage of application, select **Device Manager > Add**.
Step 2 Enter the information of the device, and then click **Add**.

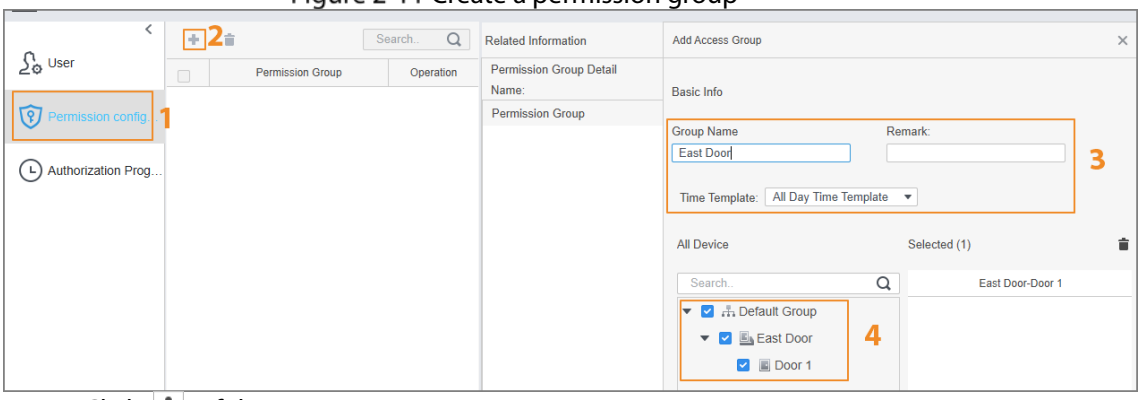
Figure 2-10 Add a device



2.3.2 Configuring Permissions

Step 1 Click **Permission configuration**.
Step 2 Click .
Step 3 Enter the group name, remarks (optional), and select a time template.
Step 4 Select the devices.
Step 5 Click **OK**.

Figure 2-11 Create a permission group



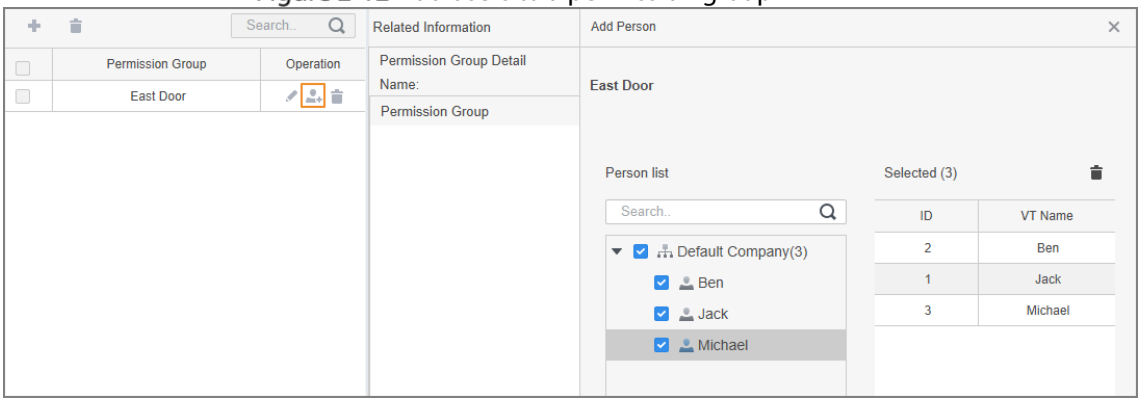
Step 6 Click  of the permission group.

Step 7 Select the users you want to add to the permission group.

Step 8 Click **OK**.

Users in the permission group can now swipe their cards, or use other unlock methods to unlock the door.

Figure 2-12 Add users to a permission group



Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.
2. **Update Firmware and Client Software in Time**
   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**
   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.
2. **Change Passwords Regularly**
   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Set and Update Passwords Reset Information Timely**
   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.
4. **Enable Account Lock**
   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.
5. **Change Default HTTP and Other Service Ports**
   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.
6. **Enable HTTPS**
   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.
7. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.
8. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
9. **Disable Unnecessary Services and Choose Secure Modes**
   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.
   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:
   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.

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

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:
    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

    If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

    If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:
    - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
    - SMTP: Choose TLS to access mailbox server.
    - FTP: Choose SFTP, and set up strong passwords.
    - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

14. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

15. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

16. **Network Log**

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

17. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:
    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.