D.one®

# 智能管理系统

## 指纹识别仪

## DW-FP1

# 使用说明书

深圳丽泽智能科技有限公司

# 前　言

DW-FP1 指纹仪有完善的用户权限管理。但为了避免拥有管理权限的用户不在场，而客户又急需设置本系统，本系统特设了一个复位密码。拥有复位密码的人可以进入系统将设备恢复到出厂时的设置。

特别注意事项：

1、　出厂时所有的 DW-FP1 的复位密码均为 888888888，客户在成功安装后，正式使用前，需自行修改此复位密码。复位密码的长度为 6～9 位。

2、　复位密码是在客户不得已的情况下才使用的。若使用复位密码恢复出厂设置，则该系统中原有的用户数据将全部丢失，参数设置也将恢复成出厂时的设置。需重新登记用户才可使用。

3、　若遗忘了复位密码则只能回厂重新更新为缺省密码，但所有的数据将全部丢失。

- **主要技术参数指标：**

| 项目 | 技术参数 |
|---|---|
| 传感器类型 | 电容式 CMOS 传感器 |
| 传感器分辨率 | 508dpi |
| 传感器有效面积 | 18.2mm×12.8mm |
| 指纹处理器外形尺寸 | 147mm×81mm×27mm |
| 拒真率 | <0.02% |
| 认假率 | <0.0003% |
| 指纹比对时间（1：1 比对） | ≤0.5S |
| 指纹接受平面角度 | ±30° |
| 验证模式 | 仅使用指纹、指纹或密码、指纹与密码 |
| 指纹验证方式 | 1：1；1：X；1：N |
| 工作方式 | 脱机工作*，可联网辅助管理 |
| 最大用户容量 | 1000 个用户（每个用户最多 3 枚指纹） |
| 最大指纹容量 | 3000 枚 |
| 最大日志容量 | 验证日志 16383 条，管理日志 4095 条 |
| 验证优先级 | 1～10 级 |
| 工作温度 | －10℃～55℃ |
| 工作湿度 | 相对湿度 40％～90％ |
| 动态功率（不含锁具功率） | 直流 12V　小于 2W |

*注：这里所说的脱机使用是指通电后在指纹处理器上即可完成用户数据的登记与存储、系统信息的查询与设置、指纹数据的验证、日志信息的记录与存储、提示信息的显示等，这些工作不需要与 PC 联网就能完成.处理器输出维根信号，配合维根控制器可控制门锁的开合。

# 目　录


1 概述 - 1 -
1.1 指纹门禁系统构成 - 1 -
1.2 指纹仪接线说明 - 1 -
1.3 名词解释 - 1 -
2 功能概述 - 3 -
2.1 界面语言选择 - 3 -
2.2 系统复位功能 - 3 -
2.3 设备管理功能 - 4 -
2.3.1 用户管理 - 4 -
2.3.1.1 增加用户 - 4 -
2.3.1.2 修改用户 - 4 -
2.3.1.3 删除用户 - 4 -
2.3.1.4 查看用户容量 - 4 -
2.3.2 日志查询 - 4 -
2.3.3 系统管理 - 5 -
2.3.3.1 设置时间和日期 - 5 -
2.3.3.2 设置时段 - 5 -
2.3.3.3 设置验证模式 - 5 -
2.3.3.4 设置安全等级 - 5 -
2.3.3.5 设置通信参数 - 5 -
2.4 开门验证功能 - 6 -
2.4.1 开门方式 - 6 -
2.4.1.1 指纹开门 - 6 -
2.4.1.2 密码开门 - 6 -
2.4.1.3 指纹与密码开门 - 6 -
2.4.1.4 手指关联开门 - 6 -
2.4.2 指纹验证的比对方式 - 6 -
2.4.2.1 完整用户编号 + 指纹 （1：1 验证） - 7 -
2.4.2.2 部分用户编号 + 指纹 （1：X 验证） - 7 -
2.4.2.3 直接指纹验证 （1：N 验证） - 7 -
2.5 日志功能 - 7 -
2.5.1 验证日志（最多 16383 条） - 7 -
2.5.2 管理日志（最多 4095 条） - 7 -

3 操作说明 - 7 -
3.1 传感器的使用 - 7 -
3.2 待机状态 - 8 -
3.3 界面语言的选择 - 8 -
3.4 系统复位功能 - 8 -
3.4.1 修改复位密码 - 9 -
3.4.2 恢复出厂状态 - 9 -
3.5 空机状态下的超管登记 - 10 -
3.6 管理员进入管理菜单 - 11 -
3.6.1 用户管理菜单 - 12 -
3.6.1.1 增加用户 - 12 -
3.6.1.2 修改用户信息 - 14 -
3.6.1.3 删除用户 - 14 -
3.6.1.4 查询用户容量 - 15 -
3.6.2 日志查询菜单 - 15 -
3.6.3 系统管理菜单 - 16 -
3.6.3.1 安全设置 - 16 -
3.6.3.1.1 验证模式 - 16 -
3.6.3.1.2 安全等级 - 17 -
3.6.3.1.3 报警韦根 - 17 -
3.6.3.1.4 离线报警 - 17 -
3.6.3.2 通信设置 - 17 -
3.6.3.2.1 节点号 - 17 -
3.6.3.2.2 通信密码 - 17 -
3.6.3.2.3 波特率 - 18 -
3.6.3.3 时钟与时段 - 18 -
3.6.3.3.1 设置日期 - 18 -
3.6.3.3.2 设置时间 - 18 -
3.6.3.3.3 设置时段 - 19 -
3.7 普通用户查看日志 - 20 -
3.8 使用指纹进行开门验证 - 20 -
3.9 使用密码进行开门验证 - 21 -
3.10 系统版本信息查询 - 22 -

# 1 概述

DW-FP1 指纹仪最多可存储 1000 个用户数据，每个用户最多可登记 3 枚指纹，即本系统最多可存储 3000 枚指纹；

### 1.1 指纹门禁系统构成

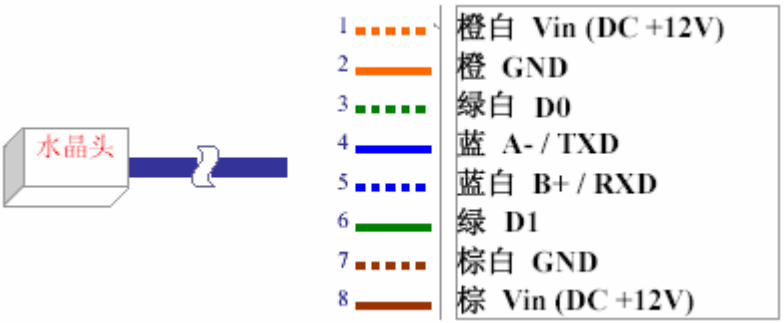
**处理器：**它实现了用户数据的登记与存储、系统信息的查询与设置、指纹数据的验证、日志信息的记录与存储、提示信息的显示等。主要包括指纹处理模块、液晶显示屏、键盘、门铃按钮、指纹传感器、复位键、外壳等部分（下文中也将之称为“设备”）.

