MANUAL DE USUARIO

G2

Versión 1.0

Green Label

Acerca de este Manual

Aviso importante

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

Nota de privacidad

Sin el previo consentimiento 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 tal vez incluye 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, invertir ingeniería, 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.

Términos y condiciones

Debido a la constante renovación de productos, la empresa no puede garantizar que el artículo actual consista en su totalidad con la información consignada en este manual. Por favor disculpe los inconvenientes causados debido a los cambios hechos sin notificación. Nos reservamos los derechos finales de modificación e interpretación.

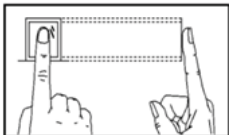
Contenido

Instrucciones de Uso

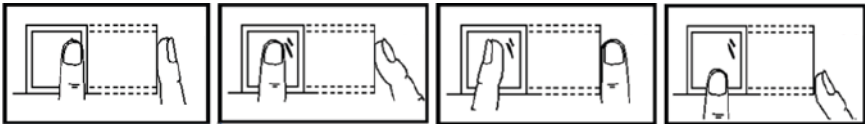
1.1 Ubicación del dedo

Los dedos recomendados son el índice, medio y el anular. El pulgar y el meñique no son recomendados (ya que a la hora de ubicarlos en el lector se muestran un poco torpes).

(1). Ubicación adecuada del dedo: La huella debe estar firme, de frente y centrada en el lector de huellas.



(2). Ubicación incorrecta: Cuando la huella se encuentra muy cerca o sobre los límites del lector, cuando el dedo inclinado hacia un lado o cuando se presiona sólo una parte de la huella.



1.2 Métodos de identificación

1.2.1 Verificación de huella digital 1:N

La terminal compara la huella actual recolectada con toda la información de huellas digitales almacenadas en el terminal.

Presione adecuadamente su huella en el lector mediante la adopción de la correcta colocación de la huella. Para más detalles, (Véase punto 1.1)

Instrucciones de Uso

La colocación de la huella.

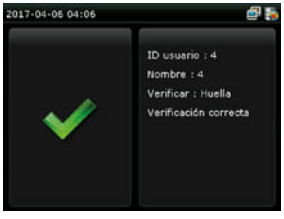
Cuando la verificación es exitosa, la pantalla se muestra de esta manera.

Cuando falla la verificación falla, la pantalla se muestra de esta manera.

1.2.2 Verificación de huella digital 1:1

En el modo de verificación 1:1, el dispositivo compara la huella actual recolectada con la información relacionada al ID de usuario ingresado. Utilice este método únicamente en situaciones en que se dificulte el reconocimiento de la huella digital.

Ingrese el ID de usuario utilizando el teclado del dispositivo, presione [OK]. Ubique adecuadamente la huella en el sensor.



Cuando la verificación es exitosa, la pantalla se muestra de esta manera..

Cuando falla la verificación, La pantalla se muestra de esta manera.

Nota:

• Cuando falla la verificación, y el aviso dice que el número ingresado es incorrecto, significa que ese número no existe o que cometió un error al ingresar los dígitos.

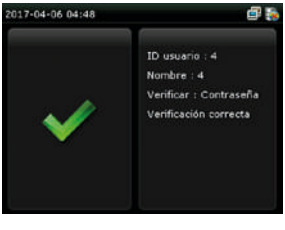
• Si el dispositivo dice "Por favor, intente de nuevo"; ubique de nuevo el dedo en el sensor. Usted puede intentarlo otras dos veces (configuración predeterminada), si falla después de estas dos veces, vuelva al paso 1 e inicie otra vez el proceso. El número de intentos puede ser cambiado (Véase punto 6.3 Huella Digital).

1.2.3 Contraseña

En la verificación por medio de contraseña, el dispositivo compara la contraseña ingresada con el ID de usuario.

Ingrese el ID de usuario utilizando el teclado del dispositivo, luego presione [OK].

Ingrese la contraseña y presione [OK].



Cuando la verificación es exitosa, la pantalla se muestra de esta manera..

Cuando falla la verificación, La pantalla se muestra de esta manera..

Nota: Si el dispositivo muestra el mensaje " ID inválido"; ingréselo de Nuevo. Usted puede intentarlo otras dos veces (configuración predeterminada), si falla después de estas dos veces, vuelva al paso 1 e inicie otra vez el proceso. El número de intentos puede ser cambiado (Véase punto 6.3 Huella Digital).

1.2.4 Tarjeta

Sólo los dispositivos integrados con módulo de tarjetas ID, soportan la verificación por medio de tarjeta. Los dispositivos que cuenten con este módulo son compatibles con los siguientes dos modos de verificación:

• Sólo tarjeta ID: El usuario sólo necesita deslizar la tarjeta para la verificación.

• Tarjeta +Huella digital: El usuario necesita deslizar la tarjeta y, acto seguido, presentar la huella digital.

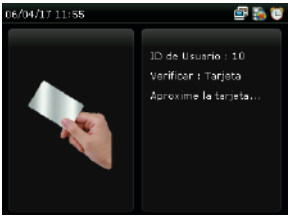
(1). Sólo tarjeta ID

Si el usuario posee una tarjeta registrada en el sistema, sólo necesita acercarla al lector de tarjetas del dispositivo y se hará la respectiva verificación.

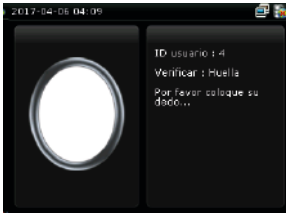
Cuando la verificación es exitosa, la pantalla se muestra de esta manera.

Cuando falla la verificación, La pantalla se muestra así.

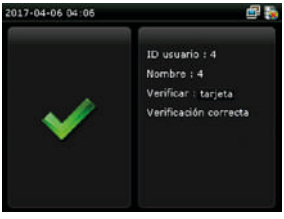
(2). Tarjeta + Huella digital



Deslice su tarjeta ID en el lector de tarjetas del dispositivo.



Después; presente de manera adecuada su huella digital en el lector de huellas del dispositivo.



Cuando la verificación es exitosa, la pantalla se muestra de esta manera..

1.3 Descripción de los iconos

Icono	Significado	Descripción
      	Señal de Celular	Si el icono de estatus se encuentra dentro de la cobertura de la red móvil celular, más barras verdes indican que la señal es más fuerte. G: Indica que la actual red móvil es la red GPRS*; con la cual, el dispositivo tiene acceso a internet. E: Indica que la red actual es la GSM; con la cual, el dispositivo tiene acceso a internet. W: Indica que el dispositivo que la red actual del dispositivo es la WCDMA; con la cual, el dispositivo tiene acceso a internet.
		Indica que no hay redes disponibles

Instrucciones de Uso

	Timbre	Indica que el timbre ha sido establecido
		Indica una alarma desmontada
	Ethernet	Conexión Ethernet establecida.
		Conexión Ethernet desconectada
	Servidor ADMS	La conexión Dispositivo-ADMS es exitosa
		La conexión Dispositivo-ADMS, falló
		Los datos de comunicación ADMS se están transmitiendo.
	Mensajes Cortos	Mensajes públicos.
		La conexión Wi-Fi es normal
		No hay conexión Wi-Fi.

Menú Principal

Cuando es dispositivo se encuentre en su interfaz inicial, presione [M/OK] para abrir el menú principal, como se muestra a continuación:

Administrador: El usuario puede navegar por la información de usuario almacenada en el terminal, incluyendo el ID de usuario, el nombre, privilegio de usuario, huella digital, número de tarjeta, contraseña, foto del usuario, añadir, modificar o eliminar la información del usuario.

Privilegios de usuario: se utiliza para establecer los privilegios que tendrá cada usuario, es decir, los permisos de entrar a los menús.

Opciones de comunicación: Puede configurar los parámetros relacionados para la comunicación entre el terminal y el PC,

incluyendo la dirección IP, puerta de enlace, máscara de subred, la velocidad en baudios, la identificación del dispositivo y clave de comunicación, etc.

Sistema: Se pueden configurar parámetros relacionados al sistema, incluyendo la fecha y hora, la asistencia, la huella digital, la cámara, reinicio y actualización de USB, para permitir que el terminal para cumplir con los requisitos de los usuarios en la mayor medida en términos de funciones y pantalla.

Personalizar: se utiliza para satisfacer las necesidades de los usuarios en la mayor medida con respecto a la pantalla, audio, sonido, y la definición del teclado.

Gestor de datos: Usted puede llevar a cabo la gestión de los datos almacenados en el terminal, por ejemplo, eliminar datos, respaldar datos y restauración de datos.

Menú Principal

Contro de acceso: Puede configurar los parámetros de las cerraduras electrónicas y dispositivos de control de acceso relacionados.

Gestión USB: Usted puede importar información del usuario y de asistencia a una unidad USB para transferirlos a un software relacionado o a otro equipo de reconocimiento de huellas.

Búsqueda de asistencia: Para consultar los registros guardados en el dispositivo, se proporciona la función de búsqueda de registros

Imprimir: Se utiliza para determinar si se deben imprimir los registros de asistencia.

Mensajes cortos: se utiliza para establecer un mensaje público o privado corto. El mensaje corto se mostrará a una persona especificada en el tiempo especificado después de comprobar la asistencia al trabajo, lo que facilita la comunicación.

Código de trabajo: se utiliza para identificar los diferentes tipos de trabajo, lo que facilita la verificación de la asistencia al trabajo.

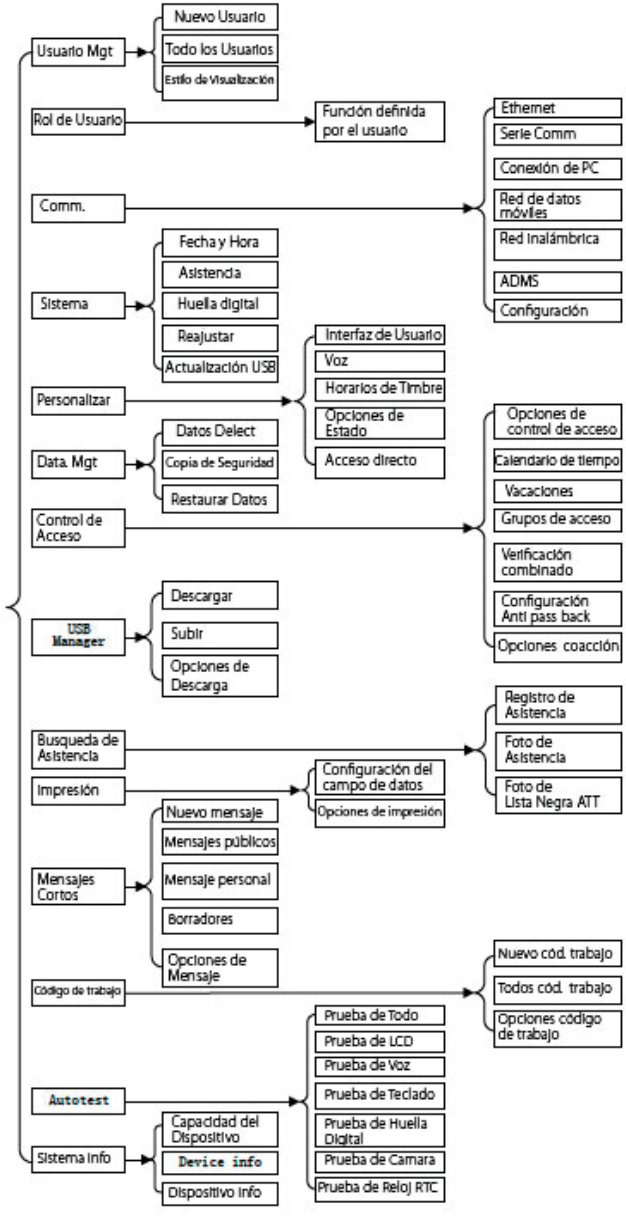
Pruebas: Este submenú permite que el sistema para probar automáticamente si las funciones de diferentes módulos

son normales, incluyendo la pantalla, huellas dactilares, voz, teclado y hora.

