Manual de Usuario

P200-P260

Versión: 1.0

Fecha: Marzo, 2017

Aviso importante

Antes que nada, queremos agradecerle por haber adquirido este producto; antes de utilizarlo, por favor lea este manual detenidamente para evitar dañar el dispositivo. Le recordamos que el uso adecuado del equipo ayudará a mejorar el rendimiento y la velocidad de verificación.

Sin el previo consentimiento escrito de nuestra empresa, ningún individuo tiene permitido extraer o copiar el contenido de este manual de manera parcial o total, ni distribuirlo en ningún formato.

El producto descrito en el manual puede incluir software cuyos derechos de autor son compartidos por los licenciantes incluyendo nuestra empresa. Con excepción de la autorización del titular correspondiente, ningún individuo puede copiar, distribuir, revisar, modificar, extraer, descompilar desensamblar, desencriptar, aplicar ingeniería inversa, transferir o sublicenciar el Software ni realizar otros actos de violación de los derechos de autor, pero se excluyen las limitaciones aplicadas por la ley.

Las funciones marcadas con * son opcionales.

Derechos de Autor

©Copyright 2017 ZKTeco Co, Ltd. Todos los derechos reservados.

Todos los derechos reservados. Con excepción una autorización específica, queda prohibido la reproducción Ninguna parte del contenido de este manual se puede reproducir ni transmitir de ninguna forma ni por ningún medio sin el escrito expreso consentimiento de la empresa.

Debido a la constante renovación de productos, la empresa no puede garantizar que el producto real consista en su totalidad con la información consignada en este manual, así como no asume responsabilidad por cualquier disputa que pueda surgir debido a la discrepancia entre los parámetros técnicos reales y este manual. Por favor disculpe los inconvenientes causados debido a los cambios hechos sin notificación. Nos reservamos los derechos finales de modificación e interpretación.

CONTENIDO

1. Introducción 1

2. Características 1

3. Especificaciones 1

4. Instrucciones de Uso 2
- 4.1 Colocación de Palma 2
- 4.2 Colocación de Dedo 3
- 4.3 Modos de Verificación 2
  - 4.3.1 Verificación de Huella Digital 3
  - 4.3.2 Verificación de Palma 4
  - 4.3.3 Verificación de Tarjeta * 5

5. Menú Principal 5

6 Gestión de Usuarios 6
- 6.1 Nuevo Usuario 6
  - 6.1.1 Introducir ID y Nombre de Usuario 6
  - 6.1.2 Introducir Privilegio de Usuario 7
  - 6.1.3 Modo de Verificación 7
  - 6.1.4 Registrar una Huella Digital 7
  - 6.1.5 Registrar una Palma 8
  - 6.1.6 Registrar una Tarjeta * 8
  - 6.1.7 Registrar una Contraseña 8
- 6.2 Todos los Usuarios 8
  - 6.2.1 Editar un Usuario 9
  - 6.2.2 Eliminar un Usuario 9
- 6.3 Estilo de Pantalla 9

7. Privilegios 9
- 7.1 Crear y definir un nuevo privilegio 10

8. Ajustes de Comunicación 10
- 8.1 Ethernet 11
- 8.2 Comunicación Serial 11
- 8.3 Conexión a PC 12
- 8.4 ADMS * 12

9. Sistema 12
- 9.1 Fecha/Hora 13
- 9.2 Asistencia 13
- 9.3 Reiniciar Equipo 14
- 9.4 Actualización por USB 14

10. Personalizar 14
- 10.1 Interfaz de Usuario 15
- 10.2 Voz 15
- 10.3 Programación de Timbre 16
  - 10.3.1 Nuevo Timbre 16
  - 10.3.2 Todos los timbres 16
  - 10.3.3 Opciones 16
- 10.4 Ajustes de Estados de Asistencia 17
- 10.5 Teclas de Función 17

11. Gestión de Datos 19
11.1 Borrar Datos 19
11.2 Respaldo de Datos 20
11.3 Restaurar Datos 20

12. Control de Acceso 20
12.1 Horarios 21
12.2 Días Festivos 22
12.3 Grupos de Acceso 22
12.4 Combinaciones de Acceso * 23
12.5 Ajustes Anti-Passback * 23
12.6 Opciones de Coacción 25

13. Gestión USB 25
13.1 Descargar en USB 26
13.2 Cargar desde USB 26
13.3 Opciones de Descarga 26

14. Búsqueda de Asistencia 27

15. Impresión 28
15.1 Ajustes de Campos de Datos 28
15.2 Ajustes de Impresión 28

16. Mensajes 29
16.1 Crear un nuevo mensaje 29
16.2 Opciones de Mensaje 30

17. Código de Trabajo 30
17.1 Nuevo Código de Trabajo 30
17.2 Todos los Códigos de Trabajo 30
17.3 Opciones de Códigos de Trabajo 31

18. Pruebas 31

19. Información del Sistema 32

20. Anexos 32

1. Introducción

El P200-P260 es un terminal de identificación multibiométrica de Tiempo & Asistencia y Control de Acceso, que puede conectarse con una cerradura eléctrica, sensor de puerta, botón de salida etc.

Con el más actual algoritmo de identificación de palma/huella digital y con una tecnología simplificada, el dispositivo puede almacenar hasta 600 plantillas de palma y hasta 20,000 plantillas de huella digital sin necesidad de dividirlas en grupos.

Con capacidad de comunicarse a través de Wi-Fi (opcional), TCP/IP y USB, se garantiza una conexión y transferencia de datos fluida. La sorprendente velocidad de verificación y su intuitiva interfaz de operación lo hacen una elección popular. Con su diseño elegante y elaborado, combina perfectamente con la estética de su oficina.

2. Características

- Verificaciones de Palma, Huella Digital y Tarjeta.
- Diseño elegante y ergonómico, fácil instalación.
- Comunicación por Wi-Fi (opcional), TCP/IP y USB.
- Algoritmo profesional de reconocimiento de palma y huella digital desarrollado por ZKTeco.
- Módulo PoE/3G/Control de Acceso General/Batería de Respaldo/Impresora.

3. Especificaciones

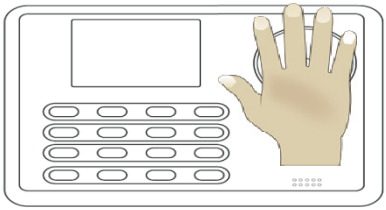
Pantalla	TFT de 2.8 pulgadas a color
Capacidad	Plantillas de Palma: 600 (estándar) Plantillas de Huella Digital: 3,000
Capacidad de Tarjetas	10,000 (opcional)
Capacidad de Registros	100,000

Comunicación	TCP/IP, USB, Wi-Fi (opcional)
Funciones Estándar	Cambio de Estado Automático, Búsqueda de Registros, Módulo de CA 1: Botón de Salida, Cerradura, Alarma, Salida de 12V, Entrada Auxiliar; Código de Trabajo, Teclado T9, ID de Usuario de hasta 9 dígitos, Horario de Verano, Programación de Timbre y Mensajes.
Funciones Opcionales	Tarjeta ID, Tarjeta MIFARE, Módulo de CA 2: Botón de Salida, Cerradura, Alarma, Salida de 12V, Entrada Auxiliar, Sensor de Puerta, RS485, Entrada/Salida Wiegand. PoE, Batería de Respaldo, ADMS.
Fuente de Poder	12V/1.5A
Velocidad de Verificación	≤ 1 Seg.
Temperatura Operativa	0-45°C
Humedad Operativa	20%-80%

4. Instrucciones de Uso

4.1 Colocación de Palma

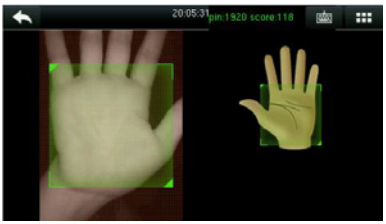
Cómo registrar una palma correctamente



Coloque su palma cerca del sensor multimodal, de forma que su palma se encuentre paralela al dispositivo. Asegúrese de mantener sus dedos separados.