### 1.2 指纹仪接线说明

DW-FP1 指纹识别仪主要实现脱机实时指纹登记、对比及安全控制、指纹数据存储、跟 PC 机进行联机通信等功能。该产品可以方便地接入 IC 卡门禁系统，取代原系统的 IC 读卡器，独立完成各项指纹处理功能，然后把指纹验证成功后得出的 ID 号（个人身份号码），以维根信号方式发送到门禁控制器进行应用处理，从而组成了韦根通信标准的指纹门禁控制系统。既可通过指纹验证控制出入，同时配合考勤管理软件也可组成高效完善的指纹考勤系统。

DW-FP1 指纹识别仪背部的 RJ45 接口用于连接主控制器的线缆。用户可根据实际需要购置相应长度的五类或超五类网线，一头使用 8P8CRJ45 水晶头压制插入 DW-FP1 的 RJ45 接口，制作方法与以太网网线的制作相同，水晶头连接线的制作图示如下图所示，连接线另一头根据具体定义连接到主控制器上。

**注：水晶头上定义顺序是左 1 右 8。**




1） 1、2、7、8 脚用于主控制器提供DC+12V电源到DW-FP1，1、8脚同时接到DC+12V，2、7脚同时接到GND；
2） 3、6 脚是DW-FP1与主控制器之间的韦根信号通讯线；
3） 4、5 脚是PC 与DW-FP1 通过RS485 方式通讯的数据收发线，如果用户需要从DW-FP1 中读取指纹数据保存到PC上时，就需要应用2、4、5 脚接线到RS232/RS485 转换器，再接到PC的串口，并使用专用的软件读取数据。
4） DC+12V 供电线路（1、2、7、8 脚）建议使用0.5 平方MM 以上线材，信号线（3、4、5、6 脚）采用16AWG~24AWG 型号的线材，尽量使用屏蔽线串管走线，减低外部干扰。
5） 如果由于距离过远，主控制器无法接收DW-FP1的信号，提供以下两点建议—— a、在DW-FP1安装位置就近取电，例如使用DC+12V电源适配器； b、建议加粗DC+12V供电线路（1、2、7、8 脚），例如使用0.5 平方MM 以上线材，或把暂时不用的信号线（4、5 脚）用于供电（使用4、5脚供电时，注意4、5脚不能接入RJ45 水晶头）。

### 1.3 名词解释

**用户的概念：**DW-FP1指纹系统存在有两类的用户概念，第一类是指DW-FP1指纹设备的用户，这类用户包括设备

的超级管理员、普通管理员及普通用户；第二类是指使用PC工具软件的用户，由于使用PC工具软件的用户可对设备的数据、参数进行设置、管理，因此也称为PC 管理员。两类用户的大体职责如下：

1) 第一类：

“超级管理员”、“普通管理员”和“普通用户”是设备的真正使用者，能根据不同的权限使用此系统进行验证开门、查询、管理等操作；其中“普通用户”只具有使用权限，而“超级管理员”、“普通管理员”具有级别不同的设备管理权限；

2) 第二类：

PC管理员的职责是使用PC 工具软件对设备的数据进行维护，主要包括管理日志和验证日志的导出及处理，系统参数的维护、用户数据的备份和恢复等。(注：PC管理员使用PC 工具软件与设备进行通讯时，应该保证设备处于空闲的待机状态，否则将无法与之成功通信)

**用户权限：**设备上的三种用户具有不同的操作权限，按从高到低，排列如下：

超级管理员 > 普通管理员 > 普通用户；

**普通用户：**普通用户不具有任何管理权限，只能进行一般的开门验证操作，或在设备上查询自己的验证日志信息，或修改设备使用的界面语言。

**普通管理员：**除了能进行普通用户所能进行的操作外，还拥有对除“超级管理员”外的用户的管理权限。即可以增加、删除或修改“普通管理员”或“普通用户”的数据；此外还可以在设备上查询任何用户的验证日志信息；

**超级管理员：**拥有系统的最高操作权限：除了能进行普通管理员所能进行的操作外，还可以进入系统的“系统管理”菜单进行各项参数的设置；可以增加、删除或修改任何用户的数据，或删除全部用户使系统重新进入空机状态；【注意：不能单独删除自己】。下文为了简便，有时会将“超级管理员”简称为“超管”。

**空机状态：**DW-FP1处于无用户状态，也就是处理器端没有登记任何用户数据（包括超级管理员、普通管理员和普通用户）或所有用户数据都已被删除：这种状态称为空机状态。

**待机状态：**当 DW-FP1没有接收到任何按键输入而处于空闲等待的状态时，就称为待机状态；在待机状态下，液晶屏幕会显示当前的日期和时间。

**门状态：**指门的开关状态。若用户安装了门状态检测开关（如门磁开关等）并接入DW-FP1指纹门禁系统，则系统可时刻检测门的开关状态。

**锁状态：**指锁的开关状态。若用户安装了锁状态检测开关（大多数电控门锁本身即带有锁状态检测开关）并接入 DW-FP1指纹门禁系统，则系统可时刻检测锁的开关状态。

**出门开关：**指纹门禁系统的一个选装部件。可安装在门内，用户在门内按动此开关即可开锁。

**脱机使用：**本文所述的脱机使用是指通电后在指纹处理器上即可完成用户数据的登记与存储、系统信息的查询与设置、指纹数据的验证、日志信息的记录与存储、提示信息的显示等，这些工作不需要与 PC 联网就能完成。

**联网辅助管理：**本门禁系统各机型都提供与 PC 机的连接方式，可通过 RS485/TCP 等实现与 PC 机的联网，使得客户可以在 PC 机端通过辅助的工具软件实现对门禁系统的管理，进行各项参数的设置，并可实现用户数据的备份和恢复等，大大方便了客户管理多台门禁系统。

下文多处提到与 PC 机的联网通讯功能。但若要成功实现与 PC 机的通讯，还需要参见下文与“通信”有关的描述来设置指纹处理器上的某些参数。若客户不需要与 PC 机联网通讯，可忽略。

**本地报警：**由锁控单元内部蜂鸣器产生报警声。在报警的门禁系统附近的人都可听到此报警声。

**远程报警：**从指纹门禁系统中向外引线至远方的报警器，在远处（例如警卫室等地方）产生报警声。在报警的门禁系统附近的人听不到此报警声。

**报警手指：**用户登记指纹时可以指定某一个手指为报警手指（未被指定为“报警手指”的手指称为“正常手指”）。

当用户用该手指完成“验证开门”操作或“菜单登录”操作时，系统将发出远程报警信号。报警手指一般在人身安全受到威胁时使用。

**正常开门：**用户使用已授权手指（包括正常手指或报警手指）通过本门禁系统来进行“验证开门”，或通过“出门开关”开门的过程，称为正常开门。

**非法开门：**在本门禁系统正常工作时，在使用过程中如有除正常开门外的其他开门动作，均称为非法开门。例如有人通过非正当手段（如使用暴力方法撬开门锁等）打开门锁或用钥匙（若用户配备的电控门锁附带钥匙）打开门锁等。

**指纹验证和密码验证：**本系统支持指纹和密码的单独验证以及指纹与密码的组合验证。其中的密码单独验证方式是针对部分用户指纹质量较差，指纹登记或验证时可能存在困难的情况，而特别设计出的验证方式。至于指纹与密码的组合验证则可以提高整个系统的安全性。