Información de sistema: Para comprobar la capacidad del dispositivo actual, la información del dispositivo y su información de firmware.

Menú Principal

Árbol de navegación



Gestión de Usuarios

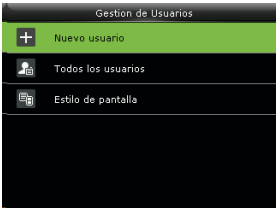
A través de este sub-menú, usted puede consultar la información almacenada en el dispositivo, incluyendo el ID de usuario, privilegio del usuario, huella digital, tarjeta, contraseña y foto; o también agregar, modificar o eliminar la información del usuario.

En la gestión de la asistencia de la empresa, al modificar a un usuario, la información en el sensor de huellas también debe modificarse. Por lo tanto, las operaciones de Agregar, Borrar, Revisar y Modificar se pueden realizar en el sensor de huellas.

3.1 Agregar usuarios

Presione la tecla M/OK para ingresar al menú principal.

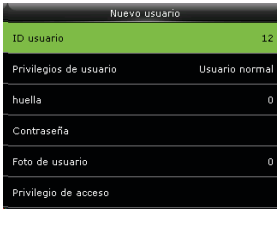
Elija la opción "Usuarios" y presione [OK].



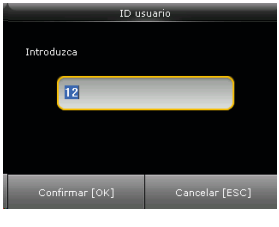
Seleccione la opción "agregar nuevo usuario" y presione [OK].

3.1.1 Agregar ID de usuario

El dispositivo asigna automáticamente un ID iniciando desde 1 y siguiendo la secuencia. Si usted utiliza el ID asignado por el terminal, puede saltar esta sección.



Elija la opción "ID de Usuario" y presione [OK].



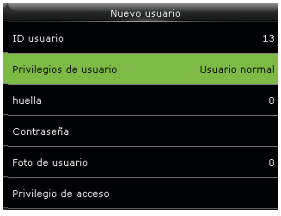
Ingrese el ID de Usuario y presione [OK] para confirmar.

TIP La terminal soporta de 1 a 9 dígitos de ID de usuario.

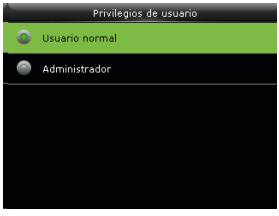
Si el mensaje de aviso "El ID de Usuario ya existe" aparece en pantalla; por favor ingrese otro ID.

Gestión de Usuarios

3.1.2 Modificar privilegio del usuario



Presione la tecla ▼ para seleccionar el privilegio



Seleccione el privilegio del usuario.

Administrador: El súper administrador tiene acceso a todas las funciones del menú del dispositivo.

Usuario normal: Si el sistema tiene un administrador; un usuario normal sólo tiene acceso a la función de verificación de identidad utilizando su huella, contraseña o tarjeta. Si el sistema no tiene un administrador; el usuario normal tiene los derechos de operación sobre todas las funciones que ofrece el menú del dispositivo.

Derechos especiales: Otras funciones del menú pueden estar disponibles para usuarios normales. El administrador, tiene la posibilidad de asignar derechos a otras funciones del menú personalizando el rol del usuario.

3.1.3 Registrar una huella digital

Presione la tecla ▼ para seleccionar "Huella Digital".

Ubique su dedo de manera adecuada en el sensor de huellas.

Presione el mismo dedo tres veces en el sensor.

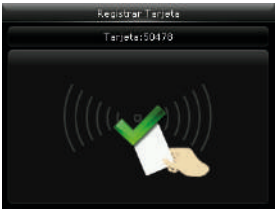
Gestión de Usuarios

El registro se realiza correctamente. Si el registro falla, el sistema mostrará un mensaje de solicitud y regresará a la interfaz de registro de huella. En este caso tendrá que repetir el proceso de registro.

3.1.4 Registrar tarjeta ID

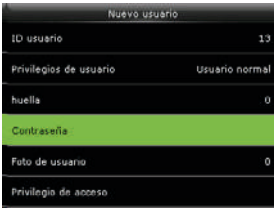
Presione la tecla ▼ para seleccionar el número de placa y pulse OK

Deslice su tarjeta de identificación en el área adecuada



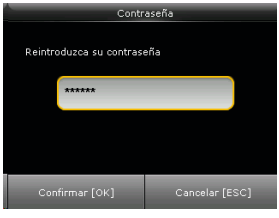
Presione el mismo dedo tres veces en el sensor.

3.1.5 Registrar contraseña



Presione la tecla ▼ para seleccionar la contraseña y pulse OK

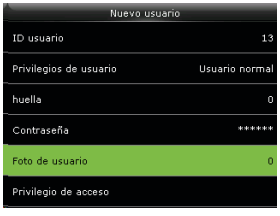
introduzca una contraseña utilizando el teclado y pulse OK. La terminal FFR es compatible con las contraseñas de 1 a 8 dígitos por defecto



Vuelva a introducir la contraseña de acuerdo con el indicador del sistema y presione OK

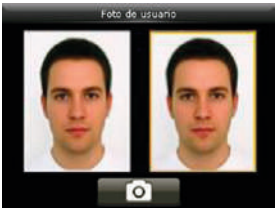
3.1 6 Registro de fotos

Si ha registrado su foto en el sistema, el sistema mostrará su foto inscrita, además de su identificación y el nombre después de que pasan la verificación.



Presione la tecla ▼ para seleccionar "Foto de usuario" y pulse OK

Colóquese de pie, de forma natural frente a la pantalla. Presione OK



Presione ESC para volver directamente a la interfaz anterior

3.1.7 Función de control de acceso

La opción de control de acceso de los usuarios sirve para configurar el acceso a la puerta, dirigido a todo el mundo, incluyendo el establecimiento de subgrupos, modo de verificación, elección de horario, la gestión de la huella digital de coacción.

Grupo de acceso: Asignar un usuario registrado a diferentes grupos para mayor comodidad de administración.

Modo de verificación:

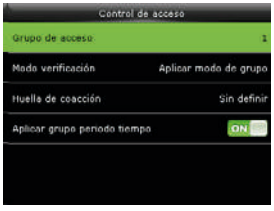
1. Tipo de verificación Grupal: Elegir si se usará el Tipo de Verificación del grupo al que pertenece el usuario.
2. Tipo de verificación individual: Seleccione el tipo de verificación del usuario. Si no se utiliza el tipo de verificación del grupo, el tipo de verificación de los otros miembros del grupo no se verán afectados.

Huellas digitales de coacción: El usuario registra una nueva huella digital o especifica una huella digital ya registrada anteriormente como la huella de coacción. En cualquier momento en cualquier lugar, alarma de coacción se activará después de que esa huella digital pase la verificación.

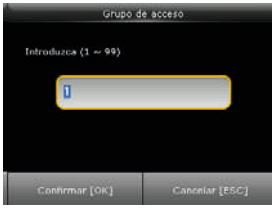
Aplicar horario de grupo

1. Seleccione "ON", en Aplicar Horario de Grupo, el usuario utilizará el horario de su grupo.
2. Seleccione "OFF", para establecer el horario de acceso del usuario. Si no se utiliza el horario del grupo, el horario de los demás miembros del grupo no se verá afectado.

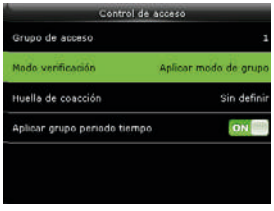
Presione la tecla ▼ para seleccionar "Privilegio de Acceso" y pulse OK



Pulse OK para acceder a la interfaz de grupo

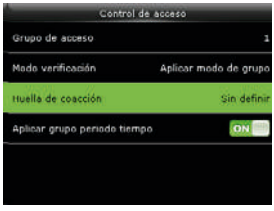


Introduzca el grupo del usuario utilizando el teclado y luego presione OK para volver



Presione la tecla ▼ para seleccionar "Modo de verificación" y pulse OK

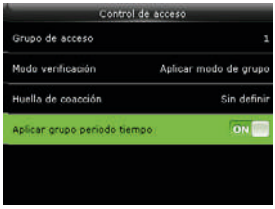
Presione la tecla ▼ para seleccionar "Modo de verificación" y pulse OK



Pulse para ▼seleccionar la huella dactilar coacción y pulse OK

Gestión de Usuarios

Presione ◄/► para seleccionar huella digital registrada y pulse OK



Seleccione "Aplicar Horario de Grupo" y actívelo (ON) para utilizar el horario del grupo al que pertenece el usuario.

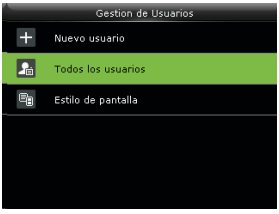
Pulse para ▼seleccionar "Todos los Usuarios" y pulse OK

3.2 Búsqueda de usuarios

Para facilitar a los administradores la búsqueda de un usuario específico entre una gran cantidad de usuarios; el dispositivo permite la búsqueda por "ID de Usuario" y "Nombre" (Ubicación de búsqueda).

Presione la tecla [M/OK], para ingresar al menú principal.

Seleccione la opción "Usuarios" y presione [OK].



Utilice la tecla ▼ para seleccionar "Todos los usuarios" y presione [OK].

Gestión de Usuarios

3.2.1 Búsqueda por ID de usuario y nombre

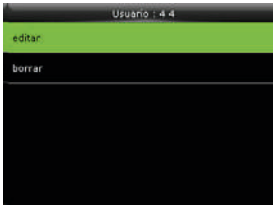
Introduzca el ID de usuario usando el teclado para buscar entre todos los usuarios.

Ubique el cursos sobre el usuario a ser consultado y presione [M/OK].

Pulse # en la interfaz de búsqueda para cambiar el método de entrada y presione letras en el teclado numérico para buscar por nombre.

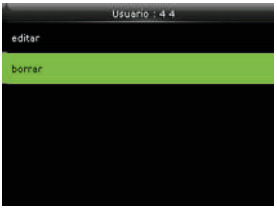
3.2.2 Editar y eliminar usuarios

Pulse ▼ seleccionar un usuario y pulse OK

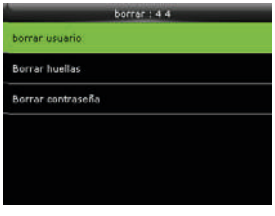


Pulse OK para entrar en la interfaz Información de usuario

El ID de usuario no puede ser modificada y las otras operaciones son similares a las realizadas para agregar usuarios



Pulse ▼ para seleccionar "Elimine" y pulse OK



Pulse ▼ para seleccionar el elemento a borrar y pulse OK

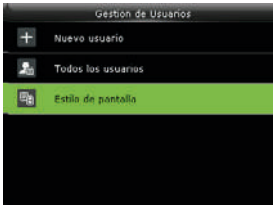
Los administradores definidos por los usuarios se borran cuando se eliminan los derechos de los usuarios

Gestión de Usuarios

3.3 Estilo de visualización

Presione la tecla [M/OK], para ingresar al menú principal.

Seleccione la opción "Usuarios" y presione [OK].



Utilice la tecla ▼ para seleccionar "Estilo de visualización" y presione [OK].

Pulse ▼ para seleccionar el estilo de visualización y pulse OK para volver

Línea sola

Línea múltiple

Línea Combinada.

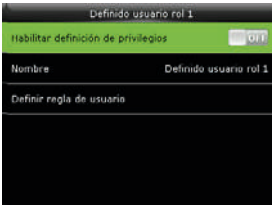
Privilegio de Usuario

Establecer los permisos de un privilegio definido por el usuario, es decir, los permisos para acceder a los menús.

