ZKTeco

MANUAL DE USUARIO

ProCapture-T & ProRF-T
Dispositivos de Control de Acceso

Green Label

Acerca de este manual

- Este manual presenta el funcionamiento de las interfaces de usuario y funciones del menú de la terminal de control de acceso ProCapture-T & ProRF-T.
- Las imágenes usadas en este manual pueden no ser completamente consistentes con las del producto adquirido. Prevalecerán las imágenes del producto real.
- Las funciones marcadas con * no están disponibles en todos los dispositivos.

Contenido

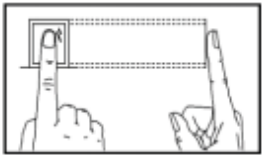
Notas de Orientación

1. Notas de Orientación

1.1 Método para Colocar la Huella Digital

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

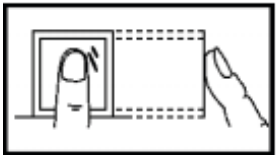
1. Forma correcta de colocar la huella digital:



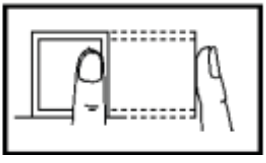
Presione el dedo horizontalmente en el sensor de huellas digitales; el centro de la huella digital se debe colocar en el centro del sensor.

2. Formas incorrectas de colocar la huella digital:

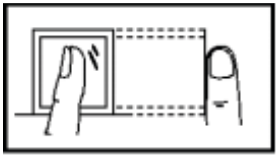
Vertical



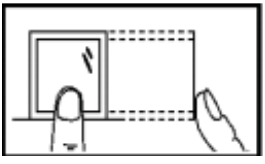
A los lados



Inclinado



Demasiado abajo



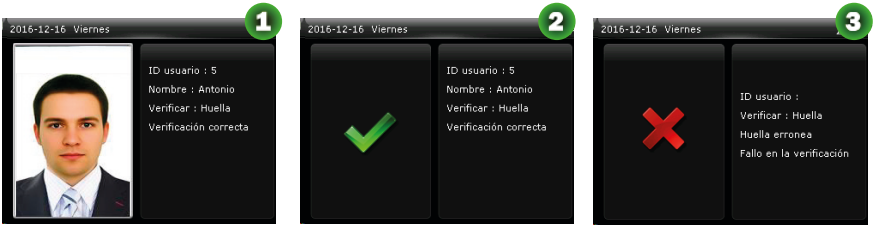
Utilice el método correcto para colocar las huellas digitales para el registro y la verificación. Nuestra empresa no asume la responsabilidad por el mal desempeño de la verificación causado por la operación incorrecta del usuario. Los derechos a la interpretación final y modificación están reservados.

1.2 Modos de Verificación

1.2.1. Verificación de Huellas Digitales 1:N

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

Nota: Utilice la forma correcta de colocar la huella digital en el sensor (para obtener instrucciones detalladas, consulte 1.1 Método para colocar la huella digital)



Verificación exitosa | Verificación exitosa | Verificación fallida

Observaciones:

1. En los dispositivos que posean la función ID con Foto y que tengan activada la opción [Mostrar Foto de Usuario], se mostrará la figura 1 en la pantalla después una verificación exitosa. Desactivar la opción [Mostrar Foto de Usuario] mostrará la figura 2 después de una verificación exitosa.

2. En la interfaz inicial, presione > Sistema > Ajustes de Registros de Acceso > Mostrar Foto de Usuario, y presione para activar o desactivar la opción [Mostrar Foto de Usuario]

* Sólo algunos productos están equipados con la función ID con Foto. Los productos sin función ID con foto no mostrarán una foto de usuario después de una verificación exitosa.

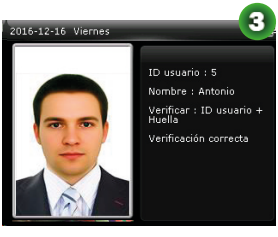
1.2.2 Verificación de Huellas Digitales 1:1

En el método de verificación de huellas digitales 1:1, la huella digital es obtenida por el sensor y se verifica con la huella digital correspondiente al ID de usuario introducido previamente. Favor de usar este método de verificación cuando sea difícil reconocer la huella en el método 1:N.

Introduzca el ID del usuario y presione ⏎

Presione ↓ para elegir "Huella" y pulse ⏎

Después coloque el dedo sobre el sensor.



Verificación exitosa

Verificación exitosa

Verificación fallida

Observaciones:

1. Introduzca el ID de Usuario y presione ⏎ Si se muestra el mensaje "¡ID de Usuario Incorrecto!" esto significa que el ID de usuario no existe.

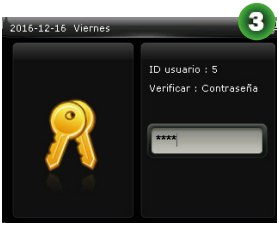
2. Cuando el dispositivo muestra "por favor coloque el dedo de nuevo", coloque de nuevo su dedo en el sensor de huellas digitales. Si la verificación falla aún después de 2 intentos, saldrá a la interfaz inicial.

1.2.3 Verificación con Contraseña

En este método de verificación, la contraseña introducida se verifica con la contraseña del ID de usuario.

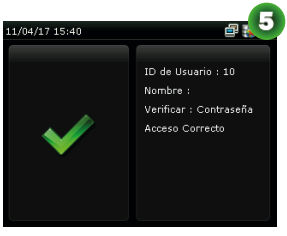
Introduzca el ID del usuario y presione

Selecciona "contraseña" y presiona



Introduce la contraseña

Verificación exitosa



Verificación exitosa

Verificación fallida

Observaciones:

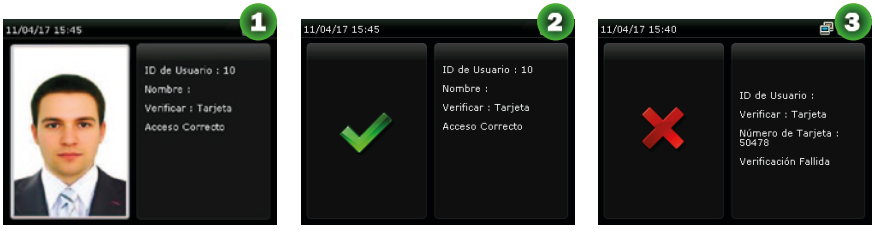
Si se muestra el mensaje "Contraseña Incorrecta", por favor introduzca la contraseña de nuevo. Si la verificación falla aún después de 2 intentos, saldrá a la interfaz inicial.

1.2.4. Verificación con Tarjeta

Observaciones:

La función de tarjeta es opcional, sólo los productos con un módulo de tarjetas integrado están equipados con la función de verificación con tarjeta. Por favor, póngase en contacto con nuestro soporte técnico según sea necesario.

1. Deslice la tarjeta por encima del lector de tarjetas (la tarjeta ya debe estar registrada)
2. Verificación exitosa
3. Verificación fallida



1.3 Interfaz Inicial

Cuando el dispositivo está encendido, la interfaz inicial se muestra a continuación:

Menú Principal

2. Menú Prinicpal

Cuando el dispositivo está en modo de espera, presione para entrar al menú principal.

Usuarios: Usted puede administrar la información de los usuarios registrados incluyendo ID de usuario, privilegios, huella digital, tarjeta * (las tarjetas ID y MiFare son opcionales), contraseña, foto de usuario * (sólo los productos con la función ID con Foto tienen esta opción) y privilegios de control de acceso.

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

Red: Establecer los parámetros relacionados con la comunicación entre el dispositivo y la PC, incluyendo parámetros de Ethernet como la dirección IP, comunicación Serial, conexión a PC, así como ajustes ADMS y Wiegand.

Sistema: Para ajustar los parámetros relacionados del sistema y actualizar el firmware, incluyendo la fecha y hora ajuste, los registros de acceso, los parámetros de huellas digitales y restablecer la configuración de fábrica.

Personalizar: Esto incluye la visualización de la interfaz, el sonido y la configuración del timbre.

Menú Principal

Datos: Borra los registros de acceso, borrar todos los datos, borrar privilegio de administrador, elimine los protectores de pantalla y copia de seguridad y restauración de datos.

Acceso: Para ajustar los parámetros de los dispositivos de control de cerradura y de acceso, incluidos los parámetros de control de acceso, horario, días de festivos, verificación multi-usuario y anti-passback.

Gestión USB: Para transferir datos tales como datos de usuario y los registros de acceso desde la unidad USB al software de apoyo u otros dispositivos.

Eventos: Para buscar los registros almacenados en el dispositivo después de la verificación exitosa.

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

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

Fecha / Hora

3. Fecha / Hora

En la interfaz inicial, pulse > Sistema> Fecha Hora para entrar en la interfaz de configuración de la fecha / hora. Se incluye el establecimiento de la fecha, hora, reloj de 24 horas, formato de fecha y el horario de verano.

Al restablecer la configuración de fábrica, el formato de fecha puede ser restaurado (AAAA-MM-DD).

Observaciones:

Al restablecer la configuración de fábrica, no se restaurará la fecha / hora del dispositivo (si la fecha / hora se ajusta a 18:30 el 1 de enero de 2020, después de reestablecer los ajustes, la fecha / hora se mantendrá en 18: 30 de 1 de enero, 2020.

3.1 Horario de Verano

El Horario de Verano, que también se llama 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 para 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 los distintos países. En la actualidad, cerca de 1 10 países adoptan el horario de verano.

Para satisfacer la demanda del horario de verano, una opción especial puede personalizarse. Hacer que el tiempo de una hora hacia adelante a las XX (hora) XX (día) XX (mes), y hacer que el tiempo de una hora hacia atrás a XX (hora) XX (día) XX (mes)

Fecha / Hora

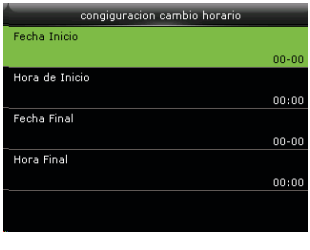
Presione [⏎] > Sistema> Fecha Hora> Cambio de Horario, a continuación, pulse [⏎] para activar el Horario de Verano

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

Configuración del Horario de Verano: Ajuste la fecha/hora o la semana/día del horario de verano de acuerdo al modo seleccionado.

¿Cómo establecer el horario de verano?
Por ejemplo, adelantar el reloj una hora a las 08:00 el 1 de abril y retrasar una hora a las 08: 00 el 1 de octubre (el sistema vuelve a la hora original).

Por el modo de fecha / hora:



Fecha / Hora

Por el modo de fecha / semana

Observaciones:

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.

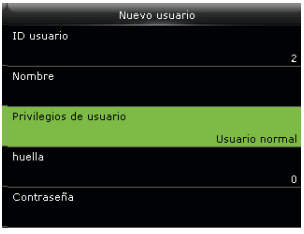
2. Supongamos que el modo de semana/día fue seleccionado en [Modo de Horario de Verano] y el horario de verano comienza desde el domingo de la sexta semana de septiembre de 2013. De acuerdo con el calendario, septiembre de 2013 no tiene seis semanas sino 5. En este caso, en 2013, el horario de verano comienza en el punto de tiempo correspondiente del último domingo de septiembre.