**手指关联：**为了提高用户本人使用系统的安全性，用户登记 2 个正常手指后可以设置 2 个手指关联；登记 3 个正常手指后可以选择设置 2 个手指关联或 3 个手指关联；若设置了手指关联，那么用户使用指纹验证身份时，必须所设关联个数的手指均验证通过才视为验证通过。

**拒真率：**其含义是指将相同的指纹误认为是不同的指纹，而加以拒绝的出错概率。常用百分比来表示，其数值越小越好。

**认假率：**其含义是指将不同的指纹误认为是相同的指纹，而加以接受的出错概率。常用百分比来表示，其数值越小越好。

# 2 功能概述

### 2.1 界面语言选择

任何用户都可以自行选择“简体中文”或“英文”作为显示界面的语言。即用户不需要验证身份，只需通过简单的几次按键就能进入语言设置界面选择自己熟悉的语言，极大地方便了使用异种语言的人能快速进入自己所熟悉的语言环境。

系统默认的界面语言为“英文”。

### 2.2 系统复位功能

DW-FP1 指纹门禁系统有完善的用户权限管理。但为了避免拥有管理权限的用户不在场，而客户又急需设置本系统，本系统特设了一个复位密码。拥有复位密码的人可以进入系统将设备恢复到出厂时的设置。

注意：

1、 出厂时所有的 DW-FP1 系列产品的复位密码均为 888888888，客户在成功安装后，正式使用前，需自行修改此复位密码。复位密码的长度为 6～9 位。

2、 复位密码是在客户不得已的情况下才使用的。若使用复位密码恢复出厂设置，则该系统中原有的用户数据将全部丢失，参数设置也将恢复成出厂时的设置。需重新登记用户才可使用。

3、 若遗忘了复位密码则只能回厂重新更新为缺省的复位密码，但所有的数据将全部丢失。

### 2.3 设备管理功能

#### 2.3.1 用户管理

用户管理功能包括了：1）增加用户，2）修改用户，3）删除用户，4）查看用户容量；

##### 2.3.1.1 增加用户

1）增加新用户必须输入新增用户的编号。系统中每个用户编号都是唯一的，不能重复；合法的编号范围为 1-65535 之间的任意数值。
2）进行新增用户登记时，可以选择新增用户的使用权限，并且可以选择：a.只登记指纹，b.只登记密码，c.同时登记指纹和密码； 但如果新增的用户权限是“超管”，则必须同时登记指纹和密码；
3）每用户最多可登记 3 枚指纹（每枚指纹采样两次），可设定其中一枚为报警手指，也可不设；
4）当用户登记的指纹（报警手指除外）数多于 1 枚时，可以指定是否启用 2 指或 3 指关联开门功能；
5）提供了设定用户验证优先级别的功能，使用户进行验证操作时所获得的比对速度能够得到相对的控制。优先级的设置范围共分 10 级（1-10）；当设定为 1 级时能获得相对最高的验证速度；
6）提供了简单的时段限制功能：如果启用此功能，则用户可以在系统设定的四个时段中选择自己适用的时段（最多选三个）：当系统时间处于用户选定的时段范围内时，用户可以通过验证开门，而其他时间则不能。
（在不启用该功能时，用户在任何时间内都可以通过验证开门）

##### 2.3.1.2 修改用户

各级管理员都可以修改权限不高于自己的用户的如下信息：
1） 验证优先级
2） 时段的选择
3） 验证密码
也就是说，用户的验证“优先级”、“时段限制”，以及验证“密码”等三项信息，在使用的过程中可以根据需要由管理员进行灵活的更改，并且超级管理员可以对任意一个用户的上述信息项进行修改；而普通管理员则只能修改普通管理员或普通用户的相关信息。
若需要修改用户的其他信息，则只能删除该用户后重新登记。

##### 2.3.1.3 删除用户

1）删除操作有两种操作形式：a.逐个删除，b.批量删除；
2）“超级管理员”可批量删除全部用户（系统将变为空机，并自动退出管理菜单，回到待机状态），或批量删除除“超级管理员”外的所有用户，或批量删除所有普通用户；也可逐个删除指定编号的用户，但不能单个删除自己；
3）“普通管理员”只能批量删除普通用户，或逐个删除权限不高于自己的用户，但不能删除自己。

##### 2.3.1.4 查看用户容量

本系统可容纳的总用户数为 1000 人（包括用户和管理员）。此功能提供了对系统现时用户容量使用情况的查询途径，可查看的信息包括：
1）已登记的管理员个数（包含了“超级管理员”和“普通管理员”）；
2）已登记的普通用户个数；
3）空闲用户数（指还可以登记的用户个数）；

#### 2.3.2 日志查询

此功能可以在液晶显示屏上列出指定用户在指定日期的当天，所有验证操作通过时的系统时间：
1）普通用户在通过身份验证后，可以查询自己的验证日志；
2）超级管理员和普通管理员在通过身份验证后，可以查询指定的任一用户的验证日志；

### 2.3.3 系统管理

系统管理功能包括了：各种安全参数、通信参数的设置，以及日期、时间和系统时段的设置；

**注意：**

**只有“超级管理员”能进入系统管理菜单，进行各项系统参数的设置；**

#### 2.3.3.1 设置时间和日期

对系统的实时时钟进行设置，支持从 2005 年到 2063 年间的所有合法日期和时间的设定，对超出范围或非法的输入将给出错误提示；

#### 2.3.3.2 设置时段

时段设置功能中，提供了 4 个时段值给超级管理员设置；而每个用户最多可以从这 4 个时段值中选择 3 个，作为自己的使用时段；

在系统及用户均启用了时段限制功能的情况下，这些时段值限定了用户能够进行开门验证的具体时间段：仅当系统时间处于这些时段值的范围内，并且用户的个人数据中也选用了这个时段时，用户才能通过验证开门，而其它时间即使验证通过也不能开门。

系统默认未启用时段限制功能。

注意：

1）如果系统的 4 个时段都设为 “未设置”，则表示系统不启用时段限制功能，所有用户都可以在任何时间内通过验证而开门；

2）如果用户的个人数据中，3 个时段都设为 “未设置”或变成“无效设置”，则表示该用户不启用时段限制功能，系统的时段限制对之无效，用户可以在任何时间内通过验证而开门。

3）时段限制功能只对“开门”验证操作进行限制，对进入管理功能的身份验证不做限制。

#### 2.3.3.3 设置验证模式

系统的验证模式可以设置为以下 3 种。当设置为其中一种验证模式之后，系统中的所有用户都只能使用该验证模式验证进入系统。系统默认的验证模式是“指纹或密码”。

**只使用指纹**

用户想进入管理功能或进行开门验证时，必须通过系统的指纹验证才能进入。也就是说，对于只登记了密码的用户，在此模式下将无法使用系统；

**指纹或密码**

用户想进入管理功能或进行开门验证时，只需要通过指纹验证或密码验证两种方式中的任意一种，就可进入系统；

**指纹与密码**

用户想进入管理功能或进行开门验证时，必须同时通过指纹验证和密码验证两种验证方式才能进入系统。也就是说，对于只登记了密码而没登记指纹，或只登记了指纹而没登记密码的用户，在此模式下将无法使用系统；