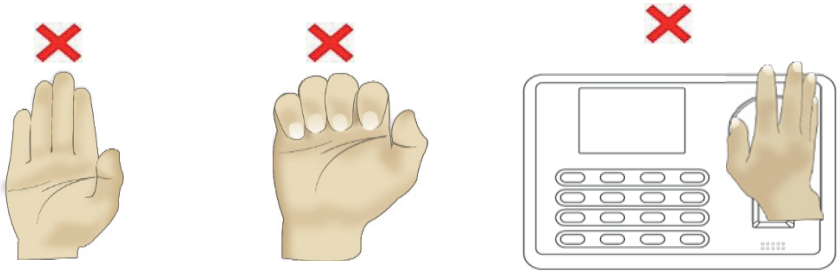
Durante el registro, coloque su palma de forma de que vea en el centro de la pantalla y siga las instrucciones de voz. El usuario deberá mover su palma hacia adelante y hacia atrás para ajustar la posición.

Verificación



Coloque su palma en el área verde, de forma paralela al dispositivo, con los dedos separados.

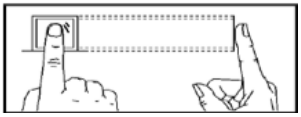
Gestos incorrectos de palma

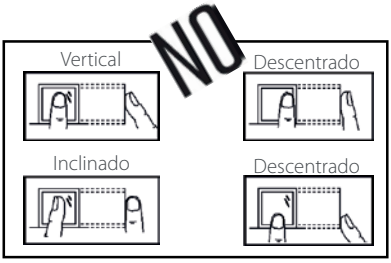


4.2 Colocación de dedo

Se recomienda utilizar el dedo índice, dedo medio o el anular; evitar el uso del pulgar o el dedo meñique.

Colocación Recomendada





4.3 Modos de Verificación

4.3.1 Verificación de Huella Digital

Verificación de Huellas Digitales 1:N

En el método de verificación de huellas digitales 1:N, una huella digital es obtenida por el sensor y se compara con todas las huellas digitales almacenadas en el dispositivo.

Utilice la forma correcta de colocar la huella digital en el sensor. Hay 2 posibles respuestas después de la verificación: Verificación Correcta o Verificación Fallida.



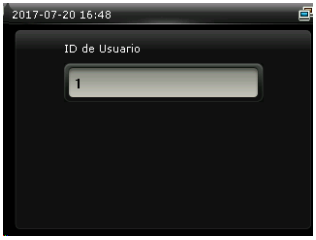
Verificación Exitosa



Verificación Fallida

Verificación de Huellas Digitales 1:1

En el método de verificación de huellas digitales 1:1, una huella digital es obtenida por el sensor y se compara con la huella digital correspondiente al ID de usuario introducido previamente. Favor de usar este método de verificación cuando sea difícil reconocer la huella en el método 1:N. Hay 2 posibles respuestas después de la verificación: **Verificación Correcta** o **Verificación Fallida**.









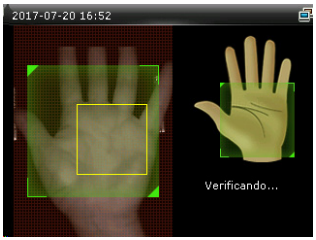
Notas:

1. Si se muestra el mensaje "¡ID de Usuario Incorrecto!" esto significa que el ID de usuario no existe.
2. El dispositivo muestra el mensaje "Por favor intente de nuevo" cuando la verificación falla. Si la verificación falla aún después de 3 intentos, saldrá a la interfaz inicial.

4.3.2 Verificación de Palma

Verificación de Palma

El dispositivo compara la palma actual con las plantillas de palma registradas. Utilice la forma correcta de registrar y verificar.



Verificación con Contraseña

En este método de verificación, la contraseña introducida se verifica con la contraseña del ID de usuario. Introduzca primero el ID del usuario, presione "Contraseña" y luego introduzca la contraseña. Hay 2 posibles respuestas después de la verificación: Verificación Correcta o Verificación Fallida.





Notas:
El dispositivo muestra el mensaje "Contraseña Incorrecta" cuando la verificación falla. Si la verificación falla aún después de 3 intentos, saldrá a la interfaz inicial

4.3.3 Verificación de Tarjeta *

Deslice una tarjeta registrada alrededor del sensor de huella cuando el dispositivo se encuentre en modo de espera.



Notas:
1. El dispositivo muestra el mensaje "Registro Duplicado" cuando desliza la tarjeta 2 veces.
2. El dispositivo emite un sonido de error cuando la tarjeta no está registrada.

5. Menú Principal

Encienda el dispositivo, presione **[M/OK]** para entrar al menú principal. Presione ▼ para desplazarse hacia abajo.





Descripción de los Menús:

Usuarios: Usted puede administrar la información de los usuarios registrados incluyendo ID de usuario, nombre, privilegios, palma, huella digital, contraseña, foto de usuario y parámetros de control de acceso.

Privilegios: Aquí puede asignar los privilegios de cada usuario de acceder a los menús y cambiar configuraciones.

Red (Ajustes de Comunicación): Establece los parámetros relacionados con la comunicación entre el dispositivo y la PC, incluyendo dirección IP, Puerta de enlace, Máscara de subred, Puerto de Comunicación, DNS, comunicación TCP/IP, etc.

Sistema: Para ajustar los parámetros relacionados al sistema como ajuste de fecha y hora, Asistencia, Parámetros de Palma y de Huella, reinicio y actualización por USB.

Personalizar: Establezca parámetros relacionados a la interfaz de usuario, como audio, volumen, programación de timbres, opciones de Estado de Asistencia y configuración de teclas de atajo.

Datos: Elimine/Respalde/Restaure los datos guardados en el dispositivo.

Control de Acceso: Establezca las opciones de acceso, programe los horarios / Días Festivos / Grupos de Acceso / Verificación Multi-Usuario, establezca las opciones de Anti-Passback y de Amago.

Gestión USB: Descargue y suba los datos de asistencia, datos de usuario, código de trabajo, mensajes, etc. Puede importar los datos almacenados en una unidad USB hacia un software de asistencia o a otro dispositivo.

Búsqueda de Asistencia: Para que los empleados busquen sus registros de asistencia almacenados en el dispositivo.

Imprimir: Para establecer la información de la función de imprimir (si se conecta una impresora al dispositivo).

Mensajes Cortos: Para ver/agregar/editar/eliminar un mensaje público o privado.

Código de Trabajo: Para ver/agregar/editar/eliminar un código de trabajo. Si se habilita esta opción, debe seleccionar o introducir un código existente después de verificar.

Pruebas: Para probar de forma automática funciones de diferentes módulos, incluyendo la pantalla LCD, voz, teclado, sensor de huellas digitales, reconocimiento de palma y el reloj de tiempo real.

Información del Sistema: Para comprobar la capacidad, información y firmware actual del dispositivo.

6 Gestión de Usuarios

6.1 Nuevo Usuario

Sólo los usuarios registrados pueden verificar su entrada en el dispositivo. Encienda el dispositivo, entre al menú principal. Entre a "Usuarios". -> "Nuevo Usuario".