Supongamos que el horario de verano se inicia desde el lunes de la primera semana de septiembre de 2015. De acuerdo con el calendario, la primera semana de septiembre de 2015 no tiene lunes. En este caso, el horario de verano se inicia desde el primer lunes de septiembre de 2015.

4. Usuarios

4.1 Agregar Usuario

Aquí puede registrar un usuario nuevo incluyendo a un administrador o a un usuario normal.



En la interfaz, pulse > Usuario > Nuevo Usuario. Los ajustes incluyen establecer el ID de usuario, elegir los privilegios de usuario (Usuario Normal /Administrador), su registro de huellas digitales y Número de tarjeta * (Tarjetas ID y Mifare son opcionales), el establecimiento de contraseña, tomar foto de usuario * (sólo los productos con la función ID con Foto tienen esta opción) y el establecimiento de privilegios de control de acceso.

Añadir Administrador: Elija "Administrador" en [Privilegios de usuario], quién está autorizado para operar todas las funciones en el menú.

Como se muestra a continuación, el usuario con el ID de usuario 1 es un administrador.

Agregar un Usuario Normal: Elija "Usuario Normal" en [Privilegios de usuario]. Cuando ya se estableció un administrador, los usuarios normales sólo pueden utilizar huella digital, contraseña o tarjeta * para la verificación; cuando el administrador aún no está establecido, los usuarios normales pueden controlar todas las funciones en el menú.

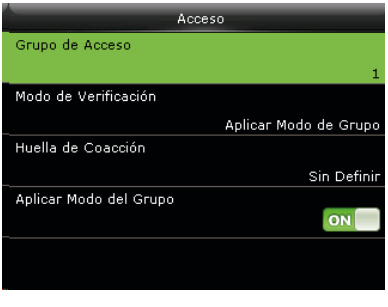
Contraseña: Se aceptan contraseñas de 1 a 8 dígitos.

Observaciones:

1. El dispositivo asigna automáticamente los ID de usuario en secuencia, pero el usuario puede configurarlo manualmente.
2. El dispositivo es compatible con IDs de usuarios de 1 a 9 dígitos.

4.2 Configuración de Control de Acceso

La opción de Control de Acceso de los usuarios se usa para configurar el acceso a la puerta, dirigido a todos, incluyendo ajustes de grupos de acceso, el uso de periodos de tiempo para acceder y la configuración de las huellas digitales para coacción.



Grupo de acceso: Para asignar los usuarios a diferentes grupos de control de acceso para su gestión. Los nuevos usuarios pertenecen a Grupo 1 en la configuración por defecto, que pueden ser reasignados a otros grupos. Un número de grupo válido oscila de 1 a 99.

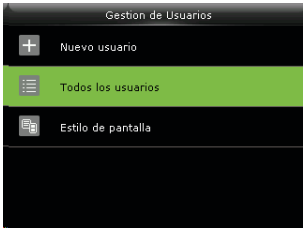
Horario: Seleccione los horarios para el usuario. Los horarios se establecen en el menú de Control de Acceso y un máximo de 50 horarios son compatibles. El tiempo efectivo de apertura de la puerta para un usuario es la suma de los horarios seleccionados.

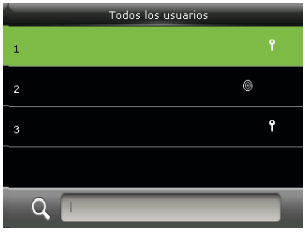
Huellas digitales de coacción: El usuario puede elegir una o más huellas digitales registradas como huellas de coacción. Cuando se verifica con esa huella digital, se activará la alarma de coacción.

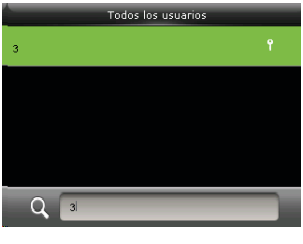
Ejemplo: Entre las huellas digitales registradas (6, 7, 8), elija la 8º como la huella digital de coacción.

4.3 Buscar Usuario

Introduzca el ID de usuario en la lista [Todos los Usuarios] para buscar un usuario.

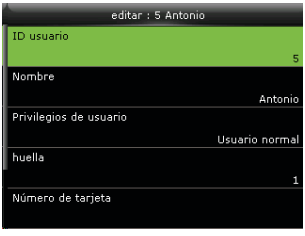






En la interfaz, presione ⇥ > Usuarios >Todos los Usuarios para entrar en la Interfaz de Todos los Usuario. Introduzca el ID de usuario en la casilla de búsqueda y aparecerá el usuario correspondiente, Como se muestra en la figura anterior, busque al usuario con el ID de usuario "2".

4.4 Editar Usuario



Después de elegir un usuario a través de 4.3 Buscar Usuarios, presione ⏎ y seleccione [Editar] para entrar en la interfaz de edición de usuario.

O desde la interfaz inicial presione ⏎ >Usuarios > Todos los usuarios > Buscar un usuario> Presione ⏎ > Editar para entrar en la interfaz de edición de usuario.

El método de operación de edición de usuario es el mismo que el de agregar usuario, pero el nombre de usuario no se puede editar.

4.5 Eliminar Usuario

Después de elegir un usuario a través de 4.3 Buscar Usuarios, presione ⏎ y seleccione [Borrar] para entrar en la interfaz de eliminación de usuario.

O desde la interfaz inicial presione ⏎ >Usuarios > Todos los usuarios > Buscar un usuario> Presione ⏎ > Borrar para entrar en la interfaz de eliminación de usuario.

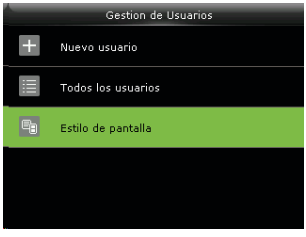
Usuarios

Nota:

1. Sólo cuando el usuario haya registrado huella digital, contraseña, tarjeta * o foto de usuario *, se mostrará elemento en la lista para su eliminación.

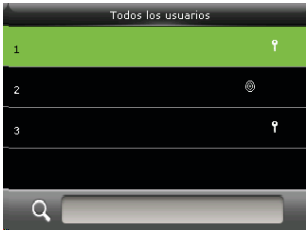
2. Las funciones ID con Foto y Tarjeta son opcionales, no todos los productos las incluyen.

4.6 Estilo de Pantalla



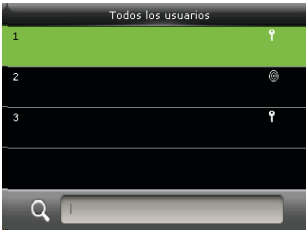
En la interfaz, pulse > Usuario. > Estilo de visualización para entrar en la interfaz de configuración de Estilo de Pantalla.

A continuación, se muestran los diferentes estilos de pantalla.



Línea sencilla

Múltiples líneas



Líneas mezcladas

Privilegios de Usuario

5. Privilegios de Usuario

Se configuran los permisos de operación del menú que puede tener un usuario (Se pueden configurar un máximo de 3 perfiles de privilegios). Cuando los Privilegios de Usuarios estás habilitados, en [Usuarios]> [Nuevo Usuario] > [Privilegios], puede asignar los privilegios adecuados a cada usuario.

Privilegios: El Administrador tiene que asignar diferentes derechos a los nuevos usuarios. Para evitar el establecimiento de derechos para cada usuario de una en una, puede configurar las funciones de usuario para categorizar diferentes niveles de permisos en la gestión de usuarios.

5.1 Habilitar Privilegios de Usuario

En la interfaz inicial, pulse > Privilegios > Privilegio de Usuario 1 (2/3)> Activar Privilegio, presione para activar el privilegio.

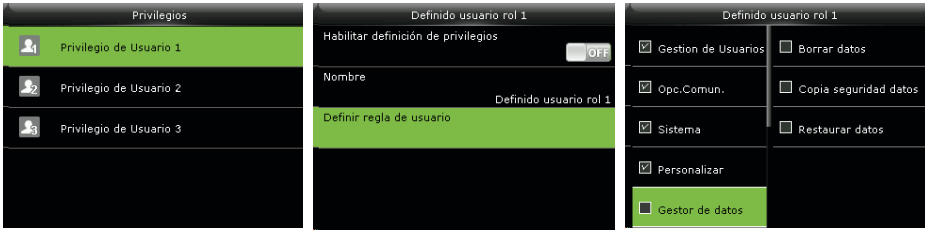
Después de activar privilegios, puede asignar estos privilegios en [Usuarios]> [Nuevo usuario]> [Privilegios de Usuario].

Privilegios de Usuario

Observaciones

Al menos se requiere un administrador registrado para habilitar la función de usuario, o bien, el dispositivo le pedirá "Por favor inscribirse Súper administrador primera".

5.2 Asignación de Derechos

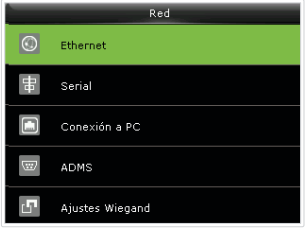


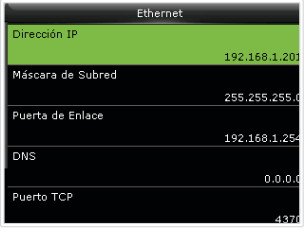
En la interfaz inicial, presione > Privilegios > Privilegio de Usuario1 (2/3)> Definir Privilegios para entrar en la interfaz de asignación de Privilegio de Usuario 1 (2/3).

Presione para seleccionar o deseleccionar el privilegio para cada menú. Después de la selección, pulse Boton ESC del procapture para volver a la interfaz de Privilegio de Usuario 1 (2/3)

6. Red

6.1 Configuración de Ethernet





En la interfaz inicial, presione > Red > Ethernet para entraren la interfaz de Configuración de Ethernet.

Los parámetros siguientes son los valores predeterminados de fábrica, por favor, ajuste de acuerdo a la situación real de la red.

Dirección IP: 192.168.1.201

Máscara de Subred: 255.255.2550

Puerta de enlace 0.0.0.0

DNS: 0.0.0.0

Puerto de comunicación TCP: 4370

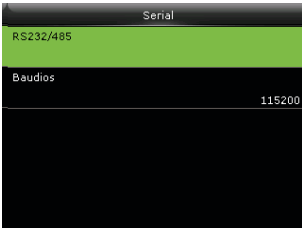
DHCP: Protocolo de Configuración Dinámica de Host (por sus siglas en inglés). Es utilizado para asignar direcciones IP dinámicas a clientes en una red a través de un servidor. Si el DHCP está activado, la dirección IP no puede ajustarse manualmente.

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

Red

En la interfaz inicial, presione [→] para entrar al Menú Principal y seleccione Red.

Presiona la tecla ↓ para seleccionar Serial y presione [→] para acceder.



Selecciona RS232/485 y presiona [→] para aceder.

6.2 Ajustes de Comunicación Serial

Encendido / Apagado de la función RS485

Seleccione RS485 y presiona [→] para aceder.