**F 在进行新增用户登记时，建议同时登记指纹和密码，以避免在系统转换验证模式后用户无法进门**

#### 2.3.3.4 设置安全等级

用户可以对系统指纹验证的“安全等级”进行设置,可选范围为 1-5；设置的等级数值越大，安全性就越高；系统默认的安全等级为 3。建议不要轻易修改此设置，尤其是不要轻易将其置低。

**注意：设置的安全等级越高，拒真率就越高（相应的误认率则越低）；设置的安全等级越低，拒真率就越低（相应的误认率就越高）**

#### 2.3.3.5 设置通信参数

系统提供了三项有关通信的参数设置：设备“节点号”、“通信密码”和“波特率”；

若客户需要使用 PC 与指纹门禁系统联网，实现远程管理，则需要在设备上设置正确的通信参数。若不需要与 PC 联网通讯，可不做任何设置、修改。

**“节点号”**是 PC 与设备通信时指定的设备目的地址，合法范围为 0～250；处于同一个局域网内的指纹处理器的节点号不能相同。

系统出厂时默认的节点号为 0。

**“通信密码”**是为了提高系统联网通讯使用的安全性而特别提供的：当设备设置了自己的“通信密码”后，PC 端的工具软件将必须通过该密码的验证，才能和此设备进行数据通信；如果设备未设置此密码或者密码已被清除，则 PC 与设备的通信就不需通过密码验证。

系统的默认通信密码是空，即未设置的。

**“波特率”**是设备与 PC 通信时设备所使用的通信速率；相应地，PC 也应该设置相同的波特率双方才能够正常通信。

系统默认的波特率为 9600bps。

### 2.4 开门验证功能

由于进入管理菜单时的身份验证操作与开门验证的操作流程基本相同，后文只针对开门验证操作进行具体说明。

两者的不同点在于：

1、 前者验证通过之后的动作是进入管理菜单，后者验证通过之后的动作是进行开门操作。

2、 前者不论在哪种验证模式下，使用何种验证方式，都必须输入完整的用户编号，即只能使用 1：1 验证；后者则在非密码开门的情况下，可由用户根据情况自行选择是否输入用户编号，即可以使用 1：1、1：X 和 1：N 验证。

如果用户使用报警手指进行验证且验证成功，则门禁系统在开锁或进入管理菜单的同时，会发出远程报警信号，但不发出本地报警信号。

#### 2.4.1 开门方式

##### 2.4.1.1 指纹开门

在“只使用指纹” 或在“指纹或密码”的验证模式下，用户可直接用已登记过的手指进行指纹验证，如果指纹比对正确则开门。(也可输入部分或完整的用户编号后再放手指，具体参见下文的“指纹验证的比对方式”)

##### 2.4.1.2 密码开门

在“指纹或密码”验证模式下，用户除了可使用上述的指纹方式开门外，还可采用输入密码的方式开门，具体步骤如下：首先输入用户完整的编号并按确认键确认后，再输入密码进行验证，如果密码验证正确则开门。

##### 2.4.1.3 指纹与密码开门

在“指纹与密码”验证模式下，用户必须同时通过上述指纹开门验证和密码开门验证，才能开门。此开门方式提高了整个系统的安全性。

在此验证模式下，用户既可先通过指纹开门验证后，再直接输入密码进行密码开门的验证；也可先通过密码开门验证后，再直接放手指进行指纹验证。

##### 2.4.1.4 手指关联开门

在进行“指纹验证”操作时，若用户登记有两个或三个手指，并且启用了手指关联功能，则此用户使用指纹验证开门时就必须验证通过所关联个数的所有手指,但不规定放手指的顺序。此开门方式提高了该用户使用本系统的安全性。

#### 2.4.2 指纹验证的比对方式

用户使用指纹验证方式开门时，根据操作方式的不同，会得到不同的比对速度：

1）输入完整用户编号并确认后再用指纹验证（**1:1**）；

2）输入部分用户编号后再用指纹验证（**1:X**）；

**3**）直接用指纹验证（1:**N**）；

以上 3 种操作方式所得到的比对速度依次为：**1:1** 最快； **1:X** 次之；**1:N** 最慢。

用户可根据需要选择不同的验证比对方式。

除了可以使用不同速度的验证比对方式，系统还提供了可为某些特殊用户设置高的用户验证优先级的方法，以提高他们在使用 1：X 和 1:N 的比对方式时的验证速度。优先级的设置方法我们在增加用户的详细操作中再做说明，这里就不细说了。以下是对 3 种不同的比对方式的详细介绍：

#### 2.4.2.1 完整用户编号 + 指纹 （1：1 验证）

在待机状态下，用户输入完整的用户编号并按确定键确认后，再用此用户已登记的某枚手指轻按传感器进行指纹比对。在此情况下，指纹比对仅对该用户编号的指纹数据进行比对，最大限度地缩小了比对范围，加快比对速度。若指纹比对成功，则验证通过。

#### 2.4.2.2 部分用户编号 + 指纹 （1：X 验证）

指纹“一比 X”验证其实是一种缩小用户范围的“一比多”验证。通过由用户输入用户编号的一部分（编号的头部任意位数字，或尾部任意位数字）来缩小指纹比对范围，从而提高验证速度。例如编号为 6618 的用户，可以在待机状态下输入 6、66、661 或 6618（或输入 8、18、618 或 6618），然后再用指纹验证；输入编号的位数越多，得到的验证速度也将越快。

**注意：**用户采用 1:X 验证，在输入部分用户编号后**不要按确定键**，而应直接放手指，否则会被视为输入完整用户编号的 1：1 验证。

#### 2.4.2.3 直接指纹验证 （1：N 验证）

指纹“一比多”验证不需要输入用户编号。在待机状态下，用户直接用已登记的某枚手指轻按传感器，该手指指纹将和设备指纹库内所有指纹进行比对，若比对成功则验证通过。

### 2.5 日志功能

#### 2.5.1 验证日志（最多 16383 条）

本系统在每次用户成功通过开门验证（或进入管理菜单的身份验证）后，都会生成一条用户的验证日志记录，保存了用户通过验证的时间和用户编号，具有完善的考勤功能；用户可以利用我公司提供的开发包，编写程序读出验证日志；可以直接在设备上查询验证日志：普通用户只能查询自己的验证日志；而超级管理员和普通管理员则可以查询设备上任一用户的验证日志。

#### 2.5.2 管理日志（最多 4095 条）

管理员对系统参数所进行的每一次修改操作，或对用户数据所进行的每一次增、删、改操作，都会使系统自动生成一条管理日志记录，保存在管理日志里；用户可以利用我公司提供的开发包，编写程序读出管理日志；