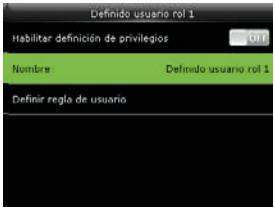
Presione la tecla [M/OK], para ingresar al menú principal.

Presione ► para seleccionar privilegios y pulse OK

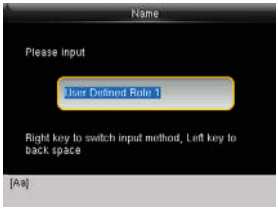
Utilice la tecla ▼ para seleccionar privilegio definido por usuario 1 y pulse OK



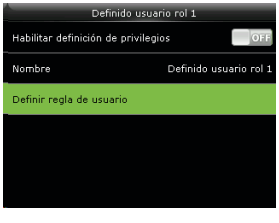
Presione ok para abrir



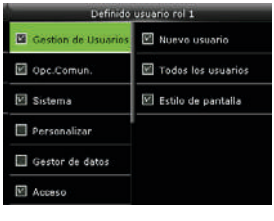
Presione ▼ para seleccionar el nombre y pulse OK.



Oprima * para cambiar de método de entrada e introduzca el nombre , pulse OK



Presione ▼ para seleccionar "Definir regla de usuario" y pulse OK



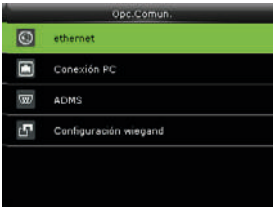
Presione ▼ y OK para seleccionar "Permisos". Para salir presione ESC.

Ajustes de comunicación

Establezca los parámetros de comunicación entre el dispositivo y el PC. Los parámetros incluyen la dirección IP, puerta de enlace, mascara de red, velocidad de transmisión, ID del dispositivo y contraseña de ingreso al sistema.

Presione la tecla [M/OK], para ingresar al menú principal.

Presione ► para seleccionar "Opc. Comun" y pulse OK



seleccione Ethernet y pulse OK

5.1 Ethernet

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

Dirección IP: La dirección IP predeterminada es 192.168.1.201. Si es necesario, se puede modificar; pero no puede ser la misma que del PC.

Máscara de red: La máscara de red predeterminada es 255.255.255.0 y puede ser modificada, de ser necesario.

Puerta de enlace: La puerta de enlace predeterminada es 0.0.0.0 y puede ser modificada, de ser necesario.

DNS: El servidor DNS predeterminado es 0.0.0.0 y puede ser modificado, si es necesario.

Ajustes de comunicación

Puerto de comunicación TCP: Es 4730 (Predeterminado) y puede ser modificado, de ser necesario.

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

Barra de estado: Utilizado para definir si mostrar o no los iconos de red en la interfaz principal.

5.2 Comunicación serial

Cuando el Puerto serie (RS232/RS485) es utilizado para la comunicación entre el dispositivo y el PC, las siguientes configuraciones necesitan ser revisadas:

RS232/USB: Si desea utilizar la interfaz RS232 o la USB para comunicación, por favor utilice la barra para activar la función.

Velocidad de transmisión/velocidad de transmisión de la USB: Utilizados para comunicación con el PC. Hay cinco opciones: 9600, 19200, 38400,57600 y 115200. Si la velocidad de comunicación es alta, la interfaz RS232/RS485 es recomendada. Si la velocidad de comunicación es lenta, la USB es recomendada.

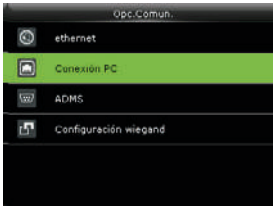
Ajustes de comunicación

5.3 Contraseña de conexión al PC

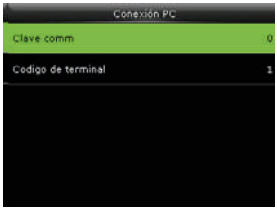
Para mejorar la seguridad de los datos de asistencia, es necesario establecer una contraseña de conexión. La contraseña de conexión se utiliza cuando el Software de PC se conecta al dispositivo para leer los datos.

Clave de comunicación: La contraseña predeterminada del sistema es 0 (Concretamente, no hay contraseña) pero puede ser establecida. Después de establecerla, la contraseña debe ser ingresada en el software para la comunicar con el dispositivo. El sistema soporta contraseñas de 1 a 6 dígitos.

ID del dispositivo: 1-254. Si la comunicación RS232/RS485 es utilizada, este ID necesita ser ingresado en la interfaz de comunicación del software.



Utilice la tecla ▼ Elija "Conexión con el PC" y presione OK.



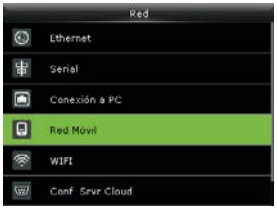
Presione OK

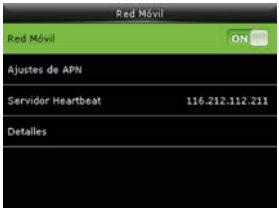
Ingrese una contraseña, utilice la tecla ▼ para seleccionar Confirmar (OK) y presione OK.

5.4 Red de datos móviles

Cuando el equipo está en el acceso telefónico a la red, asegúrese de que el dispositivo está dentro de la cobertura de la señal GPRS o WCDMA , que conoce el tipo de modem utilizado, el nombre y número de acceso del APN, etc.

Ajustes de comunicación





Red de datos móviles: si se debe permitir el acceso a una red móvil.

Configuración de APN: se utiliza para establecer la información de APN, tales como el número de acceso, nombre de usuario y contraseña

Servidor Heartbeat: Se obtienen los registros de asistencia del dispositivo mediante el software de recolección de datos proporcionado por ZKTeco. Después de configurar la dirección IP del servidor para el dispositivo de forma correcta, el dispositivo enviará registros de asistencia al servidor Heartbeat automáticamente.

Detalles: incluye información acerca de la red móvil conectado, como el modo de red, operador de telecomunicaciones, la dirección IP, y datos recibidos y enviados.

Configuración de APN:

APN: Access Point Name, que se utiliza para identificar los tipos de red GPRS/WCDMA.

Número de marcación: El número de acceso a la red GPRS/WCDMA.

Nombre de usuario y contraseña: se utiliza para comprobar si un usuario tiene los derechos para acceder a una red

Ajustes de comunicación

5.5 Red inalámbrica

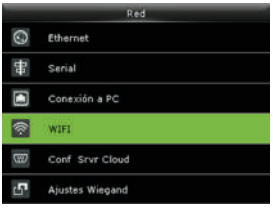
La fidelidad inalámbrica (Wi-Fi) es también conocido como el standard 802.11b velocidad de transmisión de hasta 11Mbps. Wi-Fi también cuenta con la transmisión de larga distancia y excelente compatibilidad con varios dispositivos 802.11 DSSS existentes. IEEE 802.11 b es una variante basada en radio de IEEE 802.11. El ancho de banda de IEEE 802.11 b puede ser de hasta 11 Mbps y ajustado automáticamente a 5.5Mbps, 2 Mbps y 1 Mbps dependiendo de la intensidad de la señal y el nivel de interferencia, por lo tanto garantizando de manera efectiva estabilidad de la red y la confiabilidad. Ventajas principales: Transferencia de alta velocidad y fiabilidad. las distancias de comunicación puede ser de hasta 305 metros en un área abierta y de 76 m a 122 metros en un área cerrada.

WIFI puede ser convenientemente integrada con la Ethernet alámbrica existente, por lo que el costo de red es incluso más bajo.

Nuestra terminal también es capaz de comunicarse por Wi-Fi. Es compatible ya sea con un módulo Wifi integrado o externo que implementa la transmisión inalámbrica de datos a través de Wi-Fi.

WIFI: Pulse OK para activar o desactivar la conexión Wi-Fi.

Operación



Presione ▼ para seleccionar la red inalámbrica y pulse OK

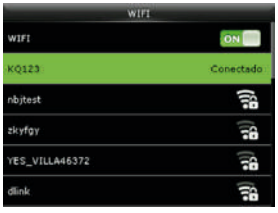
Presione WIFI para activar o desactivar la función.

Presione ▼

Pulse para seleccionar “una red Wifi “ y pulse OK

Ajustes de comunicación

Introduzca una contraseña, pulse ▼ para pulsar OK



Conectado, como se muestra en la figura

Conectado, se mostrará un símbolo en la interfaz inicial.

5.6 ADMS

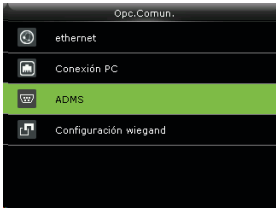
Este submenú se utiliza para configurar los ajustes relacionados con el Servidor web, tales como la dirección IP del servidor, configuración de puerto, y si se activará un proxy.

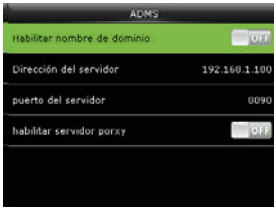
Habilitar el nombre de dominio: Cuando se activa el modo de nombre de dominio, se accede a un sitio web utilizando un nombre de dominio con el formato de http: //; de lo contrario, deberá introducir una dirección IP para el acceso web.

Dirección del servidor: dirección IP del servidor web Separar en otra linea puerto utilizado por servidor web

Habilitar servidor Proxy: Cuando se habilita la función de proxy, configurar la dirección IP y número de puerto de la opción de servidor proxy. Esto indica si se debe utilizar una dirección IP del proxy. Usted puede elegir introducir la dirección IP del proxy o del servidor de acceso a internet, lo que usted quiera.

Ajustes de comunicación

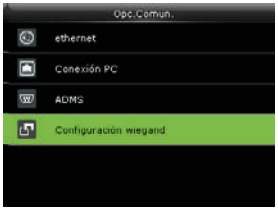




5.7 Configuración Wiegand

5.7.1 Entrada Wiegand

Operación:



Presione ▼ para seleccionar Wiegand pulse OK

Presione OK

Presione ▲ / ▼ para seleccione un elemento. presione OK para guardar y salir.

Formato Wiegand: El sistema tiene dos formatos integrados: Wiegand de 26 bits, y Wiegand 34-bits.

Bits Wiegand: especifica el número de bits ocupados por los datos Wiegand.

Ancho de pulso: Ancho de pulso es de 100 microsegundos por defecto, que se pueden ajustar de 20 a 100.

Intervalo de pulso: Es 1000 microsegundos por defecto, que puede ajustarse entre 200 y 20000.

Tipo de identificación: especifica el contenido de la señal de entrada Wiegand, que puede ser un ID de empleado o una tarjeta de identificación.

Ajustes de comunicación

5.7.2 Salida Wiegand

Formato Wiegand: El sistema tiene dos formatos integrados: Wiegand de 26 bits, y Wiegand 34-bits.

Fallo de ID: Define el valor de salida para la autenticación fallida de un usuario. El formato de salida se determina por el ajuste del formato Wiegand. El rango de valores varía desde 0 a 65535.

Código de área: Similar al que el ID de dispositivo. Pero el código se especifica por el usuario. Puede repetirse en dispositivos diferentes. (Con rango de 0-255)

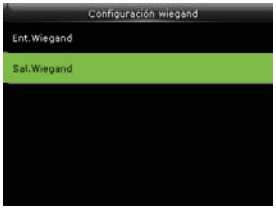
Ancho de pulso: Ancho de pulso es de 100 microsegundos por defecto, que se pueden ajustar de 20 a 100.

Intervalo de pulso: Es 1000 microsegundos por defecto, que puede ajustarse entre 200 y 20000.

Tipo de ID: Especifica el contenido de la salida para la autenticación de usuario exitosa. Puede seleccionar el número de empleado o tarjeta de identificación.

Detalles formato: Muestra la información definida por varios bits del formato de Wiegand seleccionado.