Presiona la tecla ↓ para elegir RS485 como la función de "Unidad Maestra" o para elegir desactivar el RS485.

Observaciones:

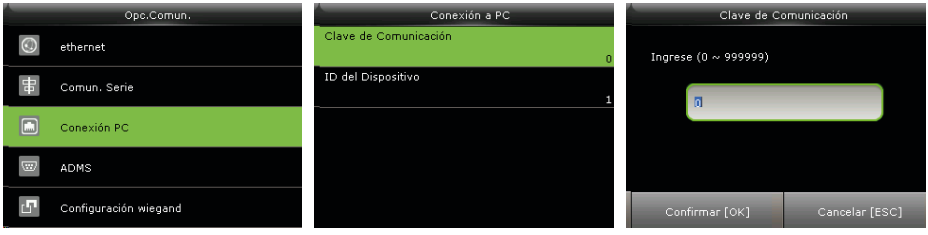
Cuando se utiliza RS485 como la función de "unidad maestra", el dispositivo actuará como "unidad maestra", y puede ser conectado a un lector de huellas digitales RS485.

6.3 Conexión a PC

Configuración de Clave de Comunicación

Para mejorar la seguridad de los datos, una Clave de Comunicación entre el dispositivo y el PC necesita ser establecida.

Si una Clave de Comunicación se establece en el dispositivo, la contraseña de conexión se debe introducir cuando el dispositivo se conecte al software de PC, de forma que el dispositivo y el software puedan comunicarse.

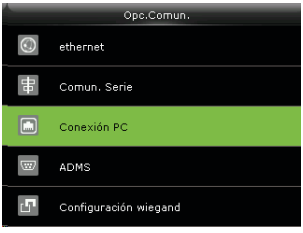


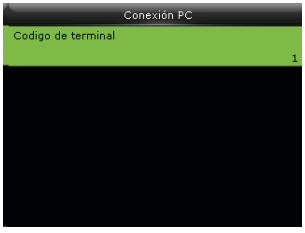
En la interfaz, pulse > Red > Conexión a PC> Clave de Comunicación.

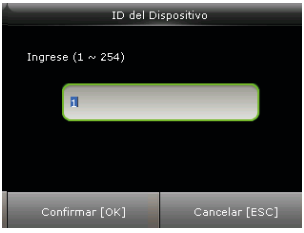
Clave de Comunicación: La clave por defecto es 0 (No hay clave). La Clave de Comunicación puede tener de 1 a 6 dígitos y oscilar entre 0 ~ 999999.

Configuración de la ID del Dispositivo

Si el método de comunicación es RS232 / RS485, se requiere introducir el ID del Dispositivo en la interfaz de comunicación con el software.





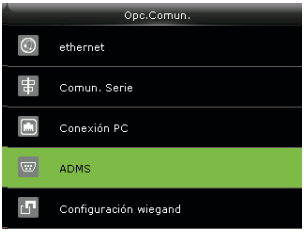


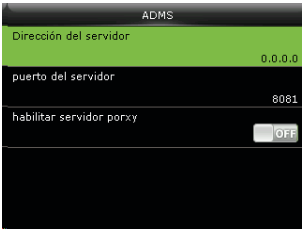
En la interfaz, pulse > Red > Conexión a PC> ID del Dispositivo

ID del Dispositivo: Número de identificación del dispositivo, que oscila entre 1 ~ 254.

6.4 ADMS

Ajustes utilizados para la conexión con el servidor ADMS, como la dirección IP y el puerto de configuración, y si conviene habilitar el servidor proxy, etc.





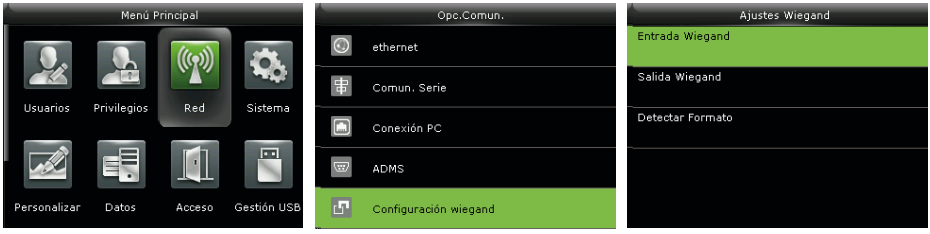
En la interfaz, pulse > Red > ADMS para entrar a la interfaz de configuración del servidor ADMS.

Dirección del Servidor: Introduzca la dirección IP del servidor ADMS (es decir, la dirección IP del servidor donde está instalado el software).

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

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

6.5 Ajustes Wiegand



En la interfaz, presione > Red > Ajustes Wiegand

6.5.1 Salida Wiegand

La conexión de entrada Wiegand es compatible con lectores de tarjetas, o conecta el dispositivo como un dispositivo maestro a otro dispositivo (dispositivo esclavo), formando un sistema maestro / esclavo.

Seleccione "Entrada Wiegand" para ajustar los parámetros en la interfaz de Entrada Wiegand.

Formato Wiegand: Los usuarios pueden elegir entre los formatos wiegand incorporados en el sistema: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a and Wiegand 50.

Amplitud de Pulso (us): La amplitud del pulso enviado por Wiegand. El valor predeterminado es 100 microsegundos, pero puede ajustarse entre 20 a 100 microsegundos.

Intervalo de Pulso (us): El valor predeterminado es 1000 microsegundos, pero puede ajustarse entre 200 a 20000 microsegundos.

Tipo de ID: El contenido de entrada incluido en la señal de entrada Wiegand. Se puede elegir entre ID de Usuario o Número de Tarjeta.

Definiciones de los formatos Wiegand:

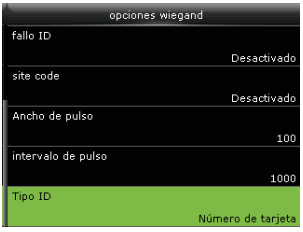
Formato Wiegand	Definición
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCO Consiste de 26 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-13, mientras el bit 26 es el bit de paridad impar para los bits 14-25. Los bits 2-15 corresponden al número de tarjeta.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Consiste de 26 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-13, mientras el bit 26 es el bit de paridad impar para los bits 14-25. Los bits 2-9 corresponden al código de área mientras que los bits 10-15 corresponden al número de tarjeta.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 34 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-17, mientras el bit 34 es el bit de paridad impar para los bits 18-33. Los bits 2-25 corresponden al número de tarjeta.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 34 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-17, mientras el bit 34 es el bit de paridad impar para los bits 18-33. Los bits 2-9 corresponden al código de área mientras que los bits 10-25 corresponden al número de tarjeta.

Red

Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consiste de 36 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-18, mientras el bit 36 es el bit de paridad impar para los bits 19-35. Los bits 2-17 corresponden al código del dispositivo. Los bits 18-33 corresponden al número de tarjeta. Los bits 34-35 corresponden al código del fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consiste de 36 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-18, mientras el bit 36 es el bit de paridad impar para los bits 19-35. Los bits 2-19 corresponden al código del dispositivo. Los bits 20-35 corresponden al número de tarjeta.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE Consiste de 37 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-18, mientras el bit 37 es el bit de paridad impar para los bits 19-36. Los bits 2-4 corresponden al código del fabricante. Los bits 5-16 corresponden al código de área. Los bits 21-36 corresponden al número de tarjeta.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consiste de 37 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-18, mientras el bit 37 es el bit de paridad impar para los bits 19-35. Los bits 2-4 corresponden al código del fabricante. Los bits 5-14 corresponden al código del dispositivo. Los bits 15-20 corresponden al código de área. Los bits 21-36 corresponden al número de tarjeta.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCO Consiste de 50 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-25, mientras el bit 50 es el bit de paridad impar para los bits 26-49. Los bits 2-17 corresponden al código de área. Los bits 18-49 corresponden al número de tarjeta.
C significa número de tarjeta, **E** significa bit de paridad par, **O** significa bit de paridad impar, **F** significa código del dispositivo, **M** significa código del fabricante, **S** significa código de área.	

6.5.2. Salida Wiegand

La conexión de salida Wiegand sirve para conectar una caja de relevador de seguridad (SRB) o para conectar el dispositivo como un dispositivo esclavo a otro dispositivo (dispositivo maestro), formando un sistema esclavo/maestro.



Seleccione "Salida Wiegand" para ajustar los parámetros en la interfaz de Salida Wiegand

SRB: Seleccione ON para activar la función SRB, seleccione OFF para desactivarla.

Formato Wiegand: Los usuarios pueden elegir entre los formatos wiegand incorporados en el sistema: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a and Wiegand 50. Aunque se soportan varios formatos, el formato real está determinado por los Bits de Salida Wiegand.

Por ejemplo, si se selecciona el formato Wiegand26, Wiegand34a, Wiegand36, Wiegand37a o Wiegand50 en Formato Wiegand, pero se eligió 36 en los Bits de Salida Wiegand, el formato que se usará será Wiegand36 de 36 bits.

Bits de Salida Wiegand: Número de bits de los datos wiegand. Después de elegir los Bits de Salida Wiegand, el dispositivo usará este valor para encontrar el formato wiegand más adecuado en Formato Wiegand

Por ejemplo, si se selecciona el formato Wiegand26, Wiegand34a, Wiegand36, Wiegand37a o Wiegand50 en Formato Wiegand, pero se eligió 36 en los Bits de Salida Wiegand, el formato que se usará será Wiegand36 de 36 bits.

ID Fallida: Se define como el valor de salida de una verificación de usuario fallida. El formato de salida depende del Formato Wiegand seleccionado. El valor predeterminado oscila de 0 a 65535.

Código de Área: Es similar al ID del dispositivo excepto que este puede establecerse manualmente y puede repetirse en diferentes dispositivos. El valor predeterminado oscila de 0 a 256.

Ancho de Pulso (us): El ancho del pulso enviado por Wiegand. El valor predeterminado es 100 microsegundos, pero puede ajustarse entre 20 a 100 microsegundos.

Intervalo de Pulso (us): El valor predeterminado es 1000 microsegundos, pero puede ajustarse entre 200 a 20000 microsegundos.

Tipo de ID: El contenido de salida después de una verificación exitosa. Se puede elegir entre ID de usuario o número de tarjeta.

6.5.3 Detección Automática de Formato de Tarjeta

La función Detección Automática de Formato de Tarjeta tiene como objetivo asistir al usuario al detectar rápidamente el tipo de tarjeta y su formato correspondiente. El dispositivo puede leer varios formatos de tarjeta. Después de presentar una tarjeta, el sistema detectará el número de la misma de acuerdo a todos los formatos. El usuario sólo necesita elegir el formato que coincida con el número real de la tarjeta y establecer ese formato Wiegand para el dispositivo. Esta función también aplica para la función de lectura de tarjetas en lectores Wiegand auxiliares.