## 3 操作说明

**特别提示：**在本说明书中，如无特别指明，在指纹处理器的键盘区域的“*”键表示“回车”、“确定”、“是”等确认键，“#”键表示“退出”、“取消”、“否”等取消键。

### 3.1 传感器的使用

指纹传感器是精密元件，应避免用尖硬物件戳其表面以防划伤（尤其是安装时更要注意!），应保持其表面干净清洁，如有污迹可用药用脱脂棉花沾水横向擦拭清洁。

**手指的放置**

为了取得清晰的指纹图像，手指指纹面应紧贴传感器并按照下图正确位置放置，如图：

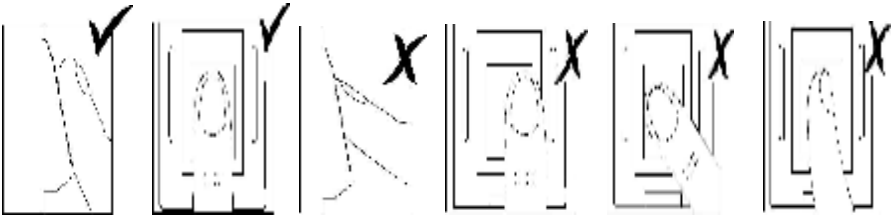


图 1a　　图 1b　　图 1c　　图 1d　　图 1e　　图 1f

说明：

图 1a 和图 1b 显示正确的手指放法，图 1a 为侧面图，图 1b 为正面图。

图 1c、图 1d、图 1e 和图 1f 为错误的手指放法，图 1c 为侧面图，图 1d、图 1e 和图 1f 为正面图。

（注：放上手指轻压传感器时应按动其下方的轻触开关，但不宜用力过大。此说明在下文中不再赘述）

### 3.2 待机状态

在连接好指纹处理器和锁控器，并给系统上电后，屏幕将显示系统版本号、节点号和设备序列号信息，数秒后进入待机状态，显示日期和时间，如下图所见：

```
2005-09-30
10:10:30
```

### 3.3 界面语言的选择

在“空机”的待机状态下按“*”键，会出现如下图 1 的屏幕信息；在非“空机”的待机状态下按“*”键，则出现如下图 2 的屏幕信息：

```
请选择
1.  菜单登录
2.  系统复位
3.  Language
```

（图 1）

```
请选择
1.  超管登记
2.  系统复位
3.  Language
```

（图 2）

此时按键 “3”，可直接进入系统的语言设置界面：

```
Language
1.  中文
2.  English
```

选择“1”或“2”，可以使系统显示的语言在这两种语言中切换。

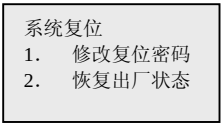
### 3.4 系统复位功能

在图 1 或图 2 的状态下按键“2”，屏幕显示如下：

```
请输入
复位密码：
```

**F** 出厂时或执行系统复位操作后，所有的 DW-FP1 产品的复位密码均为 888888888；

拥有复位密码的人可以在通过该密码的身份验证后，进入复位功能菜单：



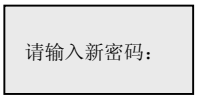

（复位功能菜单）

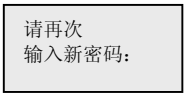
### 3.4.1 修改复位密码

**F 客户在成功安装后，正式使用前，必须自行修改此复位密码，并将之妥善保管。**

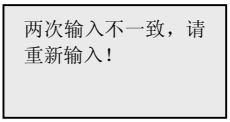
在复位功能菜单下按键 “1”，进行复位密码修改，屏幕提示如下：

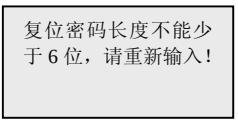

为了复位密码使用的安全性，用户修改此密码之前，需要先输入旧密码，旧密码验证成功后，才能进行新密码的设置：




复位密码的长度为 6～9 位。如上图所示，设置新密码要连续输入两次，两次相同才算设置成功；在输入的密码不符合要求时，系统可能会有如下提示：



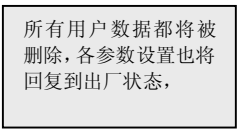




正确设置密码后，屏幕提示操作成功，并返回上层菜单。

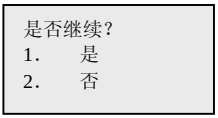
### 3.4.2 恢复出厂状态

**F 此功能是在客户不得已的情况下才使用的。若使用复位密码恢复出厂设置，则该系统中原有的用户数据将全部丢失，参数设置也将恢复成出厂时的设置。需重新登记用户才可使用。**

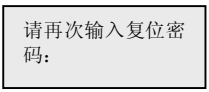
在复位功能菜单下按键 “2”，将进入把设备恢复为出厂状态的操作过程，屏幕输出信息如下：



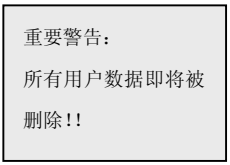

然后，询问用户是否继续进行操作：

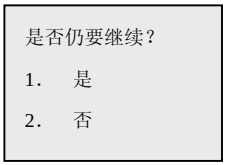



由于此操作的特殊性，为了慎重起见，在用户按“1”确认后，系统还会要求用户再进行一次复位密码的验证：

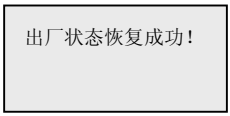


当用户通过了再次的密码验证后，系统给出最后的警告信息：




如果用户按“1”确认要执行此操作，则系统在删除所有用户数据，并把系统的所有参数设置恢复到出厂状态后，输出信息如下：



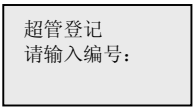

约 2 秒后返回待机状态。

此时系统已回复到空机状态，复位密码也回复到出厂时的缺省密码“888888888”；客户必须修改此复位密码，并重新登记用户数据后才可继续使用系统。

### 3.5 空机状态下的超管登记

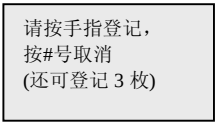
当设备的全部用户已被删除，或处于初始的无用户状态时，在待机状态下按“*”键，屏幕显示如下：


此时按键“1”，则进入系统第 1 个用户——超级管理员的登记界面，提示见下：




用户可通过键盘输入一个取值范围在 1～65535 之间的数值作为用户编号，然后按“*”键确认，将出现下面的指纹登记界面：

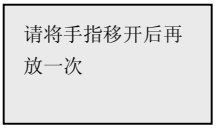
（注意：如果用户输入的“用户编号”带有前零，如“0086”，系统会自动忽略前零并将之解释为“86”，即验证通过时显示的用户编号是“86”；此说明在下文中不再重复）




（图 3）

“超级管理员”必须登记至少 1 枚的指纹以及密码，所以此时应当用需要登记指纹的手指轻按传感器，当听到“嘀”的一声响后，用户可以把手指移开。

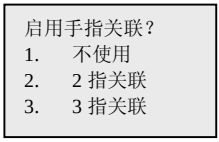
（而在登记“普通管理员”或“普通用户”时，可以按“#”键，放弃指纹登记而直接进入到后面的图 7 密码登记界面）



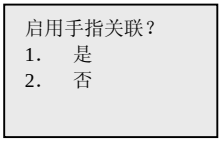

（图 4）

登记一个手指要对指纹采样两次，所以当第一次指纹图象的采集成功后，系统会提示“请将手指移开后再放一次”，如图 4 所示；这时应先拿开手指，然后再重新放上。

每个用户最多可以登记 3 个手指，并且最多只能设置其中 1 个为报警手指。根据用户的选择，以上图 3--图 4 的类似过程可能重复 1-2 次，直至完成指纹登记的处理。在用户登记的正常手指数多于 1 个的情况下，系统会询问是否启用手指关联功能，如下图 5 是用户登记了 3 枚指纹，且没有设置报警手指时的系统信息：




