Manual de Usuario

Terminal de Control de Acceso Facial

Acerca de este manual

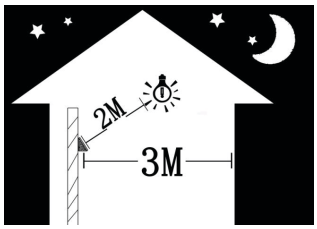
- Este manual presenta la operación de interfaces de usuario y las funciones del menú.
- Las fotos que aparecen en este manual pueden no ser exactamente compatibles con las de su dispositivo.

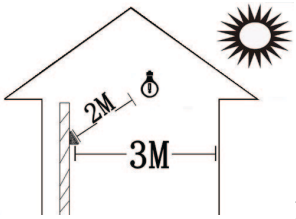
CONTENIDO

1. Introducciones de uso

1.1 Entorno operativo del dispositivo

Posición de instalación recomendada

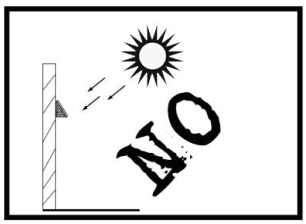




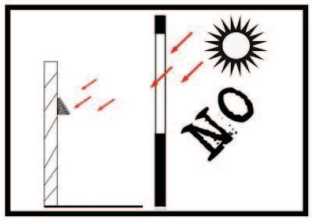
Posición de instalación recomendada (como se muestra en la figura izquierda):

Instale el dispositivo en una posición de interior que es de tres metros lejos de las ventanas y puerta y dos metros lejos de la fuente de la lámpara, con iluminación de fuente de luz ambiental siendo 0-800 LUX

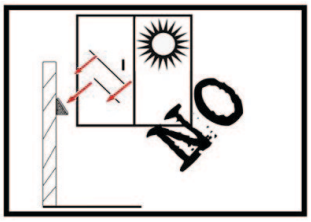
2) Varias posiciones de instalación que afectan a efecto de aplicación



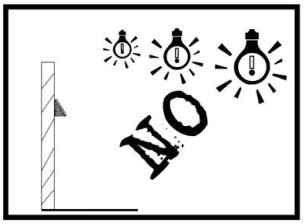
La luz solar directa (exterior)



La luz solar directa a través de las ventanas (interior)

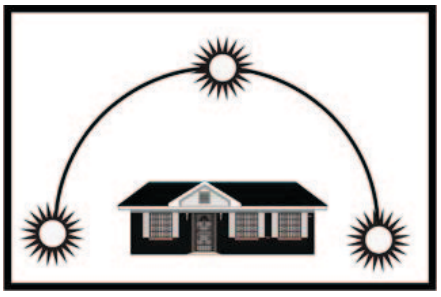


Luz del sol oblicuo por la ventana (interior)

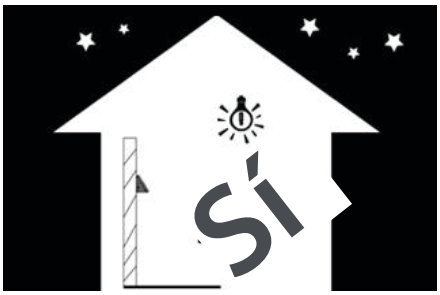


Exposición a la luz de la lámpara a corta distancia (interior)

10 lux



Mayor que 1200 lux

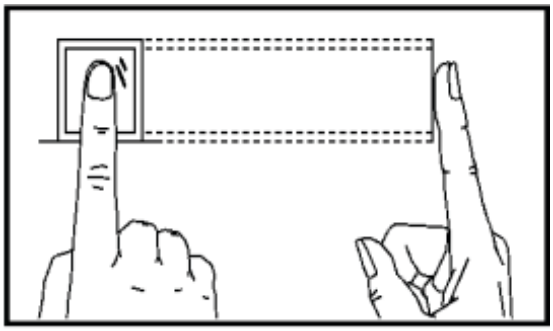


50-800 lux

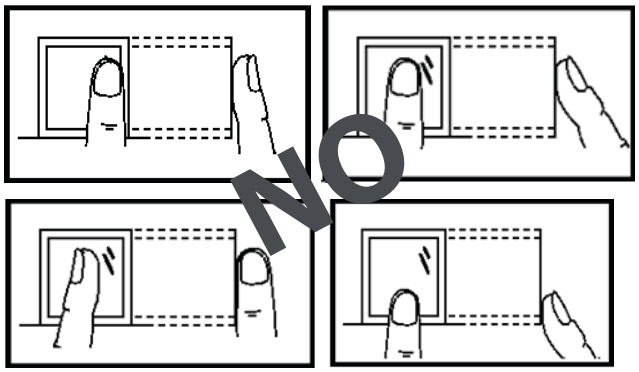
Nota: referencia iluminación valor de la fuente de luz ambiental

1.2 Método de pulsación de huella digital

Se recomienda utilizar el dedo índice, dedo medio o dedo anular; Evite usar el pulgar o dedo meñique.
Pulse la huella dactilar en el sensor de huella, con la huella dactilar derecha en el centro del sensor.



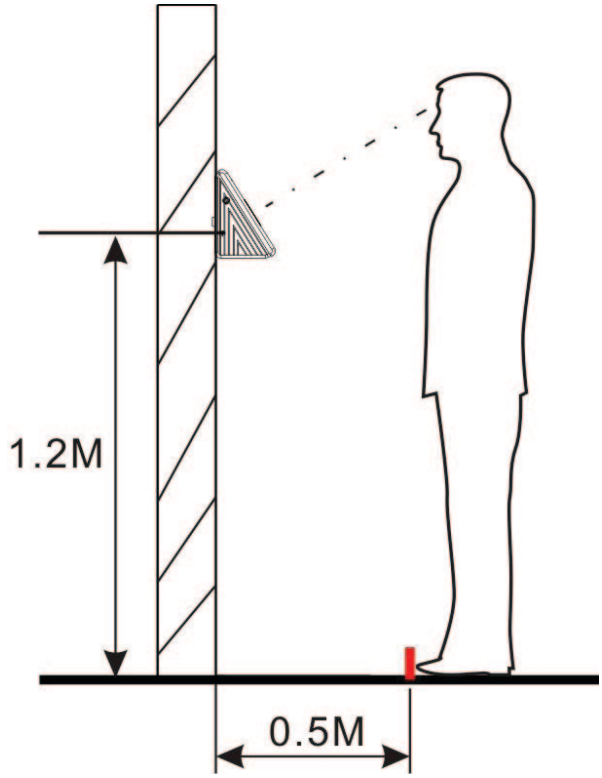
SÍ



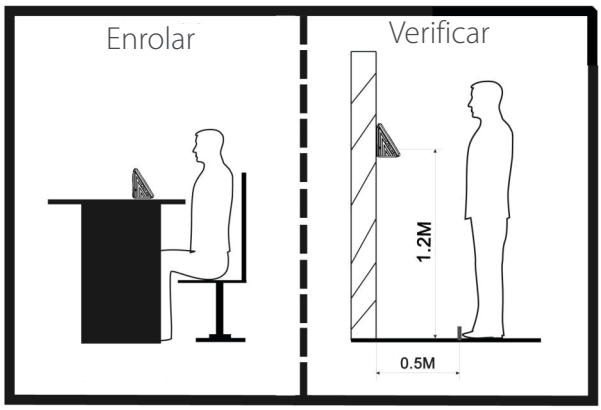
1.3 Posición de pie, expresión facial y postura

1. Posición de pie, expresión facial y postura

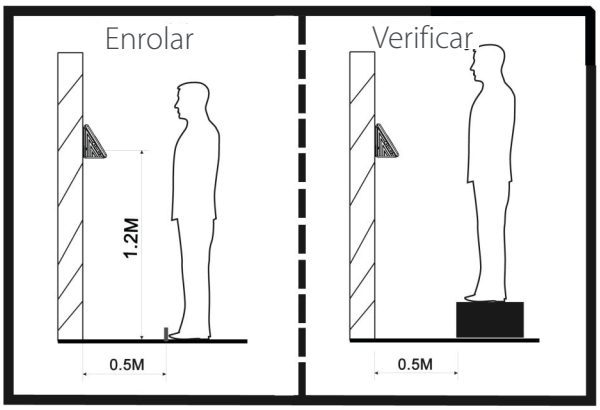
La distancia entre una persona y el dispositivo se recomienda para ser 0,5 metros (altura aplicable varían desde 1,5-1,8 metros). La distancia se puede ajustar basándose en el efecto de imagen facial capturada por el dispositivo.



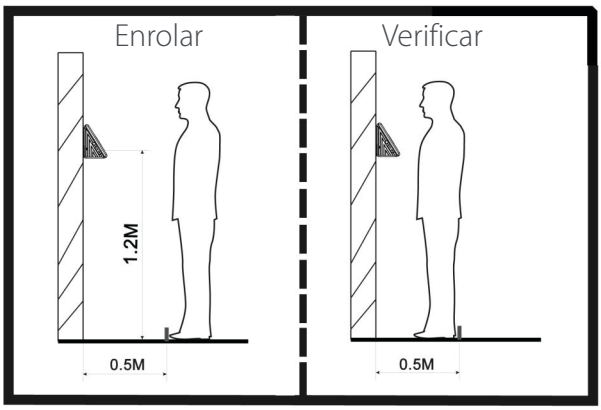
Varios métodos de aplicación que afectan el efecto de reconocimiento



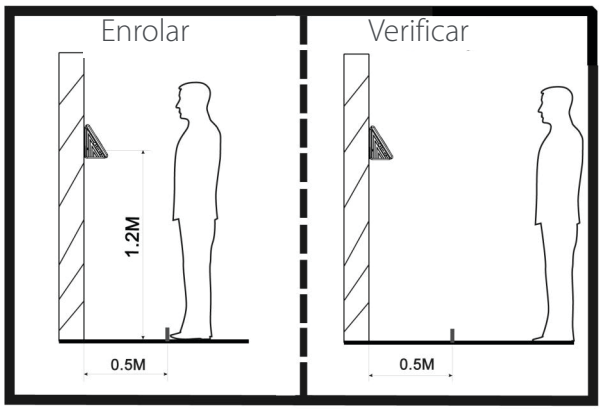
Demasiado alto



Herramienta a bajo

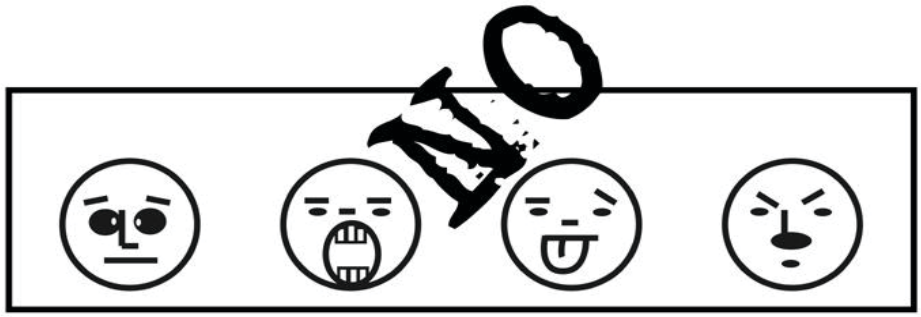


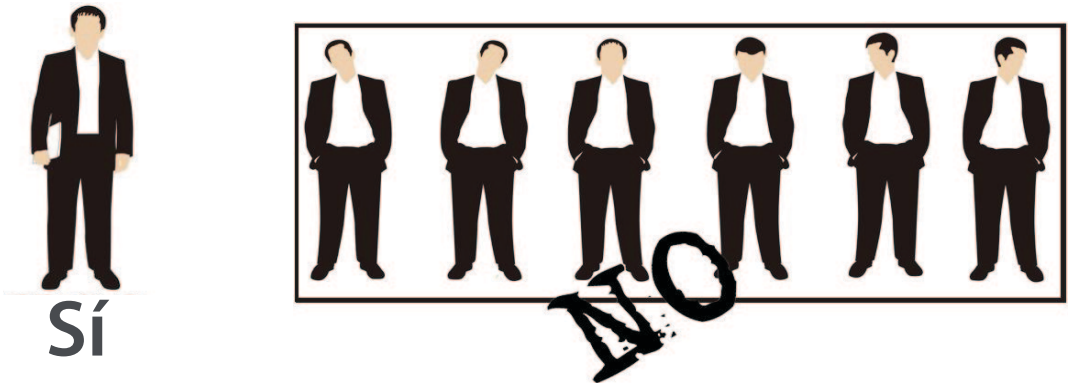
Demasiado cerca



Demasiado lejos

2. Expresión facial y postura





Nota: Durante el enrolamiento y verificación, mantener la expresión facial y postura natural.

Durante el enrolamiento, tiene que mover hacia adelante o hacia atrás para asegurarse de que sus ojos están dentro del marco verde.

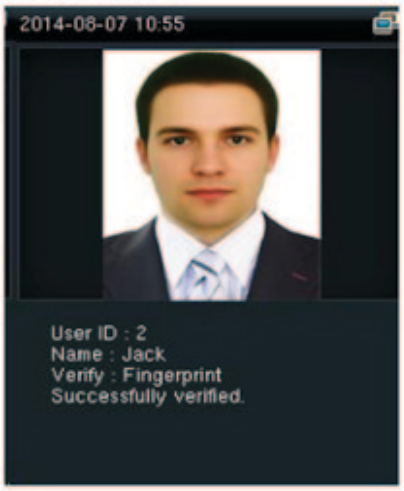
En comparación, asegúrese de que la cara se muestra en el centro de la pantalla y está dentro del marco verde.

1.4 Modos de Verificación

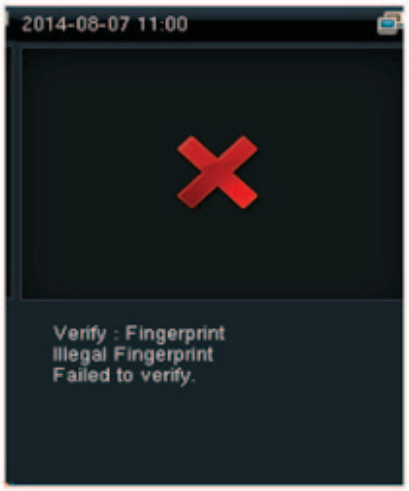
1.4.1 1: N verificación de huellas dactilares

Bajo este método de verificación de huellas dactilares, una huella dactilar recogida por el sensor se verifica con todas las huellas digitales almacenados en el dispositivo.

Por favor use la forma correcta para presionar la huella dactilar en el sensor de huellas dactilares (para la instrucción detallada, consulte *1.2 método de pulsación de huella dactilar.*



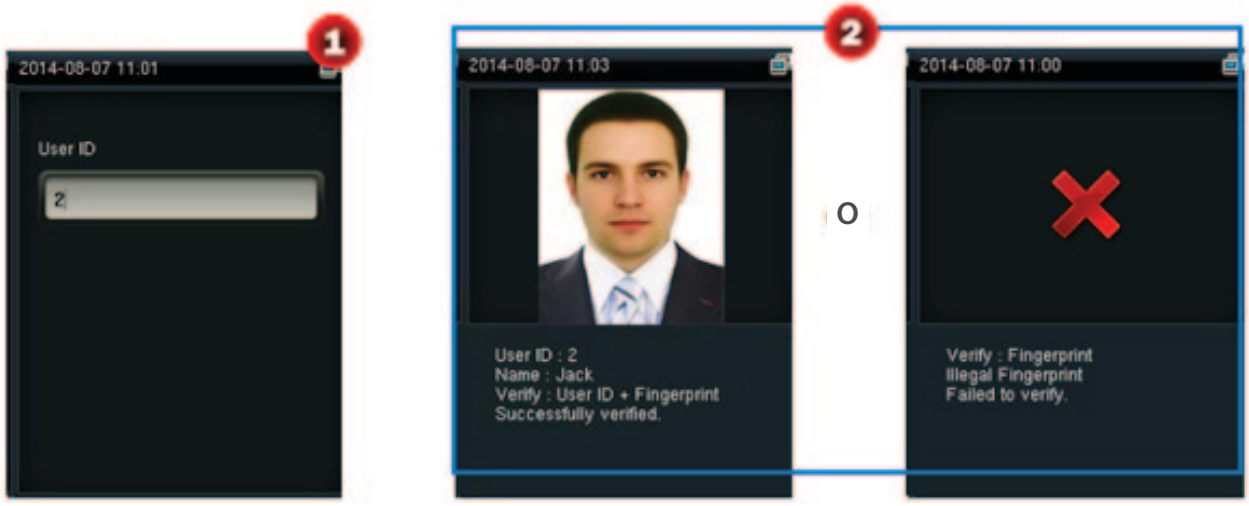
Verificación exitosa



Verificación fallida

1.4.2 1:1 la verificación de la huella digital

Bajo este método de verificación de huellas dactilares, una huella dactilar recogida por el sensor se verifica con la huella digital correspondiente al ID de usuario introducido. Por favor, use este método cuando la dificultad se encuentra en 1: N verificación de huellas dactilares.



