

2013

FIRMWARE VERSION PROFESIONAL

Guía del usuario V1.0



Índice:

Empezando	3
1.1 Colocación de la huella digital	3
1.2 Instrucciones para tarjetas de proximidad	3
1.3 Precauciones	4
Introducción al dispositivo	4
2.1 Resumen de las funciones del dispositivo	4
2.2 Medidas de Seguridad Importantes.....	4
2.2.1 Ubicación de la Instalación.....	4
2.2.2 Uso del Sensor.....	5
2.2.3 Aspecto del producto.....	5
2.3 Uso del terminal de huellas dactilares	5
2.4 Fecha / Ajuste de la Hora	6
2.5 Dar de alta Administrador / Usuario.....	6
2.6 Dar de alta contraseñas	7
2.7 Dar de alta tarjetas de proximidad	7
2.7.1 Tecnología de Identificación.....	7
2.7.2 Tecnología MF (Sólo para los terminales que incluyen módulo Mifare)	8
2.8 Gestión de usuarios	8
2.9 Eventos	9
2.10 Acceso (sólo para terminales con relé)	9
Sistema	
3.1 Comunicaciones	10
3.1.1 Red	11
3.1.2 opciones del puerto serie	11
3.1.3 Opciones de seguridad	12
3.1.4 Wiegand	12
3.1.5 La configuración inalámbrica (Sólo para terminales con WIFI).....	14
	14

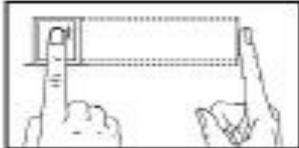
3.1.6 Marcado - seguridad de la configuración GPRS (Sólo para terminales con GPRS)..	15
3.2 idioma	15
3.3 de huellas dactilares.....	16
3.4 actualización	17
3.5 Visualización	17
3.6 Opciones avanzadas	18
3.7 Información del sistema	18
3.7.1 Capacidad de grabación	19
3.7.2 Información del dispositivo.....	19
Ajustes del terminal.....	20
4.1 teclado	20
4.2 configuración de código de barras.....	21
4.3 Gestión con Memoria USB	22
4.3.1. Descargar	22
4.3.2. Cargar	22
4.3.2. Configuración Memoria USB.....	23
4.3 Campana.....	24
4.4 Configuración del registro	24
4.4 Ajustes de verificación	25
4.5 Resetear.....	25
4.6 Auto test.....	26
Gestión de datos.....	27
Gestión de datos 5.1	27

Empezando

Colocación de la huella digital 1.1

Dedos recomendados: El dedo índice, dedo medio o el anular; No se recomienda el pulgar y el meñique (ya que suelen ser torpes en la pantalla de recogida de huellas dactilares).

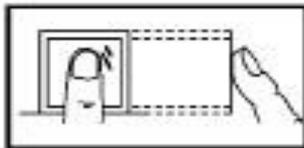
1. Proper finger placement:



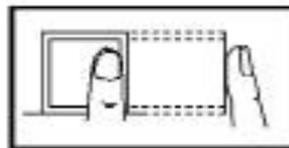
The finger is flat to the surface and centered in fingered guide.

2. Improper finger placement:

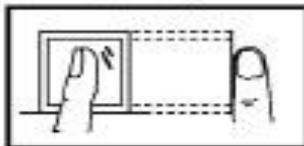
Not flat to the surface



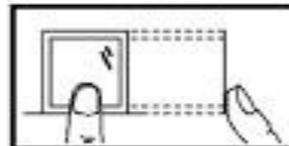
Off-center



Slanting



Off-center



Por favor, registrarse y verificar su huella digital utilizando el modo de colocación de los dedos adecuada. No nos hacemos responsables por ninguna de las consecuencias de la degradación en el rendimiento debido a la verificación de las operaciones del usuario inapropiados. Nos reservamos el derecho de interpretación final y la revisión de este documento.

1.2 Instrucción para tarjetas de proximidad.

Este dispositivo se suministra con un RFID sin contacto integrado (125 MHz) módulo lector de tarjetas. Al ofrecer múltiples modos de verificación tales como huellas digitales, tarjetas de RF y la huella digital + verificación de la tarjeta de RF, este dispositivo puede adaptarse a las necesidades de los usuarios diversificadas. Pase su tarjeta a través del área del sensor después de la indicación de voz y retirar la tarjeta después de que el dispositivo lo haya detectado. Por el área de lectura, consulte 2.2.3 El aspecto del producto.

1.3 Precauciones

Proteja el aparato de la exposición a la luz solar directa o luz fuerte, esto afecta en gran medida la recogida de huellas dactilares y conduce a las huellas digitales a dar error de comprobación. Se recomienda utilizar el dispositivo bajo una temperatura de 0 - 50 ° C a fin de lograr el rendimiento óptimo. En el caso de la exposición del dispositivo al exterior durante largos periodos de tiempo, se recomienda la protección de las instalaciones de la luz solar y de disipación de calor debido a una temperatura excesivamente alta o baja puede ralentizar el funcionamiento del dispositivo y provocar alta tasa de falsos rechazos (FRR). Al instalar el dispositivo, conecte el cable de alimentación después de conectar otros cables. Si el dispositivo no funciona correctamente, asegúrese de apagar la fuente de alimentación antes de realizar las inspecciones necesarias. Tenga en cuenta que un mal uso de la línea puede causar daños en el dispositivo quedando fuera del alcance de nuestra garantía normal. Para las cuestiones que no están cubiertos en este documento, por favor referirse a los materiales relacionados, incluyendo la guía de instalación, control de acceso manual de usuario del software.

Introducción al dispositivo

2.1 Resumen de las funciones del dispositivo

Como un dispositivo de huella digital y control de acceso integrado, nuestro producto se puede conectar ya sea con una cerradura electrónica o un controlador de acceso. Este dispositivo cuenta con operaciones simples y flexibles y es compatible con el uso de los administradores. La pantalla le guiará través de todas las operaciones. Es compatible con la función de control de acceso para una gestión de la seguridad y soporta múltiples modos de comunicación.

2.2 Medidas de seguridad importantes

2.2.1 Ubicación de la instalación

No instale el terminal en áreas que están expuestas a la luz del sol o la lluvia, como los lectores de huellas digitales no están diseñados para trabajar en esas áreas. La luz brillante interferirá con la lectura de los lectores de huellas digitales de los sensores y no son para intemperie ni antivandalicos. Se recomienda para proteger su terminal una caja o armario.