（图 5）

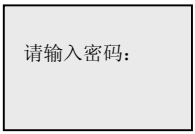


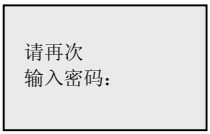

（图 6）

图 5 中，选择“1”，表示不使用手指关联功能；选择“2”，表示用户所登记的 3 个手指中，任意验证通过 2 个就算验证成功；选择“3”，表示用户必须同时验证通过所有手指才算验证成功；图 6 是用户登记了两个正常手指（包括：a.登记了 3 个手指，其中 1 个为报警手指；b.登记了 2 个手指，且都非报警手指）时的关联设置界面。如果用户只登记了 1 个手指；或登记了 2 个手指，但其中 1 个是报警手指，有关手指关联设置的信息将不会出现。

完成关联设置后，就到了密码设置过程，“超级管理员”必须登记密码，密码可以设置为 1-9 位的任意数值。（对于“普通管理员”或“普通用户”的登记，如果不想设置密码，可以按“#”跳至下一项设置界面，但指纹和密码两种登记方式，用户必须至少选择一种，否则登记操作将失败）

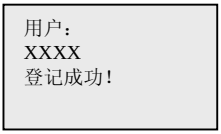
（注意：如果用户设置的“密码”带有前零：如“0123456”，则系统会保留前零；也就是用户在进行密码验证时也必须输入“0123456”，才能验证成功；此说明在下文中不再重复）




（图 7）

如上图所示，设置密码要连续输入两次，两次相同才算设置成功；正确设置密码后，屏幕显示：



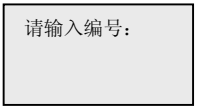

（用户登记操作成功）

约 2 秒后退回待机状态；此时，系统的第 1 个超级管理员用户就已登记成功：默认的验证优先级为最高级（1 级）；且不受系统的开门时段设置的限制；

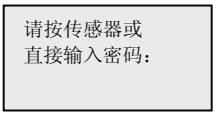
### 3.6 管理员进入管理菜单

在设备已登有用户数据的时候，待机状态下按“*”键，屏幕显示如下：

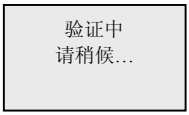
此时按“1”，进行菜单登录，屏幕提示如下：

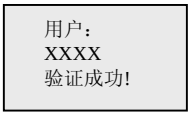



管理员输入自己的用户编号，并按“*”确认；当系统处于“指纹或密码”验证模式时，可见到如下提示：【注意：】进入管理菜单，必须输入完整的用户编号并按“*”确认。

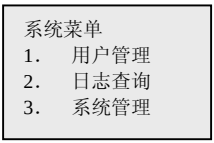



如果选择指纹验证，将看到“验证中请稍候…”的信息；如果验证通过，系统提示验证成功：

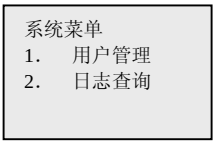



然后进入到如下的管理主菜单界面：




（主菜单 1）



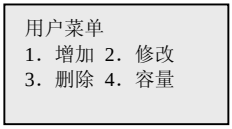

（主菜单 2）

**F** 主菜单 1：是以超级管理员身份通过验证时出现的管理界面；

**F** 主菜单 2：是以普通管理员身份通过验证时出现的管理界面。

### 3.6.1 用户管理菜单

选择主菜单中的“1”，进入用户管理菜单，见下图。在用户管理菜单里可以进行新增、修改、删除用户数据，或查看用户容量等 4 种操作：

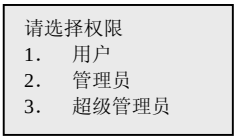



（用户管理菜单）

#### 3.6.1.1 增加用户

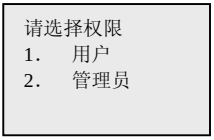
选择用户管理菜单中的“1”，进入增加新用户处理；登记新用户的过程与登记系统第一个超管用户的过程基本类似：首先需要输入新增用户的用户编号，如果输入编号已被使用，系统会给出提示，并要求重新输入；然后系统提示选择新增用户的权限，如下图 9 或图 10：

以超管身份登陆时：




（图 9）

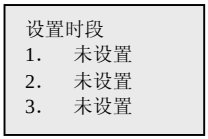
以普通管理员身份登陆时：




（图 10）

选好新增用户的权限后，将进入指纹和密码的登记操作，具体步骤与登记第 1 个超管时相类似，请参照超管登记：图 3--图 8；

完成指纹和密码的登记操作，就进入用户的时段设置界面，屏幕显示如下：

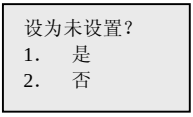



用户最多可以从系统设定的 4 个时段中选择 3 个作为自己的有效使用时段。

假设此时系统的 4 个时段值已经被分别设为“1．晚上 0 点至早上 6 点”、“2．早上 6 点至中午 12 点”、“3．中午 12 点至下午 6 点”以及“4．下午 6 点至晚上 12 点”，则当用户按下相应数字键，比如说按“2”，以设置该用户的第 2 项时段时，屏幕将输出当前系统所设置的 4 个时段值供选择，具体显示如下：


用户可以通过按数字键选择对应的时段值，比如现在按“3”，选择“中午 12 点至下午 6 点”的时段，则系统返回上层菜单，屏幕显示选择后的结果：

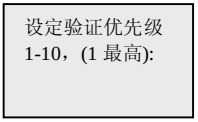

重复上述操作可继续对用户的时段 1 和时段 3 进行设置；如果需要修改某个已经设置过的时段值，则按相应数字键后，屏幕显示：



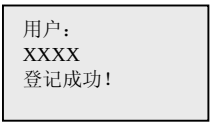

如果选择“是”，即可以把该项时段值恢复为“未设置”；而选择“否”，则可以重新选择时段值。

最后按“#”退出时段设置界面，如果用户的 3 个时段值都为“未设置”，屏幕会提示“用户没启用时段限制”，表示此用户不受系统的时段设置的限制，在全天的任何时间都可以通过验证进门；

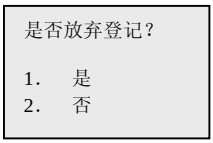
随后进入用户登记的最后一个步骤：设定新增用户的验证优先级，如下所示：




用户可以选择输入 1-10 之间的任意数值，输入数值越小得到的相对验证速度就越快，然后按“*”键确定，也就完成了增加用户的操作，屏幕提示如下：



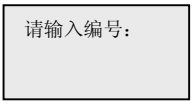
如果用户想放弃本次的登记操作，也可以在“验证优先级”的设置界面下按“#”，系统提示如下：



