MANUAL DE USUARIO

MB10

Gracias por elegir nuestro producto. Lea atentamente las instrucciones antes de la operación. Siga estas instrucciones para asegurarse de que el producto funcione correctamente. Las imágenes que se muestran en este manual son solo para fines ilustrativos. Para obtener más detalles, visite el sitio web de nuestra empresa: **www.zkteco.com**

Copyright © 2020 ZKTECO CO., LTD. Todos los Derechos Reservados

Sin el consentimiento previo por escrito de ZKTeco, ninguna parte de este manual puede copiarse o reenviarse de ninguna manera o forma. Todas las partes de este manual pertenecen a ZKTeco y sus subsidiarias (en adelante la "Compañía" o "ZKTeco").

Marca Registrada

ZKTeco es una marca registrada de ZKTeco. Las marcas registradas involucradas en este manual son propiedad de sus respectivos dueños.

Descargo de Responsabilidad

Este manual contiene información sobre la operación y mantenimiento del equipo ZKTeco. Los derechos de autor en todos los documentos, dibujos, etc. en relación con el equipo suministrado por ZKTeco se confieren y son propiedad de ZKTeco. El contenido del presente no debe ser utilizado o compartido por el receptor con ningún tercero sin el permiso expreso por escrito de ZKTeco.

El contenido de este manual debe leerse en su totalidad antes de comenzar la operación y el mantenimiento del equipo suministrado. Si alguno de los contenidos del manual parece poco claro o está incompleto, comuníquese con ZKTeco antes de comenzar la operación y el mantenimiento de dicho equipo.

Es un pre-requisito esencial para la operación y mantenimiento satisfactorios que el personal de operación y mantenimiento esté completamente familiarizado con el diseño y que dicho personal haya recibido capacitación exhaustiva sobre el funcionamiento y mantenimiento de la máquina / unidad / equipo. Es esencial para la operación segura de la máquina / unidad / equipo que el personal haya leído, entendido y seguido las instrucciones de seguridad contenidas en el manual.

En caso de conflicto entre los términos y condiciones de este manual y las especificaciones del contrato, dibujos, hojas de instrucciones o cualquier otro documento relacionado con el contrato, prevalecerán las condiciones / documentos del contrato. Las condiciones / documentos específicos del contrato se aplicarán con prioridad.

ZKTeco no ofrece garantía o representación con respecto a la integridad de cualquier información contenida en este manual o cualquiera de las modificaciones hechas al mismo. ZKTeco no extiende la garantía de ningún tipo, incluida, entre otras, cualquier garantía de diseño, comerciabilidad o idoneidad para un particular
propósito.

ZKTeco no asume responsabilidad por ningún error u omisión en la información o documentos a los que se hace referencia o se vincula a este manual. El usuario asume todo el riesgo en cuanto a los resultados y el rendimiento obtenidos del uso de la información.

ZKTeco en ningún caso será responsable ante el usuario o un tercero por daños incidentales, consecuentes, indirectos, especiales o ejemplares, incluidos, entre otros, pérdida de negocios, pérdida de ganancias, interrupción de negocios, pérdida de información comercial o cualquier pérdida material derivada de, en relación con, o relacionada con el uso de la información contenida o referenciada en este manual, incluso si ZKTeco tiene, la posibilidad de tales daños.

Este manual y la información que contiene pueden incluir imprecisiones técnicas, de otro tipo o errores tipográficos. ZKTeco cambia periódicamente la información aquí contenida que se incorporará a nuevas adiciones / modificaciones al manual. ZKTeco se reserva el derecho de agregar, eliminar, enmendar o modificar la información contenida en el manual de vez en cuando en forma de circulares, cartas, notas, etc. para una mejor operación y seguridad de la máquina / unidad / equipo. Dichas adiciones o enmiendas están destinadas a mejorar las operaciones de la máquina / unidad / equipo y dichas enmiendas no otorgarán ningún derecho a reclamar compensación o daños bajo ninguna circunstancia.