Introduzca el ID de usuario y pulse [M/OK] "huella digital" y pulse [M/OK]. Presione el dedo sobre el sensor después.

Verificación Exitosa

Verificación Fallida

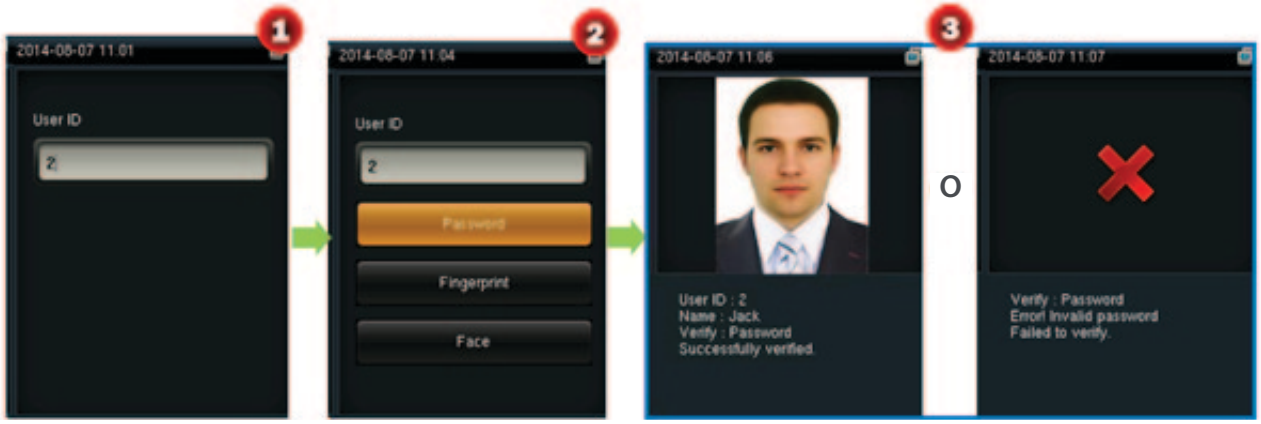
Observaciones:

1. ID de usuario de Entrada en la interfaz inicial y pulse el botón [M/OK]. Si "ID DE usuario Incorrecto" se muestra, esto significa que el ID de usuario no existe.

2. Cuando el dispositivo muestra "Presione el dedo otra vez" Presione el dedo de nuevo en el sensor de huellas dactilares. Si la verificación sigue fallando después de 2 intentos, saldrá a la interfaz inicial.

1.4.3 verificación de Contraseña

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



Introduzca el ID de usuario y pulse [M/OK]

Elija "Contraseña" y pulse [M/OK]

Verificación Exitosa

Error de Verificación

1.4.4 1: N Asistencia basada en la cara

Comparar la imagen facial capturada por la cámara con todos los datos faciales en el dispositivo.

Comparación de la conducta de la forma correcta en la interfaz principal.

Verificación aprobada.

1.4.5 1:1 Asistencia basada en la cara

Comparar la imagen facial capturada con la imagen facial asociada con el ID de usuario introducido.

Introduzca el ID de usuario en la interfaz principal utilizando el teclado y pulse [M/OK].

Seleccione [Cara] y pulse [M/OK].

Comparar las caras de la manera correcta.

Verificación aprobada

2. Menú principal

Cuando el dispositivo está en modo de espera, pulse [M/OK] para abrir el menú principal.

Funciones del menú principal se describen de la siguiente manera:

el usuario Mgt: para agregar, ver y administrar la información de usuario, incluyendo el ID de usuario, permiso, modo de verificación, huellas dactilares, cara, contraseña, Foto del usuario, y derechos de control de acceso, y para agregar, editar y eliminar información personal básica.

Rol de usuario: para configurar las funciones de usuario para acceder al menú y cambiar la configuración.

Comunicación: para establecer los parámetros relacionados de la comunicación entre el dispositivo y su PC, incluyendo parámetros Ethernet tales como dirección IP, Comunicación serial, PCconnection y configuración Wiegand.

Sistema: para establecer parámetros relacionados con el sistema para satisfacer las necesidades de los usuarios hasta el punto máximo en términos de funciones, pantalla y otros, incluyendo la hora del sistema, fecha, parámetros de asistencia, se enfrentan a parámetros, parámetros de huellas digitales, los ajustes de fábrica restauración y actualización basado en disco USB.

Personalizar: Esto incluye pantalla de interfaz, voz, bell, sacador modo clave del estado y la tecla de acceso rápido.

Datos Mgt: administrar datos en el dispositivo, por ejemplo, para eliminar registros de asistencia, todos los datos, funciones de usuario, y fotos de usuario, Borrar imágenes publicitarias, y una copia de seguridad y restaurar datos del dispositivo.

Control de acceso: para establecer el período de tiempo de acceso de usuario y los parámetros del bloqueo de control y dispositivo relacionado.

USB Manager: para cargar y descargar configuración de informes y descargar informes de asistencia. La información del usuario y los datos de asistencia en el dispositivo puede ser importado en software relacionado para el procesamiento, o la información de usuario se pueden importar en otros dispositivos de huellas dactilares a través de un disco USB.

Búsqueda de asistencia: La asistencia de búsqueda y funciones de búsqueda de excepciones permiten a los empleados para consultar registros y excepciones que se guardan en la deviceafter exitosa asistencia.

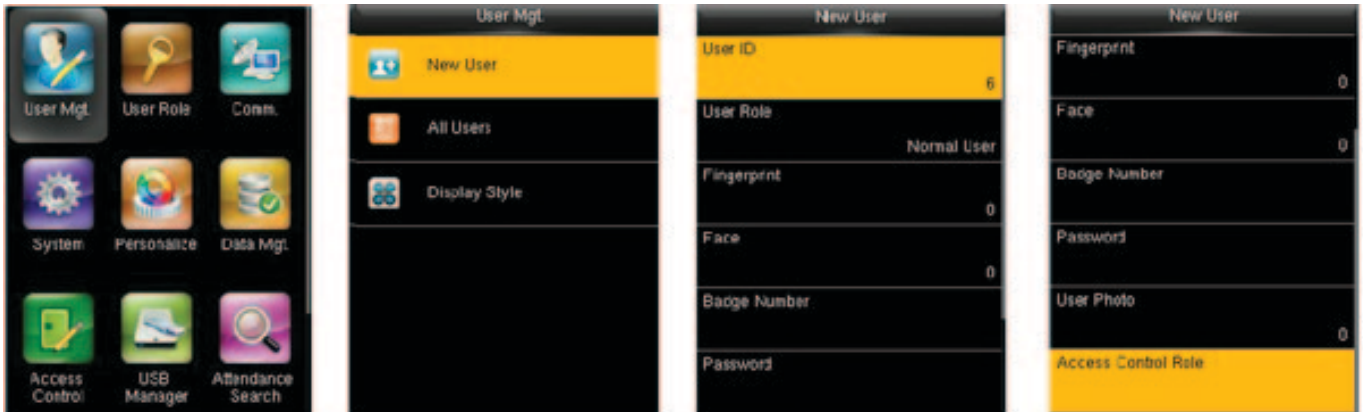
Autotest: para prueba automáticamente diferentes funciones del módulo, incluyendo el LCD, voz, teclado, sensor de huellas dactilares, cámara * y el reloj RTC prueba.

Información del sistema: para comprobar la capacidad del dispositivo, el dispositivo y firmware información.

3. Gestiones de usuarios

3.1 Agregar Usuario

La información básica de usuario en el dispositivo incluye el ID de usuario, el rol del usuario, modo de verificación, huellas dactilares, cara, número de placa, contraseña, Foto del usuario, y derechos de control de acceso. Los derechos de control de acceso incluyen el grupo perteneció, modo de verificación, si la presión se define la huella digital, y utilizar el período de tiempo. En la gestión de control de acceso de la empresa, operaciones tales como agregar, eliminar, consulta y modificación necesita llevarse a cabo en la información del personal en el dispositivo.

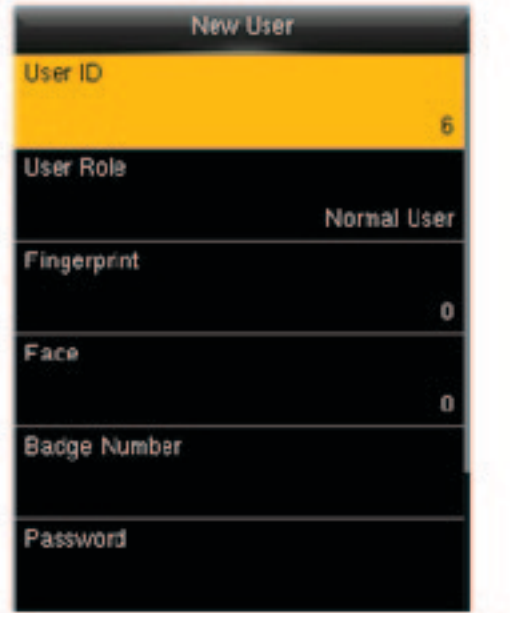


Pulse M/OK > Usuario Mgt. > nuevo usuario para acceder a la interfaz de agregar un usuario, en la que puede introducir un ID de usuario, seleccione un rol de usuario (usuario normal o superadministrador), registrar una huella digital, se registra un número de placa, establecer una contraseña, y establecer derechos de control de acceso.

En la interfaz inicial, pulse [M/OK] > Usuario Mgt. > nuevo usuario para ingresar el nuevo interfaz de configuración de usuario. Los ajustes incluyen la introducción de ID de usuario, Nombre, eligiendo el rol del usuario, registro de huellas dactilares y número de placa, establecer Contraseña y establecer la Función de Control de acceso.

3.1.1 Introducir un ID de usuario

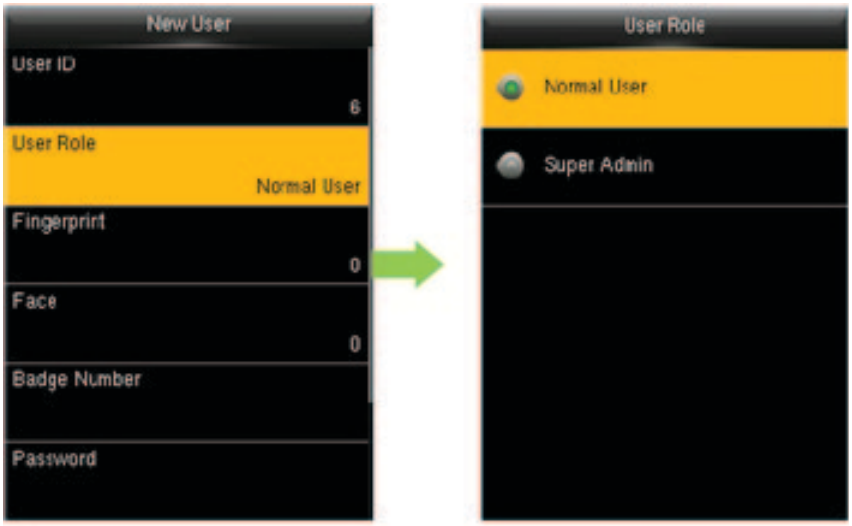
El dispositivo asigna automáticamente identificadores de usuario para el personal, a partir de 1 y así sucesivamente. El ID de usuario también puede introducirse manualmente.



Pulse para seleccionar la función de usuario y pulse M/OK.

Pulse/para seleccionar usuario Normal o Super Admin.

3.1.2 Configuración del rol de usuario

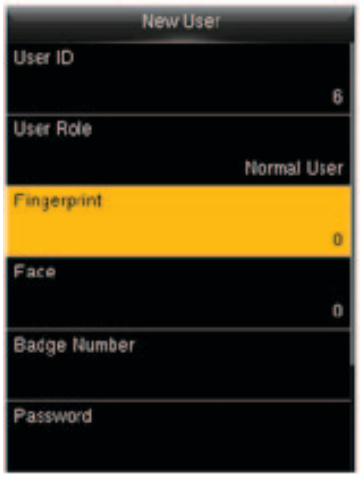


Pulse para seleccionar la función de usuario y pulse M/OK.

Pulse/para seleccionar usuario Normal o Super Admin.

Un superadministrador puede registrarse y salir mediante una huella digital, cara o contraseña y entrar en el menú. Un superadministrador tiene los permisos de operación sobre todos los elementos de menú. Un usuario normal puede registrarse y sólo mediante el uso de una huella digital, cara o contraseña.

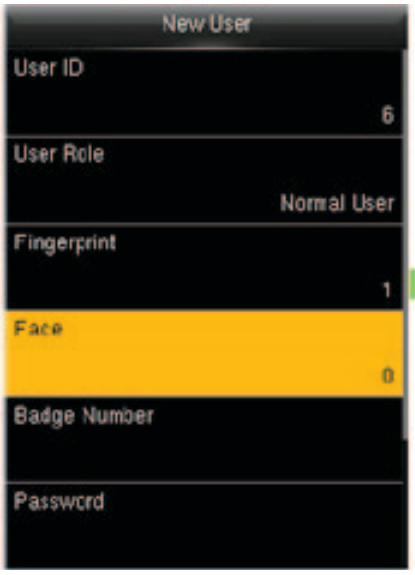
3.1.3 Registrar una huella digital



Pulse para seleccionar la huella digital y el registro tiene éxito. Pulse M/OK para la confirmación.

Presione el mismo dedo de la manera correcta de tres tiempos continuos hasta para el método de presionar una huella dactilar, ver 1,2 "Método de prensado huella digital". Si el registro falla, el dispositivo muestra una pronta y vuelve a la interfaz de registro de huellas dactilares. Repita la operación anterior.

3.1.4 Registrar una cara



Ver 1,3 "posición de pie, expresión Facial y Postura". Durante el registro de la cara, cuando el marco verde está en el medio, una foto del usuario se tomará automáticamente y se guarda en el dispositivo.

Pulse para seleccionar la cara y pulse M/OK para la confirmación.

Siga las instrucciones en el dispositivo para colocar los ojos en el marco verde hasta que el registro tiene éxito.

3.1.5 Registro de un número de tarjeta

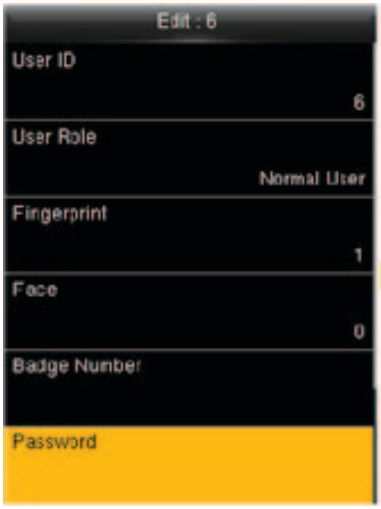
Pulse para seleccionar la tarjeta Pulse M/OK para la confirmación.

Deslizar la tarjeta ligeramente en el área de inducción hasta que el dispositivo detecta la tarjeta.

El dispositivo guarda y muestra el número de placa de lectura en la pantalla.