En la interfaz inicial, presione → > Red > Configuración Wiegand > Detección Automática de Formato de Tarjeta

Procedimiento de la Operación:

1. Después de entrar a la interfaz de Detección Automática de Formato de Tarjeta, deslice la tarjeta de identificación sobre el lector de tarjetas (ya sea en el mismo dispositivo o en el lector de tarjetas auxiliar), la interfaz mostrará los formatos wiegand detectados automáticamente y los números de tarjeta analizados.

2. Elija el elemento que corresponda al número real de la tarjeta y establézcalo como el Formato Wiegand del dispositivo. Este es el formato necesario para leer el tipo de tarjeta presentada.

Observaciones:

En la interfaz de Detección Automática de Formato de Tarjeta de un dispositivo IC, el dispositivo no puede detectar el número de la tarjeta o el formato wiegand solamente deslizando una tarjeta IC. Para detectar el formato wiegand de una tarjeta IC, es necesario conectar un lector de tarjetas IC al dispositivo y deslizar la tarjeta en el lector auxiliar.

Configuraciones de Sistema

7. Configuraciones de Sistema

7.1 Ajustes de Registros de Acceso

En la interfaz inicial, presione > Sistema > Ajustes de Registros de Acceso.

Modo de Cámara: Sirve para establecer si se tomarán y guardarán fotos durante la verificación; aplicable a todos los usuarios. Se incluyen los siguientes 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. Active la función (ON) para mostrar la foto del usuario y desactívela (OFF) si no desea mostrar una foto. (Sólo los productos con la función ID con Foto tienen esta opción).

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

Limpieza periódica de Eventos: La cantidad de registros de acceso 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.

Limpieza periódica de fotos de lista negra: La cantidad de fotos de lista negra 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 el resultado de las verificaciones. El valor oscila de 1 a 9 segundos.

7.2 Ajustes de Huella Digital

En la interfaz inicial, presione > Sistema > Huella Digital.

Umbral de Verificación 1:1: Bajo el método de verificación 1:1, la verificación sólo será exitosa cuando la similitud entre la huella digital a verificar y la huella registrada del usuario sea mayor al valor establecido.

Umbral de Verificación 1:N: Bajo el método de verificación 1:N, la verificación sólo será exitosa cuando la similitud entre la huella digital a verificar y las huellas registradas sea mayor al valor establecido.

Configuraciones de Sistema

Umbral de Verificación Recomendado:

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

Sensibilidad del Sensor de Huellas: Se recomienda dejar el valor predeterminado "Medio". Cuando el ambiente sea seco y la detección de huellas sea lenta, puede establecer el nivel a "Alto" para aumentar la sensibilidad. Cuando el ambiente sea húmedo, haciendo difícil la detección de huellas, puede establecer el nivel a "Bajo".

Detección de dedo vivo: Definir si se utiliza la función anti-huellas falsas. Cuando esta herramienta está activada y se están 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 que ocurran errores en la verificación 1:1 o en la verificación con contraseña debido a que el dedo se presiona incorrectamente o a que el usuario olvidó su contraseña. Para evitar tener que volver a escribir el ID del usuario, se permiten los reintentos. El número de reintentos puede oscilar entre 1 a 9.

Imagen de la Huella Digital: Esta función determina si desea mostrar la imagen de la huella digital durante el registro o verificación de estas. Hay 4 opciones disponibles: Mostrar en registro, Mostrar en Verificación, Siempre mostrar, No mostrar.

7.3 Reestablecer Valores de Fábrica

Reestablece información como ajustes de comunicación o de sistema a los ajustes de fábrica.

En la interfaz inicial, presione → > Sistema > Reestablecer > OK para reestablecer los valores de fábrica.

Los ajustes que se reestablecen incluyen las opciones de Control de Acceso, configuraciones Anti-passback, configuraciones de Red (esto es, las configuraciones ethernet, comunicación serial, Conexión a PC y configuraciones Wiegand), Configuraciones de Personalización (como Voz, Sonido del Teclado, Volumen y Tiempo de Espera para Reposo) etc.

Parámetros	Valores de Fábrica
Opciones de Control de Acceso	Retardo de Cerradura: 5 Segundos Retardo de Sensor de Puerta: 10 Segundos Tipo de Sensor de Puerta: Normalmente Abierta (NO) Modo de Verificación: Contraseña/Huella Digital/ Tarjeta Periodo de Tiempo de Puerta Disponible: 1 Periodo de Tiempo NO: Ninguno Usar como Maestro: Entrada Salida Auxiliar/Tiempo de abertura de Cerradura: 255 Segundos Tipo de Configuración de Salida Auxiliar: Activar Abertura de Puerta Alarma: Apagada
Dirección de Anti-Passback	Sin Anti-Passback

Ethernet	Dirección IP: 192.168.1.201 Máscara de Subred: 255.255.255.0 Puerta de Enlace: 0.0.0.0
Conexión a PC	Clave de Comunicación: 0 ID de Dispositivo: 1
Configuración Wiegand	Tipo de ID de Entrada/Salida Wiegand: ID de Usuario Amplitud de Pulso: 100 us Intervalo de Pulso: 1000 us
Tiempo de Espera para Diapositivas	30 segundos
Tiempo de Espera para Reposo	30 Segundos
Tiempo de Espera del Menú	60 Segundos
Sonido del Teclado	Activado
Sonido de Voz	Activado

Observaciones:

Al reestablecer a los valores de fábrica, la hora y fecha no se verán afectadas. Por ejemplo, si la fecha y hora del dispositivo es 18:30 del 1 de enero de 2020, la fecha y hora se mantendrá igual después de reestablecer los valores de fábrica.

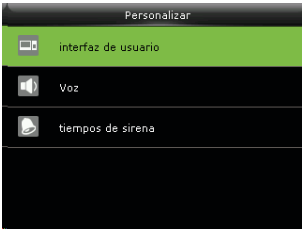
7.4. Actualización por USB

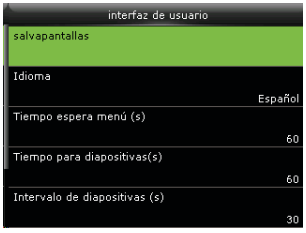
Si necesita un archivo de actualización, póngase en contacto con nuestro soporte técnico. La actualización de Firmware no se recomienda bajo circunstancias normales

Inserte la Unidad USB con el archivo de actualización en el puerto USB del dispositivo, y en la interfaz inicial presione → > Sistema > Actualización por USB para completar la operación de actualización de firmware.

8. Configuraciones de Personalización

8.1 Ajustes de Interfaz de Usuario





En la interfaz inicial, presione > Personalizar > Interfaz de Usuario.

Fondo de Pantalla: Seleccione la imagen a utilizar como fondo de pantalla, puedes encontrar varios estilos dentro del dispositivo.

Idioma: Seleccione el idioma del dispositivo.

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

Observaciones:

Si se desactiva esta opción, el sistema no regresará a la interfaz inicial cuando no haya ninguna operación. No se recomienda desactivar esta función debido al alto consumo de energía y a que representaría un problema de seguridad.

Tiempo de Espera para Diapositivas (s): Cuando no se haga ninguna operación en la interfaz inicial después del periodo de tiempo seleccionado, iniciará una presentación de diapositivas. Esta opción puede desactivarse (elija "Ninguno") o establecerse entre 3 a 999 segundos.

Intervalo de tiempo para Dispositivas (s): Se refiere al intervalo de tiempo entre dispositivas diferentes. Puede desactivarse o establecerse entre 3 a 999 segundos.

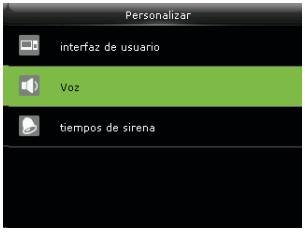
Tiempo de espera para Reposo (m): Esta función permite establecer el tiempo de espera del dispositivo para ingresar al modo de reposo. Presione cualquier tecla para sacar al dispositivo del estado de reposo. El rango de espera es de 1 a 999 minutos. Esta función se puede desactivar.

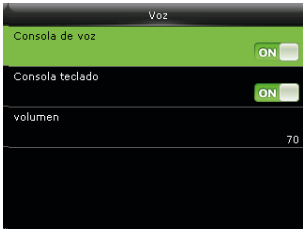
Observaciones:

No se recomienda desactivar esta función debido al alto consumo de energía.

Estilo de la Pantalla Principal: Seleccione la posición y forma del reloj y teclas de estado de la pantalla inicial.

8.2 Ajustes de Voz





En la interfaz inicial, presione [M] > Personalizar > Voz.

Sonido de Voz: Seleccione si desea activar los mensajes de voz durante la operación del dispositivo. El valor predeterminado es ON, indicando que el sonido de voz está activado. Puedes presionar [M] para cambiar entre ON y OFF. El ícono OFF indica que la opción está desactivada.

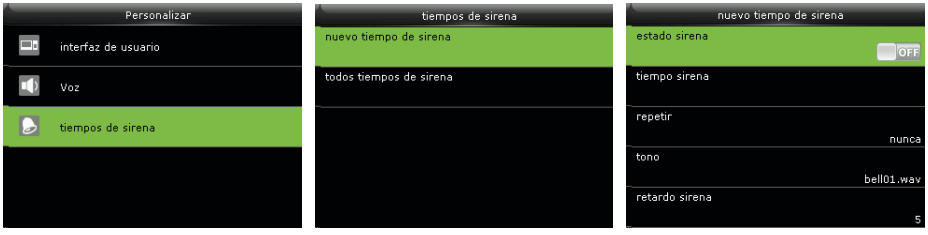
Sonido de Teclado: Seleccione si desea activar el sonido al tocar el teclado. El valor predeterminado es ON, indicando que el sonido del teclado está activado. Puedes presionar para cambiar entre ON y OFF. El ícono OFF indica que la opción está desactivada.

Volumen: Ajuste el volumen del dispositivo. El valor predeterminado es 70. Presione > para incrementar el volumen, presione < para disminuirlo.

8.3 Ajustes de Timbre

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

8.3.1 Agregar un Timbre



En la interfaz inicial, presione > Personalizar > Timbres Programados > Nuevo Horario de Timbre.

Estado del Timbre: ON es para activar el timbre, OFF es para desactivarlo.

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

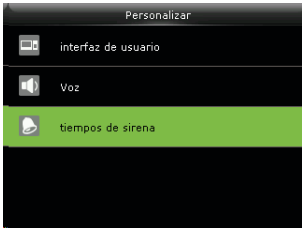
Repetir: Establecer si el timbre se repite de lunes a domingo.

Tono de Timbre: El tono que suena como timbre.

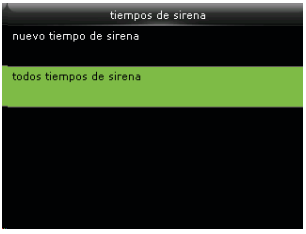
Duración del Timbre: Para establecer la duración del timbre. El valor oscila entre 1 a 999 segundos.