Operación:



Presione ▲ / ▼ Y OK para seleccionar elementos. Cuando se haya completado la configuración, pulse Aceptar para guardar la configuración y salir

Pulse OK

Sistema

Establecer los parámetros del sistema para satisfacer la demanda de la mayor cantidad de usuarios posibles. Incluyendo la fecha y hora, Asistencia, Huella digital, etc.

Pulse M / OK en la interfaz inicial del sistema.

Seleccionar sistema y oprima OK.

Esta es la interfaz que encontrará el la opción "Sistema"

6.1 Fecha/Hora

Seleccione Fecha / Hora y pulse OK

.Presione ▲/▼ y OK para seleccionar las opciones. Cuando el ajuste es completado, pulse Aceptar para guardar la configuración y salir.

Establecer Fecha/Hora: Este parámetro es utilizado para establecer a fecha y hora de la terminal.

Formato de 24 horas: Este parámetro se utiliza para establecer el modo de visualización de la hora de la interfaz inicial. Seleccione "ON" para adoptar el modo de visualización de 24 horas. Seleccione "OFF" para adoptar el modo de visualización de 12 horas.

Formato de fecha: Este parámetro permite definir el formato en que se va a mostrar la fecha en el dispositivo.

Sistema

Tipo de calendario: El dispositivo admite tres tipos de calendario, como gregoriano, Irán gregoriano e Irán. Puede modificarlo si es necesario.

Horario de verano: El Horario de Verano, que 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 el verano. Esto permite a los usuarios dormir o levantarse más temprano, y también reduce la iluminación del dispositivo para 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.

Para satisfacer la demanda del horario de verano, una opción especial puede personalizarse. Adelante el tiempo una hora a las XX (hora) XX (día) XX (mes), y retroceda el tiempo una hora a XX (hora) XX (día) XX (mes).

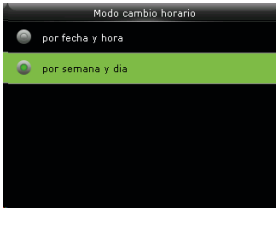
Operación:

1. Establecer el horario de verano como "Activado (ON)".
2. Introducir el horario de verano la hora de inicio y de fin.
3. Presione OK para guardar los cambios. Presione ESC para salir sin guardar.

Por ejemplo; si a las 08:00 del 1ro de abril es establecido como la hora de inicio del DST, el reloj se adelantará 1 hora. Y si el 1ro de agosto a las 08:00 es establecido como la hora final; el dispositivo volverá a la hora normal.

Active Horario de Verano

Ajuste el horario por fecha/hora.



Ajuste el horario por semana/día.

Modo de horario de verano: Se puede seleccionar el modo de la fecha (mes-día-hora) o el modo de la semana(mes-día de la semana-horas). Por defecto, se utiliza el modo de fecha.

Configuración de horario de verano: Se utiliza para ajustar la hora de inicio y de fin del horario de verano.

Descripción de modo de fecha y modo de semana:

1. Si el mes en que se inicia el horario de verano es posterior al mes en que termina, el horario de verano se extiende por dos años diferentes. Por ejemplo, la hora de inicio del horario de verano es 2014-9-1 las 4:00 y la hora de finalización es 2015-4-1 a las 4:00.
2. Suponga que se selecciona el modo de semana y el horario de verano comienza desde el domingo de la sexta semana de 2012. De acuerdo al calendario, septiembre de 2013 no tendrá seis semanas, pero tiene cinco semanas. En este caso, en 2013, el horario de verano comienza en el punto de tiempo correspondiente del último domingo de septiembre
3. Supongamos que el horario de verano se inicia desde el lunes de la primera semana de septiembre en 201 2. De acuerdo con el calendario, la primera semana de septiembre en 2012 no tiene lunes. En este caso, el DST comienza a partir del primer lunes de septiembre en 2012.

6.2 Asistencia

Pulse para seleccionar "Asistencia" y pulse OK.

Presione ▲/▼y OK para seleccionar elementos. Cuando se haya completado la configuración , pulse OK para guardar y salir.

Seleccione Fecha / Hora y pulse OK

Sistema

Tiempo de verificación duplicada (m): Si ya existe el registro de asistencia de un usuario y el usuario vuelve a verificar dentro de un periodo de tiempo establecido (unidad: minutos), la segunda asistencia del usuario no se guardará (Rango: 1-60 minutos)

Modo de cámara: Configurar si se desea tomar y guardar una foto del empleado cuando verifica su asistencia. Está dirigido a la configuración de todos los empleados.

Hay 5 modos:

No tomar foto: No se toman fotos durante la verificación del usuario.

Tomar foto sin guardar: Durante la verificación, se toma una foto, pero no se guarda.

Tomar foto y guardar: Durante la verificación, se toma una foto y se guarda.

Guardar en verificación exitosa: Se toma y guarda una foto en cada verificación exitosa.

Guardar en verificación fallida: Se toma y guarda una foto en cada verificación fallida.

Mostrar foto de usuario: Para establecer si se mostrará una foto cuando un usuario verifique exitosamente.

ID alfanumérico de usuario: Establecer si el ID del empleado soporta el uso de letras.

Alerta por memoria baja: Cuando la memoria de almacenamiento restante no es suficiente para guardar una cantidad establecida de registros, el dispositivo generará una alarma automáticamente. (Rango: 1 a 9999).

Limpieza periódica de datos de asistencia: 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.

Limpieza periódica de fotos de asistencia: La cantidad de fotos de asistencia 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 99.

Duración de pantalla de confirmación (s): El tiempo que se muestra en la pantalla la información de verificación después de un evento. El valor oscila de 1 a 9 segundos.

Guardar registro de verificación ilegal: Establecer si las verificaciones fallidas, como aquellas causadas por intentos de acceso en horario inválido o por verificaciones combinadas ilegales, se guardarán en el sistema cuando la función de control de acceso esté activada.

Reglas de usuario expirado: Puede seleccionar 3 opciones: Guardar información de usuario sin guardar registros, Guardar información de usuario y registros; y Borrar información de usuario.

6.3 Huella digital

Oprima ▼ para, seleccionar "Huella Digital" y presione OK

Utilice las teclas ▲▼ y presione OK para seleccionar las opciones. Cuando la configuración esté completa, presione OK para guardar los cambios y salir.

Sistema

Umbral de coincidencia 1:1: La similitud del ID + Verificación de huella digital y la plantilla registrada.

Umbral de coincidencia 1: N: La similitud de la verificación y la plantilla registrada.

FRR	Umbral de Coincidencia	
FAR	1:N	1:1
Alto Bajo	45	25
Medio Medio	35	15
Bajo Alto	25	10

Sensibilidad del sensor de huellas: Utilizado para establecer la sensibilidad del recolector de huellas digitales. El valor predeterminado es "medio" (recomendado). Usted puede establecer la sensibilidad "Alta" cuando el ambiente se torne seco y se estén presentando retrasos en la verificación. Cuando el ambiente se torne húmedo, se puede establecer la sensibilidad en "Baja" si las huellas digitales presentan dificultades para ser identificadas.

Detección de dedo vivo: Definir si se utiliza la función anti-huellas falsas. Cuando está activada esta herramienta y se esté registrando o verificando huellas digitales; el dispositivo puede identificar las huellas las falsas, llevando al fallo de la verificación o que no se acepte la huella.

Reintentos 1:1: Este parámetro es utilizado para establecer el número de reintentos en el caso de errores de la verificación 1:1 o verificación de contraseña debido a la ausencia de registro de la huella digital o posicionamiento incorrecto del dedo en el sensor de huellas, para prevenir operaciones reiteradas.

Algoritmo de huella digital: Este parámetro es utilizado para seleccionar la versión del algoritmo entre 9.0 y 10.0. Por favor seleccione la versión del algoritmo con cuidado, porque las plantillas de huella digital de estos dos algoritmos son incompatibles.

Imagen de la huella digital: Esta función determina si se desea o no, mostrar la imagen de la huella digital durante el registro o verificación de estas.

6.4 Reiniciar

Reiniciar los ajustes de comunicación, opciones del sistema, etc. a los ajustes de fábrica.

Oprima ▼ para seleccionar "Reiniciar y pulse OK.

Utilice las teclas ▲▼ para seleccionar "Aceptar" o "Cancelar" y pulse OK

6.4 Actualización por USB

Usted puede actualizar el Firmware de la terminal utilizando un archivo de actualización en la USB a través del siguiente parámetro:

Si usted necesita el archivo de actualización del firmware, por favor contacte a nuestro equipo técnico de su región. Generalmente, la actualización del Firmware no es recomendada.

Personalizar

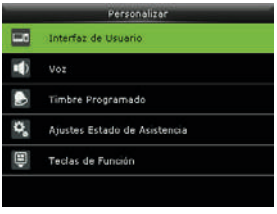
Presione M/OK para ingresar al menú principal.

Seleccione la opción "Personalizar" y presione OK.

Seleccione la interfaz de usuario y pulse OK .

7.1 Interfaz de usuario

De acuerdo con sus preferencias, el usuario puede establecer el estilo de la interfaz inicial.



Presione ▼ para seleccionar la opción "Interfaz de Usuario" y presione OK.

Utilice las teclas ▼/▲ y presione OK. Cuando la configuración esté completa, presione OK para guardar los cambios y salir.

Papel tapiz: Escoger la imagen a utilizar como fondo de pantalla.

Idioma: Seleccionar el idioma del dispositivo.

Bloquear botón de apagado: Para evitar el apagado no deseado del equipo, seleccione si desea bloquear el apagado o no. "Desactivar": El equipo se apaga luego de presionar el botón de apagado 3 segundos. "Activar": No pasa nada al presionar el botón.

Personalizar

Tiempo de espera del menú: El dispositivo mostrará la interfaz principal automáticamente cuando no se realice ninguna operación en el menú durante el tiempo de espera. (Esta función se puede desactivar, de lo contrario, el valor tiene un rango de 60 a 99999 segundos).

Tiempo de espera para diapositivas: El protector de pantalla se muestra cuando no se realiza ninguna operación en la interfaz principal dentro del tiempo de espera. (Esta función se puede desactivar, de lo contrario, el valor tiene un rango de 60 a 999 segundos).

Intervalo de tiempo para dispositivas: Este parámetro es utilizado para establecer el tiempo de duración de las diapositivas en pantalla. El rango de tiempo es de 0 a 999 segundos.

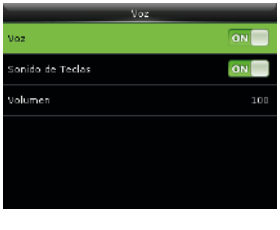
Tiempo para reposo: Esta función permite establecer el tiempo de espera del dispositivo para ingresar al modo de reposo. Usted puede sacar al dispositivo del modo reposo presionando cualquier tecla. El rango de espera es de 1 a 30 minutos, el tiempo preestablecido es de 3.

Estilo de la pantalla principal: Seleccione el estilo de la pantalla de inicio.

Nota: El nombre de la compañía, es sólo en caso de habilitar la función de impresora.

7.2 Sonido

Oprima ▼ seleccione la opción "Voz" y presione OK.



Utilice ▼▲ y presione OK para seleccionar las opciones. Cuando la configuración esté completa, presione OK para guardar los cambios y salir.

Personalizar

Voz guía: Este parámetro se utiliza para establecer si se desea reproducir mensajes de voz durante la operación de la terminal. Seleccione "ON" para activar la indicación de voz y seleccione "OFF" para silenciar.

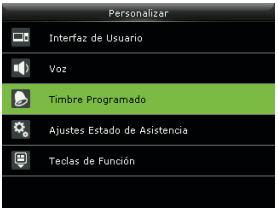
Tono del teclado: Este parámetro se utiliza para establecer si se debe generar el sonido de pitido en respuesta a cada pulsación del teclado. Seleccione "ON" para activar el sonido de aviso y seleccione "OFF" para silenciar.

Volumen: Con esta función puede ajustar el volumen de la voz guía.

