Fingerprint Enrollment Reader

Quick Start Guide

V1.0.0

Foreword

General

This manual describes the structure of 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.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	September 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 device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirement

Transport, use and store 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 device 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 device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the device.
  - Following 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 selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.
- All the electrical connections must comply with the local electrical safety standards to avoid short circuits and electrical leakage.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.

- Install the device on a stable surface to prevent it from falling.
- Secure the device to ensure its stability and security.
- 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.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- Attach an emergency door opening device to the device or set up measures for emergency power-off to ensure the safety of people in emergency.

Operation Requirements

- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.
- This product is professional equipment.
- The device is not suitable for use in locations where children are likely to be present.
- When using the device in an access control system, ensure that the permissions of the access control system are configured properly to prevent unauthorized entry.

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Introduction 1

1.1 Features 1

1.2 Dimensions 1

2 Device Operation 2

2.1 Issuing Cards 2

2.2 Collecting Fingerprint 3

3 Fingerprint Collecting Instruction 5

4 Upgrade 7

Appendix 1 Security Recommendation 8

1 Introduction

This Device integrates the card issuing and fingerprint collecting functions. It is plug-and-play using a USB cable to connect to the PC. It is applicable to industrial zones, office buildings, schools, factories, stadiums, CBD, residential area, government properties, and more.

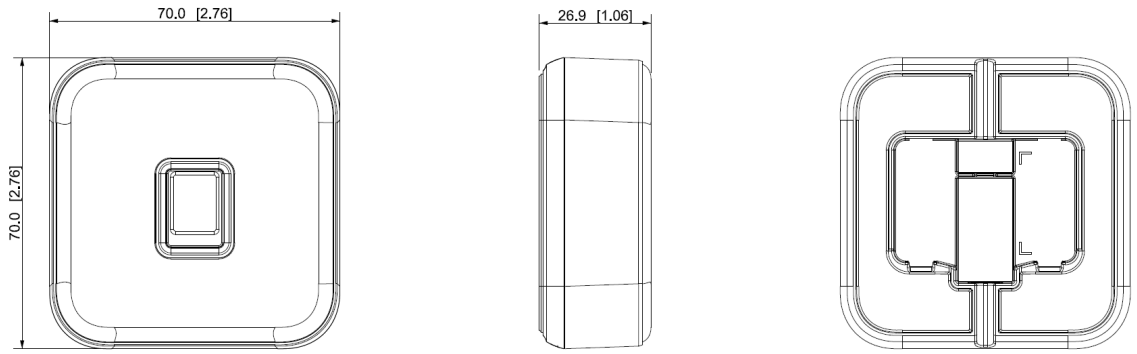
1.1 Features

- PC material and acrylic front panel with ultra-thin design.
- USB2.0 plug-and-play.
- Issue with IC (Mifare)/ID card.
- Collect fingerprints.
- Built-in buzzer and indicator light.
- Built-in watchdog to ensure Device stability.
- Safe and stable with overcurrent and overvoltage protection.

Functions vary with different models. The actual product shall prevail.

1.2 Dimensions

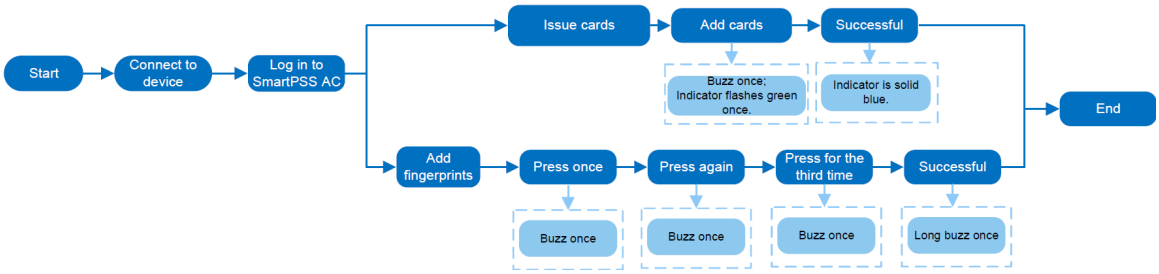
Figure 1-1 Dimensions (unit: mm [inch])



2 Device Operation

Before issuing cards, you need to install DSS Pro or SmartPSS AC on your PC, and then follow the process below. Take SmartPSS AC as an example.