6.1.1 Introducir ID y Nombre de Usuario

Presione ▼/▲ para seleccionar cualquier campo de la interfaz de Nuevo Usuario y presione **[M/OK]**:



Nota: Puede introducir un ID o dejar que el dispositivo le asigne uno.

6.1.2 Introducir Privilegio de Usuario

Presione ▼/▲ para seleccionar "Privilegio" en la interfaz de Nuevo Usuario y presione **[M/OK]**:



Administrador: Un administrador puede operar todas las funciones y menús del dispositivo.

Usuario Normal: Un usuario normal sólo tiene permitido verificar su entrada, buscar sus propios registros de asistencia y ver mensajes.

Nota: Se recomienda registrar un administrador para facilitar la gestión.

6.1.3 Modo de Verificación

Entre a Nuevo Usuario -> Privilegio de Acceso, presione ▼/▲ para seleccionar "Modo de Verificación" en la interfaz, presione **[M/OK]**:



Hay varias opciones para el método de verificación.

6.1.4 Registrar una Huella Digital

Presione ▼/▲ para seleccionar "Huella Digital" en la interfaz de Nuevo Usuario, presione **[M/OK]**:



1. Presione la tecla numérica correspondiente a la huella que desea registrar y presione **[M/OK].**

2. Presione su dedo en el sensor 3 veces según lo indique el dispositivo.

Nota: Necesita volver a registrar la huella si el dispositivo indica "Intente de nuevo por favor".

6.1.5 Registrar una Palma

Presione ▼/ ▲ para seleccionar "Palma" en la interfaz de Nuevo Usuario, presione **[M/OK]**:



Nota: Coloque su palma dentro del recuadro verde, como lo indica el dispositivo.

6.1.6 Registrar una Tarjeta *

Presione ▼/ ▲ para seleccionar "Tarjeta" en la interfaz de Nuevo Usuario, presione **[M/OK]**:



Nota: Use otra tarjeta si el dispositivo le indica "¡Error! ¡Tarjeta ya registrada!"

6.1.7 Registrar una Contraseña

Presione ▼/▲ para seleccionar "Contraseña" en la interfaz de Nuevo Usuario, presione **[M/OK]:**



Introduzca una contraseña de 1 a 8 dígitos y presione [M/OK], luego introduzca la contraseña de nuevo.

6.2 Todos los Usuarios

Encienda el dispositivo, entre al menú principal. Entre a "Usuarios" -> "Todos los Usuarios".





6.2.1 Editar un Usuario





Toda la información puede ser modificada, excepto el ID de Usuario.

6.2.2 Eliminar un Usuario

Presione ▼/▲ para seleccionar a un usuario a editar y presione **[M/OK]**. Entre en "Eliminar":





Puede elegir entre diferentes datos de usuario a eliminar.

6.3 Estilo de Pantalla

El estilo por defecto es "Una Línea". Entre a "Usuarios" -> "Estilo de Visualización".





7. Privilegios

Sirve para definir perfiles de privilegios para operar el dispositivo. Puede especificar los menús disponibles para cada perfil de privilegios. Puede definir 3 perfiles de privilegios.

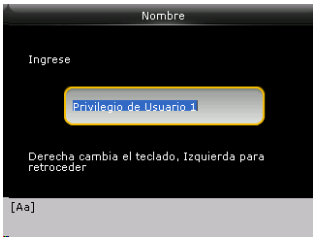
Entre a "Privilegios". Presione uno de los 3 privilegios para editar:





Debe existir un administrador registrado antes de poder definir un nuevo privilegio.

7.1 Crear y definir un nuevo privilegio



1. Introduzca un nombre con el teclado T9.

2. Puede definir más de un menú disponible para un privilegio. Presione **[M/OK]** para seleccionar.

8. Ajustes de Comunicación

Establezca los parámetros de comunicación. Entre al menú "Red"

1. Ethernet: El dispositivo puede comunicarse con una PC a través de cable Ethernet con los parámetros que establezca aquí.

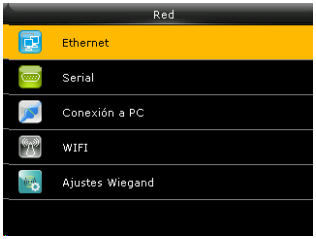
2. Serial: El dispositivo puede comunicarse con una PC a través del cable Serial con los parámetros que establezca aquí.

3. Conexión a PC: Establezca un ID de dispositivo y decida si desea establecer una contraseña para conectar el dispositivo a un software en la PC.

4. Wi-Fi: Active/Desactive el Wi-Fi.

5. ADMS: Ajustes para comunicarse con el servidor ADMS.

6. Ajustes Wiegand: El dispositivo puede comunicarse con otros dispositivos a través de comunicación Wiegand.



8.1 Ethernet

Entre a "RED" -> "Ethernet"

1. Dirección IP: Modifíquelo si es necesario, no puede ser igual a la IP de la PC.

2. Máscara de Subred: Modifíquelo si es necesario.

3. Puerta de enlace: Es necesario establecer una dirección si el dispositivo y la PC se encuentran en diferentes segmentos de Red. Modifíquelo si es necesario.

4. DNS: Establezca la dirección de su servidor DNS.

5. Puerto TCP: Establezca el puerto de comunicación TCP.

6. DHCP: Protocolo de Configuración Dinámica de Host (por sus siglas en inglés). Es utilizado para asignar direcciones IP dinámicas a clientes en una red a través de un servidor.

7. Mostrar en la barra de estado: Para establecer si se muestra el ícono de red en la barra de estado.



8.2 Comunicación Serial

1. Puerto Serial: Cuando el puerto serial (RS232/RS485) se usa para comunicar el dispositivo a la PC, se debe revisar este ajuste.

2. Baudios: Para la comunicación con la PC. Se recomienda usar RS232 para una comunicación rápida.

Nota: Hay 5 velocidades de baudios disponibles para RS232: 9600, 19200, 38400, 57600 y 115200; la velocidad 9600 no aplica para RS485. Reinicie el dispositivo para aplicar los cambios.



8.3 Conexión a PC

Para incrementar la seguridad de los datos de asistencia, puede establecer una contraseña de conexión. Entre a "RED" -> "Conexión a PC".



Clave de Comunicación: Establezca una contraseña de 1 a 6 dígitos. Deberá introducir la contraseña cuando conecte el dispositivo a un software en la PC.

ID del Dispositivo: Número de identificación del dispositivo, que oscila entre 1 ~ 254. Si se utiliza la comunicación por RS232/RS485, debe introducir este ID en la interfaz de comunicación del software.

8.4 ADMS *

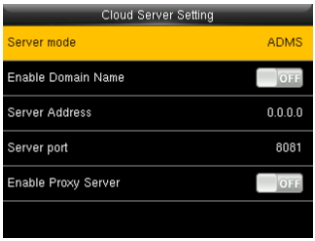
Ajustes para conectarse con el servidor ADMS. Entre a "RED" -> "Conf Server Cloud".

1.Habilitar nombre de dominio: Cuando se activa esta función, puede acceder a un sitio web usando el nombre en formato http://; de lo contrario, debe introducir la dirección IP del sitio a acceder.

2. Dirección del Servidor: Introduzca la dirección IP del servidor ADMS.

3. Puerto del Servidor: Introduzca el número de puerto utilizado por el servidor ADMS.

4. Habilitar Servidor Proxy: Para habilitar el Proxy, configure la dirección IP y número de puerto del servidor proxy. La forma de introducir la IP del Proxy y la dirección del servidor es la misma.