2.2.2 Uso del sensor

No abuse del sensor de huellas digitales por el rascado de la superficie, estar en contacto con superficies calientes o presionar con fuerza durante la colocación de la huella digital para su verificación. Limpiar el sensor de vez en cuando con cinta adhesiva para mantener el rendimiento del sensor.

Aspecto del producto 2.2.3

Vista frontal:



2.3 Uso del Terminal de huella digital

Este capítulo le guiará sobre cómo utilizar el terminal de huellas digitales con eficacia. Para obtener una buena lectura cada vez, la inscripción inicial de huellas dactilares debe hacerse adecuadamente. El Terminal de huella digital ofrece 4 tipos de métodos de inscripción:

- **registro de huellas dactilares**

Usuario inscribe su plantilla de huellas dactilares en un terminal y la plantilla se utilizará para futuras verificaciones.

- **Contraseña**

Para el usuario que tiene dificultad para inscribir las huellas dactilares debido a la mala calidad de la huella digital, se recomienda la inscripción de la contraseña. Contraseña de inscripción también es adecuado para los visitantes y trabajadores temporales.

- **Huella digital y contraseña**

En esta opción, el usuario puede inscribirse tanto la huella digital y la contraseña al mismo tiempo.

El usuario puede utilizar la huella dactilar o una contraseña para informar de su asistencia o para obtener acceso.

- **inscripción de tarjetas RFID**

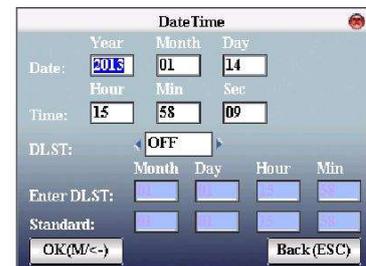
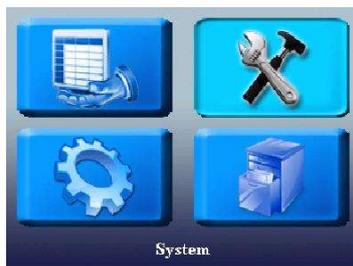
El usuario puede inscribirse tarjeta RFID

2.4 Fecha / Ajuste de la hora

La primera vez que instalamos un terminal de huella digital, es importante establecer la fecha y la hora correctas.

Siga los pasos que se muestran para acceder al menú Fecha/hora para su ajuste:

- Puede insertar elementos de entrada en los terminales a través del teclado. Contiene los números del 0-9, tecla de OK, ESC/Cancelar, desplazamiento Arriba/Abajo, Tecla Sirena y Tecla Menu



2.5 Memorizar Administrador / Usuario

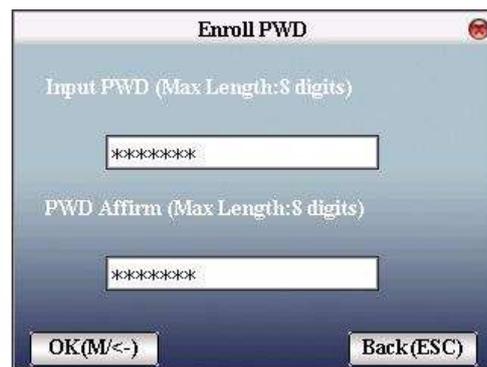
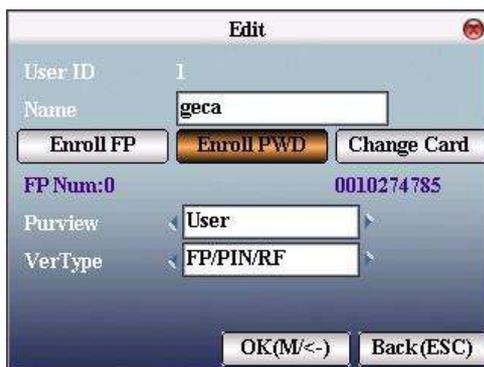
Una vez que el terminal de huella digital está encendido, aparecerá en la pantalla. Inscribir a un supervisor o un administrador, que es la persona a cargo de administrar las plantillas de huellas dactilares y los datos de la transacción en el terminal. Elija personas de confianza para esta función particular





2.6 Memorizar contraseña

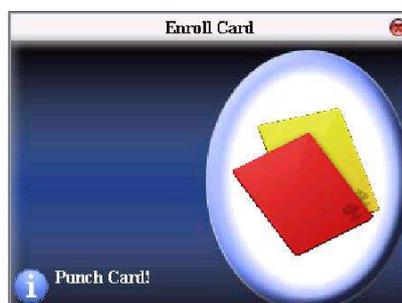
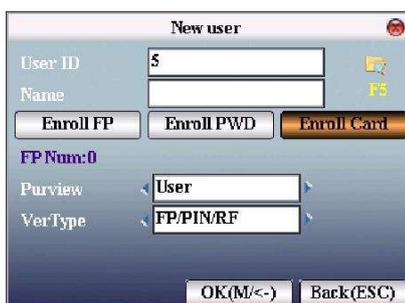
Si un usuario no puede inscribir su huella digital o quiere también otro tipo de verificación, se puede optar por utilizar contraseñas. Contraseña puede contener números que van de 1 a 8 dígitos.



2.7 RFID Tarjeta de proximidad

2.7.1 Tecnología de Identificación

Si un usuario no puede inscribir su huella digital, se puede optar por utilizar una tarjeta RFID. Tarjeta RFID está para dar mayor seguridad en la unidad o si el usuario no puede utilizar una huella dactilar.



2.7.2 Tecnología de MF (Sólo para los terminales que incluyen módulo MF (Mifare))

Sólo este menú se mostrará cuando el terminal incluye módulo Mifare y la configuración de cómo queremos que trabaje las tarjetas MF se define aquí. Las tarjetas MF son especiales y sirven para leer y escribir datos, por lo que podemos configurar las tarjetas como PIN de la tarjeta, o almacenar las plantillas en la tarjeta de MF que es muy útil para asegurar la protección de datos según las leyes de algunos países



2.8 Gestión de usuarios

Para abrir la pantalla administrar, puede hacer clic en la tecla F5. Cuando se encuentre en la pantalla de gestión de usuario usted puede hacer algunas acciones relacionadas con los usuarios. Al pulsar la tecla de menú como la búsqueda, grabar, editar, borrar y crear.