7.3 Timbre

Muchas empresas necesitan un timbre para señalar la hora de inicio/fin de la jornada laboral. Algunos utilizan timbres manuales y otros electrónicos. Para ahorrar costos y brindar un mejor rendimiento, nosotros integramos las funciones de timbre en el dispositivo. Usted puede establecer la hora de timbre: cuando llegue la hora establecida, el dispositivo activará la señal del relevador y hará sonar el timbre elegido. El timbre sonará en el lapso de tiempo establecido por el usuario. El dispositivo proporciona 15 timbres.

Agregar timbre:



Oprima ▼ para seleccionar la opción "Horario de Timbre" y presione OK.

Seleccione la opción "Nuevo Horario de Timbre" y presione OK.

Utilice las teclas ▼/▲ y presione OK para seleccionar las opciones. Presione OK para guardar y salir.

Personalizar

Estado del timbre: Activar / Desactivar este timbre.

Hora del timbre: Establecer la hora en la que debe sonar el timbre.

Repetir: Especificar los días de la semana en los que debe sonar el timbre.

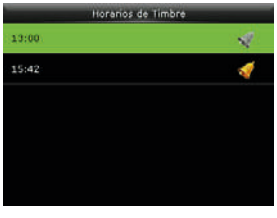
Timbre: Tono del timbre.

Duración del timbre: Especificar la duración del timbre. El rango es desde 1 a 999 segundos.

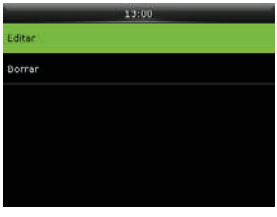
Nota: Sólo algunos modelos tienen la función de timbre externo.

Editar o eliminar timbre:

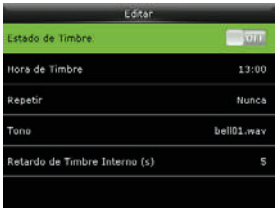
Presione ▼ para seleccionar "Todos los Timbres" y presione OK.



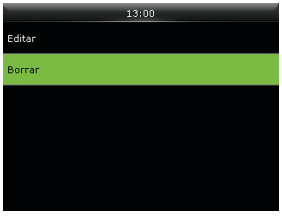
Seleccione el timbre que desea editar o eliminar y presione OK.



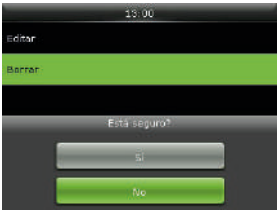
Escoja entre "Editar" o "Eliminar" y presione OK.



Seleccione un artículo.



Presione ▼ para eliminar y pulse OK



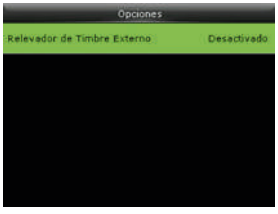
Para seleccionar " Sí " o "No" .

Personalizar

Opciones:

Cuando se utiliza la función del timbre externo, ajuste el terminal de salida de timbre externo.

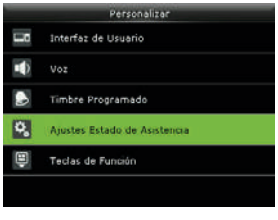
Presione ▼ para seleccionar "Opciones" y pulse OK.



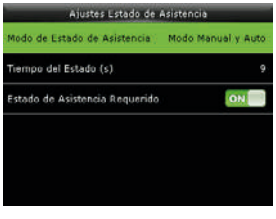
Presione OK.

Presione ▼ para seleccionar, presione OK para guardar y regresar.

7.4 Estado de opiones verificación



Presione ▼ para seleccionar "Opciones de Verificación" y pulse OK.



Presione ▼/ ▲ y presione OK para seleccionar las opciones. Cuando la configuración esté completa, presione OK para guardar los cambios y salir.

Estado de verificación: Esta opción es para seleccionar el estado de verificación. Las siguientes opciones están disponibles:

Apagado: La tecla de estado no es utilizada. La tecla de atajo definida como estado queda inhabilitada.

Modo manual: Las teclas de estado son cambiadas manualmente y la tecla de estado actual desaparecerá cuando transcurra la hora predeterminada.

Modo automático: Si una tecla de estado es configurada para ser cambiada después de cierto periodo de tiempo, la tecla de estado se cambiará automáticamente cuando transcurra la hora predeterminada.

Modo manual & automático: La interfaz principal muestra las teclas de estado que pueden ser cambiadas automáticamente, y usted también tiene la opción de cambiar las teclas de estado manualmente. Una tecla de estado que usted seleccione manualmente será cambiada de acuerdo al plan de cambios después del límite de tiempo.

Modo fijo manual: Después que la tecla de estado es cambiada, es siempre mostrada hasta que usted la cambie de nuevo.

Modo fijo: Una tecla de estado es siempre mostrada y no puede ser cambiada.

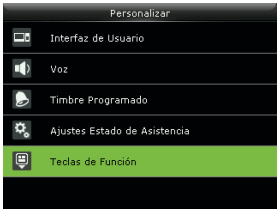
Tiempo de espera del estado de verificación: Especificar el tiempo límite de la tecla de estado mostrada en la interfaz principal.

Estado de verificación requerido: Especificar si el estado de la asistencia debe ser seleccionado durante la autenticación.

Personalizar

7.5 Atajos

Puede definir seis teclas de acceso directo como teclas de atajo a un estado de asistencia o a una función del sistema. Sobre el interfaz principal de la terminal de, pulse las teclas correspondientes y el estado de asistencia será mostrado o se dirigirá rápidamente a la interfaz de la función configurada como atajo.



Presione ▼ para seleccionar "Teclas de Función" y presione OK.

Presione ▼ para seleccionar. una tecla

Presione ▼/▲ y presione OK para seleccionar las opciones. Cuando la configuración esté completa, presione OK para guardar y salir.

Nota: Al configurar las teclas de acceso directo de estado de la asistencia, también puede establecer el parámetro "Auto Switch".Cuando se habilita "Auto Switch", el terminal cambia automáticamente el estado de la asistencia al tiempo especificado. Si se selecciona una tecla de estado, el dispositivo no utilizará ninguna tecla de estado cuando la función de Teclas de Estado esté desactivada.

Gestión de datos

Oprima M/OK la interfaz inicial

Seleccione la opción "Gestión de Datos" y oprima OK.

Seleccione borrar datos y pulse OK

8.1 Eliminar datos

A través del menú [Gestor de Datos], Puede realizar la gestión de los datos almacenados en el terminal, por ejemplo, eliminar el registro de asistencia, todos los datos y protectores de pantalla, eliminar los derechos de administrador, y restablecer el terminal a los valores predeterminados de fábrica.

Seleccione borrar datos y pulse OK

Presione ▼ y OK para seleccionar el elemento que desea eliminar

Eliminar eventos: Eliminar todos los registros de asistencia.

Eliminar todos los datos: Eliminar toda la información del personal; incluyendo huellas, imágenes faciales y registros de asistencia.

Eliminar privilegio de administrador: Cambiar todos los administradores a usuarios normales.

Gestión de datos

Eliminar fondo de pantalla: Eliminar todos los fondos de pantalla.

Eliminar protectores de pantalla: Elimine todas las imágenes cargadas desde la USB al terminal. (Para detalles sobre la carga de imágenes, por favor consulte el punto 5.4)

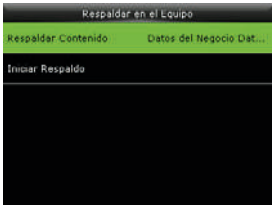
Eliminar copia de seguridad: Eliminar los datos pertenecientes a la copia de seguridad.

8.2 Copia de seguridad

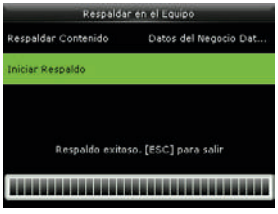
La copia de seguridad se puede hacer al dispositivo o a una USB.

Presione ▼ para seleccionar respaldar datos y pulse OK

Presione ▼ para seleccionar respaldar en el dispositivo y pulse OK.



Presione ▼ y OK para seleccionar los elementos que desea respaldar de forma local en el dispositivo.



Presione ▼ para seleccionar iniciar respaldo y pulse OK

Nota: Cuando haga la copia de seguridad a la USB, la operación es similar a los pasos descritos anteriormente.

8.3 Restaurar datos

Restaurar los datos almacenados en el dispositivo o en una USB, al dispositivo.

Presione ▼ para seleccionar Restaurar datos y pulse OK

Presione ▼ Para seleccionar respaldar desde equipo y pulse OK.

Presione ▼ Y OK para seleccionar los elementos respaldados en el dispositivo que desea restaurar.

Presione ▼ para seleccionar iniciar restauración y pulse OK

Presione ▼ Para seleccionar "SI" o "No" y presione OK.

Nota: Copia de seguridad de disco USB, las operaciones son similares a las realizadas a partir de copia de seguridad del dispositivo

Configuración de Control de Acceso

Opción de control de acceso es para establecer el horario de apertura de puerta de los usuarios, el control de la cerradura y los parámetros relacionados al dispositivo.

Pulse M / OK en la interfaz inicial.

Presione ► para seleccionar el control de acceso y pulse OK.

Presione ▼ para seleccionar opciones de control de acceso y pulsar OK.

Para poder acceder, el usuario registrado debe cumplir 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 del usuario debe estar dentro de la combinación de acceso multi-usuario (cuando hay otros grupos en la misma combinación de acceso, se requiere la verificación de los miembros de esos grupos para poder abrir la puerta).

En las configuraciones predeterminadas, 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.

9.1 Opciones de control de acceso

Establecer parámetros para controlar las cerraduras y dispositivo conectados.

Retardo de cerradura de puerta (s): Tiempo en que la cerradura electrónica permanece abierta después de recibir la señal de abertura y hasta que se cierra automáticamente (Rango de Valor: 1-10 segundos).

Configuración de Control de Acceso

Retraso del sensor de puerta (s): Cuando la puerta se abre, el sensor de la puerta se activará luego de un periodo de tiempo; si el Estado del Sensor de la puerta no coincide con el Estado Normal del Sensor de la Puerta, se activará una alarma. Este periodo de tiempo es el Retraso de Sensor de Puerta (Rango de Valor: 1-99 segundos).

Tipo de sensor de puerta: Incluye NINGUNO, Normalmente Cerrado (NC) y Normalmente Abierto (NO). NINGUNO significa que no hay sensor de la puerta. NO significa que la puerta está abierta normalmente. NC significa que la puerta está cerrada normalmente.

Retardo de alarma de puerta (s): Cuando se detecta el estado anormal de sensor de puerta, se activará una alarma después de cierto tiempo. Este tiempo se llama Retardo de alarma del sensor de la puerta. (Rango de Valor: 1-99 segundos).

Reintentos para alarma: Cuando una verificación falle un determinado numero de veces, se emitirá una alarma. (Rango de Valor: 1-9 veces).

Período de tiempo normalmente cerrado: Ajuste de zona horaria para el control de acceso Normalmente Cerrado. Nadie puede abrir durante este período de tiempo.

Período de tiempo normalmente abierto: Establecer zona horaria para el control de acceso NO. La cerradura está siempre en ese estado durante este período de tiempo.

Configuración de Control de Acceso

Operación

Seleccione las opciones de control de acceso y pulse OK

Ingrese a las opciones de control de acceso , como se muestra en la figura.

Presione ▲/▼ para mover el cursor hasta el elemento que desea ajustar. Si es el cuadro de entrada, pulse las teclas numéricas para introducir el valor. Si se trata de la caja de selección, pulse ◄/► para cambiar el valor. Después de la configuración, pulse Menú directa mente para volver a la última interfaz. Pulse la tecla "ESC" para cancelar el ajuste y volver a la última interfaz.