Configuraciones de Personalización

8.3.2 Editar un Timbre

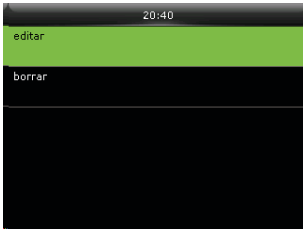


Presione V para seleccionar "Timbres Programados" y presione →



Presione V para seleccionar "Horarios de Timbre" y presione →

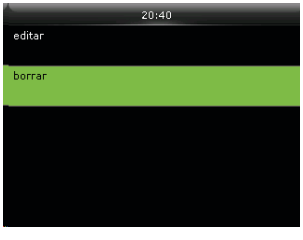
Seleccione el timbre que desea editar y presione →

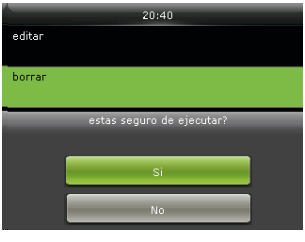


Seleccione "Editar" y presione →

Modifique los parámetros del timbre.

8.3.3 Borrar un Timbre





9. Gestión de Datos

9.1 Borrar Datos

Aquí puede gestionar los datos en el dispositivo, que incluye borrar registros de eventos, borrar todos los datos, borrar privilegios de administrador, borrar protectores de pantalla, etc.

En la interfaz inicial, presione > Gestión de Datos > Borrar Datos.

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

Borrar Fotos de Asistencia: Eliminar todas las fotos de asistencia guardadas en el equipo o borrar fotos de asistencia de un tiempo específico.

Observaciones:

1. Sólo si el Modo de Cámara está seleccionado como "Tomar foto y guardar" o "Guardar en verificación exitosa", las fotos de asistencia se guardarán en el dispositivo después de cada verificación exitosa.

2. En la interfaz inicial, presione > Sistema > Ajustes de Registros de Acceso > Modo de Cámara para seleccionar el modo "Tomar foto y guardar" o "Guardar en verificación exitosa".

Borrar Fotos de lista negra: Eliminar todas las fotos de lista negra en el dispositivo o todas las fotos de lista negra de un tiempo específico. Las fotos de lista negra son las fotos tomadas después de verificaciones fallidas.

Gestión de Datos

Observaciones:

1. Sólo si el Modo de Cámara está seleccionado como "Tomar foto y guardar" o "Guardar en verificación fallida", las fotos de lista negra se guardarán en el dispositivo después de cada verificación fallida.

2. En la interfaz inicial, presione → > Sistema > Ajustes de Registros de Acceso > Modo de Cámara para seleccionar el modo "Tomar foto y guardar" o "Guardar en verificación fallida".

Borrar Todo: Eliminar toda la información de los usuarios, huellas digitales, registros de acceso, etc.

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

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

Borrar Fotos de Usuario*: Eliminar todas las fotos de usuarios en el dispositivo. (Sólo los productos con la función ID con Foto tienen esta opción). Para más detalles sobre cómo cargar fotos de usuarios, consulte la sección 16.3 Procedimiento para Cargar Imágenes)

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

Proceso de Operación:

1- Seleccione "Borrar Fondo de Pantalla" y presione →

2- Presione < o > para cambiar el fondo de pantalla, seleccione "Borrar Imagen Seleccionada" y presione → para borrar la imagen seleccionada, o seleccione "Borrar Todas las Imágenes" y presione → para borrar todas las fotos.

Borrar Protectores de Pantalla: Eliminar protectores de pantalla seleccionados o todos los protectores de pantalla en el dispositivo. (Para más detalles sobre cómo cargar protectores de pantalla, consulte la sección 16.3 Procedimiento para Cargar Imágenes)

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

9.2 Copia de Seguridad

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

Respaldar en Unidad USB (Antes de respaldar datos en una unidad USB, inserte una unidad USB en el puerto USB del dispositivo):

Observaciones:

Las operaciones de Respaldar en el Dispositivo son iguales a las de Respaldar en Unidad USB.

9.3 Restaurar Datos

Para restaurar datos guardados en el dispositivo o en una unidad USB al dispositivo.

Restaurar desde unidad USB (Antes de restaurar datos desde unidad USB, inserte una unidad USB en el puerto USB del dispositivo):

Gestión de Datos

Presione V para seleccionar "Restaurar Datos" y luego presione [→]

Presione V para seleccionar "Restaurar desde USB" y luego presione [→]

Seleccione "Contenido", presione [→] para entrar y marque las casillas con el contenido que desea restaurar.

Observaciones:

Las operaciones de Restaurar desde el Dispositivo son iguales a las de Restaurar desde Unidad USB.

10 Control de Acceso

La opción Control de Acceso se usa para establecer todos los parámetros relacionados al control de la cerradura u otros dispositivos, así como para establecer horarios, días festivos, verificaciones multi-usuario, etc.

En la interfaz inicial, presione > Control de Acceso.

Para poder acceder, el usuario registrado debe cumplir las siguientes condiciones:

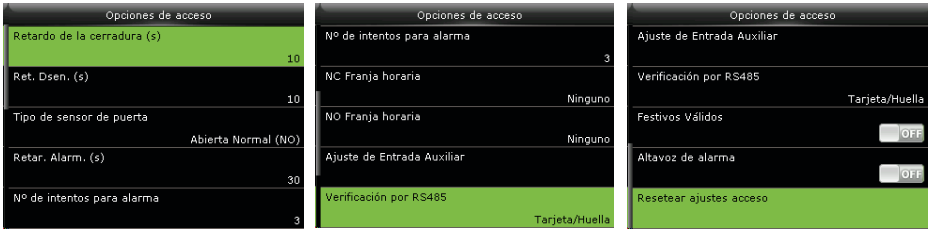
1. La hora de acceso del usuario debe estar dentro del horario personal del usuario o en el horario de su grupo.

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.

Control de Acceso

10.1 Opciones de Control de Acceso



En la interfaz inicial, presione > Control de Acceso > Opciones de Control de Acceso

Retardo de la cerradura (s): Tiempo en que la cerradura electrónica permanece abierta después de recibir la señal de abertura y hasta que se cierra automáticamente (el valor oscila entre 0 a 10 segundos).

Retardo de 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 Tipo de Sensor de la Puerta, se activará una alarma. Este periodo de tiempo es el Retardo de Sensor de Puerta (el valor oscila entre 1 a 255 segundos).

Tipo de Sensor de la Puerta: Incluye Normalmente Abierto (NO), Normalmente Cerrado (NC) y Ninguno. Ninguno significa que no está en uso el sensor de puerta; Normalmente Abierto significa que la puerta está abierta cuando tiene corriente eléctrica; Normalmente Cerrado significa que la puerta está cerrada cuando tiene corriente eléctrica.

Método de Verificación: Seleccione el método de verificación para abrir la puerta. Los métodos son: Contraseña/Huella Digital/Tarjeta, Sólo Huella Digital, Sólo ID de Usuario, Contraseña, Sólo Tarjeta, Huella Digital/Contraseña, Contraseña/Tarjeta, ID de Usuario & Huella Digital, Huella Digital & Contraseña, Huella Digital & Tarjeta, Huella Digital & Contraseña & Tarjeta, Contraseña & Tarjeta, ID de Usuario & Huella Digital & Contraseña, Huella Digital & Tarjeta & ID de Usuario.

Observaciones:

1. / Significa "O". & Significa "Y".

2. En un método de multi-verificación, la información de verificación correspondiente debe ser registrada primero. Por ejemplo: Cuando el usuario A presenta sólo su huella digital, pero el método de verificación seleccionado es "Contraseña & Tarjeta", el usuario A no pasará la verificación.

Horario de Puerta Disponible: Establece horarios para que los usuarios abran la puerta.

Horario de Tiempo NO: Establece el horario de tiempo para el modo Normalmente Abierto, de forma que la puerta siempre esté abierta durante este periodo.

Usar como Maestro: Al configurar los dispositivos maestros y esclavos, puede establecer el estado del dispositivo maestro como Salida o Entrada.

Salida: Una verificación en el dispositivo maestro es un registro de salida.

Entrada: Una verificación en el dispositivo maestro es un registro de entrada.

Configuración de Entrada Auxiliar: Para establecer la Salida Auxiliar/Horario de Cerradura Abierta y el Tipo de Salida Auxiliar del dispositivo con conector auxiliar. Los tipos de salida auxiliar incluyen: Ninguno, Abrir puerta, Activar Alarma y Activar Abrir Puerta y Alarma.

Verificar Modo con RS485 *: Para activar la función de lector RS485; es el método de verificación usado por el dispositivo cuando es el dispositivo maestro/esclavo.

Alarma de Altavoz: Cuando el altavoz de alarma está habilitado, el altavoz sonará una

alarma cuando el dispositivo esté siendo desmantelado.

Reiniciar configuraciones de acceso: Para reiniciar los parámetros de Retardo de la Cerradura, Retardo del Sensor de Puerta, Tipo de Sensor de Puerta, Método de Verificación, Horario de Puerta Disponible, Horario NO, Configuración de Entrada Auxiliar, Alarma de Altavoz, Dirección de Anti-Passback. Sin embargo, el contenido de Borrar Datos de Acceso en [Gestión de Datos] no se verá afectado.

Parámetros de Acceso	Valor de Fábrica
Retardo de la cerradura	5 s
Retardo de sensor de puerta	10 s
Tipo de Sensor de la Puerta	Normalmente Abierto (NO)
Método de Verificación	Contraseña/Huella Digital/Tarjeta
Horario de Puerta Disponible	1
Horario NO	Ninguno
Salida Auxiliar/Horario de Cerradura Abierta	255 s
Tipo de Salida Auxiliar	Abrir Puerta
Alarma de Altavoz	Apagado
Dirección de Anti-Passback	Sin Anti-passback

10.2 Ajustes de Horarios

El horario es la unidad de tiempo mínima de los ajustes de control de acceso; se pueden establecer un máximo de 50 horarios en el sistema. Cada Horario consiste de 7 secciones de tiempo (una semana) y 3 secciones de días festivos, y cada sección de tiempo es el tiempo válido dentro de 24 horas.

Usted puede establecer un máximo de 3 periodos de tiempo para cada sección de tiempo. La relación entre estos periodos de tiempo es "O". Cuando un tiempo de verificación cae dentro de cualquiera de estos periodos de tiempo, la verificación es válida.

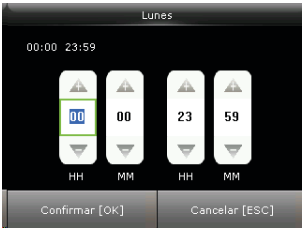
El formato del horario es HH:MM-HH:MM en el sistema de 24 horas con precisión de minutos.

En la interfaz inicial, presione > Control de Acceso > Ajustes de Horarios para entrar en la interfaz de Ajustes de Horarios. El número predeterminado de Horario es 1 (válido todo el día), y se puede editar.

Editar un Horario

Un administrador puede editar un Horario según sea necesario. La operación es la siguiente:

Introduce un número de Horario (como "2"), el horario (2) se localizará automáticamente, selecciona una sección de tiempo (como "lunes") y presione



Establezca la "Hora de inicio" y "Hora de fin" como lo requiera, después presione para guardar y salir.