New user

User ID:

Name:

Enroll FP Enroll PWD Enroll Card

FP Num: 0

Purview:

VerType:

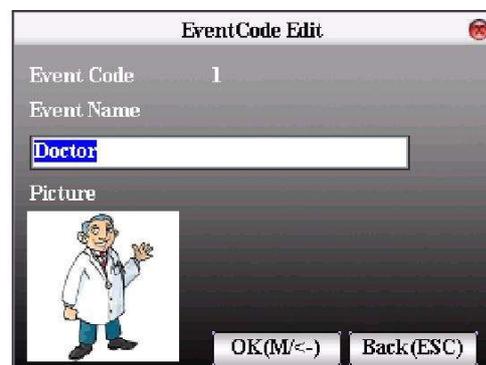
OK(M/←) Back(ESC)

User ID	Name	FP	PWD	Card
1	geca	0		
Search User		1		
Record		0		
Edit				
Del User				
New user				

Edit: OK Func: M/←

2.9 Eventos

En este menú se crearán todos los eventos que vamos a utilizar dependen del sistema de tiempo y asistencia que queremos, siendo posible crear eventos habituales, como (medico, fumar, almorzar, desayunar y así sucesivamente ...). Este sistema ofrece para controlar perfectamente el tiempo de trabajo de cada empleo. A través de SDK podemos enviar una imagen del evento al terminal de modo que cuando un empleado va a hacer un registro de un evento aparece la imagen en la pantalla de eventos que ofrece un mejor conocimiento a los usuarios sobre lo que están clicando ...

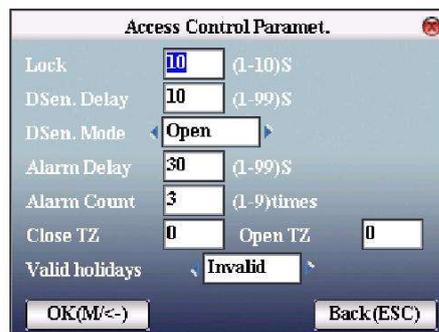
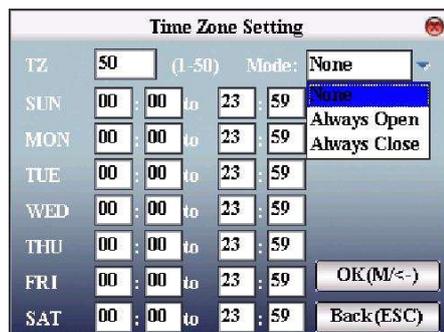


2.10 Acceso (sólo para terminales con relé)

En el menú de control de acceso que podemos configurar tantos parámetros de control de acceso, tales como: Las zonas horarias, días de fiesta, grupos, el acceso combinado, alarma y antipassback.

- **Zonas horarias:** Aquí podemos definir las zonas horarias que desea asignar a los usuarios para darles privilegios de acceso para apertura de puerta o denegar el acceso.
- **Vacaciones:** Este menú es el que se puede configurar los días festivos y los privados. Así como los días en los que el acceso es prohibido para el usuario o usuarios que se decida.
- **Grupos:** Esta funcionalidad es especialmente útil para el control de acceso debido a que podemos crear perfiles para los mismos usuarios. Imaginemos que tenemos 10 usuarios con los mismos husos horarios de control de acceso y configuración. Con este menú nos ofrece la posibilidad de incluir a todos ellos en un solo grupo, estableciendo los parámetros en el grupo en lugar de usuario por usuario.
- **El acceso combinado:** Con esta opción, podemos aumentar el nivel de seguridad de nuestros terminales de control de acceso, ofreciendo la posibilidad de obligar a los usuarios de los diferentes grupos que se identifiquen al mismo tiempo para la apertura de una puerta.

- Parámetros de alarma, y Misc. opciones:El uso de estos tres sub - menús sirve para configurar algunos parámetros como funcionamiento del relé de acción retardada, ajustes de alarma, Antipassback etc ...



SISTEMA

3.1 Comunicaciones

Cuando el terminal y el PC están en comunicación de datos, es necesario el uso de cable de comunicación para establecer los parámetros de comunicación en el dispositivo. Cuando el dispositivo está en comunicación, aparece “comunicando”. No opere con el terminal cuando esté comunicando.

Aviso: Cuando el dispositivo se está comunicando con el ordenador, compruebe la configuración aquí. Los parámetros aquí debe estar de acuerdo con el de interfaz de comunicación de software.



3.1.1 Red

Cuando se utiliza la comunicación Ethernet para la comunicación del dispositivo y el PC, los siguientes ajustes deben ser verificados:

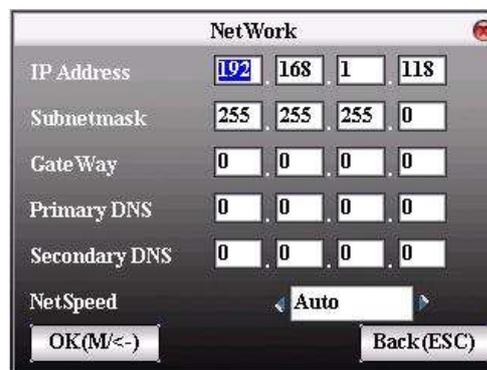
dirección IP del dispositivo: IP es 192.168.1.201 por defecto. Puede modificarlo si es necesario.

Pero no puede ser la misma que la de PC. Máscara de subred: 255.255.255.0 Es por defecto.

Puede modificarlo si es necesario.

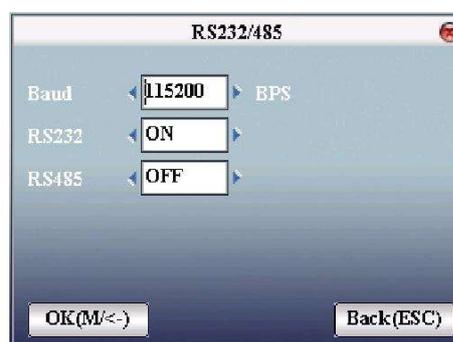
dirección de puerta de enlace: Es 0.0.0.0 de forma predeterminada. Si el dispositivo y el PC están en diferentes segmentos de red, es necesario establecer la dirección.

velocidad neta: Ajuste la velocidad de acuerdo con la LAN en la que el dispositivo esta.



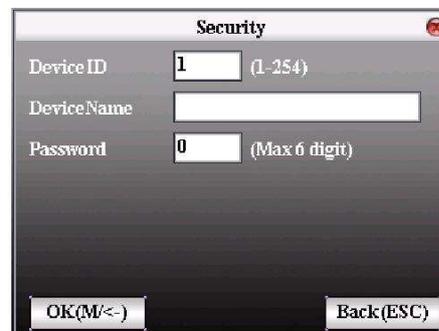
3.1.2 opciones del puerto serie

Cuando RS232 / RS485 se utiliza para la comunicación del dispositivo y el PC, es necesario programar una ID de dispositivo. ID de dispositivo: 1 - 254. Si se utiliza RS232 / RS485, esta identificación debe indicarse a través de la interfaz de comunicación de software.