ZKTeco no será responsable de ninguna manera (i) en caso de mal funcionamiento de la máquina / unidad / equipo debido a cualquier incumplimiento de las instrucciones contenidas en este manual (ii) en caso de operación de la máquina / unidad / equipo más allá de los límites de velocidad (iii) en caso de operación de la máquina y el equipo en condiciones diferentes a las prescritas en el manual.

El producto se actualizará periódicamente sin previo aviso. Los últimos procedimientos de operación y documentos relevantes están disponibles en http://www.zkteco.com.
Si hay algún problema relacionado con el producto, contáctenos.

Sede Central de ZKTeco

Dirección: ZKTeco Industrial Park, No. 26, 188 Industrial Road, Tangxia Town, Dongguan, China.

Teléfono: +86 769 - 82109991

Fax: +86 755 - 89602394

Para consultas relacionadas con el negocio, escríbanos a: sales@zkteco.com.
Para saber más sobre nuestras sucursales en el mundo, visite www.zkteco.com.

Acerca de la Compañia

ZKTeco es uno de los mayores fabricantes de lectores de RFID y biométricos (huellas dactilares, faciales, venas digitales) más grandes del mundo. Las ofertas de productos incluyen Lectores y Paneles de Control de Acceso, Cámaras de Reconocimiento Facial de rango cercano y alejado, controladores de Ascensores, Torniquetes, Cámaras de Reconocimiento de Placas Vehiculares (LPR) y productos de Consumo, que incluyen cerraduras de puerta con lector de huellas digitales y cerraduras de puertas. Nuestras soluciones de seguridad son multilingües y están localizadas en más de 18 idiomas diferentes. En las modernas instalaciones de fabricación con certificación ISO9001 de 700,000 pies cuadrados de ZKTeco, controlamos la fabricación, el diseño de productos, el ensamblaje de componentes y la logística, todo bajo un mismo techo.

Los fundadores de ZKTeco se han determinado la investigación y el desarrollo independientes de los procedimientos y la producción del SDK de verificación biométrica, que inicialmente se aplicó ampliamente en los campos de seguridad de PC y autenticación de identidad. Con la mejora continua del desarrollo y muchas aplicaciones de mercado, el equipo ha construido gradualmente un ecosistema de autenticación de identidad y un ecosistema de seguridad inteligente, que se basan en técnicas de verificación biométrica. Con años de experiencia en la industrialización de las verificaciones biométricas, ZKTeco se estableció oficialmente en 2007 y ahora ha sido una de las empresas líderes a nivel mundial en la industria de verificación biométrica que posee varias patentes y es seleccionada como la Empresa Nacional de Alta Tecnología por 6 años consecutivos. Sus productos están protegidos por derechos de propiedad intelectual.

Acerca del Manual

Este manual presenta las operaciones del producto MB10.

Todas las imágenes mostradas son sólo para fines ilustrativos. Las cifras en este manual pueden no ser exactamente consistentes con los productos reales.

Convenciones del Documento

La convención utilizada en este manual se enumeran a continuación:

Convención Gráfica

Del Software	
Convención	Descripción
Negrita	Se utiliza para identificar nombres de interfaz de software, ejemplo OK, Confirmar, Cancelar
>	Niveles múltiples de los Menús están separados por estos corchetes. Ejemplo, Archivo > Crear > Carpeta

Del Dispositivo	
Convención	Descripción
< >	Nombre de botones o teclas en el dispositivo. Ejemplo, presione <OK>
[ ]	Nombres de ventana, elementos de menú, tabla de datos y nombres de campo están entre corchetes. Ejemplo, abra la ventana [Nuevo Usuario]
/	Menús de varios niveles están separados por barras diagonales. Ejemplo, [Archivo / Crear / Carpeta]

Símbolos	
Convención	Descripción
	Esto implica sobre el aviso o prestar atención, en el manual
	Información general que ayuda a realizar las operaciones más rápido
	Información que es importante
	Para evitar errores
	Declaración o evento de advertencia

Contenido

1. Instrucción de Uso **07**
1.1 Posición y expresión facial 07
1.2 Colocación de dedos 09
1.3 Modos de verificación 09
1.3.1 Verificación de huella digital 09
1.3.2 Reconocimiento de Rostro 10
1.3.3 Verificación de contraseña 11
1.3.4 Verificación de tarjeta 11