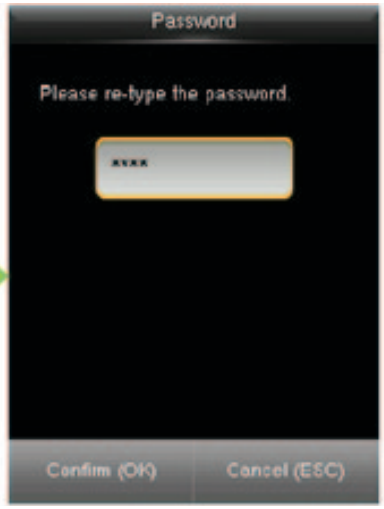
3.1.6 Registrar una Contraseña

El equipo soporta un 1-8 dígitos.



Pulse para seleccionar la contraseña y pulse M/OK para la confirmación.

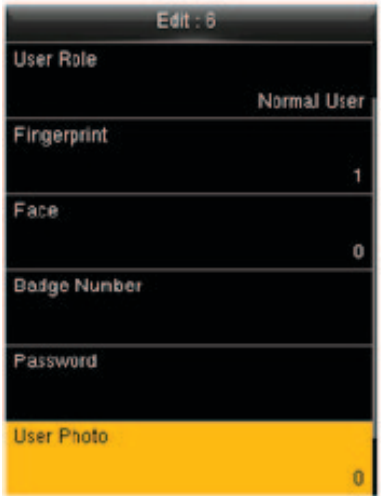
Use el teclado numérico para introducir una contraseña y pulse M/OK para la confirmación.

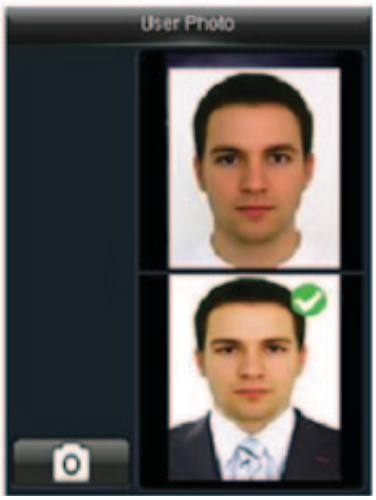


Volver a introducir la contraseña para confirmarla.

3.1.7 Registrar una foto

Cuando un usuario registrado con un retrato pasa la verificación, el retrato de usuario registrado se muestra además de información, como el ID de usuario y nombre.





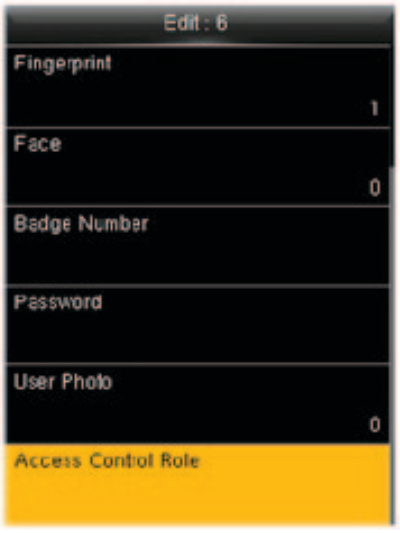
Cuando la foto tomada durante el registro facial se utiliza, no es necesario tomar la foto.

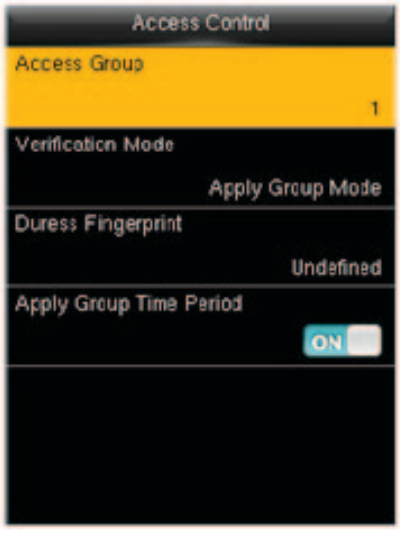
Pulse para seleccionar "foto del usuario" y pulse M/OK para la confirmación.

Párese frente a la pantalla de forma natural y pulse M/OK para tomar una foto.

3.1.8 Establecer derechos de control de acceso

Se puede establecer a qué grupo pertenece un usuario, accede al modo de verificación, ya sea para registrar una huella digital de coacción, y si se debe utilizar el período de tiempo de grupo. Por defecto, el desbloqueo se concede permiso a los usuarios recién inscritos.





Pulse para seleccionar la Función de Control de acceso y pulse M/OK.

Pulse/para seleccionar otro modo de verificación.

Grupo de acceso: seleccione el grupo pertenecía. Por defecto, anewly usuario inscrito pertenecen al grupo uno. Modo de verificación: Seleccionar un modo de verificación de usuario. Un total de 22 modos de verificación de usuario están soportados, incluyendo el modo de verificación de grupo, cara/huella/contraseña/placa, solo huella digital, sólo ID de usuario, contraseña, sólo placa, huella/contraseña, huella digital/placa, contraseña/placa, ID de usuario & huella digital, huella digital & password, contraseña & placa, huella digital & password & placa, contraseña & placa, ID de usuario & huella digital & password, huella digital & placa & ID de usuario sólo, cara, cara & fingerprint, cara & contraseña, cara & placa, cara & huella digital & placa y cara & huella digital & password.

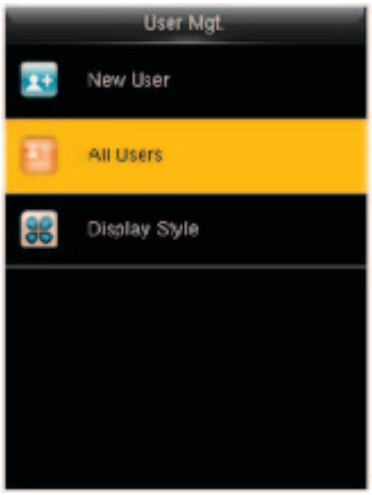
Coacción huella digital: Afingerprint registrado en el dispositivo está especialmente especificado como una huella de coacción. En cualquier caso, aduress alarma se genera cuando una huella digital coincide con una huella de coacción.

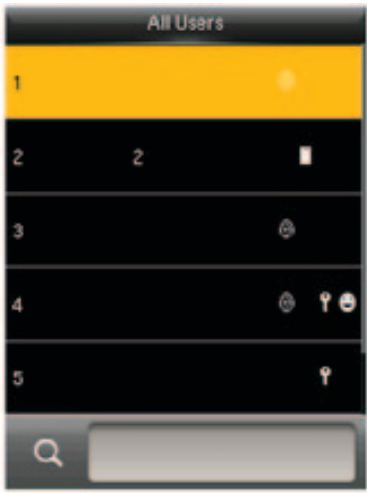
Aplicar Grupo período: el predeterminado valueis 1.

Nota: Para la configuración del grupo de control de acceso y el período de tiempo, ver 9 "Control de acceso".

3.2 Gestión de usuarios

Durante la gestión diaria de la empresa, cuando se produce un cambio del personal, la información del personal necesita ser actualizado en el dispositivo. Operaciones como usuario agregar, eliminar, consulta y modificación se puede realizar.



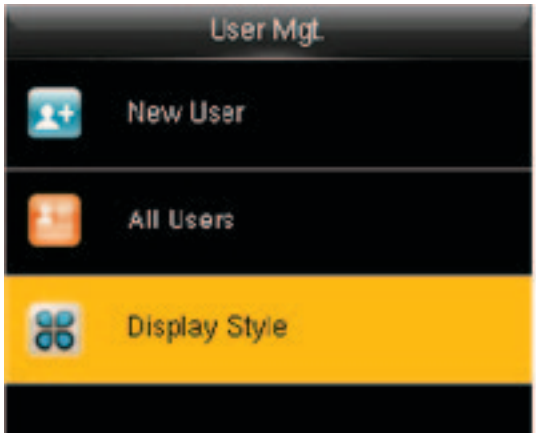


Consulta de un usuario: Introduzca un ID de usuario que se va a consultar en la lista de usuarios. El dispositivo localiza automáticamente al usuario con este ID de usuario.

Modificar la información de usuario: consulta para localizar a la persona cuya información del usuario necesita ser modificado y pulse M/OK para modificar la información de la persona.
Borrar un usuario: usted puede seleccionar para eliminar un usuario, borrar una huella digital solamente, eliminar una cara solamente, eliminar una contraseña única, o eliminar una foto del usuario solamente.

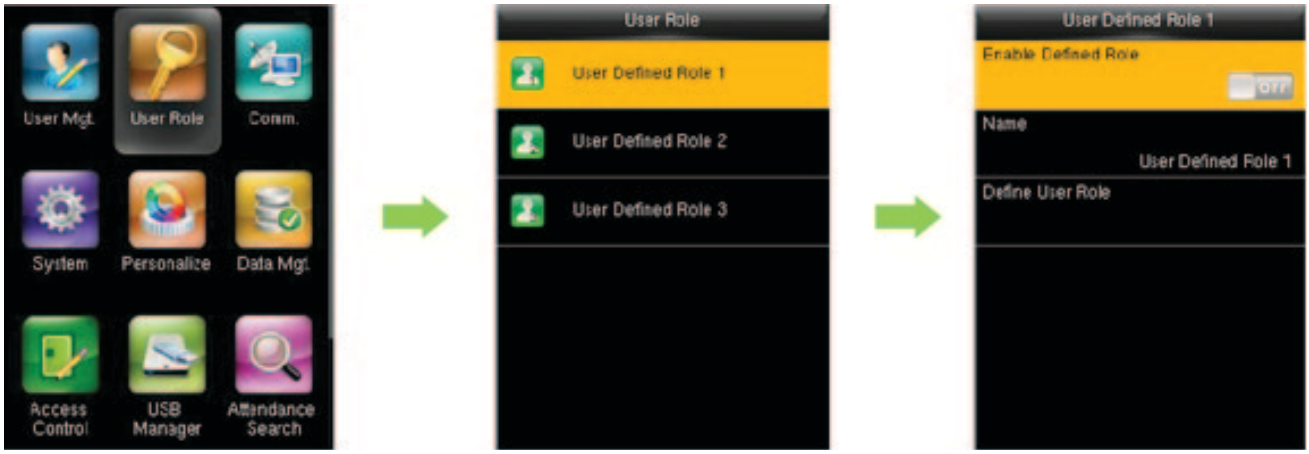
Estilo De Visualización

Seleccione el estilo de visualización de la lista de usuarios, incluyendo una sola línea, línea múltiple y línea mixta.



4. El rol del usuario

Establecer los permisos para un papel definido para realizar operaciones en el menú. Se pueden crear tres funciones a lo sumo.



Función de usuario de acceso desde el menú principal, habilitar un papel y asignar permisos. El nombre no puede ser, pero se puede cargar con software o un nombre predeterminado puede ser utilizado.

5. Configuración de comunicaciones

Establecer los parámetros relacionados con la comunicación entre el dispositivo y un PC sobre el Ethernet, incluyendo la dirección IP, gateway, mascara de subred, baudios, ID de dispositivo, y contraseña de conexión.

5.1 Configuración de Ethernet

Dirección IP: la dirección IP predeterminada es 192.168.1.201 y puede cambiar basado en los requisitos. Máscara de subred: La máscara de subred predeterminada es 255.255.255.0 y se pueden cambiar en base a requerimientos.

Gateway: La dirección del gateway predeterminado es 0.0.0.0 y puede cambiar basado en los requisitos.

DNS: La dirección DNS predeterminada es 0.0.0.0 y puede cambiar basado en los requisitos.

Puerto TCP comunicaciones: el valor predeterminado es 4370 y puede cambiar basado en los requisitos.

DHCP: este es el protocolo de configuración dinámica de Host, que utiliza el servidor para asignar direcciones IP dinámicas a los clientes de red.

Muestra el icono de red en la barra de estado: Establecer si se debe mostrar el icono de red en la barra de estado de la interfaz principal

5.2 Ajustes Serial Comm.

Cuando el dispositivo se comunica con un PC en modo serial (RS485), compruebe los siguientes ajustes: Baudrate: la tasa de la comunicación con un PC tiene cuatro opciones: 19200, 38400, 57600, y 115.200. Se recomienda utilizar 38400 para comunicación RS485.

Nota: Cuando el lector 485 función está habilitada en la gestión de control de acceso y la comunicación RS485 aquí también está habilitado, se mostrará un mensaje indicando que el dispositivo tiene que ser reiniciada para la configuración surta efecto.

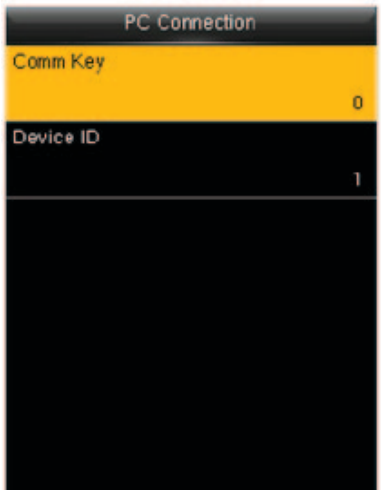
5.3 Ajuste de conexión

Para mejorar la seguridad de datos, Comunicaciones Clave para la comunicación entre el dispositivo y su PC debe ser ajustado.

Si una Llave de comunicación se establece en el dispositivo, la contraseña de conexión correcta debe ser introducido cuando el dispositivo está conectado al software de PC, para que el dispositivo y el software se puede comunicar.

Clave de comunicaciones: la contraseña predeterminada es 0 (sin contraseña) y puede ser fijado a otro valor. Después de establecer, esta contraseña se debe introducir para la comunicación entre el software y el dispositivo. De lo contrario, la conexión falla. Comunicaciones Keycan ser 1 ~ 6 dígitos.

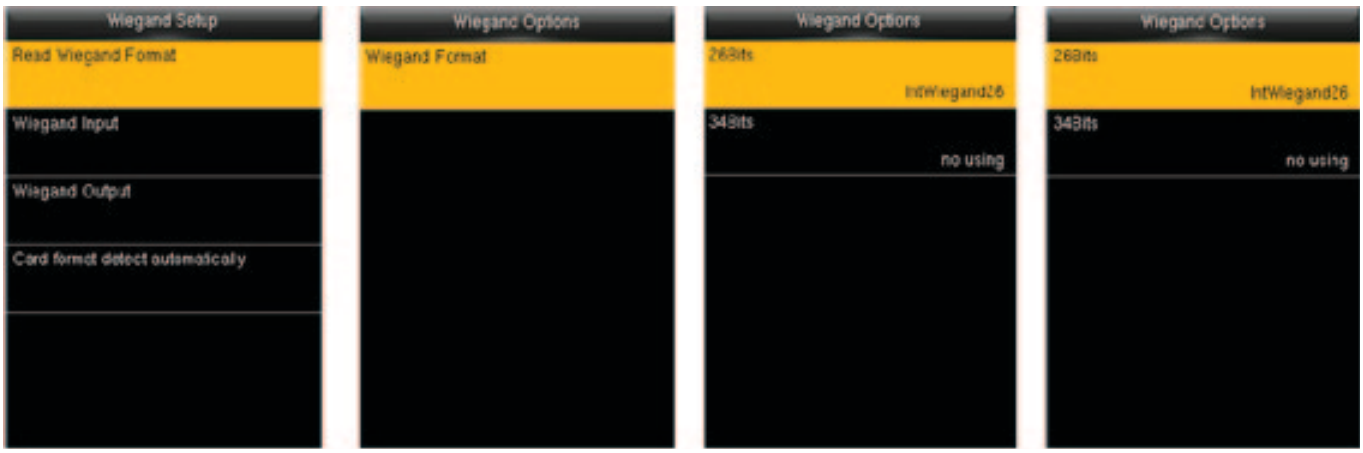
ID del dispositivo: el dispositivo rangos de ID de 1 a 254. Si el método de comunicación es RS485, introducir este ID de dispositivo en la interfaz de comunicación de software se requiere.