3.1.3 Opciones de seguridad

Cuando RS232 / RS485 se utiliza para la comunicación del dispositivo y el PC, es necesario programar una ID de dispositivo. ID de dispositivo: 1 - 254. Si se utiliza RS232 / RS485, esta identificación debe indicarse a través de la interfaz de comunicación de software. Para mejorar la seguridad de los datos de asistencia, la contraseña de conexión debe ser ajustado aquí. La contraseña de conexión debe ser introducida cuando queremos conectarnos al dispositivo para leer los datos. Contraseña de conexión: Contraseña del sistema es 0 por defecto. Es decir, no hay ninguna contraseña.) se puede configurar como otro valor. Después del ajuste, la contraseña debe ser introducida en el software para comunicarnos con el dispositivo. O la conexión fallará. La longitud de la contraseña es 1 a 6 dígitos.



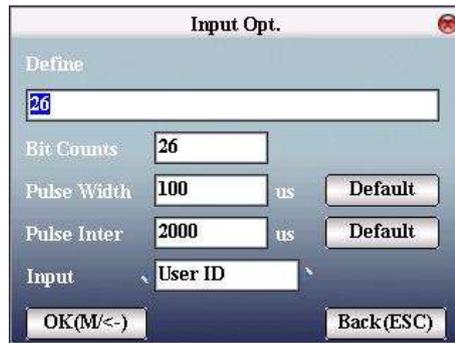
3.1.4 Wiegand

Definir entrada Wiegand y formato de salida.



3.1.4.1 Opt entrada.

Formato definido por el usuario: El usuario define los bits del formato Wiegand Anchura y longitud de los dígitos de datos: El ancho del pulso es de 100 microsegundos por defecto, los cuales se pueden ajustar desde 20 a 800. intervalo de pulso: Se encuentra a 900 microsegundos por defecto, que puede ajustarse entre 200 y 20000. Contenido de la entrada: Contenido en la señal de entrada Wiegand, incluyendo nombre de usuario o número de tarjeta.

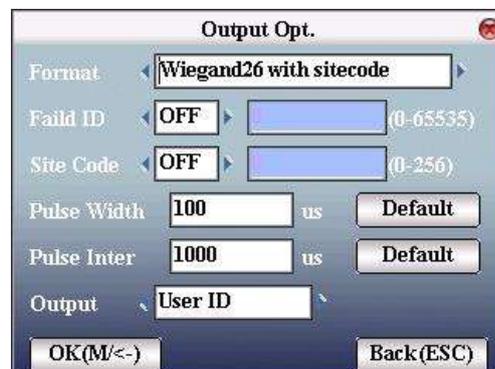


3.1.4.2 Opt salida.

- Formato: Es el formato definido en el sistema. El usuario no necesita especificar dígitos total y la posición de la información.

Hay 4 formatos de definición por defecto en el sistema: Wiegand 26 con código de sitio, Wiegand 34 con código de sitio, Wiegand 26 sin código de sitio y Wiegand 34 sin código de sitio. Wiegand26 con código de sitio significa la salida de formato W26 con el ID de dispositivo. Wiegand26 sin código de sitio significa la salida de formato W26 y sin código de sitio. Si no hay ningún código de sitio, entonces la señal de salida no contiene dicha información. Si hay código de sitio, la salida incluye el código de sitio (similar a la ID del dispositivo. Sin embargo, este código se especifica por el usuario y se puede repetir en los diferentes dispositivos, con un rango de 0-255

- Error ID: Esto es fallo de identificación después de una verificación sin éxito. " Cerrar " no significa que la salida (con un rango de 0. - 65534)
- Código del lugar: Al igual que el ID de dispositivo. Pero el código se especifica por el usuario. dispositivos diferentes pueden repetirse. (Con rango de 0-255)
- Ancho de Pulso: Ancho de pulso es de 100 microsegundos por defecto, que se pueden ajustar de 20 a 800.
- intervalo de pulso: Se encuentra a 900 microsegundos por defecto, que puede ajustarse entre 200 y 20000.
- contenido de la salida: Contenido incluido en la señal de salida Wiegand, incluyendo nombre de usuario o número de tarjeta.



3.1.5 La configuración inalámbrica (Sólo para terminales con WIFI)

Antes de que el dispositivo se utilice para la red inalámbrica, debe existir un equipo físico de redes 802.11, tales como una red Wifi. ESSID debe ser conocido para poder conectarse (ID de red).

ID de red: ID de red para conectarse a la red inalámbrica. (Se diferencia entre minúscula y mayúscula).

modelo de red: hay dos modelos: Modelo de la infraestructura (por estructura en estrella) y ad-modelo hoc (punto a punto).

El modo de autenticación: Modo de infraestructura incluye cinco modos de autenticación: abierta y compartida, WPAUTO, wpapsk y WPA2PS002E.

Anuncio-hoc modelo incluye cuatro modos de autenticación: abierta, compartida, WPAUTO, WPAPSK y WPANONE.

Encriptación: cuando seleccionamos el tipo de encriptación NINGUNA, la clave en WEP (Wired equivalent privacy) y WPA (WIFI protected Access) no debe ser editada, normalmente no es necesario introducir clave.

IP del dispositivo: En las redes inalámbricas 802.11, es DHCP. O entrar en la interfaz IP e introducir la dirección correcta, máscara de subred y así sucesivamente.



3.1.6 Marcado - seguridad de la configuración GPRS (Sólo para terminales con GPRS)

Cuando el equipo está en el acceso telefónico a redes, asegurándose de que el dispositivo está en la cobertura de GPRS o señal CDMA, se debe conocer el modem, nombre y usuario y APN.

Tipo de módem: Establecer el tipo de módem que utiliza el dispositivo según el tipo de tarjeta SIM.

Frecuencia: Seleccione la frecuencia apropiada de acuerdo con los operadores de empresas.

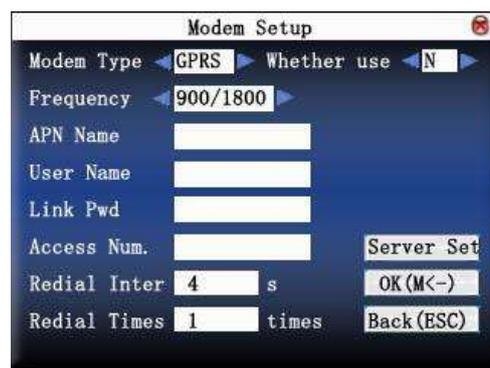
APN Nombre: Access Point Name, utilizado para identificar los tipos de GPRS / CDMA de negocio.