1. Cuando se establece un horario de puerta NO o NC, configure el modo de sensor de la puerta como Ninguno, o la señal de alarma se puede activar durante el el horario de puerta NO o NC.
2. Si la zona horaria de NO o NC no tiene una definición, el dispositivo le solicitará y añadir la definición de configuración de zona horaria.

9.2 Horario

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 es el tiempo válido dentro de 24 horas.

Cada usuario puede definir 3 horarios diferentes. La relación entre estos horarios es "O". Cuando una verificación cae dentro de cualquiera de estos 3 horarios, la verificación es válida.

El formato del horario es HH:MM-HH:MM en el sistema de 24 horas con precisión de minutos.

Configuración de Control de Acceso

Presione ▼ para seleccionar horarios y pulse OK.

Utilice las teclas numéricas para buscar un horario en el intervalo de 1 a 50. Presione ▼ para seleccionar el elemento que desea ajustar y presione OK.

Presione ◄ /► para seleccionar una opción de tiempo y presione ▲ / ▼ para ajustar la hora. Después de establecer un período de tiempo, pulse Aceptar para guardar la configuración y salir

Cuando la hora de fin es más temprana que la hora de inicio (por ejemplo, 23:57-23:56), quiere decir que se mantiene cerrado todo el día. Cuando la hora de fin es más tarde que la hora de inicio (por ejemplo, 00:00-23:59), quiere decir que este periodo de tiempo es válido.

Notas: El período de tiempo predeterminado número 1 indica el acceso durante todo el día (es decir, los nuevos usuarios registrados tienen acceso)

9.3 Ajuste de días festivos

Un horario especial de control de acceso puede necesitarse durante los días festivos. Es diferente a modificar la hora del control de acceso de todos los usuarios. Por lo que una vez establecido el control de acceso de días festivos, se aplica a todos los empleados.

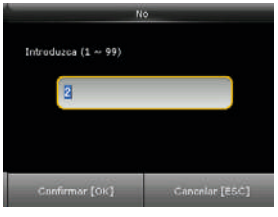
Después de que se establece un horario de control de acceso para días festivos, se puede ajustar el horario de apertura de puerta para los usuarios durante el día festivo.

Configuración de Control de Acceso

Presione ▼ para seleccionar días festivos y pulse OK.

Presione "OK" para agregar día festivo.

Presione "OK".



Introduzca el Nº usando el teclado . presione OK

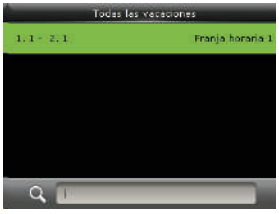
Presione ▼ para seleccionar la fecha de inicio y fecha de finalización . presione OK

Presione ◄/► para seleccionar una opción de tiempo y presione ▲/▼ para ajustar la fecha. Después de establecer una fecha, pulse Aceptar para guardar la configuración y salir

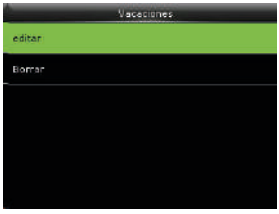
Presione ▼ para seleccionar un horario y pulse OK.

Ingrese un número de horario usando el teclado . Pulse OK para volver.

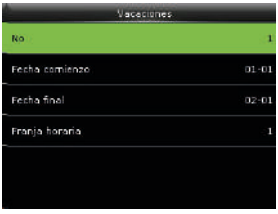
Presione ▼ para seleccionar todas las vacaciones y pulse OK.



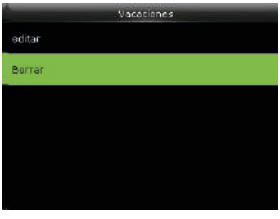
Para revisar el horario de un día festivo, seleccione un día festivo de la lista y presione OK.

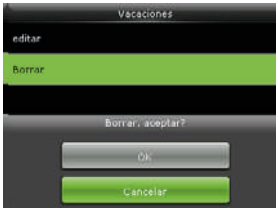


Pulse OK para editar el día festivo.



Las operaciones para editar un día festivo son similares a las operaciones de agregar día festivo.





Presione ▼ para seleccionar Eliminar y pulse OK.

9.4 Grupos de acceso

Los grupos son para administrar usuarios en grupos.

El horario de un grupo aplica para todos los miembros del grupo, pero los usuarios pueden establecer su propio horario personal. Cada grupo puede definir 3 horarios como máximo, siempre que uno de ellos sea válido, el grupo puede ser verificado correctamente.

Por defecto, los usuarios nuevos pertenecen al Grupo de Acceso 1, pero pueden ser asignados a otro grupo de acceso.

Operación

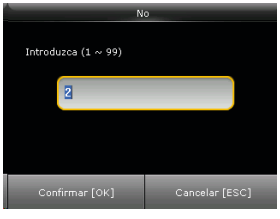
Configuración de Control de Acceso

1. Agregar zona horaria de grupo

Presione ▼ para seleccionar Grupos de Acceso y pulse OK.

Presione OK para añadir un nuevo grupo.

Presione OK.

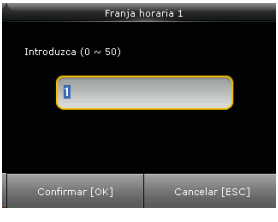


Ingresa el Nº utilizando el teclado y pulse OK

Presione ▼ para seleccionar eliminar esto modo de verificación y pulse OK

Presione ▲/▼ para seleccionar el modo de verificación, presione OK para guardar y salir.

Presione ▼ para seleccionar periodo de tiempo 1 y pulse OK



Ingresa el Nº utilizando el teclado y pulse OK

Presione ▼ para seleccionar habilitar vacaciones, pulse OK para habilitar el elemento

Configuración de Control de Acceso

Nota:

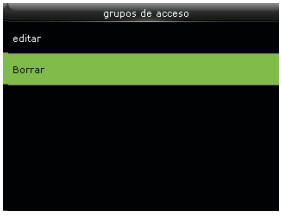
1. Si los días festivos están activados, sólo cuando haya intersección entre el horario del grupo y el horario del día festivo, los usuarios podrán abrir la puerta.
2. Si los días festivos están desactivados, el horario de acceso de los miembros de un grupo no se verá afectado por los días festivos.
3. Editar y borrar el horario de un grupo.

Presione ▼ para seleccionar "Todos los grupos" y pulse OK.

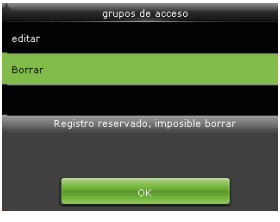
Presione ▼ para seleccionar uno de todos los grupos y pulse OK.

Presione ▼ para seleccionar editar. Pulse OK.

El N º no se puede modificar, y las otras operaciones son similares a las realizadas para agregar un nuevo grupo. pulse ESC para volver.



Presione ▼ para seleccionar " Borrar" y pulse OK.



Presione ▲ / ▼para seleccionar OK y borrar los grupos de acceso(El grupo 1 está reservado por el sistema y no se puede borrar).

9.5 Establecer verificación combinada

Combine 2 o más grupos de acceso para lograr una multi-verificación y así aumentar la seguridad.

Configuración de Control de Acceso

En la verificación combinada se pueden combinar hasta 5 usuarios; todos los usuarios pueden pertenecer a un mismo grupo de acceso o a hasta 5 grupos diferentes.

Operación:

1. Agregar verificación combinada

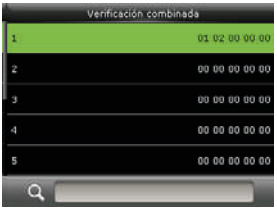
Por ejemplo, para añadir una combinación de desbloqueo que necesita la verificación de ambos grupos 1 y 2, como se muestra a continuación:

Presione ▼ para seleccionar la verificación combinada y pulse OK

Presione OK para agregar una nueva verificación combinada.

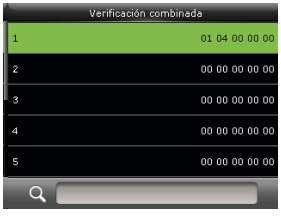
Introduzca el N° de grupo utilizando el teclado y pulse OK

2. Editar y borrar la verificación combinada.



Presione ▼ para seleccionar la línea que desea editar , pulse OK .

Introduzca el N° de grupo utilizando el teclado y pulse OK.



Al establecer con éxito, se muestra esta interfaz.

Nota: Para eliminar una verificación combinada, ajuste todos los N°s de grupo a 0.

9.6 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. Consulte el Apéndice 4 Anti-Passback para configurar el Anti-Passback.

9.7 Parámetro de alarma 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: Si está activado, presione la tecla "Tecla de coacción" y, a continuación, presione cualquier huella registrada (en 3 segundos) o introduzca un número de ID, la alarma de coacción será enviada después de verificar exitosamente. Si la función está desactivada, presionar "Tecla de coacción" no activará la alarma.

(La tecla de coacción puede definirse como una tecla de atajo).

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

Configuración de Control de Acceso

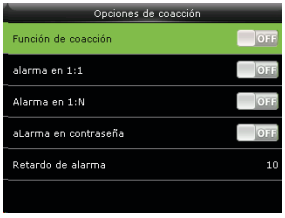
Alarma en 1:N Si está activada, cuando un usuario utilice el método de verificación 1:N, la alarma se activará. Si está desactivada, no se activará ninguna señal de alarma.

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, la señal de alarma no se activa inmediatamente, pero el retardo puede configurarse. La alarma se activará después del tiempo definido (0-255 segundos).

Operación:

Presione ▼ para seleccionar Opciones de coacción y pulse OK.



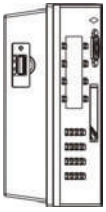
Defina las opciones de coacción, como se muestra en la figura.

Presione ▲/▼ para mover el cursor hasta el elemento que va a ajustar. Si se trata de la caja de entrada , pulse las teclas numéricas del teclado para introducir el valor. Si es el cuadro de selección, pulse ▲/▼ para cambiar los valores . Después del ajuste, pulse menú directamente volver a la última interfaz. pulse la tecla "ESC " para cancelar el ajuste y volver a la ultima interfaz.

USB

Usted puede exportar información de usuarios, plantillas de huellas, registros de accesos y otros datos desde el dispositivo a un software relevante para su procesamiento, o importar datos de usuarios hacia el dispositivo por medio de una unidad USB.

Antes de cargar o descargar información desde o a una USB, inserte la USB en el puerto del dispositivo.



Conecte la USB al dispositivo por medio del puerto USB.

Presione M/OK en la interfaz inicial.

Presione ▼ y elija la opción Gestion USB y presione OK.

10.1 Descargar datos

Elija la opción "Descargar" y presione OK

Presione ▼ y OK para seleccionar el tipo de elemento que desea descargar y presione OK

USB

Descargar datos de asistencia: Importar todos los datos de asistencia desde el terminal en un disco USB.

Descarga de datos de usuario: Importar todos los datos de usuario, huellas dactilares e imágenes faciales de la terminal a un disco USB.

Descargar foto del usuario: Importar fotos de los empleados de la terminal en un disco USB.

Descargar fotos de asistencia: Descargar fotos de asistencia guardados en el dispositivo en una unidad USB. El formato de la foto es JPG.

Descargar fotos de lista negra: Descargar fotos guardadas en la lista negra del dispositivo en una unidad USB. El formato de las fotos es JPG.

Descargar código de trabajo: Se utiliza para guardar los ID de trabajo en el dispositivo a una unidad USB

10.2 Cargar datos

Presione ▼ para seleccionar la opción "Cargar" y presione [OK]

Presione ▼ para seleccionar el tipo de información que desea cargar.

USB

Cargar datos de usuario: Cargar toda la información de usuario y huellas digitales desde la unidad USB al dispositivo.

Cargar fotos de usuario: Cargar las fotos en formato JPG nombradas con el ID de los usuarios desde una unidad USB, de forma que se muestren las fotos de los usuarios después de que verifiquen exitosamente.

Cargar código de trabajo: Se utiliza para cargar los códigos de trabajo desde una unidad USB al dispositivo.