5.4 Configuración Wiegand

5.4.1 Ajuste del formato de tarjeta para el dispositivo

Establecer los formatos de comunicación Wiegand el módulo tarjeta interna y dispositivo Wiegand externo.



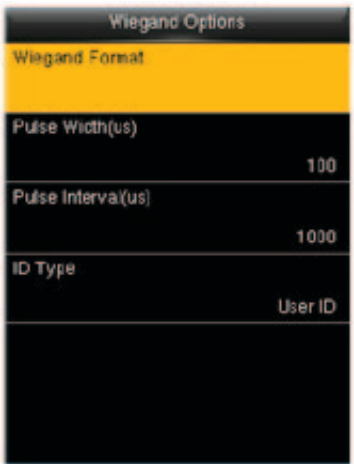
Establecer el formato Wiegand coincida con el módulo de la tarjeta del dispositivo. Después de un formato unificado de Wiegand se utiliza, la tarjeta correcta numberscan ser leída. El formato Wiegand puede ajustarse a IntWiegand26, IntWiegand26a, IntWiegand34, o IntWiegand34aso que los números de la tarjeta leída por el dispositivo están en el formato preestablecido.

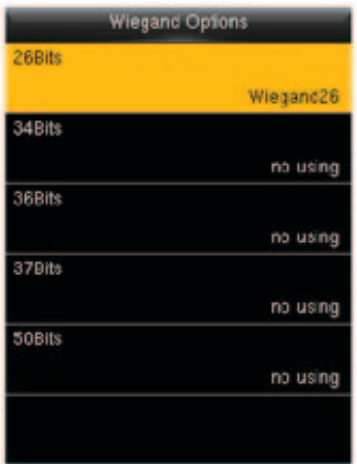
Formato Wiegand	Descripción
IntWiegand26	ECCCCCCCCCCCCCCCCCCCCCCO Esta está compuesta por 26 números binarios, con poco 1 siendo la paridad incluso comprobar poco para bits 2-13
IntWiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Esta está compuesta por 26 números binarios, con bit1 siento la paridad incluso comprobar poco para bits2-13, bit26 siendo la paridad impar cheque por bits14-25, bits2-9 siendo el código de área y bits10-15 siendo el número de tarjeta
IntWiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Este se compone de 34 números binarios, con bit1 siendo la paridad incluso comprobar poco para bits2-17 y bit34 ser la comprobación de paridad impar bit para bits 18-33 y bits2-15 siendo el número de tarjeta
IntWiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Este se compone de 34 números binarios, con bit1 siendo la paridad incluso comprobar poco para bits2-17, bit34 ser la comprobación de paridad impar bit para bits 18-33, bits2-9 siendo el código de área y bits10-15 siendo el número de tarjeta

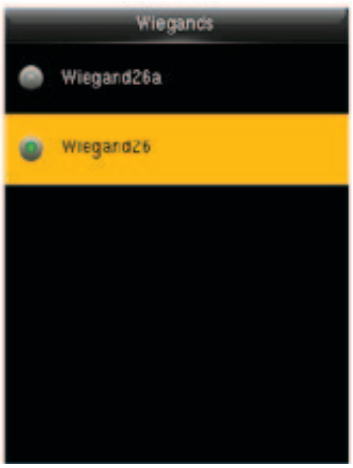
Nota: C representa el número de tarjeta, E está parada para comprobación de paridad par, y O representa la comprobación de paridad impar.
Nota: este artículo está disponible para la máquina de tarjetas de identificación pero no MF máquina de tarjeta.

5.4.2 Entrada Wiegand

Establecer el formato Wiegand de un lector conectado externamente







Formato Wiegand: los usuarios pueden elegir entre los siguientes formatos: Wiegand incorporado Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a y Wiegand 50, en la que no significa usar el formato con este número de bit no se utiliza. La tabla siguiente se describen todos los formatos.

Ancho de pulso (nosotros): el ancho del pulso enviado por Wiegand. El valor predeterminado es 100 microsegundos, que se puede ajustar dentro de la gama de 20 a 100 microsegundos.
Intervalo de pulso (nosotros): el valor predeterminado es 1000 microsegundos, que se puede ajustar dentro del rango de 200 a 20000 microsegundos.

Tipo ID: entrada contenido incluido en la señal de entrada Wiegand. ID de usuario o número de placa puede ser elegido.

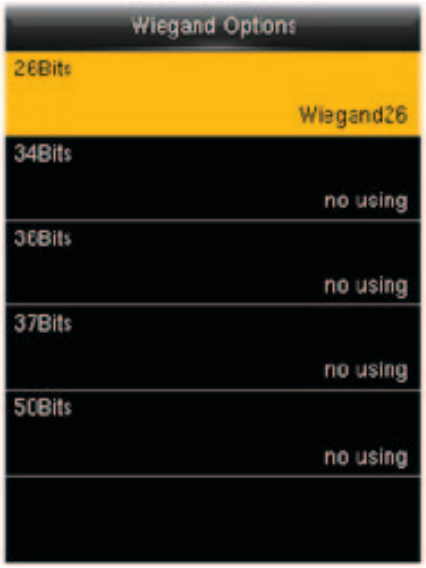
Definiciones de Formatos Wiegand:

Formato Wiegand	Descripción
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El primer bit es el bit de paridad del 2 al 13 bits, mientras que el 26 bit es el bit de paridad impar del 14 al 25 bit. El segundo de 25 bits son el número de tarjeta
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El primer bit es el bit de paridad del 2 a 13 bits, mientras que el 26 bit es el bit de paridad impar del 14 al 25 bits. El segundo a 9 bits son el código del sitio, mientras que el 10 a 25 bits son el número de tarjeta.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El primer bit es el bit de paridad del 2° a 17 bits, mientras que el 34 bit es el bit de paridad impar del 18 a 33 bits. El 2 al 25 bit es el número de tarjeta.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario., El primer bit es el bit de paridad del 2 º a 17 bits, mientras que el 34 bit es el bit de paridad impar del 18 a 33 bits. El segundo a 9 bits son el código de sitio, mientras que el 10 a 25 bits son el número de tarjeta.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El primer bit es el bit de paridad impar del 2 a 18 bits, mientras que el 36 bit es el bit de paridad incluso el 19 de 35 bits. El segundo a 17 bits son el código del dispositivo, el 18 de 33 bits son el número de tarjeta, y el 34 a 35 bits son el código del fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consta de 36 bits de código binario. El primer bit es el bit de paridad del 2 a 18 bits, mientras que el 36 bit es el bit de paridad impar del 19 al 35 bits. El segundo a 19 bits son el código del dispositivo, y el 20 a 35 bits son el número de tarjeta
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE Consta de 37 bits de código binario. El primer bit es el bit de paridad impar del 2 a 18 bits, mientras que el 37 es el bit incluso bit de paridad del 19 a 36 bits. El segundo a 4 bits son el código del fabricante, el 5 de 16 bits son el código de sitio, y el 21 a 36 bits son el número de tarjeta.

Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCO Consta de 37 bits de código binario. El primer bit es el bit de paridad del 2 a 18 bits, mientras que el 37 bit es el bit de paridad impar del 19 al 35 bits. El segundo a 4 bits son el Código fabricante, 5 a 14 bits son el código del dispositivo, del 15 al 20 bits son el código de sitio, y el 21 a 36 bits son el número de tarjeta.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 50 bits de código binario. El primer bit es el bit de paridad del 2 a 25 centavos, mientras que el 50 es la paridad impar poco del 26 a 49 bits. El segundo a 17 bits son el código de sitio, y 18 a 49 bits son el número de tarjeta.

Nota: C denota el número de tarjeta, E incluso denota el bit de paridad, denota odd bit de paridad, F denota el código del dispositivo, M denota Código fabricante, P denota el bit de paridad, y S denota el código de sitio.

5.4.3 salida Wiegand



Formato Wiegand: Userscan seleccionar los formatos Wiegand estándar construido en el sistema. Ver las definiciones de todo tipo de formatos Wiegand general en 5.4.2 "Entrada Wiegand". Aunque varias opciones son compatibles, el formato real está determinado por los bits de salida Wiegand.

Salida Wiegand bits: la longitud del bit de datos Wiegand. Después de la salida Wiegand bitsis set, el devicewill encontrar el formato Wiegand de este número de bits en formato Wiegand.

Por ejemplo, si Wiegand26, Wiegand34a, Wiegand36, Wiegand37a y Wiegand50are seleccionado para formato Wiegand, pero salida Wiegand bitsis set to36, el formato Wiegand36 36 bits será adoptada finalmente.

Error ID: se define como el valor de salida de verificación de usuario fallido. El formato de salida depende del [formato Wiegand]. El valor predeterminado varía desde 0 a 65535.

Código de sitio: es similar a la identificación del dispositivo, excepto que puede ajustarse manualmente y repetible con diferentes dispositivos. El valor predeterminado varía de 0 a 256.
Ancho de pulso (μs): el ancho del pulso enviado por Wiegand. El valor predeterminado es 100 microsegundos, que se puede ajustar dentro de la gama de 20 a 100 microsegundos.

Intervalo de pulso (µs): el valor predeterminado es 1000 microsegundos, que se puede ajustar dentro del rango de 200 a 20000 microsegundos.

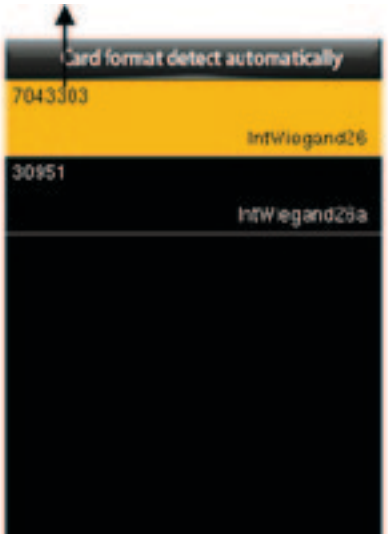
Tipo ID: contenido de salida después de la verificación exitosa. ID de usuario o número de tarjeta puede ser elegido.

5.4.4 Formato de tarjeta Detecta Automáticamente

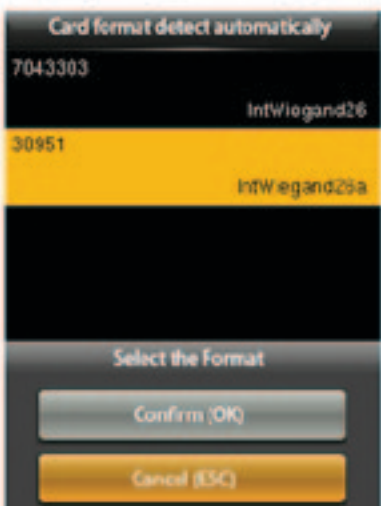
[Formato de tarjeta Detecta Automáticamente] tienen por objeto ayudar al usuario con rápidamente detectar el tipo de tarjeta y su formato correspondiente. Varios formatos de tarjetas han sido programados en el dispositivo. Después de deslizar la tarjeta, el sistema lo detectará como números de tarjetas diferentes según cada formato; el usuario sólo requiere para elegir el elemento equivalente al número de tarjeta real, y establecer el formato como el formato Wiegand para el dispositivo. Esta función también es aplicable a la función de lectura de la tarjeta y el lector Wiegand auxiliar.

Después de entrar en detección automática, desliza la placa en el área de birlar la tarjeta (en el dispositivo, o lector).

Número de tarjeta obtenida basado en el formato IntWiegnad26 análisis.



El formato Wiegand y se analiza el número de la tarjeta se detecta automáticamente.



Seleccione el número consistente con el número de tarjeta real, y el formato correspondiente es el formato Wiegand que debe ser seleccionado para la lectura de este tipo de tarjeta.

6. Configuración del sistema

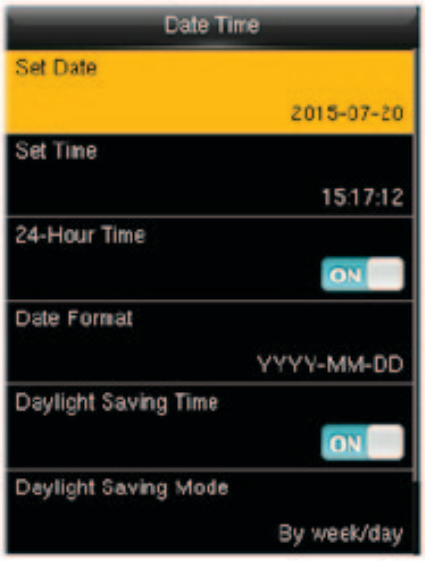
Establecer parámetros relacionados con el sistema para satisfacer las necesidades de los usuarios hasta el punto máximo en términos de funciones, pantalla y otros, incluyendo la hora y fecha, parámetros de asistencia, y parámetros de huellas dactilares.

6.1 La hora y la fecha

Establecer fecha y hora establecida: defina la fecha y la hora para el dispositivo.

24 horas: Establecer el modo de visualización del tiempo en el maininterface. Cuando está activado, el tiempo se muestra en el sistema de 24 horas; cuando está desactivado, el tiempo se muestra en el sistema de 12 horas.

Formato de fecha: establecer las fechas formatof aparece en todas las interfaces del dispositivo.



Horario: El horario de verano o DST, es un sistema que artificialmente estipula hora local para el ahorro de energía. El tiempo unificado utilizado durante la implementación de este sistema se llama horario de verano. En verano cuando el amanecer es temprano, el tiempo se fija generalmente una hora por delante artificialmente para que la gente dormir y levantarse temprano, lo que reduce el consumo de iluminación y hace el uso completo de la luz solar recurso para ahorrar potencia de iluminación.

Cuando llega el otoño, el tiempo es un retroceso. Los países que adoptan el horario de verano tienen diferentes disposiciones específicas.

Con el fin de cumplir con los requisitos de horario de verano, el dispositivo está especialmente modificado para requisitos particulares con una característica que establece la hora una hora por delante a XX: XX en día XX de mes XX y establece el tiempo de vuelta a XX: XX en día XX de mes XX.

Instrucciones de operación: Establecer el horario de verano.

2) Introduzca la hora de inicio y finalización de DST.

Por ejemplo, el dispositivo está configurado para empezarlo en 8:00 1 de abril y el tiempo se establece una hora por delante; el dispositivo se reanuda el tiempo normal en 8:00 1 de octubre.

3) Pulse OK para guardar el ajuste. Presione ESC para salir sin guardar.

Habilitar DST

Modo de conversión de DST ajuste de tiempo en modo fecha

Ajuste del tiempo en modo semana

Modo de ahorro de luz: El modo fecha (mes-día-hora) (predeterminado) o modo semana (mes-semana-hora) puede ser seleccionado.

Configuración de ahorro de luz: ajustar la hora de inicio y finalización de DST.

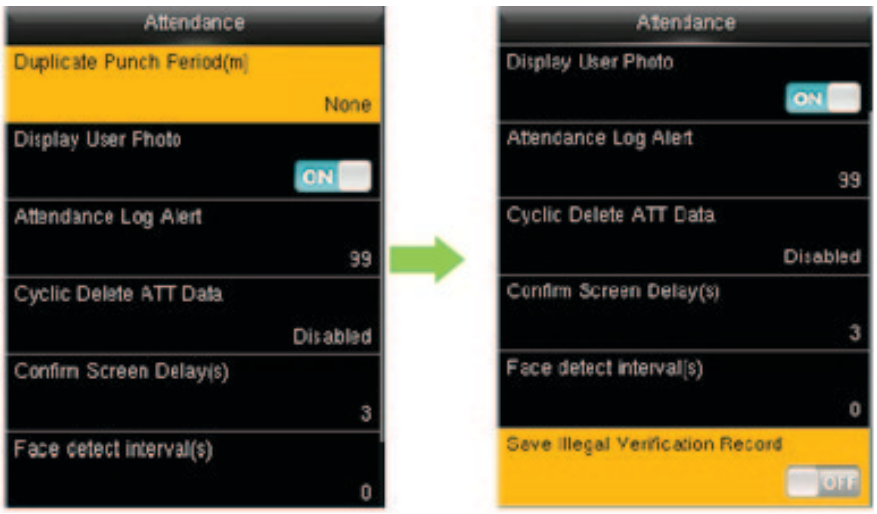
El modo fecha y semana modeare descrito como sigue:

1. Si el mes de inicio DST está dispuesto a ser más tarde de la DST mes final, el DST mes final es en el año próximo del mes de inicio DST. Por ejemplo: El DST empieza en 4:00, 2012-9-1, y termina en 4:00, 2013-4-1.