Nombre de usuario y contraseña: Verificar si el usuario tiene permiso para usar esta red.

Número de acceso: El número de acceso de los negocios GPRS / CDMA.

intervalo de rellamada: El intervalo de rellamada automática después de que se desconecta de la red.

tiempos de rellamada: Los tiempos de intentar volver a marcar el número si la red está desconectado.



3.2 idioma

La versión del firmware Profesional incluye texto y voces en todos los idiomas europeos, las voces se han grabado en un estudio profesional, poniendo muy alto sonido

calidad. Cuando se pone en marcha por primera vez el terminal le pedirá que seleccione el idioma

Si usted quiere puede más adelante modificar en este menú la nueva configuración.

La versión del firmware Profesional proporciona la capacidad de seleccionar, si lo prefiere voces masculinas o femeninas.



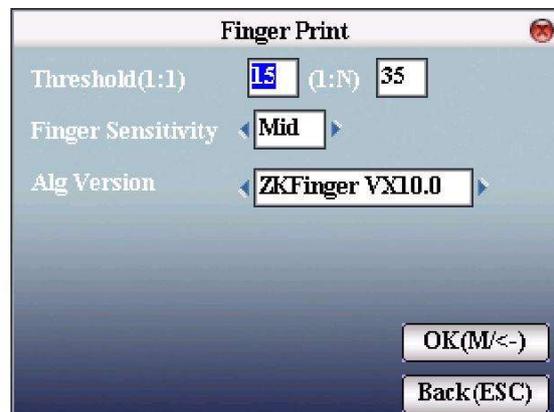
3.3 Huellas dactilares

- 1: 1 matching valor umbral: La similitud de verificación de ID + huella digital y la plantilla cargada
- 1: N valor de coincidencia umbral: La similitud de la verificación y la plantilla cargada

Recomendado valor umbral a juego:

<i>Coincidencia de valor umbral</i>					
	FRR	LEJOS		1: N	1: 1
	Alto	Bajo		45	25
	Medio	Medio		35	35
	Bajo	Alto		25	45

- sensibilidad en los dedos controlar la reacción del sensor con una luz externa, la luz puede afectar siempre a un sensor óptico, con este parámetro podemos hacer este efecto menor sobre si nuestro terminal hay una fuente de luz.
- Alg. Versión: se puede ajustar 9.0 o 10.0 siendo este último más rápido y mejorar la Tasa de error. Tenga cuidado porque el tamaño de la información de rastreo grabado con 10.0 algoritmos es el doble de tamaño de 1,2 kb más de 9,0 algoritmos, no puede cargar plantillas de 9.0 10.0 y viceversa.



3.4 actualización

Utilice el software para actualizar el firmware del programa.

Aviso: Si usted necesita tal archivo de actualización, por favor, póngase en contacto con técnico.

Por lo general, no se recomienda la actualización del firmware.

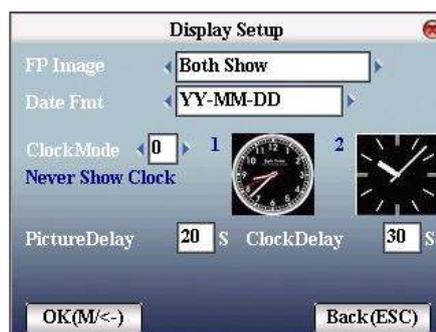
Operación

Inserte el disco de U con el archivo de actualización en la ranura. El dispositivo identificará el archivo automáticamente. El dispositivo le indicara si es correcto o no.

3.5 Visualización

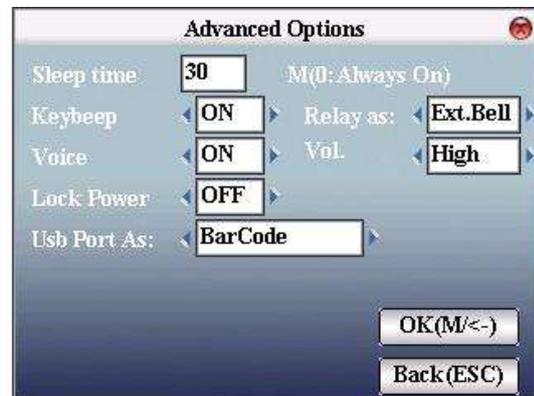
Los parámetros relacionados con la pantalla.

- FP imagen: Es para saber si queremos mostrar la imagen FP cuando estamos inscribiendo un dedo o búsqueda en el dispositivo.
- Formato de fecha: AA - MM - DD, AA / MM / DD, AA.MM.DD, MM - DD - AA, MM / DD / AA, MM.DD.AA, DD - MM - AA, DD / MM / AA, DD. MM.YY y AAAAMMDD. Seleccione el formato de fecha deseado.
- Modo de reloj: Puede ser que no se muestre o elegir entre dos tipos de reloj para mostrar en la pantalla.
- Retardo en la imagen: El tiempo que se mostrará en la pantalla valores posibles 3 a 999 segundos.
- Retardo del reloj: La duración del tiempo de visualización de imágenes de reloj después de la verificación. Después de que el retardo de visualización, la imagen mostrada en la interfaz de inicialización de nuevo (con valor efectivo de 0 a 999 segundos, y 0 mientras muestra el reloj todo el tiempo).



3.6 Opciones avanzadas

- Tiempo de reposo: Cuando se ha programado la hora de apagado, el dispositivo entrará en estado de reposo. Pulse cualquier tecla o un dedo para despertarlo. (0 Ajuste siempre encendido).
- Tono de teclas: Controla el sonido de las teclas al activarlas o no.
- Voz: para seleccionar si se debe dar aviso de la voz o no. El dispositivo dará aviso de la voz durante la operación correspondiente.
- Bloqueo de energía: Para evitar un apagado imprevisto, seleccione si desea bloquear el apagado o no.
" Desactivar " : el equipo está apagado 3 segundos después de presionar el apagado. " Habilitar " , es ineficaz después de pulsar el apagado.
- Relé como: Para seleccionar cómo queremos utilizar el relé, puede ser para cerradura de la puerta o la alarma de la sirena externa.
- Puerto USB como: seleccionar el modo en que queremos usar el puerto USB, puede ser como código de barras (para conectar un escáner de código de barras) o como pen drive (para gestionar los datos usando un pen drive)



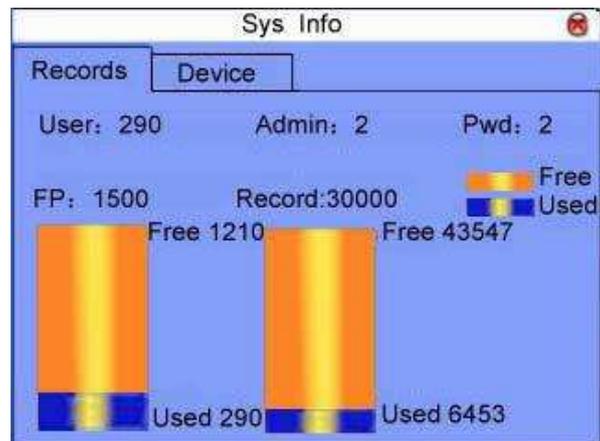
3.7 Información del sistema

Utilice opción información del sistema para comprobar el dispositivo actual, la información de la versión y así sucesivamente.