Pantalla: Puedes establecer la hora de inicio y hora de fin presionando ↑/ ↓ o escribirla directamente, presione ←/→para cambiar de casilla de edición.

Usted puede establecer otras secciones de tiempo según sea necesario, después de configurar la sección de tiempo para lunes, presione Boton ESC del procapture para salir.

Nota:

(1) 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.

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

(3) De forma predeterminada, el Horario 01 indica validez de todo el día (00:00-23:59).

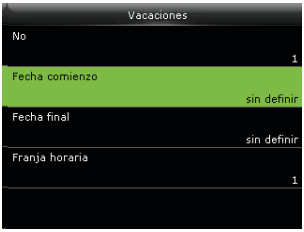
10.3 Ajustes de Días Festivos

Usted puede agregar días festivos al dispositivo de control de acceso y establecer los periodos de tiempo para dichos días festivos según sea necesario.

En la interfaz inicial, presione > Control de Acceso > Días Festivos.

10.3.1 Agregar Día Festivo

Seleccione "Agregar Día Festivo" y presione [OK] para entrar.



Seleccione "Fecha" y presione [OK] para entrar.

Establezca la fecha para el día festivo, presione [OK] para guardar y salir.

Los parámetros de día festivos son los siguientes:

No.: El dispositivo automáticamente asigna un número a un día festivo. También puede seleccionar No. y presionar botón OK del procapture [OK] para entrar a la interfaz de Número. Introduce el número de un día festivo y presione botón OK del procapture [OK] para guardar los ajustes y regresar a la interfaz de Días Festivos.

Nota: El número de un día festivo puede variar de 1 a 24.

Fecha: Establezca la fecha de un día festivo. Presione ↑/↓ o escriba directamente la fecha, presione ←/→ para cambiar de casilla de edición, luego presione @ para guardar los cambios y regresar a la interfaz de Días Festivos.

Tipo de Día Festivo: Puede clasificar el día festivo en 3 tipos (1/2/3). El periodo de tiempo válido para cada tipo de día festivo se puede editar en la interfaz de Ajustes de Horario. Para más detalles sobre editar horarios, consulte la sección 10.2 Ajustes de Horario.

Repetir o no: El valor predeterminado de "Repetir o no" es Encendido [ON]. Puede presionar botón OK del procapture para cambiar entre Encendido [ON] y Apagado [OFF].

Para días festivos fijos de cada año, por ejemplo, Año Nuevo el 1º de Enero, "Repetir o no" puede activarse". Para días festivos no fijos de cada año, por ejemplo, el Día de las Madres en el segundo domingo de Mayo (depende del país), no hay una fecha fija por lo que "Repetir o no" puede desactivarse.

Por ejemplo, cuando la fecha de un día festivo se establece para 1º de Enero de 2016 y el tipo de día festivo se establece en 1, el control de acceso para el 1º de enero se lleva a cabo de acuerdo al periodo de tiempo establecido para los Días Festivos Tipo 1 en vez del periodo de tiempo establecido para el viernes.

10.3.2 Todos los Días Festivos.

Observaciones:

Los métodos para editar o borrar un día festivo son iguales a los usados para editar o borrar un usuario por lo que no se describen aquí. Para más detalles, consulte la sección 4.4 Editar Usuario y 4.5 Eliminar Usuario.

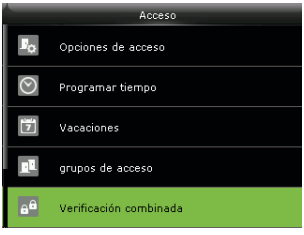
10.4. Ajustes de Verificación Multi-Usuario.

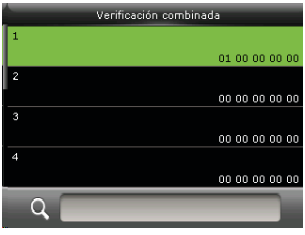
Combine 2 o más grupos de acceso para lograr una multi-verificación y así aumentar la seguridad.

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

Observaciones:

Los grupos de acceso se asignan cuando se agregar un usuario (en la interfaz inicial, presione > Usuarios > Nuevo Usuario > Privilegios de Control de Acceso > Grupo de Acceso, para asignar el grupo de acceso al que pertenece el usuario), el número de grupo de acceso puede oscilar entre 1 a 99.





En la interfaz inicial, presione > Control de Acceso > Verificación Multi-Usuario

Control de Acceso

En la figura anterior, la Verificación Multi-Usuario 1 está compuesta de cinco miembros de cinco grupos de acceso diferentes --- Grupo de acceso 1, 3, 5, 6, 8 respectivamente.

En la figura anterior, la Verificación Multi-Usuario 2 está compuesta de cinco miembros de tres grupos de acceso diferentes: dos miembros del grupo de acceso 2, dos miembros del grupo de acceso 4 y un miembro del grupo de acceso 7.

La Verificación Multi-Usuario 3 está compuesta de cinco miembros, todos ellos del grupo de acceso 9.

La Verificación Multi-Usuario 4 está compuesta de tres miembros de tres grupos de acceso diferentes --- Grupos de acceso 3, 5, 8 respectivamente.

En la figura anterior, la Verificación Multi-Usuario 4 está compuesta de tres miembros de tres grupos de acceso diferentes --- Grupos de acceso 3, 5, 8 respectivamente.

Eliminar una Verificación Multi-Usuario

Para eliminar una Verificación Multi-Usuario, establece todos los números de grupos de acceso a 0.

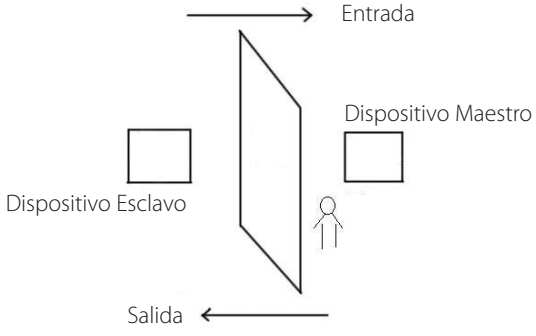
Si todos los números de grupos de acceso de la Verificación Multi-Usuario 3 se establecen a 0, la verificación queda eliminada.

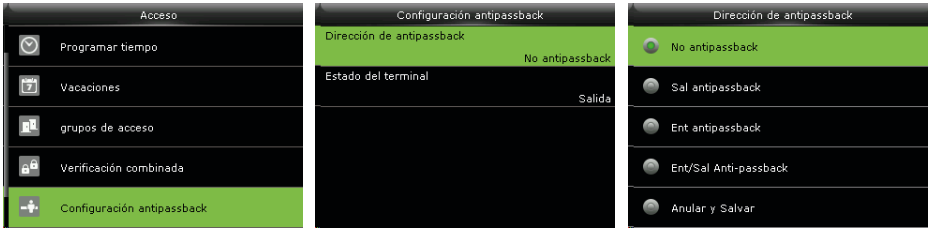
10.5 Ajustes Anti-Passback

Para evitar que una persona que sigue a un usuario consiga acceder sin verificación, lo cual resulta en un problema de seguridad, los usuarios pueden activar la función Anti-Passback. Bajo esta función el registro de entrada debe coincidir con el registro de salida para poder abrir una puerta.

Esta función requiere de 2 dispositivos trabajando juntos: Uno instalado dentro de la puerta (dispositivo maestro) y otro instalado fuera de la puerta (dispositivo esclavo). Ambos dispositivos se comunican a través de una señal Wiegand.

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





En la interfaz inicial, presione > Control de Acceso > Ajustes Anti Passback

Control de Acceso

Dirección de Anti-Passback

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

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

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

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

11 Gestión USB

Usted puede exportar información de usuarios, fotos de usuarios *, 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.

Observaciones:

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

11.1 Descargar en USB

En la interfaz inicial, presione → >Gestión USB > Descargar.

Descargar registros de acceso: Descargar registros de acceso de un periodo de tiempo específico en la unidad USB.

Datos de Usuario: Descargar toda la información de usuarios y huellas digitales del dispositivo en la unidad USB.

Fotos de Usuario*: Descargar todas las fotos de usuario del dispositivo en la unidad USB (sólo los productos con la función ID con Foto tienen esta opción).

Fotos de Asistencia: Descargar las fotos de asistencia de un periodo de tiempo específico desde el dispositivo a la unidad USB.

Fotos de Lista Negra: Descargar las fotos de lista negra (fotos tomadas durante las verificaciones fallidas) de un periodo de tiempo específico desde el dispositivo a la unidad USB.

11.2 Cargar desde USB

En la interfaz inicial, presione → >Gestión USB > Cargar.

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

Fotos de Usuario*: Para cargar una foto de la unidad USB al dispositivo (sólo los productos con la función ID con Foto tienen esta opción). Durante la carga, seleccione [Cargar Foto Seleccionada] o [Cargar Todas las Fotos]. Para más detalles sobre cargar fotos de usuario, consulte la sección 16.3 Procedimiento para Cargar Imágenes.

Protector de Pantalla: Para cargar protectores de pantalla de la unidad USB al dispositivo. Durante la carga, puede seleccionar Cargar Foto Seleccionada o Cargar Todas las Fotos. Las imágenes se mostrarán en la interfaz de espera del dispositivo después de la carga. Para las especificaciones de protectores de pantalla, consulte la sección 16.3 Procedimiento para Cargar Imágenes.

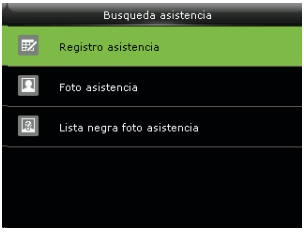
Fondo de Pantalla: Para cargar fondos de pantalla de la unidad USB al dispositivo. Durante la carga, puede seleccionar Cargar Foto Seleccionada o Cargar Todas las Fotos. Las imágenes se mostrarán en la pantalla principal después de la carga. Para las especificaciones de fondos de pantalla, consulte la sección 16.3 Procedimiento para Cargar Imágenes.

12. Búsqueda de Registros

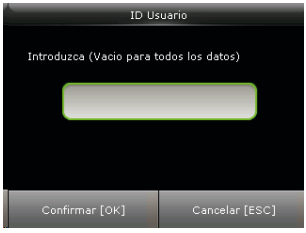
Cuando los usuarios verifican exitosamente, se guarda un registro en el sistema. Esta función permite a los usuarios ver registros de acceso, fotos de asistencia y fotos de lista negra.