2. En modo semana, supongamos que el día de inicio DST se establece en el sexto domingo de septiembre, y el año actual es 2012, pero el calendario muestra que Septiembre de 2013 tiene cinco no seis semanas. En este caso, el sistema se inicia DST en la hora correspondiente en el último domingo de este mes.

3. Asumir que el día de inicio DST se establece en el lunes de la primera semana de septiembre, y el año actual es 2012, pero el calendario muestra que la primera semana de septiembre no tiene el lunes. En este caso, el sistema localiza automáticamente el primer lunes de este mes.

6.2 Parámetros de asistencia



Período de checado: dentro de un período de tiempo definido (unidad: minutos), los registros de asistencia duplicados no serán reservados (valor varía desde 1 a 999.999 minutos).

Mostrar la foto del usuario: indica si se debe mostrar foto de usuario cuando el usuario pasa el cheque de asistencia.

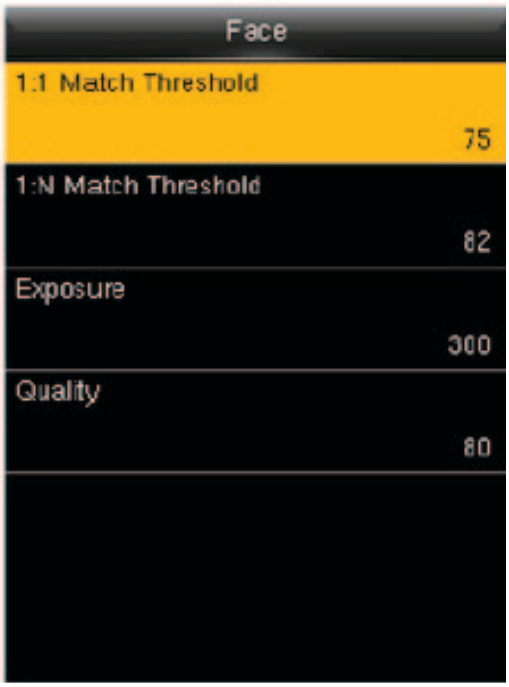
Registro de asistencia alerta: cuando el almacenamiento restante es menor que el valor determinado, el dispositivo se Alerte automáticamente a los usuarios la información de almacenamiento restante. Puede ser desactivado o ajustado a un valor osciló de 1 a 9999.

Cíclico Eliminar Datos ATT: el número de registros de asistencia permite ser borrado en un momento en que el almacenamiento máximo es alcanzado. Puede ser desactivado o ajustado a un valor osciló de 1 a 999.

Intervalo de Detección de cara: establecer el intervalo timebetween comparaciones por la misma cara.

Guardar Registro de verificación Ilegal: para establecer si falló verificaciones, tales como los causados por el acceso en Horarios no válida o ilegal Verificación Combinada, se salvarán cuando la función de control de acceso avanzado está activada.

6.3 Parámetros de Cara



1:1 Partido Umbral: la similitud con la cara plantilla registrada en el dispositivo en modo de verificación 1:1. Cuando la similitud es mayor que este valor, concordando tiene éxito. De lo contrario, concordando falla. El valor válido está en el rango de 70-120. Cuanto mayor sea el umbral se fija, cuanto menor es el juicio erróneo, que conduce a una mayor tasa de rechazo, y viceversa.

1:1: N Match Umbral: la similitud con la cara plantilla registrada en el dispositivo 1: N modo de comparación. Cuando la similitud es mayor que este valor, concordando tiene éxito. De lo contrario, concordando falla. El valor válido está en el rango de 80-120. Cuanto mayor sea el umbral se fija, cuanto menor es el juicio erróneo, que conduce a una mayor tasa de rechazo, y viceversa.

Umbrales recomendados:

Rechazo de error	Tasa de error	Umbral de coincidencia	
		1:N	1:1
Alto	Bajo	85	80
Mediano	Mediano	82	75
Bajo	Alto	80	70

Exposición: para establecer el valor de exposición de la cámara, 300 por defecto.

Calidad: el umbral de calidad para la adquisición de la imagen facial. Cuando la calidad de una imagen es mayor que este valor, el dispositivo recibe esta imagen facial y comienza el procesamiento de algoritmo. De lo contrario, los filtros de dispositivo esta imagen facial. El valor predeterminado es 80 (dentro de 50-150).

Nota: los ajustes Incorrectos de exposición y Calidad afectar seriamente el efecto de servicio del dispositivo. Si necesita ajustar los parámetros, por favor, siga las instrucciones de nuestro personal de servicio post-venta para operaciones.

6.4 Parámetros de huellas dactilares

1:1 Partido Umbral: Bajo 1:1 método de verificación, sólo cuando la similitud entre la verificación de huella digital y huella dactilar registrada del usuario es mayor que este valor puede la verificación éxito.

1: N Match Umbral: Bajo 1: N método de verificación, sólo cuando la similitud entre la verificación de huella digital y todas las huellas dactilares registradas es mayor que este valor puede la verificación éxito.

Umbral De Fósforo Recomendados:

Rechazo de error	Tasa de error	Umbral de coincidencia	
		1:N	1:1
Alto	Bajo	45	25
Mediano	Mediano	35	15
Bajo	Alto	20	10

FP la sensibilidad del Sensor: para ajustar la sensibilidad de la colección de huellas dactilares. Se recomienda utilizar el nivel predeterminado "medio". Cuando el ambiente está seco, resultando en la detección de huellas dactilares lenta, puede establecer el nivel de "alto" para elevar la sensibilidad; Cuando el ambiente es húmedo, por lo que es difícil identificar la huella digital, puede establecer el nivel a "bajo".

1:1 Retry Veces: En 1:1 verificación o verificación de la Contraseña, los usuarios pueden olvidar la huella dactilar registrada o contraseña, o presione el dedo incorrectamente. Para reducir el proceso de volver a entrar en ID de usuario, retry se permite; el número de reintentos puede estar dentro de 1 ~ 9.

Imagen de la huella digital: para establecer si se debe mostrar la imagen de la huella digital en la pantalla de registro o verificación. Cuatro opciones están disponibles: Mostrar para inscribirse, espectáculo para el partido, Mostrar siempre, Ninguno.

6.5 Restablecer a los ajustes de fábrica

Restablecer datos como la configuración de la comunicación y la configuración del sistema a la configuración de fábrica.

Observaciones: cuando el restablecimiento de la configuración de fábrica, la fecha de usuario y los registros de asistencia no serán afectados.

6.6 actualizaciones USB

Esta opción permite que el dispositivo firmware para ser actualizado con el archivo de actualización en un disco USB.

Si el archivo de actualización se necesita, por favor póngase en contacto con soporte técnico fuera. Actualización del firmware no se reanudó en circunstancias normales.

La actualización con un disco USB es posible sólo para las máquinas que apoyan la función de disco flash USB.

7. Personalizar Configuración

7.1 Configuración de la interfaz de usuario

Los usuarios pueden personalizar el estilo de visualización de la interfaz principal basada en su preferencia personal.

Fondo de pantalla: Seleccione el fondo de pantalla principal como sea necesario, usted puede encontrar fondos de varios estilos en el dispositivo.

Idioma: Seleccione el idioma del dispositivo según sea necesario.

Pantalla de menú Timeout (s): cuando no hay operación en la interfaz de menú y el tiempo excede el valor determinado, el dispositivo saldrá automáticamente a la interfaz inicial. Puedes desactivarlo o establecer el valor a 60 ~ 99999 segundos.

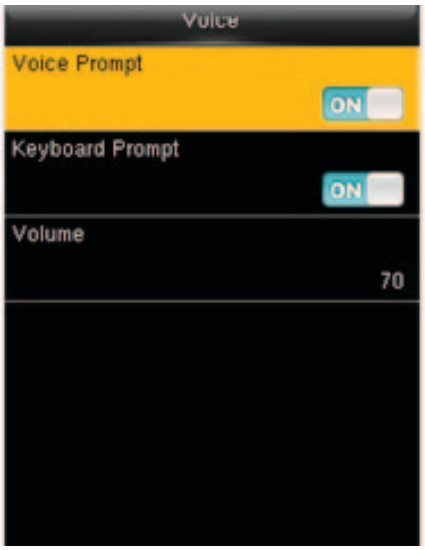
Tiempo de inactividad Para Diapositivas (s): cuando no hay operación en la interfaz inicial y el tiempo excede el valor determinado, una presentación con diapositivas aparecerá. Puede ser desactivado (ajustada a "ninguno") o ajustado a 3 ~ 999 segundos.

Intervalo de diapositivas (s): esto se refiere al intervalo entre mostrar diferentes imágenes de diapositivas. Puede ser desactivado o ajustado a 3 ~ 999 s.

Tiempo de inactividad para dormir: cuando no hay operación en el dispositivo y el tiempo de sueño es alcanzado, el dispositivo entrará en modo de espera. Pulse cualquier tecla o dedo para cancelar el modo de espera. Puede desactivar esta función, o establecer el valor a 1 ~ 999 minutos. Si esta función se da vuelta a **[deshabilitado]**, el dispositivo no entrará en modo de espera.

Pantalla principal estilo: Elegir la posición y formas del reloj y el estado clave.

7.2 Configuración de voz



Mensaje de voz: Seleccione si desea habilitar los mensajes de voz durante el funcionamiento, pulse [M/OK] para activarlo.

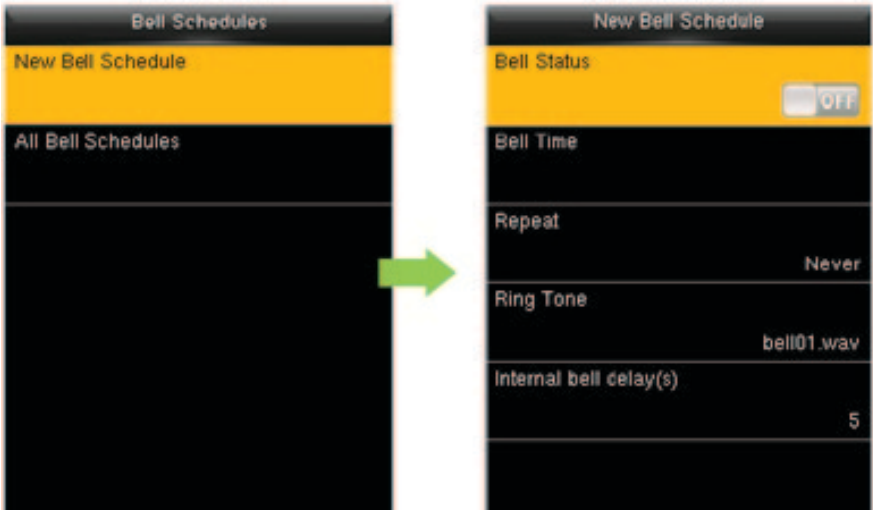
Indicador de teclado: Seleccione si desea habilitar la voz de teclado mientras presiona el teclado, pulse [M/OK] para activarlo.

Volumen: ajustar el volumen del dispositivo. Pulse la tecla para aumentar el volumen, pulse la tecla para disminuir el volumen.

7.3 Configuración de campanas

Muchas empresas optan por utilizar campana para significar en servicio y tiempo fuera de servicio. Al llegar a la hora programada para bell, el dispositivo reproducirá el tono seleccionado automáticamente hasta la duración de llamada se pasa.

1. Adición de un horario



Estado de Bell: [ON] es permitir que la campana, mientras que [OFF] es para desactivarlo.

Campana: La campana automáticamente al alcanzar el tiempo especificado.

Repito: para establecer si se debe repetir la campana.

Tono de timbre: Tono jugó para bell.

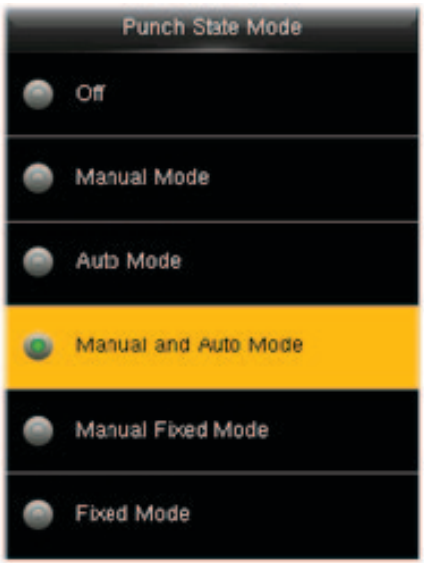
Campana de intervalo delay (s): para ajustar la longitud del timbre. El valor varía de 1 a 999 segundos.

2. Editar y eliminar un horario La operación de edición es similar a la operación de añadir un horario.

Para eliminar un horario, seleccionar el horario que desea eliminar y luego realice la eliminación.

7.4 Configuración de Estados Punch

Modo de estado Punch: para elegir el modo de estado de Ponche, que incluye los siguientes modos:



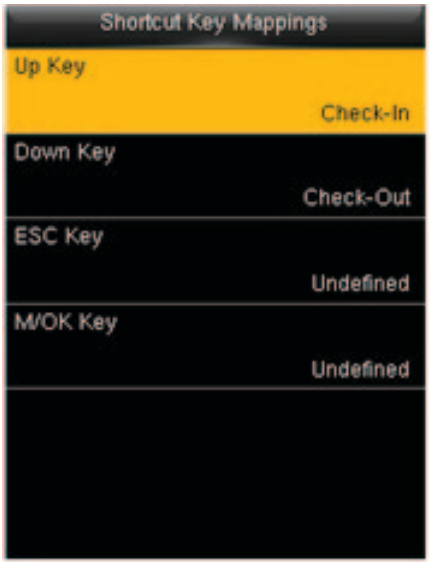
1. Off: desactivar la función clave del estado del sacador. El golpe de estado clave bajo el menú de Teclas de acceso directo quedará invalidada.
2. Modo Manual: para cambiar el estado del sacador llave manualmente, y el golpe de estado clave desaparecerá después de golpe de Estado de espera.
3. Modo automático: después de este modo es elegido, establecer el tiempo de conmutación de ponche estado clave en Teclas de acceso directo; Cuando el tiempo de conmutación se alcanza, el estado set punch clave será cambiada automáticamente.
4. Manual y modo automático: Bajo este modo, la interfaz principal mostrará el golpe de estado de conmutación automática clave, mientras tanto soporta conmutación manualmente punch estado clave. Después de tiempo de espera, el ponche de conmutación manualmente estado clave se convertirá en golpe de estado de conmutación automática.
5. Modo Fijo Manual: tras golpe estado clave se conmuta manualmente, el punzón tecla estado permanecerá sin cambios hasta ser cambiado manualmente la próxima vez.
6. Modo fijo: sólo el sacador fijo estado clave aparecerá y no puede ser cambiado.

Ponche de espera de Estado (s): El tiempo de espera de la pantalla de estado del sacador. El valor varía desde 5 ~ 999 segundos.
Punch Estado requerido: Si es necesario escoger el estado de asistencia en la verificación.

7.5 Configuración de Teclas de acceso directo

Teclas de acceso directo puede definirse como punch teclas de estado o tecla de función de menú. Cuando el dispositivo está en la interfaz principal, presionando la tecla de acceso directo set mostrará el estado de asistencia o entrar en la interfaz de la operación del menú.