3.7.1 Capacidad de grabación

Mostrar el número de usuarios, contraseña de administrador inscrito y la capacidad de huellas digitales, la huella digital registrada, registro de asistencia y el registro de asistencia guardado en forma de diagrama, como se muestra a continuación:

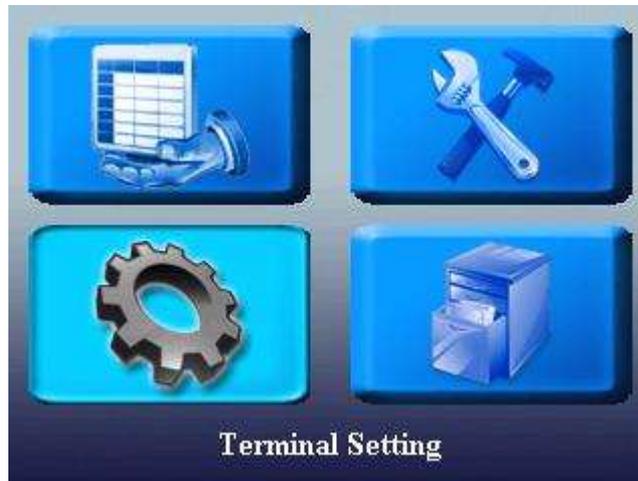


3.7.2 Información del dispositivo

Visualización del nombre de dispositivo, número de serie, información de la versión y la fecha de fabricación del dispositivo para su comprobación:

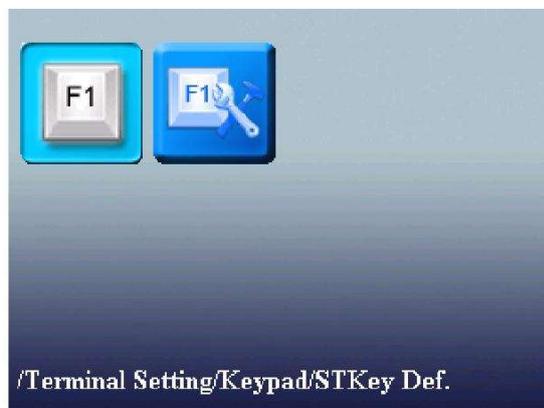


Ajustes del terminal



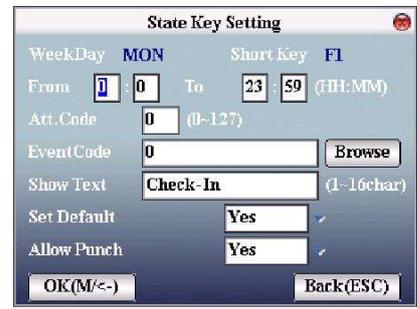
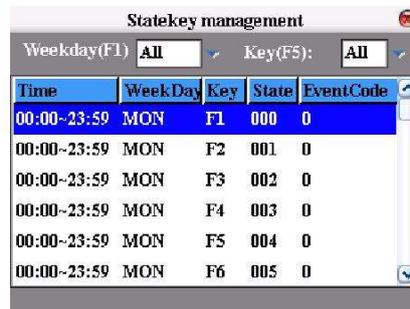
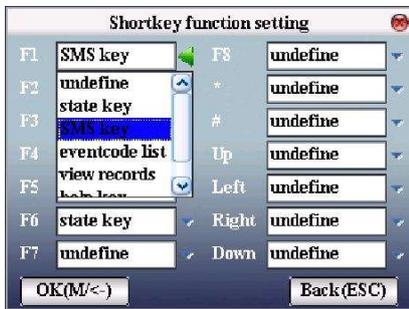
4.1 teclado

En este menú se configura todas las teclas de función del terminal como deseemos dándole al terminal una flexibilidad total, como explicaremos en el siguiente punto. Este menú tiene dos secciones que detallaremos a continuación.



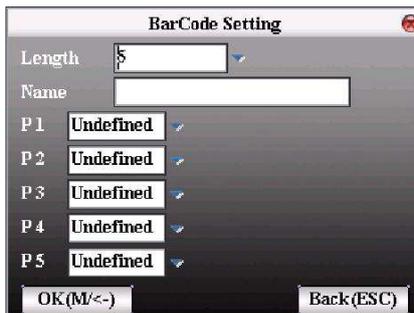
- Ajuste de las teclas de funciones: Desde este menú se puede definir la función que desee para cada teclas de función disponibles en el terminal, puede seleccionar una de estas opciones: (estado indefinido, estado teclas, consulte SMS, lista de eventos, ver el historial y la tecla de ayuda).

- **Conf. Las teclas de estado:** La flexibilidad ofrecida por la versión profesional de firmware nos permite definir una tecla de estado , como F1 = Doctor, esa tecla se puede configurar para cambiar automáticamente el estado, una de las claves para un tiempo puede tener un estado y cambiar automáticamente a otro estado y se puede incluso fijar el día de la semana que desea que esta operación ocurra. Con lo que podemos jugar con las teclas de función a voluntad permitiendo todo tipo de combinaciones para hacer más fácil el uso del terminal para el usuario final. También tenemos la capacidad de definir el código que desea que aparezca ATT y si un estado clave permite realizar registros o no.



4.2 configuración de código de barras

Una de las principales características de la versión profesional es la capacidad de definir el uso del puerto USB, cuando se define como lector de código de barras y reiniciar la computadora, en lugar de encontrar la unidad de menú de pendrive, encontramos en el menú el código de barras en el que podemos definir la longitud del código, nombre e incluso pueden definir como pendrive, los campos de código de barras.