Cargar mensajes cortos: Se utiliza para cargar mensajes cortos en una unidad USB al dispositivo.

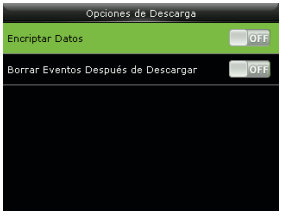
Cargar protector de pantalla: Cargar fotos en formato JPG cuyo nombre empieza con las letras "ad" guardadas en una memoria USB al dispositivo. Después de la carga, se podrán mostrar las fotos en la interfaz inicial del dispositivo. (Para más detalles, consulte el Apéndice 2 Procedimiento para cargar.

Cargar fondo de pantalla: Cargar fotos en formato JPG cuyo nombre empiece con "1 - 10.jpg" guardadas en una memoria USB al dispositivo. Después de la carga, se podrán mostrar las fotos en la interfaz inicial del dispositivo. (Para más detalles, consulte el Apéndice 2 Procedimiento para cargar imágenes).

10.3 Opciones de descarga

Puede cifrar los datos en una unidad USB y configurarlo para que se eliminen los datos después de ser descargados. Cuando se descargan los registros de asistencia, también puede establecer el tipo de calendario con el que se mostrarán. El dispositivo soporta 3 tipos de calendario: gregoriano, Irán gregoriano, Irán Lunar para elegir.

Presione ▼ para seleccionar "Opciones de Descarga" y presione OK



Utilice la tecla ▼ y OK para seleccionar los ítems Cuando la configuración se ha completado, presione OK para guardar la configuración y salir

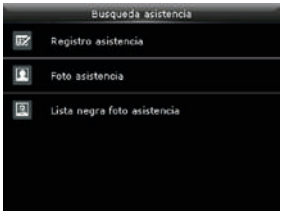
Asistencia

Los registros de asistencia de los empleados se guardarán en el dispositivo. Para poder consultarlos de una manera sencilla, se proporciona la función de búsqueda de registros.

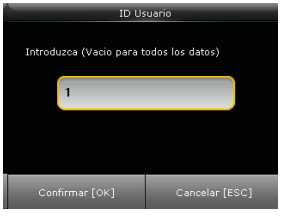
1. Registro de asistencia

Presione la tecla M/OK para ingresar al menú principal.

Presione ▼ para seleccionar "Búsqueda Asistencia" y presione OK.

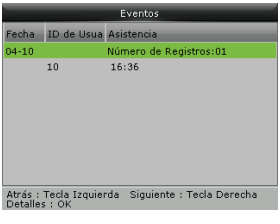


Presione ▼ para seleccionar "Registro de Asistencia" y presione OK.



Ingrese el ID del usuario y presione OK.

Presione ▼ para seleccionar el tiempo y presione OK.



Se mostrarán los registros de acuerdo con las condiciones

ID de usuario: Introduzca el ID de usuario del empleado a consultar. Si este campo es dejado en blanco, usted puede consultar los datos de asistencia de todos los empleados. Si usted ingresa un ID de Usuario, se consultarán sólo los datos vinculados al ID.

Rango de tiempo: Seleccione el periodo de tiempo que desea consultar, entre las opciones usted puede encontrar: Hoy, Ayer, Esta semana, Semana pasada, Este mes, el Mes pasado, Todos los registros y también puede buscar un día y hora específicos.

2. Fotos de Asistencia y Fotos de Asistencia en Lista Negra

Las operaciones son similares a las realizadas en Registro de asistencia.

Impresión

Usted puede conectar el dispositivo a una impresora, para obtener los datos de registro de manera física.

Presione la tecla M/OK para ingresar al menú principal.

Presione ▼ para seleccionar "Imprimir" y presione OK.

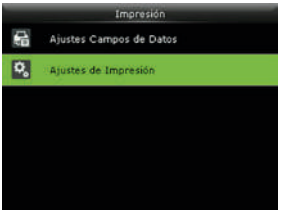
Presione ▼ elejir "Configuración de datos" y pulse OK

12.1 Seleccionar datos

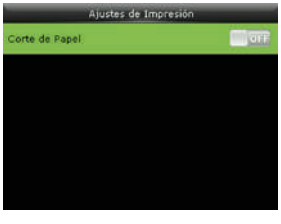
Presione ▼ para seleccionar "Seleccionar Datos" y presione OK.

Presione ▼ para seleccionar el elemento que desea ajustar y pulse OK para activar o desactivar la opción.

11.2 Opciones de impresión



Presione ▼ para seleccionar Opciones de Impresión" y OK



Presione ▼ para seleccionar las opciones que desea ajustar y pulse OK. para activar o desactivar la opción.

Nota: Para habilitar la función recorte de papel conecte el dispositivo a una impresora equipada con la función.

Mensajes Cortos

SMS es similar a una nota. El operador puede editar el contenido de aviso por adelantado y convertirlo en SMS para que aparezca en la pantalla un . SMS incluye la opción de SMS público y SMS privado. Si se configura un SMS público, se mostrará en la columna de información en la parte superior de la interfaz de espera en el tiempo especificado. Si es un SMS privado, el empleado puede ver el SMS después de una asistencia exitosa.

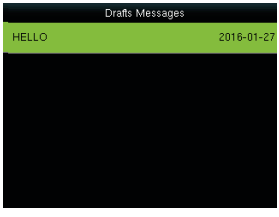
Pulse M / OK en la interfaz inicia

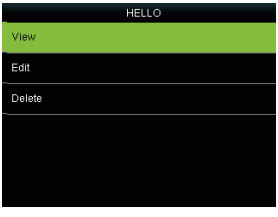
Presione ▼ para seleccionar "Mensaje corto" y presione OK.

Seleccionar un nuevo mensaje , pulse OK

Nota: Es necesario crear el SMS en la PC e importarlo al dispositivo a través de una unidad USB.

13.1 Mensajes públicos, personales y borradores.





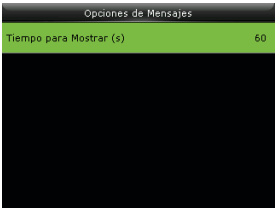
Presione ▼ Para seleccionar la lista de mensajes y pulse OK . Puede ver, editar o borrar el que ha seleccionado. El editar mensajes, las operaciones son similares a las realizadas para añadir un SMS

Mensajes Cortos

13.2 Opciones de mensajes

Establezca el tiempo que se mostrará un mensaje personal en la interfaz inicial.

Presione ► para seleccionar Opciones de mensajes pulse OK .

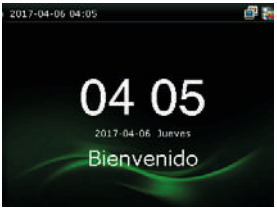


Presione OK.

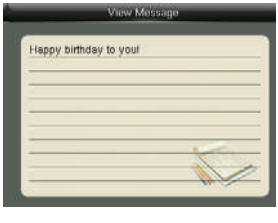
Presione ► para seleccionar el tiempo y pulse OK

13.3 Visualización de mensajes

Después de la configuración de un mensaje corto público, dentro del período de tiempo especificado, la interfaz principal muestra el icono de mensajes cortos en la esquina superior derecha y muestra el contenido del mensaje público en el modo de desplazamiento en la parte inferior de modo que todos los empleados puedan ver la información. El contenido de los mensajes cortos privados para un usuario aparece cuando el usuario verifica exitosamente.



Mensajes públicos



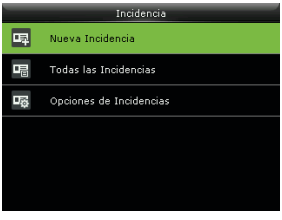
Si la autenticación es exitosa se mostrará el mensaje personal al usuario

Código de Trabajo

Los sueldos de los empleados están sujetos a sus registros de asistencia. Los empleados pueden ser contratados en los distintos tipos de trabajo que pueden variar con el tiempo. Considerando los sueldos varían de acuerdo con los tipos de trabajo, el dispositivo proporciona un parámetro para indicar el tipo de trabajo correspondiente para cada registro de asistencia para facilitar la rápida comprensión de diferentes situaciones de asistencia durante la manipulación de los datos de asistencia.

Pulse M / OK en la interfaz inicial

Presione ► para seleccionar "Código de trabajo" y presione OK.



Presione ▼ Nuevo código de trabajo y pulse OK.

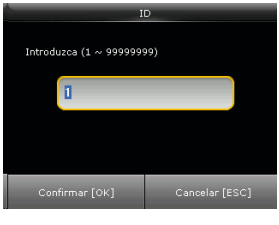
14.1 Añadir un código de trabajo

ID: Un código digital del código de trabajo.

Nombre: El significado del código de trabajo.

1. Introduzca el ID

Seleccione ID y pulse OK.

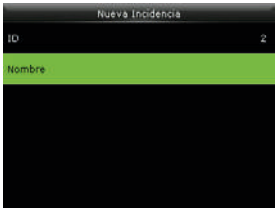


Introduzca el ID del código de trabajo utilizando el teclado, presione OK

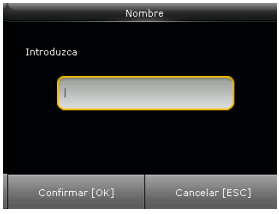
Nota: El dispositivo es compatible con IDs de 1 a 99999999 dígitos por defecto. Si se muestra el mensaje "¡Duplicado!", introduzca otro ID.

Código de Trabajo

2. Introduzca el nombre



Seleccione el nombre y pulse Aceptar.



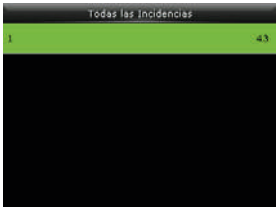
Introduzca el nombre y, a continuación, pulse OK.

La terminal soporta nombres con 1 a 23 caracteres por defecto. Para detalles de como introducir el nombre, consulte Anexo 1 Instrucciones de entrada de texto.

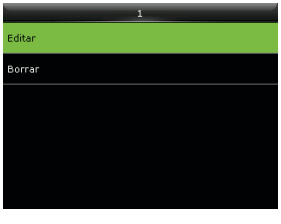
14.2 Todos los códigos de trabajo

Puede ver, editar o borrar el código de trabajo de la lista de códigos. El código no puede ser modificado, y las demás operaciones son similares a los realizados para agregar un código de trabajo eliminar esto.

Presione ► para seleccionar todos los códigos de trabajo y pulse OK.



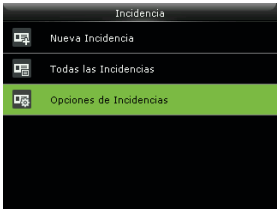
Ver todos los códigos de trabajo.



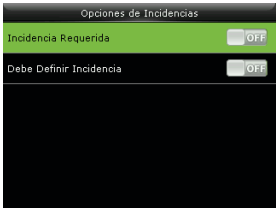
Presione ▼ para seleccionar editar o eliminar.

14.3 Opciones de código de trabajo

Establecer si se debe introducir un código de trabajo al verificar y si el código de trabajo debe existir previamente.



Presione ► para seleccionar las opciones de código de trabajo y pulse OK.



Pulse OK para abrir o cerrar

Pruebas

La prueba automática permite que el sistema pruebe automáticamente si las funciones de diferentes módulos son normales, incluyendo las pruebas de LCD, de voz, sensores, teclado y reloj.

Pulse M / OK en la interfaz inicia

Presione ► Para seleccionar "Pruebas" y pulse OK

Presione ▼ Para seleccionar el que desea ver y pulse OK.

Probar todo: El dispositivo examinará automáticamente el LDC, el sonido, el teclado y la hora. Presione OK para confirmar y ESC para salir.

Probar LCD: La terminal verificará los efectos de color de la pantalla mostrando imágenes en colores vivos, blanco y negro para comprobar si la pantalla está funcionando adecuadamente. Presione OK para confirmar y ESC para salir.