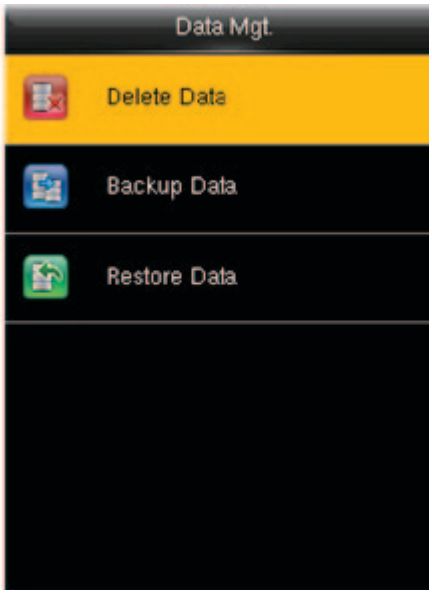
1. Cuando se selecciona la clave del estado, cambio automático pueden configurarse. Conmutación automática se refiere a que el dispositivo cambia automáticamente el estado del sacador cuando un punto de tiempo preestablecido se alcanza.
2. Cuando se selecciona la clave del estado, el dispositivo no habilitar la clave del estado si el modo de prohibición está habilitado en modo clave del estado.



Seleccione la tecla de atajo para definirse y pulse M/OK.

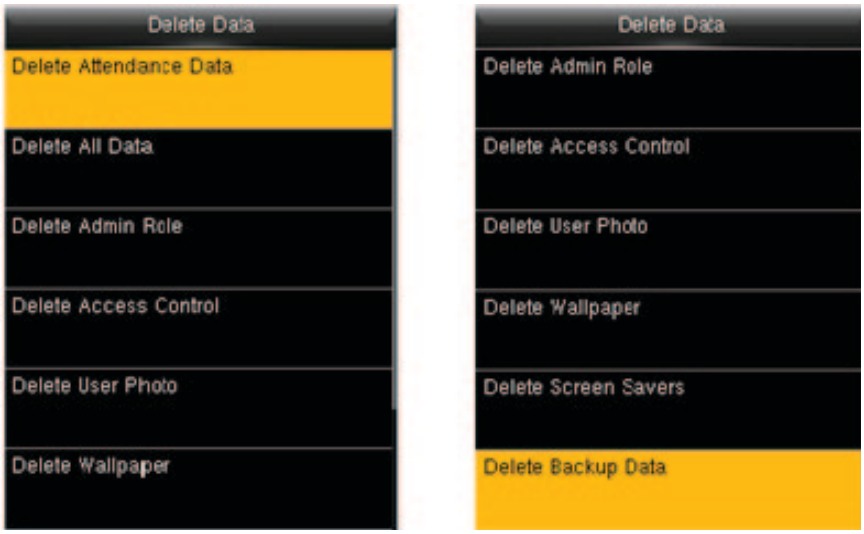
Establezca el estado.

8. Datos Mgt



8.1 Eliminar datos

Para administrar los datos en el dispositivo, que incluye eliminar datos de asistencia, eliminar todos los datos, eliminar el papel de administrador y eliminar los protectores de pantalla etcetera.



Eliminar Datos de asistencia: para eliminar todos los datos de asistencia en el dispositivo.

Eliminar todos los datos: para borrar toda la información del usuario, las huellas digitales y registros de asistencia etcetera.

Eliminar Papel Admin: para que todos los administradores se convierten en usuarios normales.

Eliminar el Control de acceso: para eliminar todos los datos de acceso.

Eliminar la foto del usuario: para borrar todas las fotos de usuario en el dispositivo.

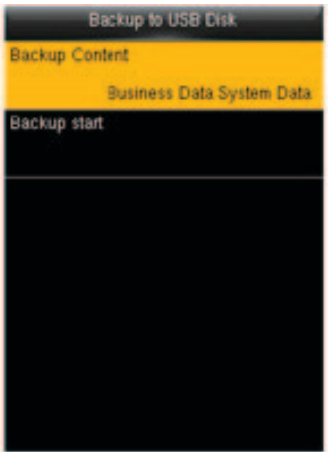
Eliminar fondos: para eliminar todos los fondos de pantalla en el dispositivo.

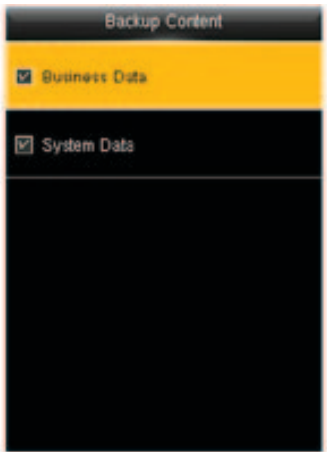
Eliminar protectores de pantalla: para eliminar todos los protectores de pantalla en el dispositivo. (Para detalles de subir los protectores de pantalla, por favor consulte el apéndice 1 Imagen Subiendo la regla.

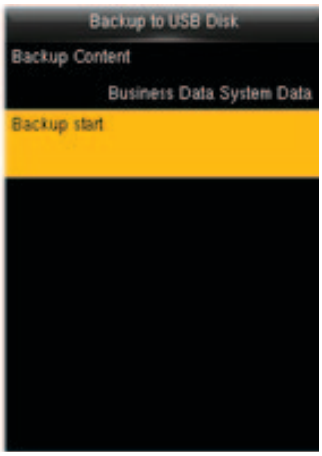
Eliminar Datos de copia de seguridad: para eliminar todos los datos de backup.

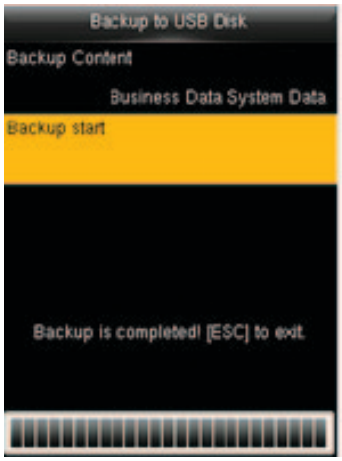
8.2 Copia de seguridad de datos

Una copia de seguridad de los datos de negocio, o los datos de configuración para el disco de U.



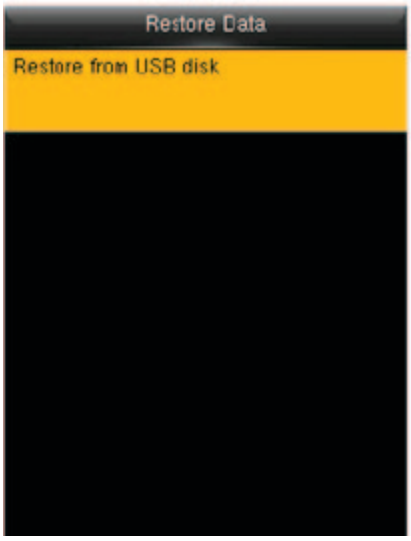




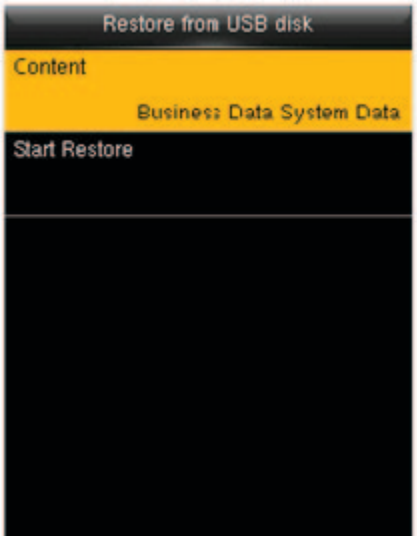


8.3 la restauración de datos

Para restaurar los datos en el disco de U para el dispositivo.



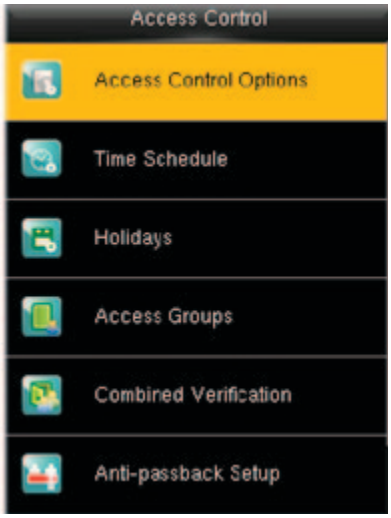
Seleccione el modo de restauración



Seleccione el contenido para ser restaurado y luego comenzar la restauración.

9 Control de acceso

Control de acceso se utiliza para establecer el período de tiempo de acceso de usuario y los parámetros del bloqueo de control y dispositivo relacionado.



Para tener acceso, el usuario registrado debe cumplir con las siguientes condiciones:

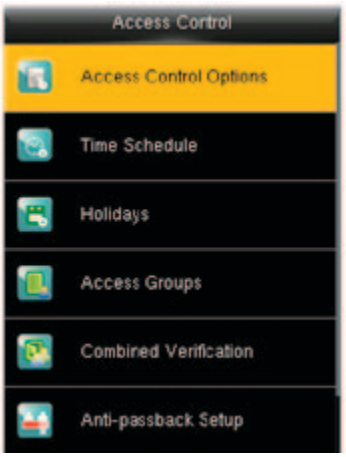
1. tiempo de acceso del usuario cae dentro de cualquier zona horaria personal del usuario o grupo zona horaria.

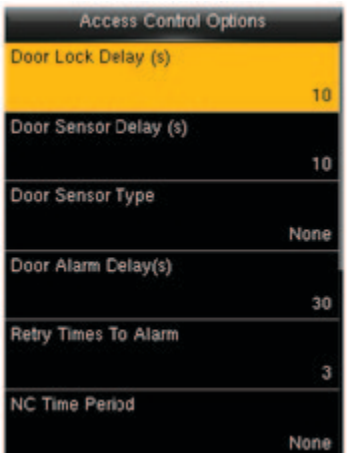
2. el grupo de Usuario debe estar en el combo de acceso (cuando hay otros grupos en el mismo combo de acceso, la verificación de los miembros de esos grupos también están obligados a abrir la puerta).

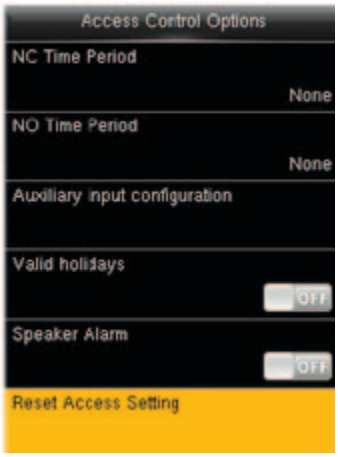
En la configuración predeterminada, los nuevos usuarios se asignan en el primer grupo con el grupo predeterminado de zona horaria y acceso combo como "1", y puso en estado de desbloqueo.

9.1 Configuración de opciones de Control de acceso

Establecer los parámetros de control de dispositivos de bloqueo y dispositivo relacionado.





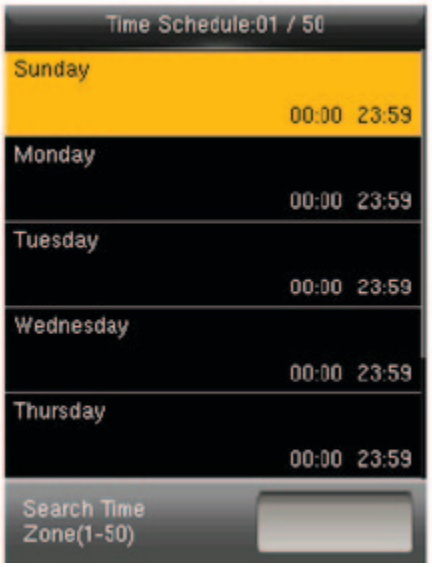


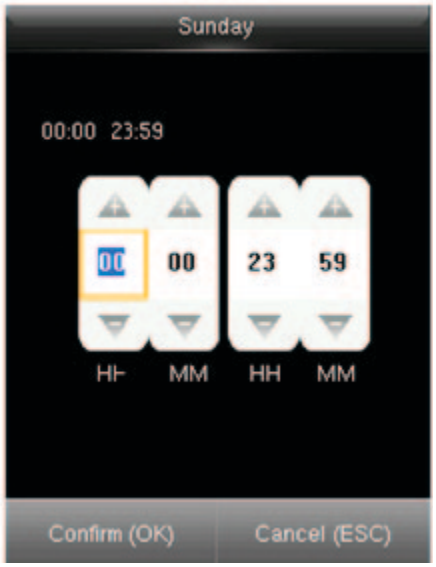
Retardo de bloqueo de la puerta (s): El período de tiempo de desbloqueo (apertura de puerta para cerrar automáticamente) después de la cerradura electrónica activada la contraseña y el retardo de alarma. Sin embargo, el contenido de los datos de acceso Eliminación en [Datos Mgt.] no serán afectados.

Observaciones: después de establecer NC período de tiempo, por favor cierra la puerta bien, de lo contrario la alarma puede ser activada durante el período de NC.

9.2 Configuración de Horario

ACH usuario puede establecer un máximo de tres períodos de tiempo, que están en o relación. El tiempo es válido mientras el tiempo durante la verificación se encuentra con uno de los períodos. El formato de cada intervalo de tiempo en un período de tiempo es HH: MM-HH: MM, es decir, con la precisión de minutos en 24 horas.





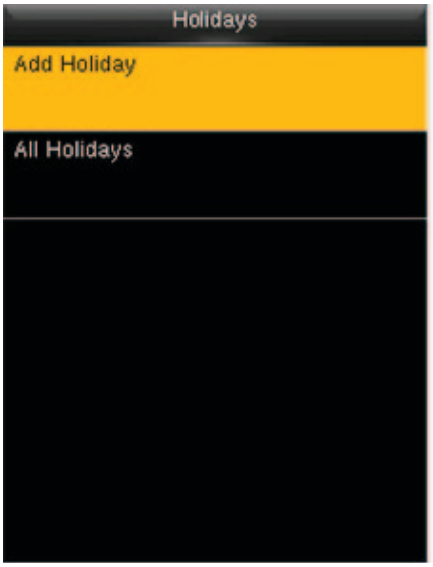
Cuando el tiempo final es anterior a la hora de inicio (por ejemplo, 23:57-23:56), esto significa cerrar todo el día. Cuando el tiempo final es posterior a la hora de inicio (por ejemplo, 00:00-23:59), esto significa que este intervalo es válido.

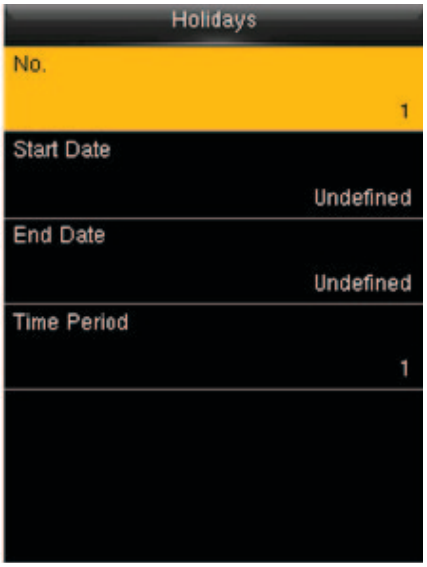
Horario válido: 00:00 ~ 23:59 (todo el día válido) o cuando el tiempo final es mayor que el tiempo de inicio. Nota: de forma predeterminada, el período del sistema significa abrir todo el día (es decir, abriendo para los nuevos usuarios inscritos).

9.3 Feriado para el grupo de acceso

El concepto de vacaciones y el festival se introduce en el control de acceso. En días festivos o festivales, tiempo de control de acceso especial puede ser necesario, pero cambiando el tiempo de control de acceso a todo el mundo es muy tedioso. Por lo tanto, el tiempo de control de acceso en los días festivos y festivales, que se aplica a todo el personal, se puede ajustar.

Si el tiempo de control de acceso en los días festivos y festivales se establece, el periodo de apertura de tiempo en días festivos y festivales sujetos al período de tiempo establecido aquí.





9.4 Configuración de grupos de acceso

La agrupación es gestionar los usuarios en grupos.

Agrupar usuarios "zona horaria predeterminada está dispuesto a ser la zona horaria del grupo, mientras que los usuarios pueden establecer su zona horaria personal.