4.3 Gestión del Pendrive



4.3.1. Descarga

- *Descargar datos de usuarios*

Guarde toda la información de los usuarios y huellas en un Pendrive.

- *Descargar SMS*

Guardar los SMS añadidos al equipo en un Pendrive

- *Descargar fotos de usuario*

Guarde las fotos de los empleados en un Pendrive.

4.3.2. Cargar

- *Cargar sus datos*

Cargar información de los usuarios y huellas desde un Pendrive.

- *Cargar SMS*

Cargar SMS en desde un Pendrive.

- *Cargar imágenes definido por el usuario*

La Carga de imágenes JPG desde un Pendrive. Estas fotos se mostrarán en la interfaz de inicialización

- *Cargar fotos de usuario*

Cargar imágenes JPG nombradas con ID de usuario desde el Pendrive. A continuación, el empleado verá su foto tras la verificación de huellas dactilares.

4.3.2. Configuración del Pendrive

Desde la unidad de menú del Pendrive puede realizar todas las descargas de datos desde el dispositivo, éstas descargas pueden hacerse: (Registros, la información del usuario, SMS, foto del usuario, y terminales que tienen cámara las fotos descargadas de captura también.) De la misma manera se puede cargar datos en el terminal si queremos mover los datos de forma rápida y segura desde un terminal a otro. Dentro de la descarga de los registros podemos definir una gran cantidad de parámetros que nos ayudarán a lograr más informes de asistencia en la forma que desee.

parámetros definibles para la descarga de registros

- Nombre del archivo.
- Fijar texto.
- Eliminar o no después de la descarga.
- carácter separador
- valor ASCII
- Los campos de datos: tenemos 10 campos de datos configurables por el usuario en el que podemos definir la información que desea descargar y la posición de que la información ocupa, estos datos son los siguientes: (Indefinido, código de usuario fijo, fecha y hora, la terminal de bacalao, Nombre del terminal, ATT código, nombre de ATT, verificación del sistema, código, descripción).

Att.Log Download Setting

File Name Mode **attlog & datetime & dev. id**

Fixed Text (1~16 char)

Del. AttLog after Download **No**

Separator Char Type **Tab Char**

ASC Val. (1~255)

Data Fields **Edit Field Info**

OK(M/←) Back(ESC)

Field Setting

Field1: **userid** Field6: **event id**

Field2: **datetime** Field7: **undefine**

Field3: **dev. id** Field8: **undefine**

Field4: **att. code** Field9: **undefine**

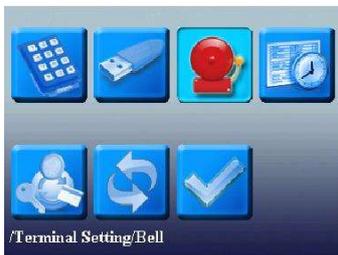
Field5: **ver. type** Field10: **undefine**

Fixed Text (1~16 char)

OK(M/←) Back(ESC)

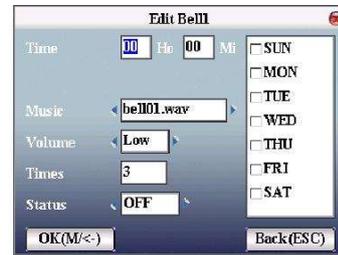
4.3 Sirena

Muchas empresas necesitan sirena para el inicio y el fin de la jornada. Algunos utilizan la sirena manual. Algunos utilizan sirena electrónica. Para ahorrar costes y proporcionar comodidad para la gestión, integramos las funciones de la campana para el dispositivo. Puede establecer el tiempo de campana. Cuando es la hora programada, el dispositivo hará sonar automáticamente la sirena. Y la sirena se detendrá automáticamente cuando es la hora de finalización. Si es una sirena externa utilizaremos la salida de relé para conectar una sirena externa y el dispositivo enviará la señal A través del relé de la sirena externa para activarlo.



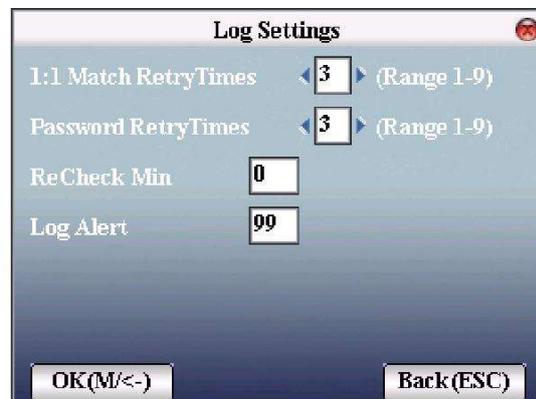
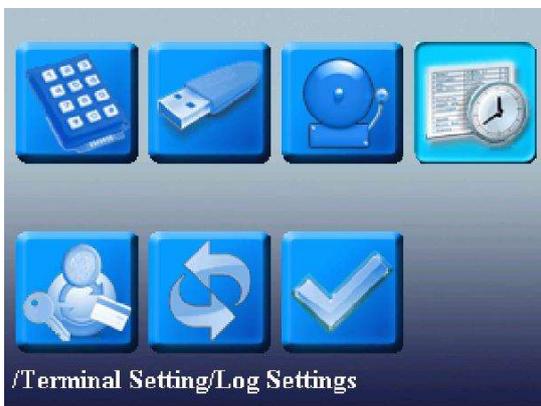
Bell	Bell Time	Ring	State
Bell 1	00: 00	Bell101.wav	
Bell 2	00: 00	Bell101.wav	
Bell 3	00: 00	Bell101.wav	
Bell 4	00: 00	Bell101.wav	
Bell 5	00: 00	Bell101.wav	
Bell6	00: 00	Bell101.wav	
Bell7	00: 00	Bell101.wav	
Bell8	00: 00	Bell101.wav	