12.1 Buscar registros de acceso

En la interfaz inicial, presione [OK] para entrar en el menú principal, presione > para seleccionar "Búsqueda de Eventos" y presione [OK]



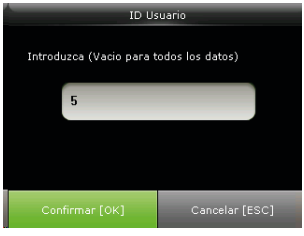
Seleccione "Registros de Acceso" y presione [OK]



Introduzca el ID de usuario de quien desee buscar registros (o deje en blanco para buscar todo) y presione [OK]

12.2 Buscar Fotos de Asistencia

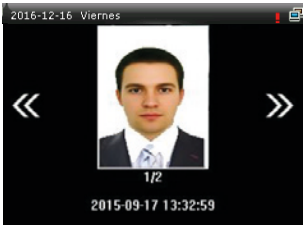
Presione V para seleccionar "Foto de Asistencia" y presione [OK]



Introduzca el ID de usuario de quien desee buscar fotos (o deje en blanco para buscar todo) y presione [OK]

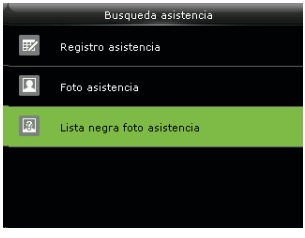
Seleccione un rango de tiempo para la búsqueda y presione [OK]

Búsqueda de Registros



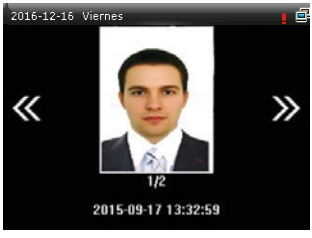
Se muestran las fotos de asistencia correspondientes.

12.3 Buscar Fotos de lista negra.



Presione V para seleccionar "Fotos de Lista Negra" y presione

Seleccione un rango de tiempo para la búsqueda y presione

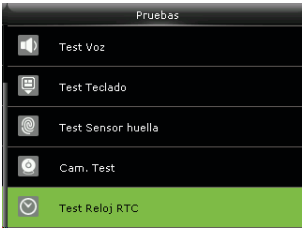


Se muestran las fotos de lista negra correspondientes.

Test Automático

13 Test Automático

El test automático permite al dispositivo comprobar el correcto funcionamiento de sus módulos, incluyendo la pantalla LCD, sonido, sensor de huellas, teclado, cámara y reloj.



En la interfaz inicial, presione > Test Automático

Probar Todo: Probar pantalla LCD, sonido, teclado, sensor de huellas, cámara y reloj. Durante la prueba, presione botón OK del procapture para continuar a la siguiente prueba, o presione # para salir de la prueba.

Probar LCD: Probar los efectos de color de la pantalla LCD mostrando imágenes en colores vivos, blanco y negro para comprobar si la pantalla está funcionando adecuadamente. Durante la prueba, presione botón OK del procapture para continuar a la siguiente prueba, o presione botón ESC del procapture para salir de la prueba.

Probar Sonido: La terminal probará automáticamente si los archivos de voz están completos y que la calidad del sonido sea la adecuada reproduciendo los archivos de sonido almacenados dentro de la misma. Durante la prueba, presione botón OK del procapture para continuar a la siguiente prueba, o presione botón ESC del procapture para salir de la prueba.

Probar Teclado: Probar si todas las teclas funcionan correctamente. Presione cualquier tecla en la interfaz de pruebas de Teclado; si la tecla presionada coincide con el símbolo que se muestra en pantalla, la tecla funciona correctamente. Presione botón OK del procapture o botón ESC del procapture para salir de la prueba.

Test Automático

Probar Sensor de Huellas: Probar si el sensor de huellas digitales encuentra funcionando con normalidad y si la calidad de las imágenes de las huellas es apta. Cuando el usuario presione el dedo en el sensor, la imagen de la huella será mostrada en pantalla. Presione botón OK del procapture o botón ESC del procapture para salir de la prueba.

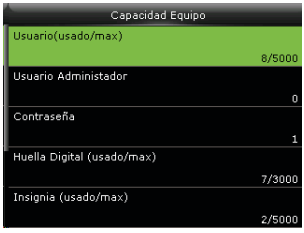
Probar Cámara: Probar si la cámara funciona adecuadamente verificando que las fotos capturadas sean claras. Presione botón OK del procapture o botón ESC del procapture para salir de la prueba.

Probar Reloj RTC: Probar el Reloj en Tiempo Real. La terminal revisará el rendimiento del reloj examinando el cronómetro. Presione @ para iniciar el conteo, presione botón OK del procapture de nuevo para detenerlo y ver si el cronómetro toma el tiempo de forma precisa. Presione botón OK del procapture para salir de la prueba.

14 Información del Sistema

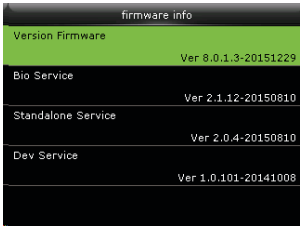
Con este parámetro usted puede ver la capacidad de almacenamiento de datos, información del dispositivo y del firmware.

En la interfaz inicial, presione > Información de Sistema.



Capacidad del Dispositivo

Información del Dispositivo



Firmware del Dispositivo

Información del Sistema

Capacidad del Dispositivo: Muestra la cantidad de usuarios registrados, administradores, contraseñas, huellas digitales, tarjetas *, registros, fotos de asistencia, fotos de lista negra y fotos de usuarios*. También muestra la capacidad total de almacenamiento de usuarios, huellas, tarjetas*, registros, fotos de asistencia, fotos de lista negra y fotos de usuario.

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

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

Observaciones:

La forma en que se muestra la capacidad del dispositivo, información del dispositivo y de firmware en la interfaz de información de sistema de diferentes productos puede variar; prevalecerá el producto real.

15 Resolución de Problemas

• El sensor de huellas no puede de leer y verificar una huella de forma efectiva.

➤ Revise si el dedo esta mojado o si el sensor de huella está mojado o polvoriento.

➤ Limpie el dedo y sensor de huellas e intente de nuevo.

➤ Si el dedo está muy seco, sóplele e intente de nuevo.

• Se muestra el mensaje "Horario Inválido" después de una verificación.

➤ Contacte al administrador para verificar si el usuario tiene privilegio de acceder dentro de ese horario.

• La verificación se realiza con éxito, pero el usuario no puede abrir la puerta.

➤ Revise si el privilegio del usuario está establecido correctamente.

➤ Revise si el cableado de la cerradura es correcto.

• Suena la alarma Tamper (Sabotaje)

➤ Revise si el dispositivo y la placa posterior están unidas; si no, el botón tamper en la parte trasera del dispositivo se activará y lanzará una alarma, el icono ⚠ aparecerá en la esquina superior derecha de la interfaz.

Sólo cuando la función [Alarma de Altavoz] (Control de Acceso > Opciones de Control de Acceso > Alarma de Altavoz) esté activada, el altavoz lanzará una alarma.

16 Anexos

16.1 Función ID con Foto*

Aquí puede gestionar los datos en el dispositivo, que incluye borrar registros de eventos, borrar todos los datos, borrar privilegios de administrador, borrar protectores de pantalla, etc.

Observaciones: Algunos modelos soportan la función ID con Foto.

Cuando la función ID con Foto está activada y el usuario verifica exitosamente, no sólo el ID y nombre del usuario se mostrarán en la pantalla, sino también la foto registrada por el usuario o guardada en la unidad USB.

Observaciones:

Necesita activar la opción [Mostrar Foto de Usuario] (en la interfaz inicial, presione botón OK del procapture > Sistema > Ajustes de Registros de Acceso > Mostrar Foto de Usuario, y presione botón OK del procapture para activarla) para que se muestre la foto de usuario después de cada verificación exitosa. Si la opción está desactivada, no se mostrará la foto de usuario, aunque el dispositivo cuente con la función ID con Foto.

Procedimiento de Operación

Si se usa la foto de usuario tomada por el dispositivo, la foto se mostrará justo después de la verificación del usuario.

Si la foto de usuario está en una unidad USB, el proceso de operación es el siguiente:

(1) Cree una carpeta con el nombre "photo" en la unidad USB, y guarde la foto de usuario en la carpeta.

(2) El formato de la foto debe ser JPG, y el archivo debe llamarse como el ID del usuario. Por ejemplo: La foto correspondiente al usuario con el número de ID 154 debe llamarse 154.jpg

(3) Inserte la unidad USB en el puerto USB del dispositivo, y vaya a Gestión USB > Cargar > Foto de Usuario para cargar las fotos de usuario. Ahora la foto se mostrará cada vez que el usuario verifique exitosamente.

Nota:

(1) El nombre de la foto no puede tener más de 9 dígitos.

(2) El tamaño de la foto debe ser menor a 15Kb.

(3) La nueva foto cargada reemplazará la foto original del usuario.

(4) Al descargar fotos de usuario (vaya a Gestión USB > Descargar > Fotos de Usuario), una carpeta llamada "photo" se creará automáticamente dentro de la unidad USB, donde se guardarán todas las fotos descargadas.

16.2 Introducción a Wiegand

El protocolo Wiegand26 es un protocolo estándar de control de acceso desarrollado por el Subcomité de Estándar de Control de Acceso afiliado a la Asociación de la Seguridad Industrial (SIA por sus siglas en inglés). Es un protocolo usado para puertos y salidas de lectores de tarjetas IC sin contacto.

El protocolo define la conexión entre el lector de tarjetas y el controlador los cuales son ampliamente usados en la industria del control de acceso, seguridad, entre otras. Esto ha estandarizado el trabajo de los diseñadores de lectores de tarjetas y fabricantes de controladores. Los dispositivos de control de acceso producidos por nuestra empresa también aplican este protocolo.

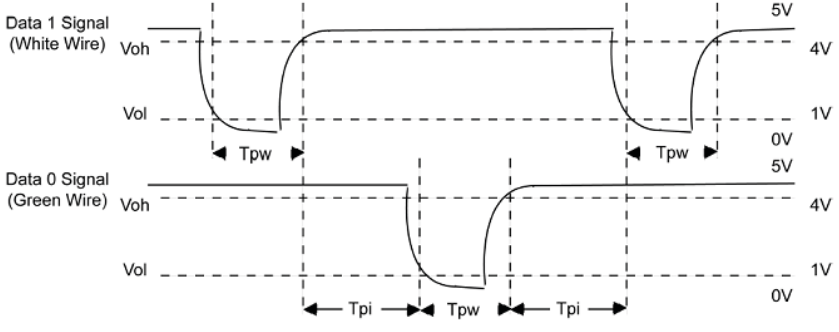
Señal Digital

La figura 1 muestra el diagrama secuencial del lector de tarjetas que envía señales digitales en bits hacia el controlador de acceso. El Wiegand en este diagrama sigue el protocolo estándar de control de acceso de la SIA, que tiene como objetivo lectores de tarjetas Wiegand de 26 bits (con un tiempo de pulso de entre 20us hasta 100us y un tiempo de salto de pulso de entre 200us hasta 20ms). Las señales Data0 y Data1 son de alto nivel (más que Voh) hasta que el lector de tarjetas está listo para enviar un flujo de datos. El lector de tarjetas envía un pulso asíncrono de bajo nivel (menor que vol), transmitiendo un flujo de datos a través de los cables Data1 y Data0 para acceder a la caja de control (como se ve en el diente de sierra de la figura 1). Los pulsos Data0 y Data1 no se traslapan ni sincronizan. La figura 1 muestra la máxima y mínima amplitud de pulso (pulsos sucesivos) y el tiempo de salto de pulso (el tiempo entre 2 pulsos) permitido por las terminales de control de acceso de huellas digitales de la serie F.