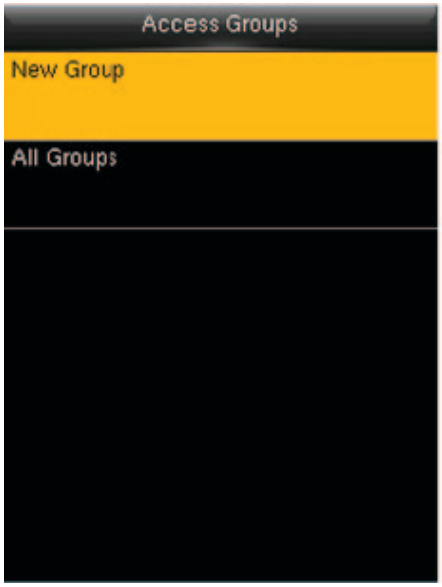
Cuando el grupo modo de verificación se superpone con el modo de verificación de usuario, los modos de verificación de usuario prevalece.

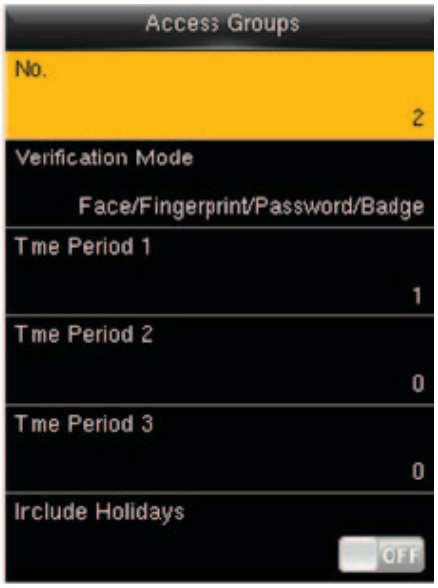
Cada grupo puede establecer 3 zonas horarias a lo sumo, mientras uno de ellos es válido, el grupo puede ser verificado con éxito.

Por defecto, el usuario recién matriculados pertenece al grupo de acceso 1, y también puede asignarse a otro grupo de acceso.

Instrucciones de operación:

- Lla adición de un período de tiempo de grupo





Un total de 21 modos de verificación son compatibles: face/huella/contraseña/placa, solo huella digital, sólo ID de usuario, contraseña, sólo placa, huella/contraseña, huella digital/placa, contraseña/placa, ID de usuario & huella digital, huella digital & password, contraseña & placa, huella digital & password & placa, contraseña & placa, ID de usuario & huella digital & password, huella digital & placa & ID de usuario, sólo cara, cara & huella digital , face & contraseña, cara & placa, cara & huella digital & placa y cara & huella digital & password.

Período de tiempo en vacaciones y fiestas:

1. Cuando el día de fiesta o festival está dispuesto a ser válido, el personal en el grupo puede abrir la puerta sólo cuando el grupo período traslapos vacaciones y período del festival.

2. Cuando el día de fiesta o festival está dispuesto a ser inválido, el tiempo de control de acceso del personal en este grupo no se ve afectada por vacaciones o festivales.

- Editar y eliminar un grupo período

Durante la edición, el número no puede ser modificado, y otras operaciones son similares a los de añadir un grupo de control de acceso. Presione ESC para salir.

Para eliminar un período de tiempo de grupo, seleccione el grupo de control de acceso que se va a eliminar y eliminarlo.

9.5 Configuración de Verificación Combinada

Combinar dos o más miembros para lograr la verificación de múltiples y mejorar la seguridad.
En una Verificación Combinada, el rango de número de usuario es: 0 = N = 5; los usuarios pueden pertenecer a un solo grupo, o pertenecen a 5 grupos diferentes a lo sumo.

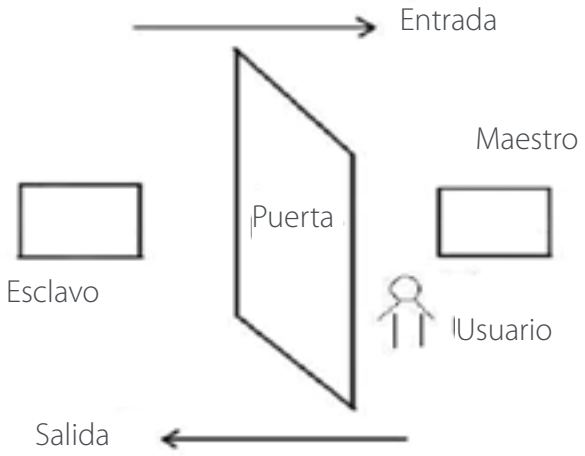
Instrucciones de operación: la adición de una combinación de desbloqueo por ejemplo, las siguientes figuras muestran cómo agregar una combinación que puede ser desbloqueado sólo cuando ambos Grupo 1 y 2 tener éxito en la verificación:

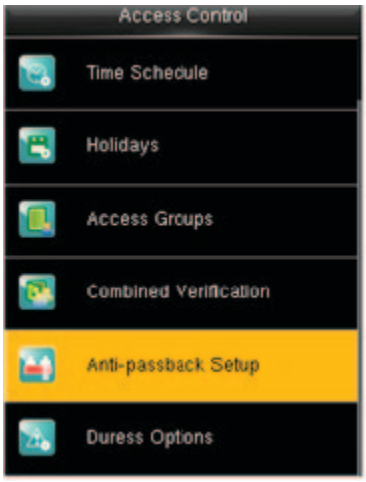
2) editar y eliminar una combinación de desbloqueo para la edición, entrar directamente a modificar el Grupo combinado, similar a la operación de la adición de una combinación de desbloqueo.
Para eliminar una Verificación Combinada, establecer todos los números de grupo de acceso a 0.

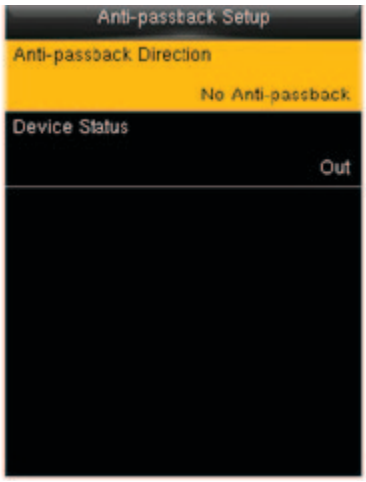
9.6 Configuración Anti-Passback

Para evitar algunas personas siguientes usuarios para entrar en la puerta sin verificación, resultando en un problema de seguridad, los usuarios pueden habilitar la función anti-passback. El registro debe coincidir con el check-out registro así como para abrir la puerta.

Esta función requiere dos dispositivos para trabajar juntos: uno se instala dentro de la puerta (dispositivo maestro), el otro está instalado fuera de la puerta (dispositivo esclavo). Los dos dispositivos se comunican a través de señal Wiegand. El formato Wiegand y tipo de salida (ID de usuario/número de placa) adoptado por el dispositivo maestro y esclavo dispositivo debe ser consistente.







Pulse para seleccionar la Configuración Anti-Passback. Pulse OK para entrar en la interfaz de configuración Anti-Passback.

- Dirección Anti-Passback

No Anti-Passback: función Anti-Passback está desactivado, lo que significa pasar la verificación de cualquier dispositivo maestro o esclavo dispositivo puede abrir la puerta. Estado de asistencia no es reservado.
Anti-Passback: después de que un usuario desprotege, sólo si el último registro es un registro en el registro puede el usuario comprobar de nuevo; de lo contrario, la alarma se disparará. Sin embargo, el usuario puede registrarse libremente.

En Anti-Passback: después de que un usuario se registra, sólo si el último registro es un registro de salida puede el usuario comprobar de nuevo; de lo contrario, la alarma se disparará. Sin embargo, el usuario puede consultar libremente.

In/Out Anti-Passback: después de un usuario in/out, sólo si el último registro es un registro de salida puede el usuario comprobar de nuevo, o un registro en el registro puede el usuario comprobar de nuevo; de lo contrario, la alarma se disparará.

Nulo y Guardar: función Anti-Passback está desactivado, pero el estado de asistencia está reservada.

- Estado Del Dispositivo

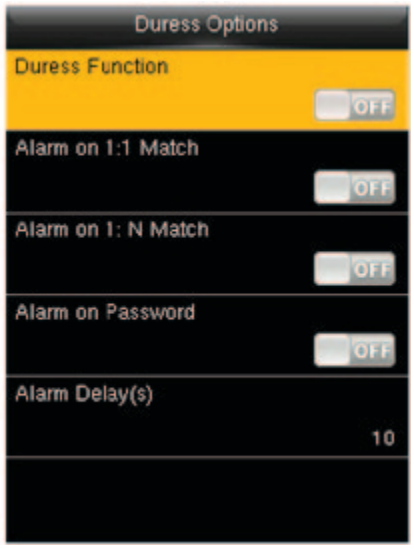
Ninguno: para desactivar la función Anti-Passback.

Fuera: todos los registros en el dispositivo son registros de check-out.

En: todos los registros en el dispositivo son registros de registro.

9.7 Configuración de opciones de Coacción

Cuando los usuarios vienen a través de coacción, seleccione modo de alarma, el dispositivo se abrirá la puerta como de costumbre y enviar la señal de alarma a la alarma entre bastidores.



Función de coacción: En [EN] Estado, presione "Coacción Clave" y pulse cualquier huella dactilar registrada o número de identificación (dentro de 10 segundos), la alarma se disparará después de la verificación exitosa. En [OFF] Estado, presionando "Coacción Clave" no se activa la alarma.

Alarma en 1:1 Partido: En [EN] Estado, cuando un usuario utiliza 1:1 método de verificación para verificar cualquier huella dactilar registrada, la alarma se disparará. En [OFF] Estado, ninguna señal de alarma se disparará.

Alarma en 1: N Partido: En [EN] Estado, cuando un usuario utiliza 1: N método de verificación para verificar cualquier huella dactilar registrada, la alarma se disparará. En [OFF] Estado, ninguna señal de alarma se disparará.

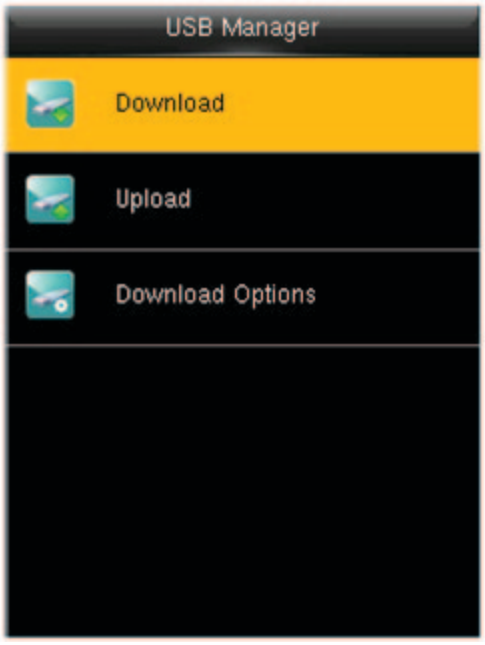
Alarma en contraseña: En [EN] Estado, cuando un usuario utiliza el método de verificación de contraseñas, la alarma se disparará. En [OFF] Estado, ninguna señal de alarma se disparará.

Retardo de alarma (s): cuando la alarma se activa, el dispositivo enviará la señal de alarma después de 10 segundos (predeterminado); el tiempo de retardo de alarma puede cambiar (valor va desde 0 a 999 segundos).

10. Gerente USB

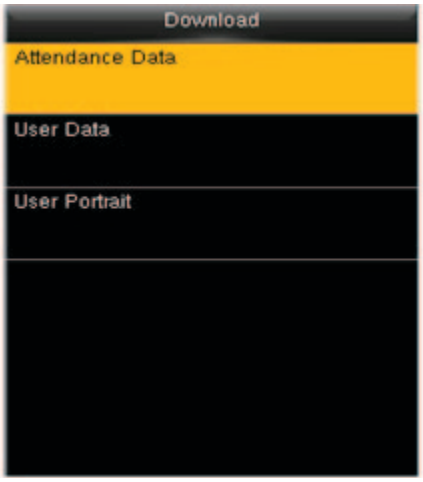
La información del usuario, plantilla de huella digital y datos de asistencia en el dispositivo puede ser importado en software relacionado para el procesamiento, o la información del usuario y las huellas digitales se pueden importar en otros dispositivos de huellas dactilares a través de un disco USB.

Antes de cargar/descargar datos desde/hasta el disco USB, inserte el disco USB en la ranura USB primero.



Seleccione USB Manager en el menú principal.

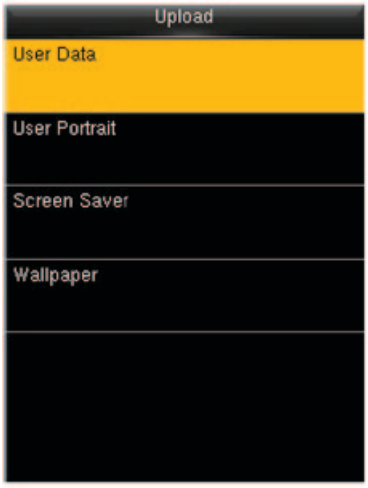
10.1 Descarga USB



Datos de asistencia: para descargar los datos de asistencia en el período de tiempo especificado en un disco USB.
Datos de usuario: para descargar toda la información del usuario y las huellas digitales del dispositivo en un disco USB.

Retrato de usuario: para descargar todas las fotos de usuario del dispositivo en un disco USB.

10.2 carga USB



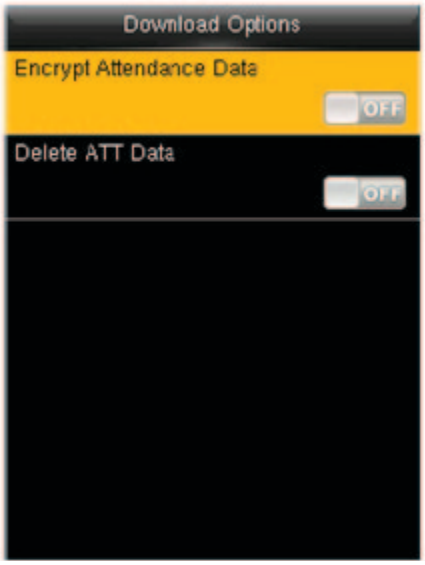
Datos de usuario: para cargar toda la información del usuario y huellas digitales de disco USB en el dispositivo. Retrato de usuario: subir a. JPG archivo de imagen llamado el ID de usuario en un disco USB al dispositivo, y el retrato de usuario en el disco USB se mostrará en el dispositivo para la vista previa. Durante la carga, puede elegir Cargar imagen seleccionada o cargar todas las imágenes. Después de subir, el retrato se muestra cuando el dispositivo es verificar la huella dactilar de un empleado.

Protector de pantalla: para cargar todos los protectores de pantalla de disco USB en el dispositivo. Usted puede elegir **[Subir imagen seleccionada]** o **[Subir todas las imágenes]**. Las imágenes se mostrarán en la interfaz principal del dispositivo después de subir.

Wallpaper: subir todos los fondos de disco USB en el dispositivo. Usted puede elegir **[Subir imagen seleccionada]** o **[Subir todas las imágenes]**. Las imágenes se mostrarán en la pantalla después de cargar.

10.3 Configuración de opciones de descarga

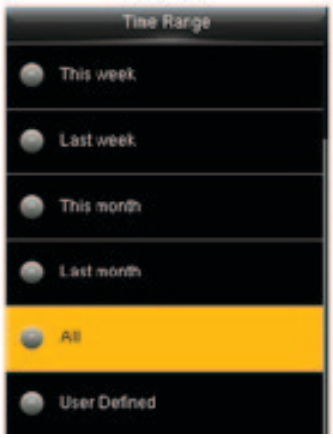
Para cifrar datos de asistencia en el disco USB o eliminar datos de asistencia.