9. Sistema

Establezca los parámetros del sistema de acuerdo a sus necesidades. Se incluyen parámetros de Hora/Fecha, Asistencia, Huella Digital, etc.





9.1 Fecha/Hora

Establezca la fecha y hora del sistema. Entre a "Sistema" -> "Fecha/Hora".

1. Fecha/Hora: Establezca la fecha y hora del dispositivo.

2. Formato de 24 Horas: Decida si desea usar el formato de 24 horas. Si lo desactiva, se usará el formato de 12 horas.

3. Formato de Fecha: Establezca el formato para la fecha: AA-MM-DD, AA/MM/DD, AA.MM.DD, DD-MM-AA, etc.



Cambio de Horario: El Horario de Verano, también llamado DST, es un sistema de ajuste de la hora local con el fin de ahorrar energía.

El tiempo que se adopta durante las fechas establecidas se llama "Horario de Verano". Por lo general, se adelanta una hora en verano para aprovechar mejor la iluminación y ahorrar energía. En otoño, el tiempo se reanudará el tiempo estándar. Las regulaciones son diferentes en distintos países. En la actualidad, cerca de 110 países adoptan el horario de verano.

El dispositivo puede adoptar el cabio de horario adelantando una hora a las XX (hora) XX (día) XX (mes), y retrocediendo una hora a las XX (hora) XX (día) XX (mes). Por ejemplo, ajuste el reloj para que se adelante una hora a las 08:00 del 1 de Abril y que retroceda una hora a las 08:00 el 1 de Octubre.

Modo de Cambio de Horario: Elija el modo del cambio de horario. Puede elegir entre el modo por fecha/hora o el modo por semana/día.

Ajustes de Cambio de Horario: Ajuste la fecha/hora o la semana/día del cambio de horario de acuerdo al modo seleccionado.

Nota: No puede configurar el fin del cambio de horario para el siguiente año, es decir, el fin del cambio de horario debe ser en el mismo año del inicio del cambio de horario.

9.2 Asistencia

Entre a "Sistema" -> "Asistencia"





Los parámetros de asistencia son los siguientes:

Periodo de Acceso Duplicado (m): Durante un tiempo definido (Unidad: minutos), los registros de asistencia duplicados no se guardarán (el valor varía de 1 a 999999 minutos).

Alerta por Memoria Baja: Cuando la memoria de almacenamiento restante es menor al valor establecido, el dispositivo alertará automáticamente a los usuarios sobre la cantidad de almacenamiento restante. La función puede desactivarse o establecerse a un valor de entre 1 a 9999.

Borrado cíclico de Eventos: La cantidad de registros de asistencia que serán eliminados cada vez que se llega a la máxima capacidad de almacenamiento. La función puede desactivarse o establecerse a un valor de entre 1 a 999.

Mostrar Confirmación (s): El tiempo que se muestra en la pantalla el resultado de las verificaciones. El valor oscila de 1 a 9 segundos.

Reglas de Usuario Expirado: Elija las acciones de acuerdo a la validez del usuario.

Opciones de Reglas de Expiración: Las opciones para el fin de la validez de un usuario.

9.3 Reiniciar Equipo

Reinicie los ajustes de comunicación, de sistema, de personalización, etc.





9.4 Actualización por USB



El firmware del dispositivo puede actualizarse mediante un archivo de actualización guardado en una unidad USB. Normalmente no se recomienda actualizar el firmware. Si necesita la actualización, contacte a nuestro personal de soporte técnico.

10. Personalizar

Para configurar algunos parámetros y funciones del dispositivo. Entre a "Personalizar".





10.1 Interfaz de Usuario

Para configurar los siguientes parámetros, entre a "Personalizar" -> "Interfaz de Usuario".





Fondo de Pantalla: Seleccione la imagen a utilizar como fondo de pantalla.

Idioma: Seleccione el idioma del dispositivo.

Tiempo de Espera del Menú (s): El dispositivo vuelve automáticamente a la interfaz inicial si no se hace ninguna operación después del periodo de tiempo seleccionado (el rango es de 60 a 99999 segundos).

Tiempo para Protector de Pantalla(s): Cuando no se haga ninguna operación en la interfaz inicial después del periodo de tiempo seleccionado, iniciará el protector de pantalla. El tiempo válido es de 3 a 999 segundos.

Intervalo de Imágenes (s): Establezca el intervalo de tiempo entre las imágenes del protector de pantalla. El tiempo válido es de 3 a 999 segundos.

Tiempo de espera para reposo (m): Esta función permite establecer el tiempo de espera del dispositivo para ingresar al modo de reposo. Presione cualquier tecla para sacar al dispositivo del estado de reposo. El tiempo válido es de 1 a 999 minutos.

Estilo de la Pantalla Principal: Seleccione el estilo de la pantalla principal (3 estilos disponibles).

10.2 Voz

Voz: Seleccione si desea activar los mensajes de voz durante la operación del dispositivo.

Sonido de Teclas: Seleccione si desea activar el sonido al tocar el teclado.

Volumen: Ajuste el volumen de los sonidos del dispositivo.



10.3 Programación de Timbre

Muchas empresas eligen utilizar un timbre para dar aviso del inicio/fin de la jornada laboral. Cuando llegue la hora programada de un timbre, el dispositivo hará sonar automáticamente el tono seleccionado durante el tiempo establecido por el usuario.

10.3.1 Nuevo Timbre

Entre a "Personalizar" -> "Timbre Programado" -> "Nuevo Timbre Programado"

Estado del Timbre: Active/Desactive un timbre.

Hora de Timbre: El timbre suena automáticamente cuando se llega a la hora especificada.

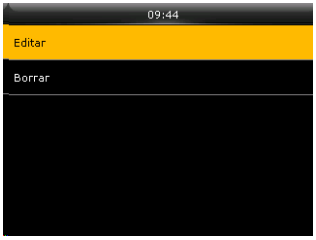
Repetir: Establecer si el timbre se repite de lunes a domingo.

Tipo de Timbre: Puede seleccionar entre el timbre interno o un timbre externo. En el timbre interno, el tono suena desde el altavoz del dispositivo. En el timbre externo, el tono suena desde un timbre eléctrico externo que se conecta al dispositivo.

Tono: El tono que suena como timbre.

Duración del Timbre: Para establecer la duración del timbre. El valor oscila entre 1 a 999 segundos.

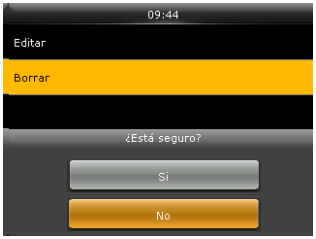
10.3.2 Todos los timbres



Para editar un timbre programado.

1. Seleccione el timbre que desea editar.

2. Presione "Editar" para modificar los ajustes.



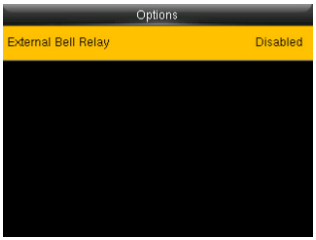
Para eliminar un timbre programado.

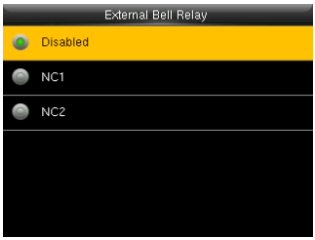
1. Seleccione el timbre que desea borrar.

2. Presione "Borrar" para eliminar el timbre.

10.3.3 Opciones

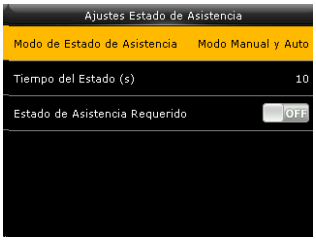
Cuando se use un timbre externo, establezca la terminal de salida del timbre externo.