Pageup PageDown # Edit OK Menu 0/4



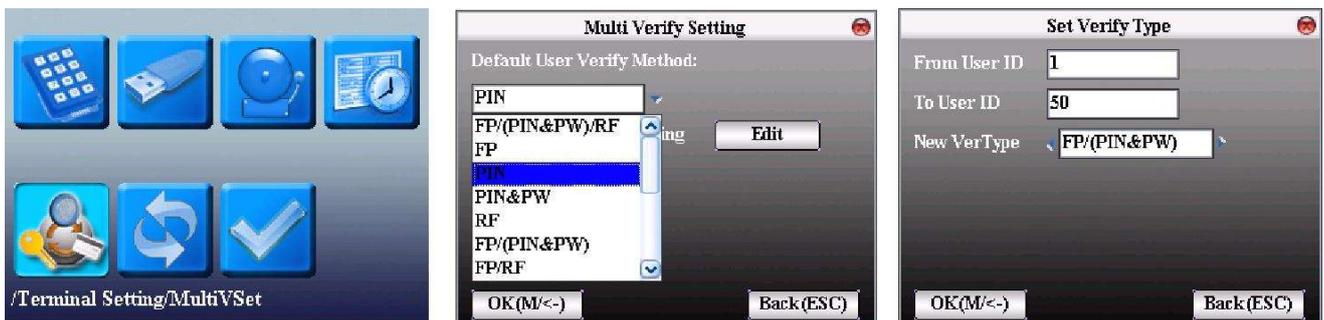
4.4 Configuración del registro

En este menú definimos el número de intentos fallidos para permitir al usuario realizar registros. Vamos a seleccionar el tiempo entre los registros, así (es el tiempo mínimo que debe transcurrir entre los registros de un mismo usuario). En los parámetros de registros podemos encontrar la opción de configurar cuando desea omitir el mensaje de advertencia de memoria llena de eventos.



4.4 Ajustes de Multi-verificación

Al usar la versión profesional del firmware estará disponible la opción de establecer por el terminal al modo de verificación por defecto. Si cada usuario no ha definido su modo de verificación específica el sistema comprobará este valor que será por defecto para todos los usuarios en el terminal. Somos capaces de hacer varias modificaciones para muchos usuarios al mismo tiempo.



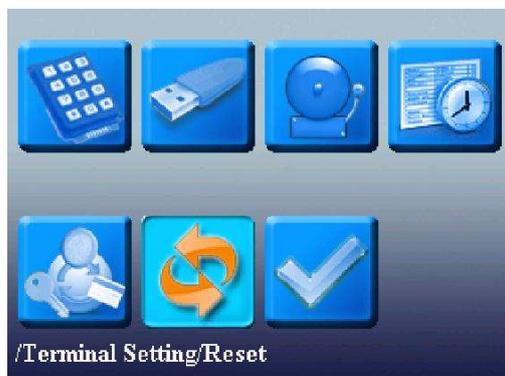
4.5 Restablecer

Vaya a la opción de comunicación, opciones del sistema y así sucesivamente restablecimiento al estado de valores de fábrica.

Restablecimiento de fábrica: Pasar todos los parámetros en el dispositivo al estado de valores de fábrica. Restablecer definición del teclado: restablecer el ajuste correspondiente de definición del teclado a la de fábrica.

campana opción cero: opción campana para restablecerla a opciones de fabrica.

Restablecer otros parámetros: la opción de comunicación, los parámetros del sistema, opción de interfaz y así hasta el estado de fábrica sólo se restablecerá



4.6 Auto test

El dispositivo puede probar varios módulos de forma automática para ayudar al operador juzgar el módulo con fallos de forma rápida, incluyendo la prueba de pantalla TFT, mensaje de voz, reloj, el teclado y el sensor de huellas digitales.

- **prueba de la pantalla TFT**
 El dispositivo puede probar automáticamente el color TFT (a través de la exhibición de color, pantalla en blanco y negro de la pantalla) para ver si la pantalla funciona normalmente
- **prueba de voz**
 El dispositivo puede probar automáticamente la voz a través de la reproducción de archivos de voz en el dispositivo para ver si los archivos están completos y el efecto de voz son buenas o no.
- **prueba del teclado**
 El dispositivo puede probar automáticamente varias teclas para ver si las teclas funcionan normalmente o no.
 Pulse cualquier tecla en la interfaz de prueba (a excepción de OK y " ESC ").
- **Prueba del sensor**
 El dispositivo comprobará automáticamente el sensor para ver si funciona con normalidad. Poner la huella digital para ver si la imagen es clara y utilizable.
 Ponga el dedo en la huella dactilar en la imagen de la huella dactilar ventana del sensor y aparecerá en la pantalla.
- **Prueba de RTC**
 El dispositivo puede probar automáticamente el reloj para ver si funciona con normalidad. Pulse OK para iniciar el tiempo y, a continuación, pulse OK para detener el tiempo.
 Pulse " ESC " para salir.



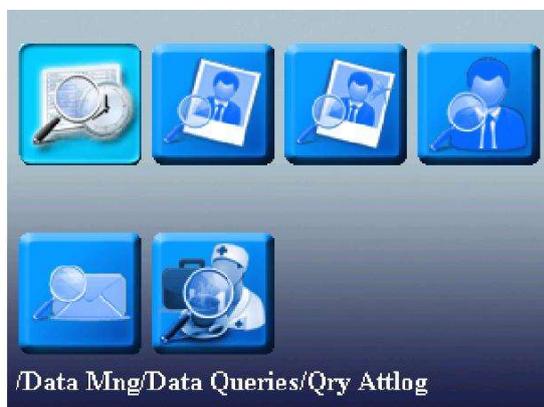
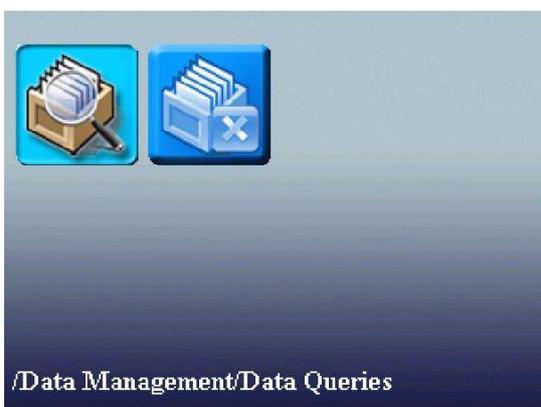
Gestión de datos



Gestión de datos 5.1

Los registros de asistencia se guardaran en el dispositivo. Para mayor comodidad de consulta, se proporciona la función de registro de la consulta.

- **consulta de datos**
 - *consultas de asistencia:* De acuerdo con el usuario la condición de consulta de entradas, los registros se mostrarán en la pantalla para el usuario seleccionado. Sólo muestra el registro relacionado con la asistencia y el coste del trabajo sólo con la fecha y la hora.
 - *Consultas usuario:* Para consultar al usuario actual en el dispositivo.
 - *SMS consulta:* Para consultar SMS en el dispositivo.



- **Borrar datos**

Para borrar todos los datos grabados en el dispositivo, como: Eventos, usuarios, fotos).



ZKTeco Europe
 Avda. Somosierra, 24
 28703 S.S. de los Reyes
 Madrid. Spain

ZKTeco[®] EU
 Security and Time Management Solutions