2. Menú Principal **12**

3. Gestión de Usuarios **13**
3.1 Agregar usuario 13
3.1.1 Ingresar nombre y número de usuario 12
3.1.2 Seleccionar privilegios 14
3.1.3 Enrolar una huella 14
3.1.4 Agregar un rostro 14
3.1.5 Enrolar una tarjeta 15
3.1.6 Agregar una contraseña 15
3.1.7 Capturar foto 15
3.1.8 Control de acceso 16
3.2 Gestión de usuarios 17
3.3 Estilo de pantalla 18

4. Privilegios del Usuario **18**

5. Ajustes de Comunicación **19**
5.1 Ethernet 20
5.2 Comunicación serial 20
5.3 Conexión a PC 20
5.4 ADMS 21
5.5 Ajustes Wiegand 21

6. Configuración de Sistema **23**
6.1 Fecha y hora 24
6.2 Ajustes de asistencia 24
6.3 Parámetros para validación de rostro 26
6.4 Ajustes de Huella 27
6.5 Restablecer valores de fábrica 28
6.6 Actualización por USB 28

7. Configuración de Personalización **28**
7.1 Interfaz de usuario 29
7.2 Ajustes de voz 30
7.3 Ajustes de timbres 30
7.4 Ajustes de estados de asistencia 31
7.5 Asignación de teclas de atajo 32

8. Gestión de Datos **33**
8.1Eliminar datos 33

8.2 Respaldar datos 34
8.3 Restaurar datos 35

9. Control de Acceso **35**
9.1 Opciones de control de acceso 35
9.2 Configuración de horarios 36
9.3 Ajustes de días festivos 37
9.4 Grupos de acceso 38
9.5 Ajustes de verificación múlti-usuario 38
9.6 Ajustes de anti-passback 39
9.7 Ajustes de opciones de coacción 41

10. Gestión USB **41**
10.1 Descarga 42
10.2 Carga desde USB 41
10.3 Opciones de descarga 43

11. Búsqueda de Registros **43**

12. Mensajes **44**
12.1 Agregar y visualizar nuevo mensaje 45
12.2 Opciones de Mensaje 46

13. Código de Trabajo **46**
13.1 Agregar código de trabajo 47
13.2 Editar y Borrar un código de trabajo 47
13.3 Opciones de Código de Trabajo 47

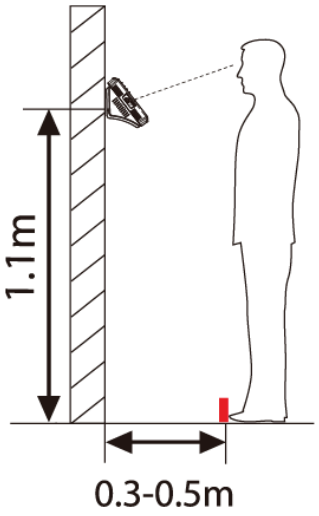
14. Autopruebas **48**

15. Información del Sistema **48**

16. Apéndice **49**

1. Instrucción de uso

Distancia recomendada

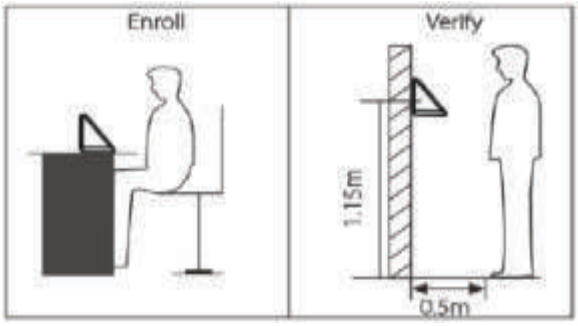


1.1 Posición y expresión facial

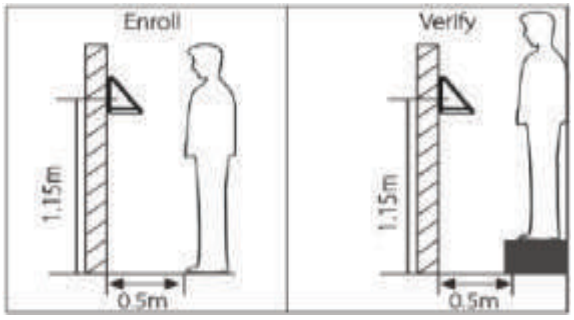
Para usuarios que midan entre 1.5 m y 1.8 m, se recomienda instalar el dispositivo a 1.15 m de altura sobre el suelo (puede modificarse de acuerdo a la altura promedio de los usuarios).