10.4 Ajustes de Estados de Asistencia

Para configurar las teclas con las que selecciona un Estado de Asistencia. Entre a "Personalizar" -> "Opciones de Estados de Asistencia".





Modo de Estado de Asistencia:

Apagado: El Estado de Asistencia no es utilizado.

Modo Manual: Los Estados de Asistencia son cambiados manualmente al presionar la tecla de atajo correspondiente.

Modo Automático: Cuando llegue la hora establecida, el Estado de Asistencia cambiará automáticamente.

Modo Manual & Automático: Los Estados de Asistencia cambian automáticamente y además usted tiene la opción de cambiar el Estado de Asistencia manualmente. Un Estado de Asistencia que usted seleccione manualmente cambiará automáticamente cuando pase el tiempo de espera configurado.

Modo Fijo Manual: Cuando el Estado de Asistencia sea cambiado manualmente, se mantendrá fijo hasta que sea cambiado manualmente de nuevo.

Tiempo del Estado (s): Especificar el tiempo que se muestra el Estado de Asistencia seleccionado. El valor varía de 5 a 999 segundos. Al cumplirse el tiempo, el Estado no se muestra o cambia a otro.

Estado de Asistencia Requerido: Especificar si el Estado de Asistencia debe ser seleccionado durante la verificación.

Observaciones: Hay 4 Estados de Asistencia: Entrada, Salida, Entrada a Tiempo Extra y Salida de Tiempo Extra.

10.5 Teclas de Función

Puede definir 6 teclas de atajo como atajos a un Estado de Asistencia o como atajo a una función del dispositivo. En la interfaz principal del dispositivo, presione la tecla de atajo y se mostrará el Estado de Asistencia configurado o entrará a la interfaz de la función del dispositivo configurada.

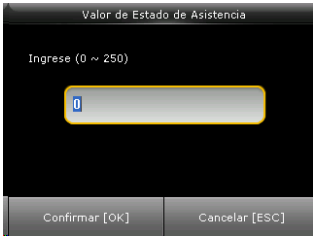


Nota: Cuando el Estado de Asistencia es seleccionado como una función del sistema, entrará a la interfaz de configuración del Estado de Asistencia (Nombre, Valor, Hora de Cambio). El estado puede establecerse para que cambie automáticamente a la hora configurada.

Si selecciona el modo de estado de asistencia como "Apagado", el estado de asistencia no se mostrará, aunque configure una tecla de atajo para un estado de asistencia.

Valor de Estado de Asistencia: El dispositivo le establece un valor diferente a cada Estado de Asistencia por defecto. El valor 0 corresponde al estado de Entrada, 1 a Salida, 4 a Entrada a Tiempo Extra, 5 a Salida de Tiempo Extra. Puede establecerles un valor con un rango de 0 a 250.





Función: Seleccione una opción de Estado de Asistencia o una opción de función del menú.





Nombre: Introduzca el nombre del Estado de Asistencia.





Fijar hora de Cambio: Establezca el horario automático del estado de asistencia.





11. Gestión de Datos

Gestione los datos almacenados en el dispositivo. Entre a "Datos".





11.1 Borrar Datos

En el menú Datos puede gestionar los datos guardados en el dispositivo, por ejemplo, borrar los registros de asistencia, todos los datos, los protectores de pantalla, eliminar los privilegios de administrador y reiniciar el dispositivo a los valores de fábrica.





Borrar Eventos: Eliminar todos los registros de asistencia guardados en el dispositivo o borrar registros de acceso de un rango de tiempo específico.

Borrar Todo: Eliminar toda la información de los usuarios, huellas digitales, palmas, registros de asistencia, códigos de trabajo, etc.

Borrar Privilegios de Administrador: Convertir a todos los administradores en usuarios normales.

Borrar Control de Acceso: Borrar todos los ajustes de acceso.

Borrar Fondos de Pantalla: Eliminar todos los fondos de pantalla en el dispositivo.

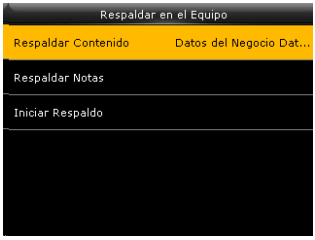
Borrar Protectores de Pantalla: Eliminar todos los protectores de pantalla en el dispositivo.

Borrar Datos de Respaldo: Eliminar los datos pertenecientes a la copia de seguridad.

11.2 Respaldo de Datos

Usted puede respaldar los datos de la empresa o datos de configuración en el dispositivo o en una unidad USB.





Nota: Cuando respalde los datos en una unidad USB, primero debe insertar una unidad USB en el dispositivo y luego presionar **[M/OK]** para iniciar el respaldo.

11.3 Restaurar Datos

Restaure los datos guardados en el dispositivo o en una unidad USB.





1. Seleccione una ruta.
2. Seleccione el tipo de datos a restaurar.
3. Inicie la restauración.

Nota: Cuando restaure los datos desde una unidad USB, primero debe insertar una unidad USB que contenga los datos a restaurar en el dispositivo.

12. Control de Acceso

El menú de control de acceso se usa para configurar los horarios y restricciones para la apertura de la puerta.





Para poder acceder, los usuarios registrados deben cumplir con las siguientes condiciones:

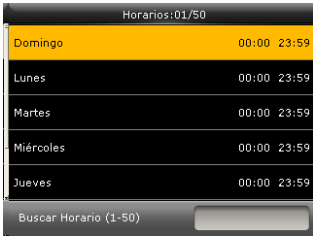
1. La hora de acceso del usuario debe estar dentro del horario personal del usuario o en el horario de su grupo.

2. El grupo al que pertenece el usuario debe existir dentro del control de acceso. Los usuarios nuevos son asignados en el primer grupo de acceso con el horario de grupo predeterminado [1] y combinación de acceso "1", además quedan en estado desbloqueado.

12.1 Horarios

El **Horario** es la unidad de tiempo mínima de los ajustes de control de acceso; se pueden establecer un máximo de **50 horarios** en el sistema. Cada Horario consiste de 7 secciones de tiempo (una semana) y cada sección de tiempo contiene el periodo válido dentro de 24 horas. Entre a "Acceso" -> "Horarios".





El horario por defecto es el número 1 (válido todo el día), el cual puede editarse.

Horario Válido: 00:00-23:59 (Válido todo el día) o cuando la hora de fin es mas tarde que la hora de inicio (por ejemplo: 08:00-23:59).

Horario Inválido: Cuando la hora de fin es antes de la hora de inicio. Lo que significa que un horario no puede ocupar 2 días diferentes.

Ejemplo de horario válido e inválido:



Válido



Inválido

12.2 Días Festivos

Usted puede agregar días festivos al dispositivo y establecer los horarios de acceso para dichos días festivos según sea necesario. Entre a "Acceso" -> "Días Festivos", presione "Agregar Día Festivo" para entrar a la interfaz.





Los ajustes incluyen número, fecha de inicio, fecha de fin y horario.



Nota: La fecha de inicio y de fin requieren que introduzca el mes (MM) y día (DD).

Horario: El horario válido a usar durante el día festivo.

Como se muestra en la figura anterior, el Día Festivo 1 comienza el 1° de Mayo y termina el 3 de Mayo de cada año.