Figure 2-1 Process

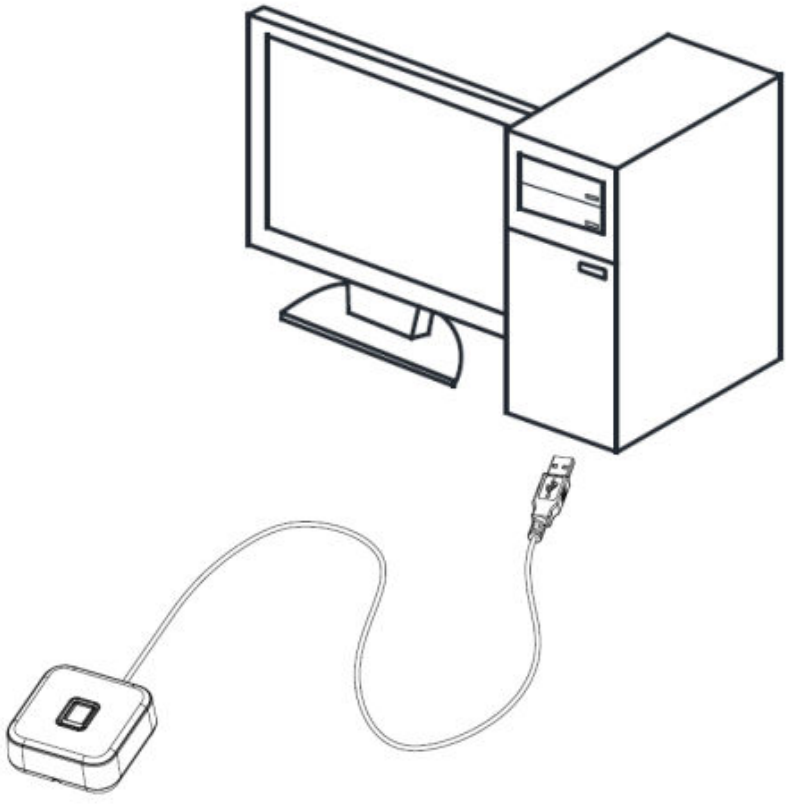


2.1 Issuing Cards

Procedure

Step 1 Connect the USB cable of the Device to the PC, and then the indicator of the Device will be solid blue.

Figure 2-2 Connect the Device to the PC



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

Step 3 Click **Card Issuing Type**, and then select the type as needed.

Step 4 Click **User** on the left menu.

- If you need to add a new user, click **Add** , enter the basic information, and then click **Certification**.
- For an existing user, click on the right, and then click **Certification**.

Step 5 On the right of the **Card** section, click , select the card reader, and then click **OK**.

Step 6 Click **Add**. The Device buzzes once, and the indicator flashes green.

Step 7 Swipe the card on the Device and it buzzes once.

The system reads the card number, and the indicator flashes green.

Step 8 Click **OK** to finish the process.

The Device indicator turns solid blue as standby mode.

- The card reader can only read one card at a time. When multiple cards stack together, it cannot work properly.
- Each user can have five cards at most.

Related Operations

Click **User** , select the users as needed, and then click **Batch Issue Card**.

- Automatically read card number.
  1. Select **Card Issuer**.
  2. Click **Issue**.
  3. Swipe the cards in the order of the user list, and the system will automatically read the card numbers. You can configure the information for each user, including the start and end time. Click **OK**.
- Enter card numbers manually.

  Select each user and enter the corresponding card number, and then click **OK**.

2.2 Collecting Fingerprint

Procedure

Step 1 Connect the USB cable of the Device to the PC, and then the indicator of the Device will be solid blue.

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

Step 3 Click **User** on the left menu.

- If you need to add a new user, click **Add** , enter the basic information, and then click **Certification**.
- For an existing user, click on the right, and then click **Certification**.

Step 4 On the right of the **Fingerprint** section, click , select **Fingerprint Scanner**r, and then click **OK**.

Step 5 Click **Add**.

Each user can have 3 fingerprints at most.

Step 6 Click **Add Fingerprint**, and then follow the instruction to press your finger three times on the fingerprint collecting area of the Device.

Table 2-1 Description of sound prompt when collection fingerprints

Situation	Sound Prompt
Press finger once	Success: Buzz once; Timeout: Buzz three times.
Press finger for the second time	Success: Buzz once; Timeout: Buzz three times.
Press finger for the third time	Success: Buzz once; Timeout: Buzz three times.
Result	Success: Long buzz once; Failure: Buzz three times.

3 Fingerprint Collecting Instruction

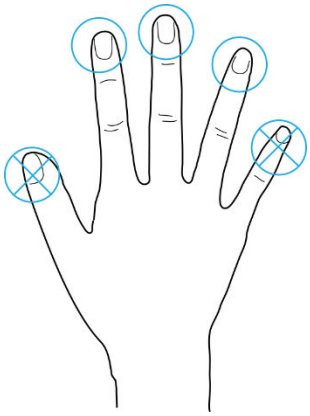
When you register the fingerprint, pay attention to the following points:

- Make sure that your fingers and the scanner surface are clean and dry.
- Press your finger on the center of the fingerprint scanner.
- Do not put the fingerprint sensor in a place with intense light, high temperature, and high humidity.
- If your fingerprints are unclear, use other unlocking methods.