Durante el enrolamiento y la verificación, la posición de instalación del dispositivo debe permanecer igual. Si es necesario mover el dispositivo mantenga la misma altura de instalación o de lo contrario, la función de reconocimiento será deficiente.

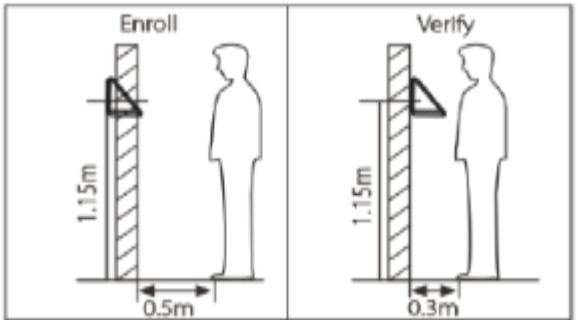
Factores que provocan una verificación deficiente:



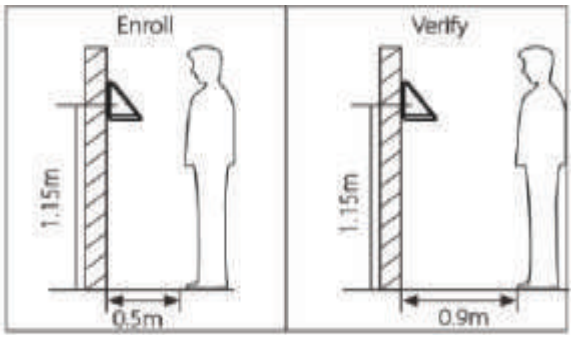
Posturas de registro y verificación diferente.



Alturas de registro y verificación distintas.

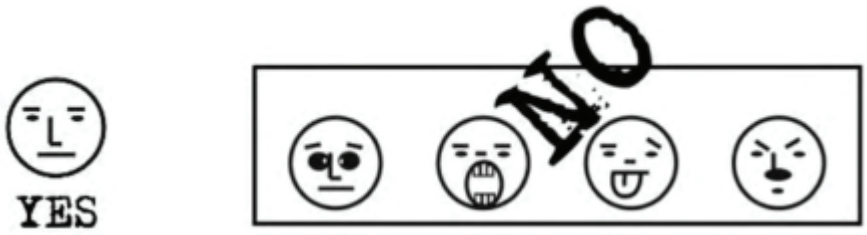


Distancias al dispositivo en el registro y en la verificación diferentes.

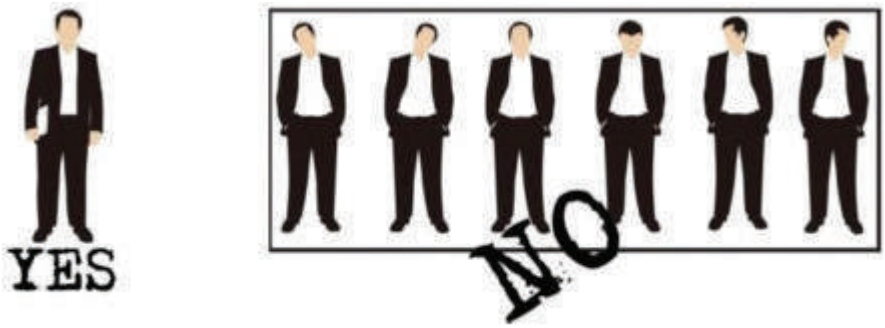


Distancias al dispositivo en el registro y en la verificación diferentes.