12.3 Grupos de Acceso

Sirve para asignar a los usuarios a diferentes grupos de control de acceso y facilitar la gestión.
El horario por defecto de los miembros de un grupo se establece en el horario del grupo, pero los usuarios también pueden tener asignados un horario personal. A cada grupo se le pueden configurar hasta 3 horarios, siempre que al menos uno de esos horarios sea válido, los miembros del grupo pueden acceder exitosamente.

Por defecto, los usuarios nuevos pertenecen al grupo 1, pero pueden asignarse a otro grupo. Entre a "Acceso" -> "Grupos" -> "Nuevo Grupo".





Como se muestra en las siguientes imágenes, el **Modo de Verificación del Grupo de Acceso 5** es sólo huella; los Horarios 1, 2 y 3 fueron establecidos y se incluyen los días festivos.





12.4 Combinaciones de Acceso *

Combine 2 o más usuarios para crear una verificación multi-usuario y así aumentar la seguridad.
En una Combinación de Acceso puede combinar hasta 5 usuarios, los usuarios pueden ser de grupos diferentes o pertenecer al mismo grupo.



Nota: En una Combinación de Acceso sólo puede combinar los grupos que haya configurado en la interfaz Grupos de Acceso.

Por ejemplo:



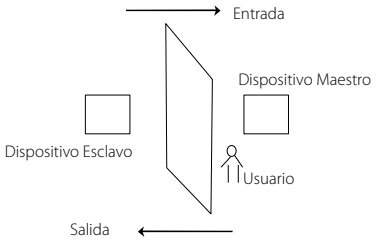
Como se muestra en la figura, la Combinación de Acceso 1 está compuesta de 5 miembros de diferentes grupos: Grupos 1, 3, 5, 6 y 8 respectivamente.

Nota: Para borrar una Combinación de Acceso, configure todos los grupos de la combinación a 0.

12.5 Ajustes Anti-Passback *

Para evitar que una persona que sigue a un usuario consiga acceder sin verificación, lo cual resulta en un problema de seguridad, los usuarios pueden activar la función Anti-Passback. Bajo esta función el registro de entrada debe coincidir con el registro de salida para poder abrir una puerta.
Esta función requiere de 2 dispositivos trabajando juntos: Uno instalado dentro de la puerta (dispositivo maestro) y otro instalado fuera de la puerta (dispositivo esclavo). Ambos dispositivos se comunican a través de una señal Wiegand.

El formato Wiegand y el tipo de salida (ID de Usuario/Número de Tarjeta) de ambos dispositivos debe ser consistente.



Dirección de Anti-Passback





No Anti-Passback: La función Anti-Passback está desactivada, lo que significa que la verificación, ya sea en el dispositivo maestro o esclavo, puede abrir la puerta. Los registros de acceso no se guardan.

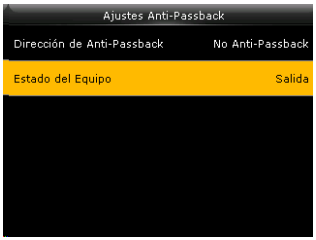
Anti-Passback Salida: Después de que el usuario registre una salida, sólo si el registro más reciente es una entrada, el usuario puede volver a registrar una salida; de lo contrario, se activará la alarma. Sin embargo, el usuario puede registrar entradas libremente.

Anti-Passback Entrada: Después de que el usuario registre una entrada, sólo si el registro más reciente es una salida, el usuario puede volver a registrar una entrada; de lo contrario, se activará la alarma. Sin embargo, el usuario puede registrar salidas libremente.

Anti-Passback Entrada/Salida: Después de que el usuario registre una entrada/salida, sólo si el registro más reciente es una entrada, el usuario puede volver a registrar una salida, y sólo si el registro más reciente es una salida, el usuario puede volver a registrar una entrada; de lo contrario, se activará la alarma.

Desactivar y Guardar: La función Anti-Passback se desactiva, pero el estado de asistencia se guarda.

Estado del Dispositivo





Ninguno: Para desactivar la función Anti-Passback.

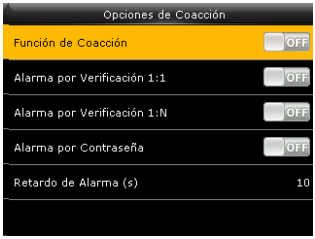
Salida: Todos los registros en el dispositivo son registros de salida.

Entrada: Todos los registros en el dispositivo son registros de entrada.

12.6 Opciones de Coacción

Cuando los usuarios se encuentran en una situación de coacción, el dispositivo se encargará de abrir la puerta como de costumbre y enviará la señal de alarma discreta.





Función de Coacción: Cuando la función está activada, presione la "Tecla de Coacción" y luego presione cualquier huella registrada (en los siguientes 10 segundos), la alarma de coacción será enviada al verificar exitosamente. Si la función está desactivada, presionar la tecla de coacción no activará la alarma.

Alarma en 1:1: Si está activada, cuando un usuario utilice el método de verificación 1:1 para verificar cualquier huella registrada, la alarma se activará. Si está desactivada, no se activará ninguna señal de alarma.

Alarma en 1:N: Si está activada, cuando un usuario utilice el método de verificación 1:N para verificar cualquier huella registrada, la alarma se activará. Si está desactivada, no se activará ninguna señal de alarma.

Alarma con Contraseña: Si está activada, cuando un usuario utilice el método de verificación con contraseña, la alarma se activará. Si está desactivada, no se activará ninguna señal de alarma.

Retardo de alarma (s): Cuando se activa la alarma de coacción, el dispositivo enviará una señal de alarma después de 10 segundos (por defecto); el tiempo de retardo de la alarma puede modificarse (el valor varía de 0 a 999 segundos).

13. Gestión USB

Importar la información (datos de Usuario, plantillas de huella/palma, registros de asistencia, etc.) guardada en el dispositivo hacia un software de asistencia o hacia otro dispositivo por medio de una unidad USB.
Entre a "Gestión USB" -> "Descargar/Cargar".





Nota: Antes de descargar/cargar datos desde/hacia una unidad USB, inserte una unidad USB en el puerto USB del dispositivo.

13.1 Descargar en USB

Descargar datos del dispositivo en una unidad USB.



Datos de Asistencia: Descargue los registros de asistencia en una unidad USB.

Datos de Usuario: Descargue todos los datos de usuario en una unidad USB.

Fotos de Usuario: Descargar las fotos de asistencia en una unidad USB.

Código de Trabajo: Descargue todos los códigos de trabajo en una unidad USB.

Mensajes: Descargue todos los mensajes en una unidad USB.

13.2 Cargar desde USB

Cargue datos al dispositivo desde una unidad USB.



Protector de Pantalla: Cargue protectores de pantalla guardados en una unidad USB.

Fondo de Pantalla: Cargue fondos de pantalla guardados en una unidad USB.

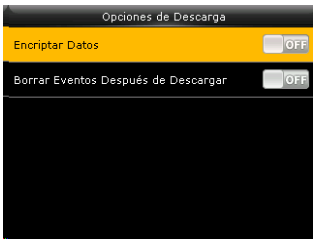
Datos de Usuario: Cargue los datos de usuario guardados en una unidad USB.

Fotos de Usuario: Cargue las fotos de usuario guardados en una unidad USB.

Cargar Códigos de Trabajo: Cargue todos los códigos de trabajo guardados en una unidad USB.

Mensajes: Cargue todos los mensajes guardados en una unidad USB.