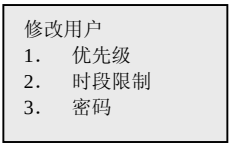

如果按“1”，当前正在登记的用户数据将被取消，并退回到上层的用户管理界面；如果按“2”，则返回“验证优先级”设置界面，用户可以继续完成当前用户的登记操作。

#### 3.6.1.2 修改用户信息

在“用户管理菜单”中按“2”，选择“修改”，屏幕提示输入要进行修改的用户的编号：




正确输入需要查询或修改信息的用户编号，然后按“*”确定，屏幕显示如下：

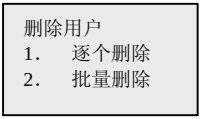



选择对应的信息项，并按照屏幕的提示进行操作，可对用户的优先级、时段限制、密码等三个信息项进行查看或修改。

**注意：**若当前做修改操作的管理员权限低于要修改的用户权限，则被视为越权操作，系统会给出操作非法的提示信息；若所输入编号的用户不存在，也会有相应的提示。

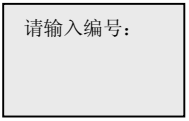
#### 3.6.1.3 删除用户

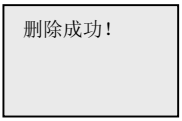
“用户管理菜单”中按“3”，进入删除用户的操作界面，如下：



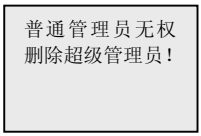

（图 11）

删除操作分逐个删除和批量删除两种，选择逐个删除方式时，系统要求输入要删除的用户编号：

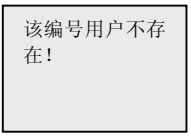



如果输入的编号存在，并且不是越权操作，则系统在确认操作后显示“删除成功”（如上图所示）；否则提示如下的相关信息，约 3 秒后再返回 图 11 的上层界面，等待再次的操作选择：



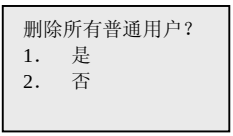





**F** 删除操作中的越权行为包括：1）普通管理员企图删除超级管理员； 2）管理员企图删除自己。

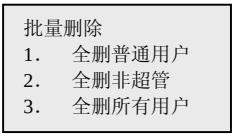
当选择批量删除方式时，系统出现提示如下：

以普通管理员身份登录时：




（图 12）

以超管身份登录时：

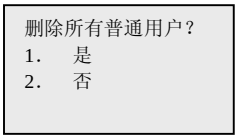



（图 13）

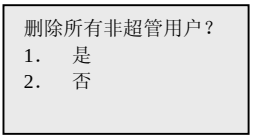
**F** 图 12：普通管理员选择“是”，则系统执行删除所有普通用户的操作后返回图 11 的上层界面；

图 13：超级管理员可以选择批量删除的操作对象，选择后系统会出现相应的确认信息：

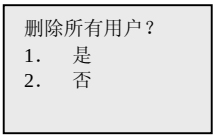
选择“1”时：




选择“2”时：



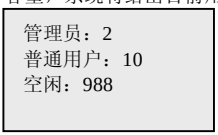

选择“3”时：




在“删除所有用户”的操作完成后，系统将直接退出到待机显示界面，此时的设备已回复到“空机状态”。其他两种删除操作完成后，则会返回图 13 的界面，等待用户的下一个选择。

#### 3.6.1.4 查询用户容量

“用户管理菜单”中按“4”，查看用户容量，系统将给出目前用户容量使用情况的信息，例如：



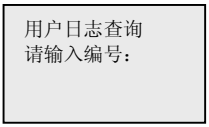

**F** 已登记的管理员个数（包括“超级管理员”和“普通管理员”）：2 个；

已登记的普通用户个数：10 个；

空闲用户数（指还可以登记的用户个数）：988 个。

### 3.6.2 日志查询菜单

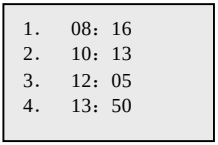
选择主菜单中的“2”，进入日志查询功能，系统提示输入要查询的用户编号；如果输入的编号存在，系统将提示输入要查询的日期，见下：



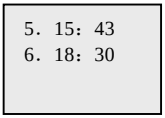


（图 14）

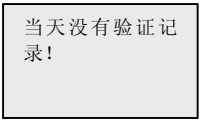
此时用户应该输入自己所关心的日期，然后按“*”键确认；如果被查询用户在这个指定日期的全天 24 小时内曾经通过了系统的身份验证，系统将会按用户通过验证的时间顺序列出这一天的所有记录信息，例如：



每条记录上的“时：分”，表示了该条验证记录在当天发生的具体时间；如果信息多于 4 条，屏幕显示不完时，可以通过按“*”键翻屏，继续查阅余下信息（也可以按“#”键，直接退回到图 14 的界面）：

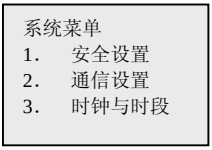



如果被查询用户在这个指定的一天内并没有使用（或验证通过）系统，则可以看到如下信息：




**3.6.3 系统管理菜单**

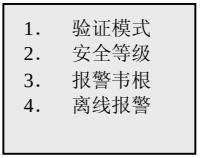
超级管理员可以选择主菜单 1 中的“3”，进入系统管理菜单，见下图。系统管理菜单包括了安全设置、通信设置，以及时钟与时段的设置：




（系统管理菜单）

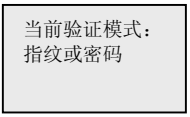
**3.6.3.1 安全设置**

系统管理菜单中按“1”，进入安全设置界面：

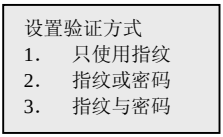



**3.6.3.1.1 验证模式**

安全设置菜单中按“1”，屏幕将提示当前系统正在使用的验证模式，比如当前方式为“指纹或密码”，则可看到如下提示：



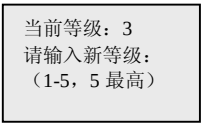

数秒后，进入验证方式的设置界面，如下：




按“1”、“2”或“3”键，将设定系统为相应的验证方式。

#### 3.6.3.1.2 安全等级

安全设置菜单中按“2”，屏幕显示如下：




用户可以对系统的“安全等级”进行设置,可选范围为 1-5；设置的等级数值越大，系统的安全性就越高；

#### 3.6.3.1.3 报警韦根

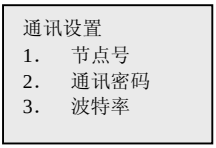
设置胁迫报警用。韦根号即为门禁系统对应的胁迫码。

#### 3.6.3.1.4 离线报警

设置离线报警的时间。离线报警设置为 0 时，离线报警功能不启用。

### 3.6.3.2 通信设置

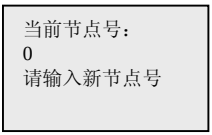
系统管理菜单中按“2”，进入通信设置界面：




（通信设置菜单）

#### 3.6.3.2.1 节点号

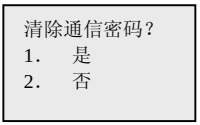
通信设置菜单中按“1”，屏幕显示如下：




用户可以根据需要设置当前设备的节点号,可取值范围为 0-250；

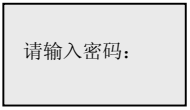
#### 3.6.3.2.2 通信密码

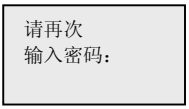
通信设置菜单中按“2”，屏幕提示如下：




如果按“1”选择清除通信密码，则系统提示“操作成功!”，然后返回“通信设置菜单”界面；此后 PC 端的工具软件不必通过通信密码的验证就能和设备进行数据通信；

如果按“2”选择“否”，就进入了新通信密码的设置过程，屏幕显示如下：




通信密码设置与用户密码设置一样，密码长度最多 9 位，且需要重复输入两次，两次输入一致才能设置成功。

#### 3.6.3.2.3 波特率

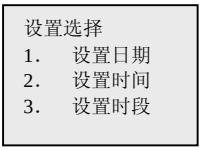
通信设置菜单中按“3”，屏幕提示现时系统所使用的通信波特率（默认 9600），比如：