Tabla 1: Tiempo de Pulso

Señal	Definición	Valor Típico del Lector de Tarjeta
Tpw	Amplitud de Pulso	100 µs
Tpi	Intervalo de Pulso	1 ms

Figura 1: Diagrama Secuencial



16.2.1 Introducción a Wiegand 26

El sistema tiene integrado un formato Wiegand de 26 bits.

La composición del formato Wiegand de 26 bits contiene 2 bits de paridad y 24 bits para contenido de salida ("ID de Usuario" o "Número de Tarjeta"). El código binario de 24 bits representa hasta 16,777,126 (0 - 16,777,215) valores diferentes.

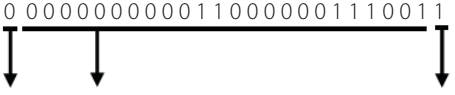
1	2 ... 25	26
Bit de paridad par.	ID de Usuario/ Número de Tarjeta	Bit de paridad impar

La siguiente tabla define de los campos:

Campo	Descripción
Bit de paridad par	Evaluado desde el bit 2 al bit 13. El bit de paridad par es 1 si el carácter tiene un número par de 1 bit; de lo contrario, el bit de paridad par es 0.
ID de Usuario/Número de Tarjeta (bit 2 – bit 25)	ID de Usuario/Número de Tarjeta (Código de Tarjeta, 0 – 16777215). El bit 2 es el Bit Más Importante (MSB por siglas en inglés)
Bit de paridad impar	Evaluado desde el bit 14 al bit 25. El bit de paridad impar es 1 si el carácter tiene un número par de 1 bit; de lo contrario, el bit de paridad impar es 0.

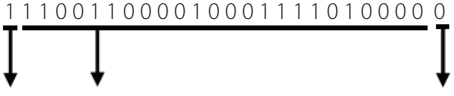
Por ejemplo: Para un usuario con ID de usuario 12345, con número de tarjeta 0013378512 y el número de ID fallida se estableció en 1.

1. Cuando la salida se establece como "ID de Usuario", la salida Wiegand es la siguiente después de la verificación exitosa:



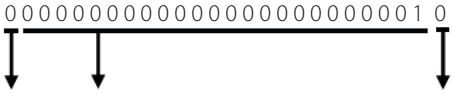
Bit de Paridad Par | ID de Usuario= Código Binario para 12345 | Bit de Paridad Impar

2. Cuando la salida se establece como "Número de Tarjeta", la salida Wiegand es la siguiente después de la verificación exitosa:



Bit de Paridad Par | No. de Tarjeta = Código Binario para 0013378512 | Bit de Paridad Impar

3. Cuando la verificación falla, la salida Wiegand es la siguiente.



Bit de Paridad Par | ID Fallida = Código Binario para 1 | Bit de Paridad Impar

Nota: Si el contenido de salida excede el alcance de todos los valores permitidos por el formato Wiegand, los últimos bits se tomarán y los primeros bits se descartarán automáticamente. Por ejemplo, el ID de Usuario 888 888 888 es 110 100 111 110 110 101 111 000 111 000 en formato binario. Wiegand 26 sólo soporta 24 bits, eso es, sólo toma en cuenta los últimos 24 bits, mientras que los primeros 6 bits "110 100" son automáticamente descartados.

16.2.2 Introducción a Wiegand 34

El sistema tiene integrado un formato Wiegand de 34 bits.

La composición del formato Wiegand de 34 bits contiene 2 bits de paridad y 32 bits para contenido de salida ("ID de Usuario" o "Número de Tarjeta"). El código binario de 32 bits representa hasta 4,292,967,296 (0 - 4,292,967,296) valores diferentes.

1	2 ... 33	34
Bit de paridad par.	ID de Usuario/ Número de Tarjeta	Bit de paridad impar

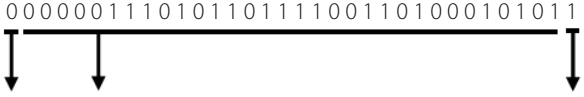
La siguiente tabla define los campos:

Campo	Descripción
Bit de paridad par	Evaluado desde el bit 2 al bit 17. El bit de paridad par es 1 si el carácter tiene un número par de 1 bit; de lo contrario, el bit de paridad par es 0.
ID de Usuario/Número de Tarjeta (bit 2 – bit 25)	ID de Usuario/Número de Tarjeta (Código de Tarjeta, 0 – 16777215). El bit 2 es el Bit Más Importante (MSB por siglas en inglés)

Bit de paridad impar	Evaluado desde el bit 18 al bit 33. El bit de paridad impar es 1 si el carácter tiene un número par de 1 bit; de lo contrario, el bit de paridad impar es 0.

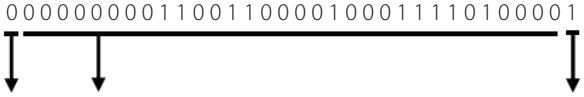
Por ejemplo, para un usuario con ID de usuario 123456789, con número de tarjeta 0013378512 y el número de ID fallida se estableció en 1.

1. Cuando la salida se establece como "ID de Usuario", la salida Wiegand es la siguiente después de la verificación exitosa:



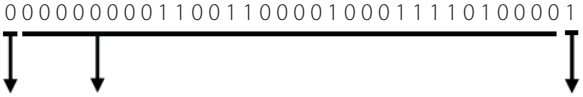
Bit de Paridad Par | ID de Usuario= Código Binario para 123456789 | Bit de Paridad Impar

2. Cuando la salida se establece como "Número de Tarjeta", la salida Wiegand es la siguiente después de la verificación exitosa:



Bit de Paridad Par | ID de Usuario= Código Binario para 0013378512 | Bit de Paridad Impar

3. Cuando la verificación falla, la salida Wiegand es la siguiente.



Bit de Paridad Par | ID de Usuario= Código Binario para 1 | Bit de Paridad Impar

16.3 Procedimiento para Cargar Imágenes

1. Foto de Usuario*: Se necesita crear una carpeta llamada "Photo" en la unidad USB y agregar las fotos de usuario dentro de esa carpeta. La capacidad es de 3000 imágenes, que no excedan los 15Kb cada una. El nombre de la imagen es x.jpg (x siendo el número de ID del usuario, máximo 9 dígitos). El formato de la foto debe ser JPG.

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

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

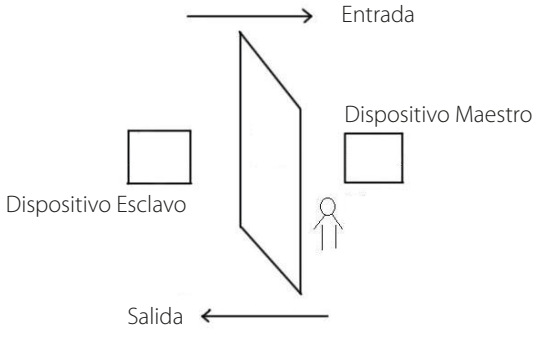
Nota: Cuando cada foto de usuario y foto de asistencia no exceden 10Kb, el dispositivo puede guardar un total de 10000 fotos de usuario y de asistencia (considerando la capacidad real del dispositivo, se recomienda ampliamente agregar a lo mucho 5000 fotos de usuario y de asistencia.

16.4 Ajustes de Anti-Passback

Para evitar que una persona que sigue a un usuario consiga acceder sin verificación, lo cual resulta en un problema de seguridad, los usuarios pueden activar la función Anti-Passback. Bajo esta función el registro de entrada debe coincidir con el registro de salida para poder abrir una puerta.

Esta función requiere de 2 dispositivos trabajando juntos: Uno instalado dentro de la puerta (dispositivo maestro) y otro instalado fuera de la puerta (dispositivo esclavo). Ambos dispositivos se comunican a través de una señal Wiegand.

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



Principio de Funcionamiento

El dispositivo maestro soporta la función de Entrada Wiegand y el dispositivo esclavo soporta la función de Salida Wiegand. Después de que el puerto de salida Wiegand del dispositivo esclavo se conecte con la entrada Wiegand del dispositivo maestro, las señales Wiegand salientes del dispositivo esclavo no pueden contener el ID del dispositivo y los números enviados desde el dispositivo esclavo al dispositivo maestro deben existir en el dispositivo maestro. Es decir, la información de usuario en el dispositivo esclavo que soporta la función anti-passback debe coincidir con la información de usuario en el dispositivo maestro que soporta la función anti-passback.

Descripción de la 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. Nota: Si un usuario no tiene registros previos, dicho usuario sólo puede registrar entrada.

Cuando se establece **Entrada Anti-Passback** para un usuario en el dispositivo maestro, el último registro del usuario debe ser de salida si el usuario requiere registrar una entrada o salida libremente. De lo contrario, el usuario no puede registrar una entrada y la solicitud de entrada del usuario es negada por el anti-passback. Nota: Si un usuario no tiene registros previos, dicho usuario sólo puede registrar salida.

Cuando se establece **Entrada/Salida Anti-Passback** para un usuario en el dispositivo maestro, si el último registro del usuario es de entrada o de salida, el siguiente registro del usuario debe ser de entrada o de salida para que el usuario pueda entrar/salir libremente. Es decir, el registro de salida debe coincidir con el registro de entrada en todos los casos.

Descripción de la Operación

(1) Selección del Modelo

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

Dispositivo Esclavo: Dispositivos compatibles con la función Salida Wiegand.

Resolución de Problemas

(2) Ajustes de Menú

➤ Dirección de Anti-Passback

Las opciones de Dirección de Anti-Passback incluyen Entrada/Salida Anti-Passback, Salida Anti-Passback, Entrada Anti-Passback y Sin Anti-Passback.

Salida Anti-Passback: Después de que el usuario registre una salida, sólo si el registro más reciente es una entrada, el usuario puede volver a registrar una salida.

Entrada Anti-Passback: Después de que el usuario registre una entrada, sólo si el registro más reciente es una salida, el usuario puede volver a registrar una entrada.

(3) Modificar el formato de Salida Wiegand para el dispositivo.

Cuando 2 dispositivos de comunican mutuamente, sólo se aceptan señales Wiegand que no contienen el ID del dispositivo. Puede elegir el formato en Red >Ajustes Wiegand desde el menú principal o puede hacerlo mediante el software en Configuración Básica > Administración de Dispositivos > Wiegand y establecer el Formato Definido a Wiegand26-bits o 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:

Dispositivo Maestro		Dispositivo Esclavo
IWD0	⟷	WD0
IWD1	⟷	WD1
GND	⟷	GND

16.5 Declaración de Derechos Humanos y de Privacidad

Apreciado consumidor:

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

Por esta razón consignamos en este documento la siguiente información:

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

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

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

Resolución de Problemas

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

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

Nota: Las siguientes son regulaciones ligadas a las leyes de la República popular de China acerca de la libertad personal:

1. Detención, reclusión o búsqueda ilegal de ciudadanos de la República 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, por ejemplo, baterías. El EFUP de las baterías es de 5 años.

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

O: Indica que esta sustancia tóxica o nociva 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