13.3 Opciones de Descarga

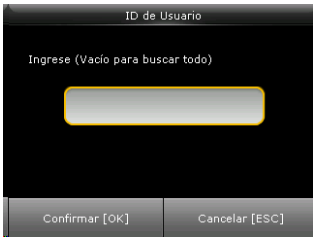


Es posible encriptar los datos en una unidad USB, así como configurar el dispositivo para que borre los datos una vez descargados en la USB.
Durante la descarga de los registros de asistencia, también puede configurar el tipo de calendario mostrado en la hora de asistencia.
El dispositivo soporta 3 tipos de calendario: Gregoriano, Irán Gregoriano e Irán Lunar.

14. Búsqueda de Asistencia



Cuando los usuarios verifican exitosamente, se guarda un registro en el sistema. Esta función permite a los usuarios consultar los registros de asistencia.

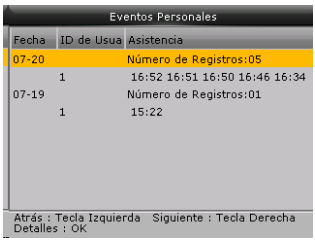




1. Introduzca el ID del usuario que desea buscar.

2. Seleccione el periodo en el que desea buscar registros.

Nota: Puede buscar los registros de todos los usuarios si deja en blanco la caja de entrada de ID.





3. Se muestra la lista de los registros.

4. Seleccione cualquiera para ver los detalles.

15. Impresión

Los dispositivos con la función de imprimir pueden imprimir los registros de asistencia cuando se le conecta una impresora.

15.1 Ajustes de Campos de Datos

En la interfaz inicial, presione **[M/OK]** > Imprimir > Campos de Datos > presione **[M/OK]** en cada campo para activar aquellos que desea imprimir.









15.2 Ajustes de Impresión

Entre a "Impresión" -> "Ajustes de Impresión" presione **[M/OK]** para activar o desactivar la función **Corte de Papel**.





Nota: Para activar la función Corte de Papel, necesita conectar una impresora que incluya la función de corte de papel, de forma que la impresora se encargue de cortar el papel de acuerdo a la información seleccionada para imprimir.

16. Mensajes



Es posible crear, editar, eliminar y enviar mensajes públicos o personales. Puede guardar los mensajes en borradores. A la hora asignada, un mensaje público se mostrará a todos los usuarios en el fondo de la pantalla principal, mientras que un mensaje personal se le mostrará al usuario específico después de que verifique exitosamente.

16.1 Crear un nuevo mensaje



Mensaje: Escriba el mensaje.

Fecha/Hora de inicio: Establezca la fecha y hora en que desea se muestre el mensaje.

Duración del Mensaje (m): El tiempo en minutos antes de que desaparezca el mensaje, calculado a partir de la hora de inicio.

Tipo de Mensaje: Público, Personal y Borrador.



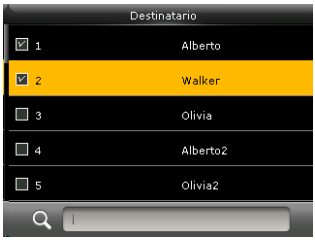
Público: Mensaje que puede ser visto por todos los usuarios.

Personal: Dirigido a un usuario en específico.

Borrador: Un mensaje preestablecido, sin diferencia a un mensaje público o personal.

Ver o editar un mensaje:

Presione **V** para seleccionar un mensaje de la lista y presione OK. Puede ver, editar o eliminar el mensaje seleccionado



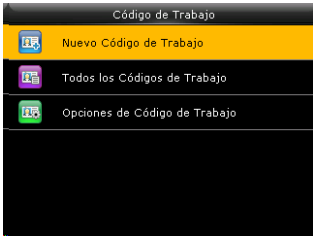
Al editar un mensaje personal, puede seleccionar más de un usuario que recibirá e mensaje. Presione [Esc] para guardar y salir.

16.2 Opciones de Mensaje



Tiempo para mostrar (s): Es el tiempo en segundos que se mostrará un mensaje personal en la pantalla. Una vez pasado este tiempo, el sistema regresará a la interfaz inicial. El valor es de 1 a 99999 segundos.

17. Código de Trabajo



El salario que perciben los empleados está sujeto a sus registros de asistencia. Algunos empleados pueden realizar diferentes tipos de trabajo que pueden manejar diferentes periodos de tiempo. Considerando que el salario puede variar según los tipos de trabajo, la terminal proporciona un parámetro para indicar el correspondiente tipo de trabajo para cada registro de asistencia. Los códigos de trabajo se descargan junto con los registros de asistencia.

17.1 Nuevo Código de Trabajo

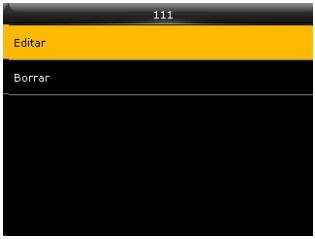


ID: Es el número asignado al código de trabajo. El rango es 1-99999999.

Nombre: Introduzca un nombre para el código de trabajo. El límite son 23 caracteres.

Nota: El código de trabajo no puede ser modificado una vez confirmado.

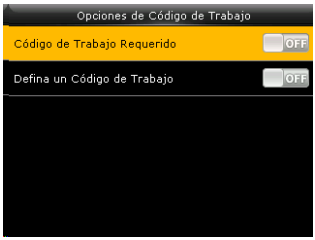
17.2 Todos los Códigos de Trabajo



Usted puede ver, editar o eliminar un código de trabajo de la lista. El ID no puede ser modificado.

1. Seleccione un Código de Trabajo
2. Presione "Editar" para modificar el nombre. Presione "Borrar" para eliminar.

17.3 Opciones de Códigos de Trabajo



Código de Trabajo Requerido: Se debe introducir un Código de Trabajo durante la verificación. Seleccione si desea activar esta función.

Código de Trabajo Definido: El código de trabajo que se introduzca durante la verificación debe estar definido previamente. Seleccione si desea activar esta función.

18. Pruebas

Las pruebas automáticas le permiten al dispositivo comprobar el correcto funcionamiento de sus módulos, incluyendo la pantalla LCD, sonido, sensor de huellas, teclado y reloj.





Probar Todo: Probar pantalla LCD, sonido, teclado, sensor y reloj. Durante la prueba, presione **[M/OK]** para continuar a la siguiente prueba, o [ESC] para salir de la prueba.

Probar LCD: Probar la pantalla LCD.

Probar Voz: Probar si los archivos de voz están completos y que la calidad del sonido sea la adecuada.

Probar Teclado: Probar si todas las teclas funcionan correctamente.

Probar Sensor de Huellas: Probar si el sensor de huellas digitales encuentra funcionando con normalidad.

Probar Reloj RTC: Probar el Reloj en Tiempo Real.

Al probar los módulos, siga las instrucciones de la pantalla.

19. Información del Sistema

Con este parámetro usted puede ver la capacidad de almacenamiento de datos, información del dispositivo y del firmware.





Capacidad del Equipo: Muestra la cantidad de usuarios registrados, administradores, contraseñas, huellas digitales, palmas, registros de asistencia y fotos de asistencia.

Información del Equipo: Muestra el nombre del dispositivo, número de serie, dirección MAC, algoritmo de huella digital, algoritmo de palma, información de la plataforma, fabricante y fecha de fabricación.

Información de Firmware: Muestra la versión de firmware, Servicio Bio, Servicio Standalone y Servicio Dev.