数秒后，进入通信波特率设置界面，如下：


用户可根据需要，选择合适的通信速率。

### 3.6.3.3 时钟与时段

系统管理菜单中按“3”，进入时钟与时段的设置；包括日期、时间、以及系统时段值的设定：




（设置选择菜单）

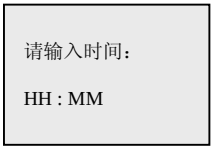
#### 3.6.3.3.1 设置日期

“设置选择”菜单中按“1”，进入系统日期的设置，屏幕提示：


超级管理员可以根据需要设定系统的日期。输入完成后按“*”键进行确认，系统支持从 05-01-01 至 63-12-31 间的所有合法日期的输入，如果输入日期非法或超出范围，系统会给出错误提示，此时用户应该按“#”键删除错误的设置，并重新输入；如果用户想放弃日期设定，可以通过按“#”键删除所有输入，直至返回到上层菜单。

#### 3.6.3.3.2 设置时间

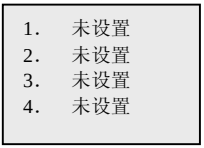
“设置选择”菜单中按“2”，进入系统时间的设置，屏幕提示：




超级管理员可根据需要设定系统的时间（24 小时制）。输入完成后按“*”键进行确认，如果输入时间非法或超出范围，系统会给出错误提示，此时用户应该按“#”键删除错误的设置，并重新输入；如果用户想放弃时间设定，可以通过按“#”键删除所有输入，直至返回到上层菜单。

**3.6.3.3.3 设置时段**

“设置选择”菜单中按“3”，进入时段限制设置，在系统的初始状态时，屏幕可能有如下提示：




（图 15）

如上，系统一共有 4 个时段可供设置。用户可以按数字键“ 1 ”－“ 4 ”分别对每个时段进行设定；例如，此时按“ 2 ”，将进入对第 2 个时段的设置，屏幕显示如下：

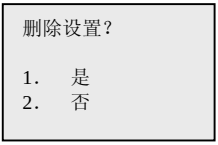

（图 16）

比如，用户想把这个时段设定为从早上 6 点到中午 12 点，则输入“06 ： 00”，然后按“*”确定，屏幕进入如下显示：


（图 17）

此时再输入“12 ： 00”，按“*”确定，即完成了对第 2 个时段的设置；系统重新返回时段的设置界面（见下图），用户可以继续对余下的其他时段进行设置：


如果需要修改某个已经设好的时段值，则按相应数字键后，屏幕显示：




如果按“1”，选择“是”，则该项时段值被重新设置为“未设置”，并返回时段的设置界面；否则进入图 16 - 17 的设置过程，用户可以重新输入新的时段值；

设置完毕后，可以按“#”键退出，屏幕将提示“操作成功!”，然后返回上层的“设置选择菜单”；

特别说明：

1） 如果想取消系统的时段限制功能，只需把系统的 4 个时段值都设为“未设置”（如图 15 的状态），则系统时段限制功能无效，所有合法用户在任何时间内都可以通过成功的验证而进入系统；

2） 当系统设定的某个时段值从一个有效值取消为“未设置”时，则原来选择了该项时段的用户，相应的设置项会被标识为“无效设置”，其效果相当于“未设置”；

3） 设置时段的结束时间不能小于或等于起始时间

### 3.7 普通用户查看日志

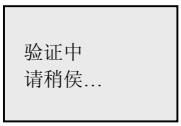
普通用户只能查看自己的验证日志：

在待机状态下按“*”键，然后通过类似“管理员进入管理菜单”的身份验证过程，进入用户的日志查询界面，如下：


用户输入指定日期后，将看到自己在那一天内的所有验证信息（具体操作与管理员查看用户日志相同，请参考 3.6.2 节的日志查询菜单 ）。

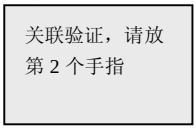
### 3.8 使用指纹进行开门验证

在待机状态下用登记过的手指，直接轻压传感器；当听到“嘀”的一声响后（表示系统已取图成功）用户可以把手指移开，屏幕提示如下：

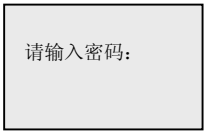



如果验证失败，在比较急促的“嘀嘀嘀嘀”4 声响后，屏幕显示“验证失败!”，然后返回待机状态；

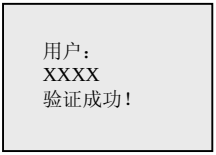

若验证成功，将听到“嘀嘀”2 声的提示声；在用户启用了手指关联功能的情况下，屏幕会提示用户验证其它的已登手指，如下图所示；否则直接跳到下一步：



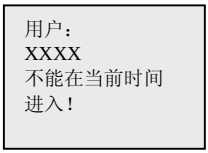

如果所有手指都验证成功，在“指纹与密码”验证模式下，屏幕还会提示用户输入密码：




密码验证成功后，屏幕再输出验证成功的信息（而在“只使用指纹”或“指纹或密码”模式下，则会跳过密码验证，直接显示这个信息）：



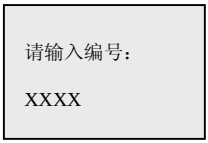
此时，如果当前的系统时间处于用户选定的时段范围内（或用户没有启用时段限制功能），则：
**F**以 wiegand 方式送出通过了开门验证的用户编号；
否则系统提示信息如下，用户将不能进门：



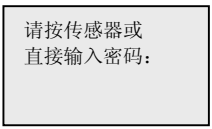

特别说明：
用户进行指纹验证前，还可以通过输入完整或部分用户编号的方式来提高验证速度，具体说明见 2.4.2 节的指纹验证的比对方式。

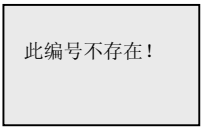
### 3.9 使用密码进行开门验证

只有在“指纹或密码”验证模式下，才可以仅使用密码（不使用指纹）而能通过验证开门；以下说明假定系统已设置为该模式：
在待机状态下按数字键输入完整的用户编号，屏幕显示如下：




把用户编号完整输入后，再按“*”键，如果编号存在，屏幕显示如图 18；否则提示“此编号不存在”，然后返回待机状态：

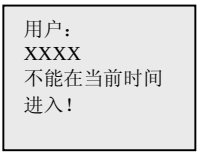



（图 18）

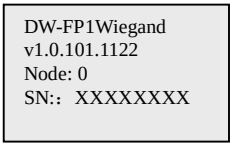
此时输入用户设置的密码，再按“*”键确认，如果验证成功，屏幕显示如下：


此时，如果当前的系统时间处于用户选定的时段范围内（或用户没有启用时段限制功能），则：
**F**以 wiegand 方式送出通过了开门验证的用户编号；
否则系统提示信息如下，用户将不能进门：



### 3.10 系统版本信息查询

在待机状态下，按“#”键，可以查询系统版本号、序列号及设备节点号等信息。屏幕显示：




（B 型机的版本信息）

“DW-FP1Wiegand vx..x..x.xx.xxxx”是处理器固件的版本号；“Node: XXX ”是设备的节点号；“SN:: XXXXXXXX”是产品序列号；数秒后会返回待机状态。

D.one®

**Shenzhen NeaTech Intelligent & Technology Co.，Ltd.**