Probar voz: : La terminal comprueba automáticamente si los archivos de voz están completos y la calidad de la voz es buena al reproducir los archivos de voz almacenados en la terminal. Puede continuar con la prueba presionando OK o salir pulsando la tecla [ESC].

Probar teclado: La terminal verifica que todas las teclas estén funcionando normalmente. Presione cualquier tecla en la interfaz [Probar Teclado] para revisar que la tecla oprimida coincida con la que se está mostrando en pantalla. Presione ESC para salir.

Test Automático

Probar sensor de huellas: El terminal examinará automáticamente si el sensor se encuentra funcionando con normalidad y revisa también que la calidad de las imágenes son claras y aptas. Cuando el usuario presente el dedo en el sensor, la imagen de la huella será mostrada en tiempo real. Presione ESC para salir.

Probar cámara: El dispositivo comprueba automáticamente si la cámara funciona correctamente comprobando si las imágenes son claras y aceptables. Presione [ESC]] para salir de la prueba.

Probar reloj: La terminal revisará el rendimiento del reloj examinando el cronómetro del reloj. Oprima la tecla [OK] para iniciar el conteo, y presiónela de nuevo para detenerlo. Presione ESC para salir de la prueba.

Información del Sistema

Puede comprobar el estado de almacenamiento, así como información sobre el firmware del terminal a través de la opción Información de sistema.

Pulse M / OK en la interfaz inicia

Presione ► para seleccionar la información del sistema y pulse OK.

Presione ▼ para seleccionar el que desea ver y pulse OK.

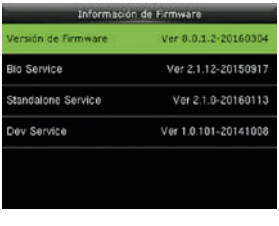
Capacidad del dispositivo: El número de usuarios inscritos, administradores, contraseñas, el almacenamiento total de huellas y la capacidad ocupada hasta el momento, tarjetas ID, y la capacidad de registros de asistencia se muestran, respectivamente.

Información del dispositivo: el nombre del dispositivo, número de serie, la dirección MAC, el algoritmo de huella digital, fabricante y fecha de fabricación se muestran en la interfaz de dispositivo.

Datos de firmware: La versión de firmware, Servicio Bio, Servicio PUSH, , Servicio Standalone y servicio Dev se muestran en la interfaz de Información de Firmware.

Capacidad del dispositivo

Información del dispositivo



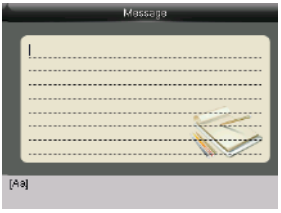
Información de Firmware

Anexo

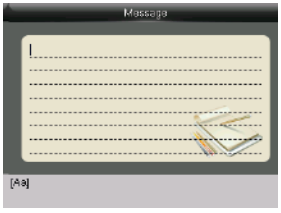
Anexo 1 Descripción del método de entrada de texto.

El dispositivo puede reconocer las letras, símbolos y números. Presione * para mostrar el método de entrada y pulse * Nuevo para cambiar el método de entrada. Pulse # para ingresar un espacio. Pulse ESC para salir del método de entrada.

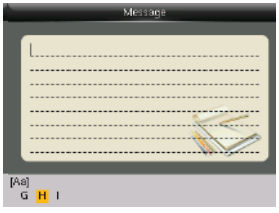
Descripción de la entrada de letras y símbolos (por ejemplo, la creación de un mensaje corto).



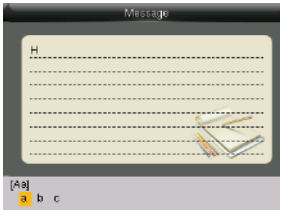
Pulse * para visualizar el método de entrada



Pulse * de nuevo para cambiar el método de entrada. Seleccione Aa, a, o A para el uso de mayúsculas y minúsculas en función de los requisitos.

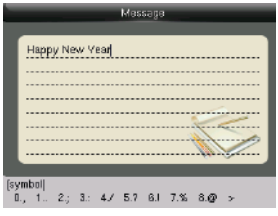


Presion 4 dos veces para seleccionar la H.



Pulse * para visualizar el método de entrada

Presione # para introducir un espacio si es necesario.



Pulse * para cambiar al método de entrada el símbolo y presione el número correspondiente a un símbolo. Cuando termine la entrada, pulse ESC para salir.

Anexo

Apéndice 2 Procedimiento para cargar imágenes.

Foto del usuario: Cree una nueva carpeta llamada "photo" en la raíz de la unidad USB. Un máximo de 8.000 fotos pueden ser almacenadas y el tamaño de cada foto no puede superar los 15 KB. El nombre de la imagen es X. jpg (X es el ID de empleado, que no está limitado en el número de dígitos). Las imágenes deben estar en formato .jpg.

Protectores de pantalla: Cree una nueva carpeta llamada "advertise" en la raíz de la unidad USB y agregue en ella los protectores de pantalla. Un máximo de 20 imágenes se puede almacenar y el tamaño de cada imagen no puede superar los 30 KB. No hay restricciones en el nombre de la imagen y el tipo.

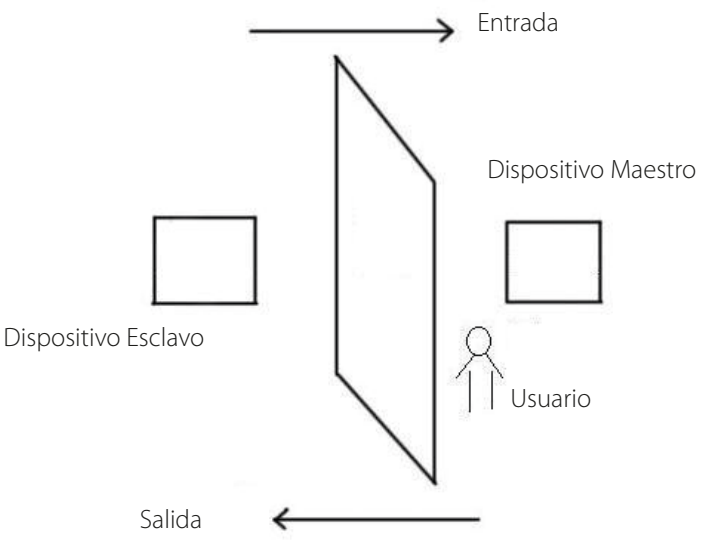
Fondo de pantalla: Cree una nueva carpeta llamada "wallpaper" en la raíz de la unidad USB y agregue en ella los fondos de pantalla. Se pueden almacenar un total del 20 fondos de pantalla y el tamaño de cada uno no puede superar los 30 KB. No hay restricciones en el nombre y tipo de la imagen.

Nota: Si el tamaño de una sola foto de usuario o foto de asistencia es de 10 KB o menos, un total de 10.000 fotos se pueden almacenar.

Apéndice 3 Anti-pass Back

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.



Principio de funcionamiento

El dispositivo maestro tiene Entrada Wiegand y el dispositivo esclavo tiene una Salida Wiegand. Conecte la salida Wiegand del dispositivo esclavo a la entrada Wiegand del dispositivo maestro. El equipo esclavo no debe tener su propio ID de dispositivo sino que el número enviado al equipo maestro desde el esclavo debe ser encontrado en el equipo maestro.

Función

El dispositivo detecta el anti-passback basándose en el último registro de entrada o de salida de los usuarios. El registro de entrada debe coincidir con el registro de salida. El dispositivo soporta salida anti-passback, entrada anti-passback y entrada/salida anti-passback.

Cuando se establece Salida Anti-Passback para un usuario en el dispositivo maestro, el último registro del usuario debe ser de entrada si el usuario requiere registrar una entrada o salida libremente. De lo contrario, el usuario no puede registrar una salida y la solicitud de salida del usuario es negada por el

anti-passback. Por ejemplo, si el primer registro reciente de un usuario es de entrada, el segundo registro puede ser de entrada o de salida, pero el tercer registro se basa en el segundo registro, asegurando que el registro de salida coincide con un registro de entrada. (Si un usuario no tiene registros previos, dicho usuario sólo puede registrar entrada).

Por ejemplo, un usuario de reciente disco es "en", su segundo disco puede estar

Operación

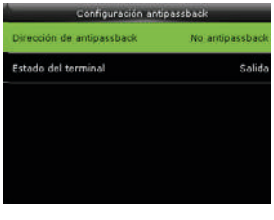
1) Seleccione el modelo

Dispositivo maestro: Dispositivos compatibles con la función Entrada Wiegand, excepto el lector F10.

Dispositivo esclavo: Dispositivos compatibles con la función Salida Wiegand.

2) Configuración del menú

Presione ▼ para seleccionar Configuración Anti-Passback y pulse OK.



Ingrese a la interfaz de configuración anti-passback

Anexo

Anti-Passback

Salida Anti-Passback: Si el dispositivo no tiene almacenado el registro de un usuario, el usuario puede registrar una salida como primer verificación. Si ya existe un registro del usuario en el dispositivo, se activará una alarma cuando el usuario intente registrar una salida sin haber registrado una entrada previamente. Si solo está activado el Anti-Passback de salida, el usuario puede entrar en cualquier momento.

Entrada Anti-Passback: Si el dispositivo no tiene almacenado el registro de un usuario, el usuario puede registrar una entrada como primer verificación. Si ya existe un registro del usuario en el dispositivo, se activará una alarma cuando el usuario intente registrar una entrada sin haber registrado una salida previamente. Si solo está activado el Anti-Passback de entrada, el usuario puede salir en cualquier momento.

Entrada/Salida Anti-Passback: Si el dispositivo no tiene almacenado el registro de un usuario, el usuario puede registrar una entrada o salida como primer verificación. Si ya existe un registro del usuario en el dispositivo, se activará una alarma cuando el usuario intente registrar una entrada o salida sin haber registrado una entrada o salida correspondiente previamente.

Sin Antipassback: Se abre la puerta sólo cuando una persona es autenticado por el host maestro.

Estado del dispositivo

Control de entrada: Cuando se utiliza un dispositivo para controlar la entrada, el dispositivo guarda sólo los registros de entrada.

Salir de control: Cuando se utiliza un dispositivo para controlar la salida, el dispositivo guarda sólo los registros de salida.

Ningun: Cuando el estado de un dispositivo se establece en Ninguno, la función Anti-Passback está desactivado en el dispositivo.

3) Modificar el formato de salida Wiegand del dispositivo

Cuando los dos dispositivos se comunican, sólo se reciben señales de Wiegand sin ID de dispositivo. Entre al menú del dispositivo -> Opciones de Comunicación -> Configuración Wiegand; o en un software entre a Configuración Básica -> Configuración de Dispositivo -> Wiegand y modifique el "formato definido" como "Wiegand26 sin ID de dispositivo".

4) Registro de usuario

Los IDs de los usuarios deben existir y coincidir tanto en el dispositivo maestro como en el esclavo. Por lo tanto, los usuarios deben estar registrados en ambos dispositivos.

5) Descripción de cableado

Los dispositivos maestro y esclavo se comunican entre sí a través de Wiegand y el cableado es el siguiente:

Maestro		Esclavo
IND0	<----->	WD0
IND1	<----->	WD1
GND	<----->	GND

Declaración de Derechos Humanos

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 violen 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 equipos de huella digital de uso policíaco o 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.

Declaración de Privacidad

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 Popular 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, como por ejemplo, las 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
Condensa-dor	x	o	o	o	o	o
Inductor	x	o	o	o	o	o
Diodo	x	o	o	o	o	o
Compo-nentes 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

El EFUP (Periodo de Uso Amigable con Medio Ambiente, por sus siglas en inglés)

O: Indica que esta sustancia tóxica o nociva está presente en todos los materiales homogéneos de esta pieza, por debajo de los límites requeridos en SJ/T11363-2006.

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

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

Green Label

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.