Fingers Recommended

Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Figure 3-1 Recommended fingers



How to Press Your Fingerprint on the Scanner

Figure 3-2 Correct placement

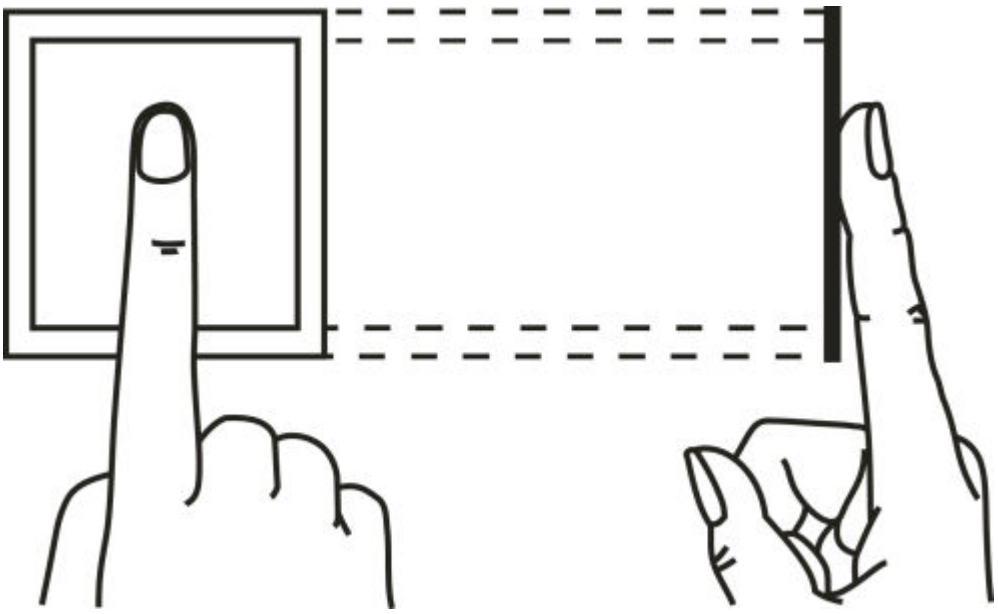
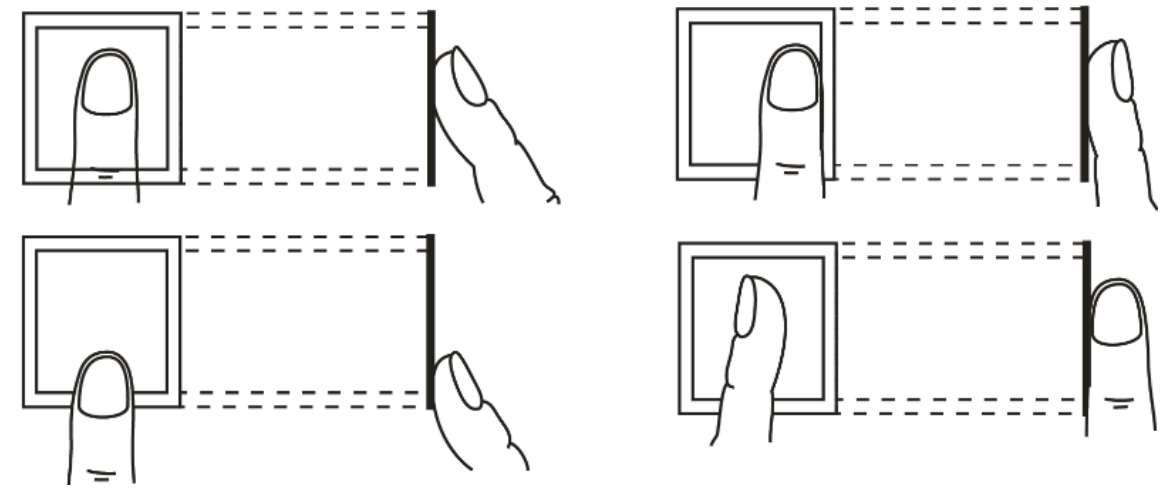


Figure 3-3 Wrong placement



4 Upgrade

Use the USB upgrade tool to upgrade the program of the Device.

Prerequisites

- Download the USB upgrade tool to your PC.
- Use a USB cable to connect the Device to your PC.

Procedure

Step 1 Double-click to run the program.

Step 2 Click **Search Device**.

Step 3 Click **Browse**, and then select the update file.

Step 4 Select the device as needed, and then click **Upgrade**.

When the progress bar reaches 100%, the upgrade completes.

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).