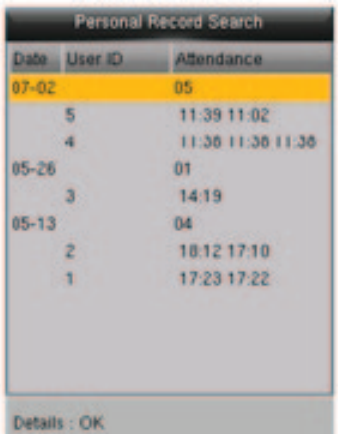
11. Búsqueda de asistencia

Después de un empleado con éxito controles dentro y fuera, el registro se guardará en el dispositivo. La búsqueda de asistencia permite a los empleados para consultar los registros de asistencia de empleados. Búsqueda De Registro De Asistencia.

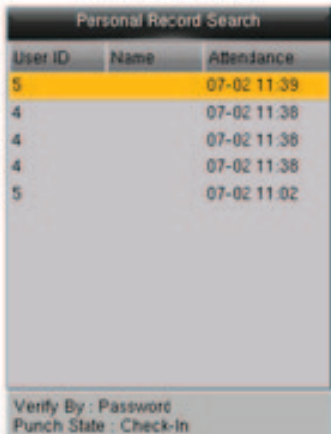
Introduzca el ID de usuario de un empleado cuyos registros de asistencia deben ser consultado. Si se especifica ningún ID de usuario, los registros de asistencia de todos los empleados se preguntan.



Seleccione el período de tiempo para la consulta.



Pulse para seleccionar un registro de asistencia y pulse M/OK.



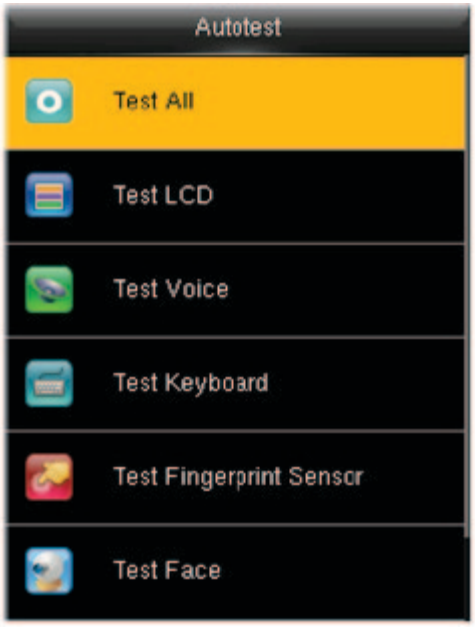
Detalles del registro

Datos de registro de ID de usuario: ID de usuario de un empleado cuyos registros de asistencia deben ser consultado. Si se especifica ningún ID de usuario, los registros de asistencia de todos los empleados se preguntan. Después se ingresa un ID de usuario, registros de asistencia del empleado con el ID de usuario se preguntan.

Rango de tiempo: Seleccione el período de tiempo para la consulta, incluyendo definido por el usuario, ayer, esta semana, la semana pasada, este mes, el mes pasado y todos los períodos de tiempo.

12. Autotest

Para probar si todos los módulos en el dispositivo funcione correctamente, que incluyen el LCD, voz, teclado, sensor de huellas dactilares y RTC (reloj en tiempo Real).



Prueba: para probar LCD, voz, teclado, sensor de huellas dactilares y RTC. Durante la prueba, pulse [M/OK] para continuar con la siguiente prueba, mientras que presiona **[ESC]** para salir de la prueba.

LCD de prueba: para probar el efecto de la exhibición de pantalla LCD, mostrando a todo color, blanco puro y negro puro para comprobar si la pantalla muestra los colores correctamente. Durante la prueba, pulse [M/OK] para continuar con la siguiente prueba, mientras que presiona **[ESC]** para salir de la prueba.

Prueba de voz: el dispositivo automáticamente comprueba si los archivos de voz almacenados en el dispositivo son completos y la calidad de voz es buena. Durante la prueba, pulse **[M/OK]** para continuar con la siguiente prueba, mientras que presiona **[ESC]** para salir de la prueba.

Teclado de prueba: para probar todas las llaves para ver si cada llave funciona correctamente. Pulse cualquier tecla en el teclado del interfaz de la prueba; Si la tecla presionada es coherente con el signo clave que se muestra en la pantalla, entonces la llave funciona correctamente. Pulse **[M/OK]** o **[ESC]** para salir de la prueba.

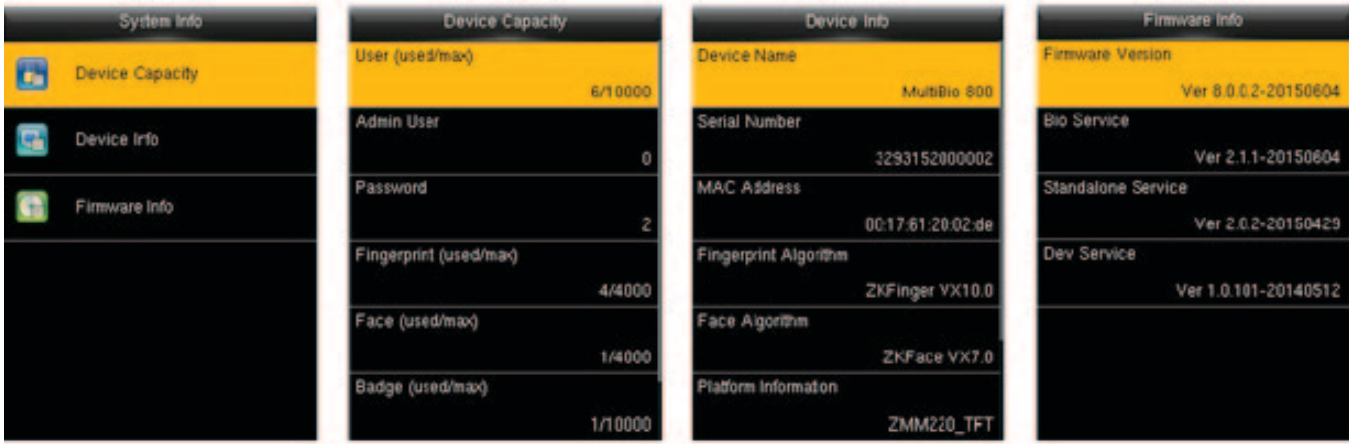
Prueba Sensor de huellas digitales: para probar el sensor de huellas dactilares presionando la huella digital para comprobar si la recogida la imagen de la huella digital es clara. Al presionar la huella digital en el sensor, la imagen se mostrará en la pantalla. Pulse **[M/OK]** o **[ESC]** para salir de la prueba.

Prueba: el dispositivo automáticamente comprueba si la cámara está en funcionamiento y comprueba si las imágenes capturadas son claras y útiles. Presione ESC para salir de esta prueba.

Prueba Reloj RTC: para probar el reloj de tiempo Real. El dispositivo comprueba si el reloj funciona correctamente y con precisión al marcar el cronómetro. Pulse **[M/OK]** para empezar a contar el tiempo, y púlselo de nuevo para dejar de contar, para ver si el cronómetro cuenta tiempo con precisión. Presionar la tecla **[ESC]** para salir de la prueba.

13. informaciones del sistema

Comprobar la capacidad de datos, información del dispositivo y el firmware.



Seleccione "información del sistema" en el menú principal	Capacidad de datos	Información del dispositivo	Información sobre el firmware

Capacidad del dispositivo: para mostrar el número de usuarios registrados, administradores, contraseñas, huellas dactilares, placas, registros de asistencia y así sucesivamente.

Información del dispositivo: para mostrar el nombre del dispositivo, número de serie, dirección MAC, algoritmo de huellas digitales, información de la plataforma, fabricante y fecha del fabricante.

Firmware Info: para mostrar la versión de firmware, Bio service, servicio push, servicio independiente y servicio Dev.

14. Apéndices

Apéndice 1. Regla de imagen cargada

- Foto del usuario: se requiere para crear un archivo denominado como "foto" er el archivo de disco USB, y poner userphotos en el archivo. La capacidad es de 8000 imágenes, con cada uno de ellos no superior a 15 k. El nombre de imagen es x.jpg (x es el ID DE usuario real, max. 9 dígitos). El formato de la foto debe ser JPG.
- Imagen publicitaria: se requiere para crear un archivo denominado como "publicidad" bajo el archivo de disco USB, y poner imágenes publicitarias en el archivo. La capacidad es de 20 imágenes con cada uno de ellos no exceda de 30 k. Nombre de imagen y formato no son restrictos.
- Papel pintado: se requiere para crear un archivo denominado como "wallpaper" bajo el archivo de disco USB, y poner fondos en el archivo. La capacidad es de 20 imágenes con cada uno de ellos no exceda de 30 k. Nombre de imagen y formato no son restrictos.

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

Apéndice 2. Wiegand Introducción

Wiegand26 protocolo es un protocolo estándar en el control de acceso desarrollado por el Subcomité de Control de acceso Estándar afiliada a la Asociación de la industria de Seguridad (SIA). Es un protocolo utilizado para el puerto lector de tarjetas sin contacto del IC y de salida.

El protocolo define el puerto entre el lector de tarjetas y el controlador que son ampliamente utilizados en el control de acceso, seguridad y otras industrias relacionadas. Esto ha estandarizado el trabajo de diseñadores y fabricantes de controlador del lector de tarjetas. Los dispositivos de control de acceso producidos por nuestra compañía también aplicar este protocolo.

Señal Digital

La figura 1 muestra el diagrama de secuencia del lector de tarjetas enviando señal digital en bits al controlador de acceso.

El Wiegand en este diagrama sigue el protocolo estándar de control de acceso A SÍA, que se enfoca en el lector de tarjetas Wiegand 26 bits (con un tiempo de pulso dentro de 20 μs a 100 μs y pulso tiempo saltando dentro de 200 μs y 20ms).

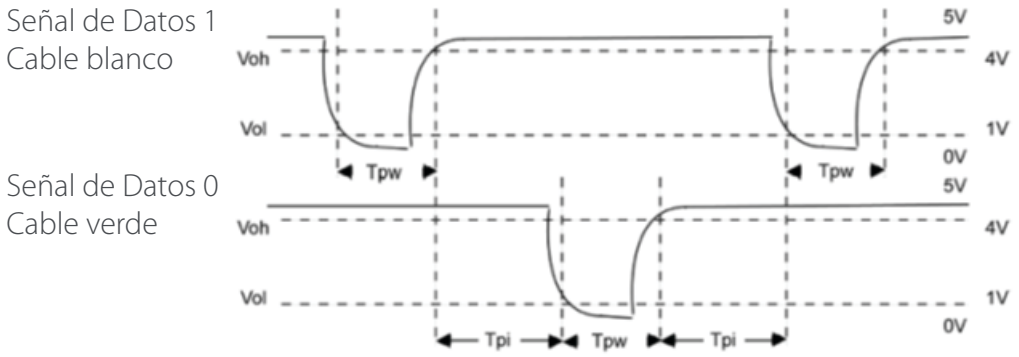
Las señales de las líneas Data0 y data1 de alto nivel (mayor que Voh) hasta que el lector de tarjetas está listo para enviar un flujo de datos.

El lector de tarjetas enviar pulso bajo nivel asincrónica (menos de vol), transmitiendo el flujo de datos a través de Data1 o las líneas Data0 alambre para acceder a la caja de control (como la onda del sawtooth en la figura 1). Data1 y las líneas Data0 pulsos no se superponen o sincronizar. La figura 1 muestra el ancho del pulso máximo y mínimo (pulsos sucesivos) y pulso salto de tiempo (el tiempo entre dos pulsos) permitido por la serie F terminales de control de acceso de huellas digitales.

Table1: Tiempo De Pulso

Signo	Definición	Valor típico de lector de tarjeta
Tpw	Ancho de pulso	100 us
Tpi	Intervalo de pulso	1 ms

Figura 1: Secuencia del Diagrama



Apéndice 3. Declaración sobre los derechos humanos y la privacidad

Estimados clientes: Gracias por elegir los productos biometricos híbridos diseñados y fabricados por nosotros. Como un proveedor de renombre mundial de tecnologías biométricas y servicios, prestamos mucha atención al cumplimiento de las leyes relacionadas con los derechos humanos y la privacidad en todos los países mientras que constantemente realizando investigación y desarrollo.

Nos hacemos las siguientes declaraciones:

1. Todos nuestros dispositivos de reconocimiento de huellas digitales para uso civil sólo recoger los puntos característicos de las huellas dactilares en lugar de las imágenes de huellas dactilares, y por lo tanto no hay problemas de privacidad están involucrados.

2. Los puntos característicos de las huellas dactilares recogidas por nuestros productos no se pueden utilizar para restaurar las imágenes de huellas dactilares originales, y por lo tanto no hay problemas de privacidad están involucrados.

3. Nosotros, como el proveedor del equipo, no se hace legalmente responsable, directa o indirectamente, por las consecuencias que surgen debido al uso de nuestros productos.

4. Para cualquier controversia que involucra a los derechos humanos o privacidad al utilizar nuestros productos, póngase en contacto con su empleador directamente.

Nuestros productos de huellas dactilares para el uso de la policía, o las herramientas de desarrollo apoyan la colección de las imágenes de huellas dactilares originales. En cuanto a si un tipo de colección de huellas digitales constituye una infracción de su privacidad, por favor póngase en contacto con el gobierno o el proveedor del equipo final. Nosotros, como el fabricante de equipo original, no se hace legalmente responsable por cualquier infracción que surja de los mismos.

La ley de la República Popular de China cuenta con las siguientes regulaciones con respecto a la libertad personal:

1. Detención ilegal, detención o búsqueda de ciudadanos de la República Popular de China está prohibida; violación de la privacidad individual 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 la privacidad de la correspondencia de los ciudadanos de la República Popular de China están protegidos por ley.

Por fin recalcamos una vez más que la biometría, como una tecnología de reconocimiento avanzado, se aplicará en muchos sectores, incluyendo el comercio electrónico, banca, seguros y asuntos legales. Cada año, personas de todo el mundo sufren grandes pérdidas debido a la inseguridad de las contraseñas. Los productos biométricos en realidad proporcionan protección adecuada para su identidad bajo un entorno de alta seguridad.

Apéndice 4. Descripción de uso al medio ambiente

• El período de uso del medio ambiente (EFUP) marcado en este producto se refiere al período de seguridad de tiempo en el que el producto se utiliza en las condiciones especificadas en las instrucciones del producto sin fugas de sustancias nocivas y sustancias nocivas.

• El EFUP de este producto no cubre las partes consumibles que necesitan ser reemplazados de forma regular, tales como baterías y así sucesivamente. El EFUP de baterías es 5 años.

Nombres y concentración de Sustancias o elementos tóxicos y peligrosos						
Nombre De Piezas	Tóxicos y sustancias peligrosas o elementos					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip resistor	X	O	O	O	O	O
Chip capacitor	X	O	O	O	O	O
Chip inductor	X	O	O	O	O	O
Chip diode	X	O	O	O	O	O
ESD componentes	X	O	O	O	O	O
Buzzer	X	O	O	O	O	O
Adapter	O	O	O	O	O	O
Screws	O	O	O	X	O	O

O: Indica que este tóxico o sustancia peligrosa contenida en todos los materiales homogéneos para esta parte está por debajo del límite requisito en SJ/T11363-2006.

X: Indica que este tóxico o sustancia peligrosa contenida en al menos uno de los materiales homogéneos para esta parte está por encima del límite requisito en SJ/T11363-2006.

Nota: 80% de las piezas en este producto se fabrican con no peligrosos materiales favorables al medio ambiente.

Las sustancias peligrosas o elementos contenidos no pueden ser reemplazados con materiales favorables al medio ambiente en la actualidad debido a las limitaciones técnicas o económicas.

German Centre 3-2-02, Av. Santa Fe No. 170, Lomas de Santa Fe,
Delegación Alvaro Obregón, 01210 México D.F.
Tel: +52 (55) 52-92-84-18
www.zktecolatinoamerica.com
www.zkteco.com