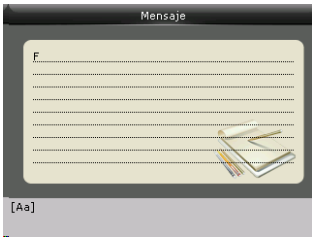
20. Anexos

1. Procedimiento para introducir Textos

El teclado T9 (texto predictivo) es rápido y eficiente. Hay 3 o 4 letras en las teclas numéricas (2-9), por ejemplo, A,B y C se encuentran en la tecla 2. Presione la tecla correspondiente una vez y el sistema le mostrará las letras correspondientes. Consulte los siguientes ejemplos:



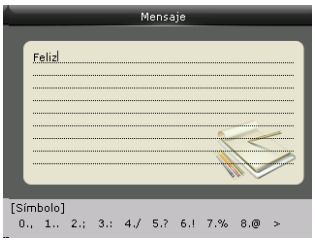
Entre a "Nuevo Mensaje"



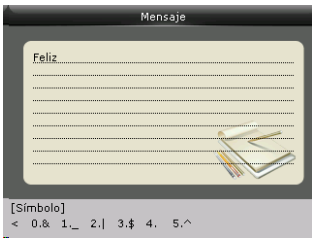
Presione [3] tres veces para introducir una F.



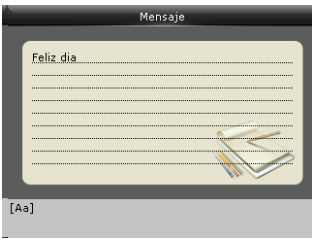
Escriba "eliz" de la misma forma.



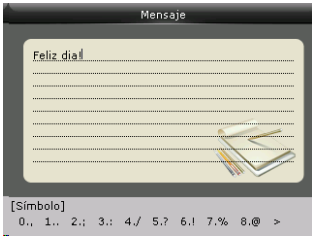
Presione ▶ para cambiar a los símbolos.



Presione ▶ hasta encontrar [4] correspondiente a un espacio en blanco. Presione [4].



Escriba "Día" de la misma manera.



Presione ▶ para cambiar a los símbolos. Presione [6] para introducir un "!"

2. Procedimiento para cargar imágenes.

- **Foto de Usuario:** Se necesita crear una carpeta llamada "photo" en la unidad USB y agregar las fotos de usuario dentro de esa carpeta. La capacidad es de 8000 imágenes, que no excedan los 15Kb cada una. El nombre de la imagen es X.jpg (X siendo el número de ID del usuario, máximo 9 dígitos). El formato de la foto debe ser JPG.

- **Protector de Pantalla:** Se necesita crear una carpeta llamada "advertise" en la unidad USB y agregar las fotos a usar como protectores de pantalla dentro de esa carpeta. La capacidad es de 20 imágenes, que no excedan los 30Kb cada una. El nombre y formato de la imagen no está restringido.

- **Fondo de Pantalla:** Se necesita crear una carpeta llamada "wallpaper" en la unidad USB y agregar las fotos a usar como fondos de pantalla dentro de esa carpeta. La capacidad es de 20 imágenes, que no excedan los 30Kb cada una. El nombre y formato de la imagen no está restringido. El formato puede ser jpg, png, bmp, etc.

Nota: Cuando cada foto de usuario y foto de asistencia no exceden 10Kb, el dispositivo puede guardar un total de 10000 fotos de usuario y de asistencia.

Declaración de Derechos Humanos y de Privacidad.

Apreciado consumidor:
Gracias por elegir los productos biométricos híbridos diseñados y fabricados por el equipo ZK. Como proveedor líder en el mercado de productos y soluciones biométricas, nos esforzamos por cumplir los estatutos relacionados con los derechos humanos y privacidad de cada país al mismo tiempo que continuamos con la investigación y desarrollo de nuevos productos.

Por esta razón consignamos en este documento la siguiente información:
1.- Todos dispositivos de reconocimiento de huella digital ZKTeco para uso civil, sólo recogen puntos característicos de las huellas digitales, no imágenes como tal. Gracias a esto no se suscitan problemáticas que involucren o vio¬len la privacidad de los usuarios.

2.- Los puntos característicos de las huellas digitales recolectadas por nuestros dispositivos no pueden ser utilizadas para reconstruir la imagen original de la huella.

3.- ZKTeco, como proveedor de los equipos, no se hace legalmente responsable, directa o indirectamente, por ninguna consecuencia generada debido al uso de nuestros productos.

4.- Para cualquier inconveniente que involucre derechos humanos o privacidad al usar nuestros productos, por favor contacte directamente a su empleador.

Nuestros otros equipos de huella digital de uso policíaco u herramientas de desarrollo pueden proporcionar la función de recolección de las imágenes originales de las huellas digitales. Cuando considere que este tipo de recolección de huellas infringe su privacidad, por favor contacte al gobierno local o al proveedor final. ZKTeco, como el fabricante original de los equipos, no se hace legalmente responsable de ninguna infracción generada por esta razón.

Nota: Las siguientes son regulaciones ligadas a las leyes de la República popular de China acerca de la libertad personal:
1. Detención, reclusión o búsqueda ilegal de ciudadanos de la República Popu¬lar de China es una violación a la intimidad de la persona, y está prohibida.
2. La dignidad personal de los ciudadanos de la República Popular de China es inviolable.
3. El hogar de los ciudadanos de la República Popular de China es inviolable.
4. La libertad y privacidad correspondiente a los ciudadanos de la República Popular de China están protegidos por la ley.

Recalcamos que la biometría, como avanzada tecnología de reconocimiento, será aplicada en diversos sectores; incluyendo el comercio electrónico, sistemas bancarios, aseguradoras y cuestiones legales. Cada año alrededor del mundo, una gran cantidad de personas sufren inconvenientes causados por la inseguridad de las contraseñas.
En la actualidad, el reconocimiento de huellas digitales es utilizado para una protección adecuada de la identidad de las personas brindando un ambiente de alta seguridad en todo tipo de empresa.

Descripción de Uso amigable con el Medio Ambiente

- El EFUP (Periodo de Uso Amigable con Medio Ambiente, por sus siglas en inglés) marcado en este producto se refiere al periodo de seguridad en el cual el producto es utilizado bajo las condiciones establecidas en las instrucciones del mismo, sin riesgo de fuga de sustancias nocivas o perjudiciales.
- El EFUP de este producto no cubre las partes consumibles que necesiten ser reemplazadas regularmente, por ejemplo, baterías. El EFUP de las baterías es de 5 años.

Nombre y concentración de sustancias o elementos nocivos						
Nombre de las piezas	Sustancias o elementos nocivos					
	Pb	**Hg**	**Cd**	**Cr6+**	**PBB**	**PBDE**
Resistencia	X	O	O	O	O	O
Condensador	X	O	O	O	O	O
Inductor	X	O	O	O	O	O
Diodo	X	O	O	O	O	O
Componentes ESD	X	O	O	O	O	O
Buzzer	X	O	O	O	O	O
Adaptador	X	O	O	O	O	O
Tornillos	O	O	O	X	O	O

o: Indica que esta sustancia tóxica o nociva presente en todos los materiales homogéneos de esta pieza está por debajo de los límites requeridos en SJ/T11363- 2006.
x: Indica que esta sustancia tóxica o nociva presente en al menos uno de los materiales homogéneos de esta pieza está por encima de los límites requeridos en SJ/T11363-2006.

Nota: El 80% de las partes de este producto están fabricadas con materiales no-peligrosos para el medio ambiente. Las sustancias o elementos nocivos contenidos no pueden ser reemplazados por materiales ecológicos por razones técnicas o restricciones económicas.



www.zkteco.com

www.zktecolatinoamerica.com

Derechos de Autor © 2017, ZKTeco CO., LTD. Todos los derechos reservados.
ZKTeco puede, en cualquier momento y sin previo aviso, realizar cambios o mejoras en los productos y servicios o detener su producción o comercialización.
El logo ZKTeco y la marca son propiedad de ZKTeco CO., LTD.