Expresión facial correcta y expresiones incorrectas:

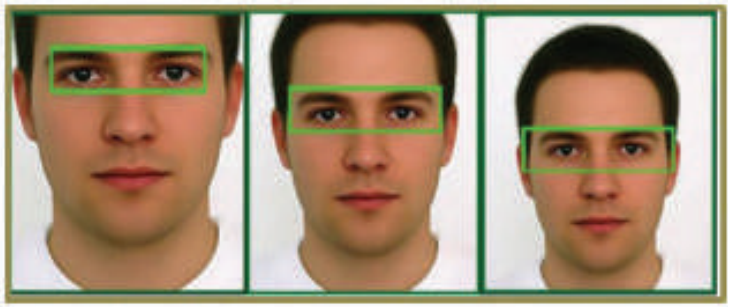


Postura correcta y posturas incorrectas:



Nota: Mantenga una postura y expresión natural durante el enrolamiento y la verificación.

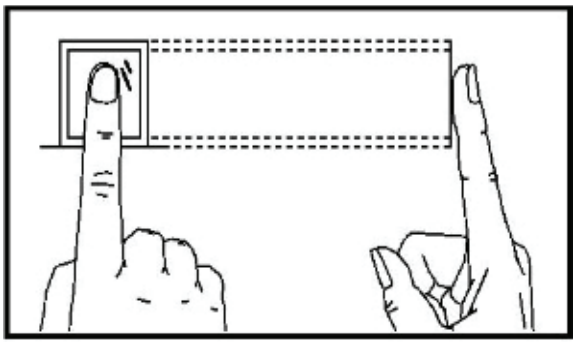
Enrolamiento efectivo de rostro:



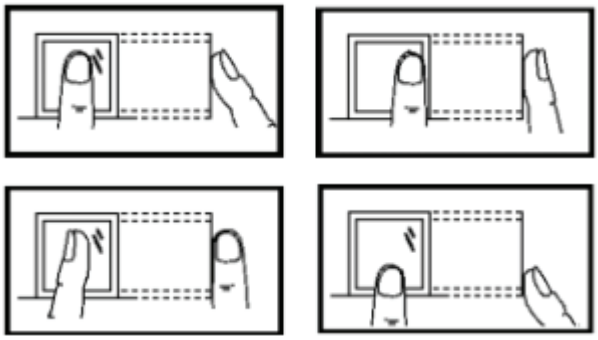
Durante el registro, coloque su rostro en el centro de la pantalla del dispositivo, y siga las indicaciones "Coloque sus ojos dentro del cuadro verde". El usuario debe avanzar y retroceder para ajustar la posición de los ojos durante el registro.

1.2 Colocación de dedos

Dedos recomendados: Dedo Índice, dedo medio o dedo anular; el dedo pulgar y el dedo meñique no son recomendables (porque usualmente es difícil colocar la huella en el lector). El dedo deber ser colocado completamente plano y al centro de la superficie del lector.



Posición correcta del dedo



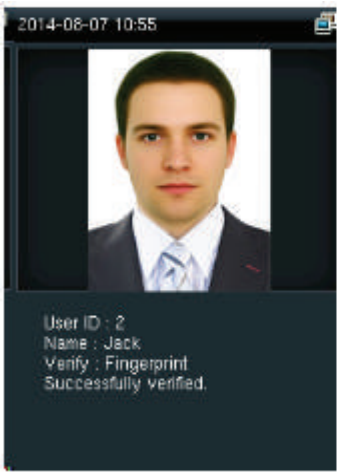
Posición incorrecta del dedo

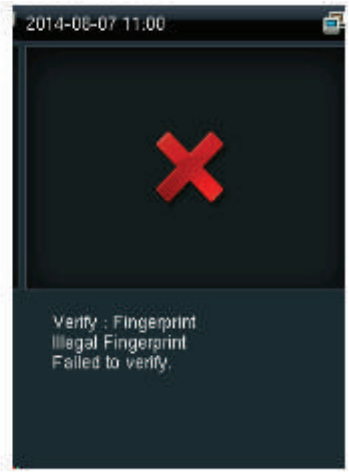
1.3 Modos de Verificación

1.3.1 Verificación de Huella dactilar

Verificación de huella 1:N: La terminal compara la huella digital recopilada por el lector con todos los datos almacenados en la terminal. Utilice la forma correcta con uno de los dedos recomendados para enrolar y verificar.

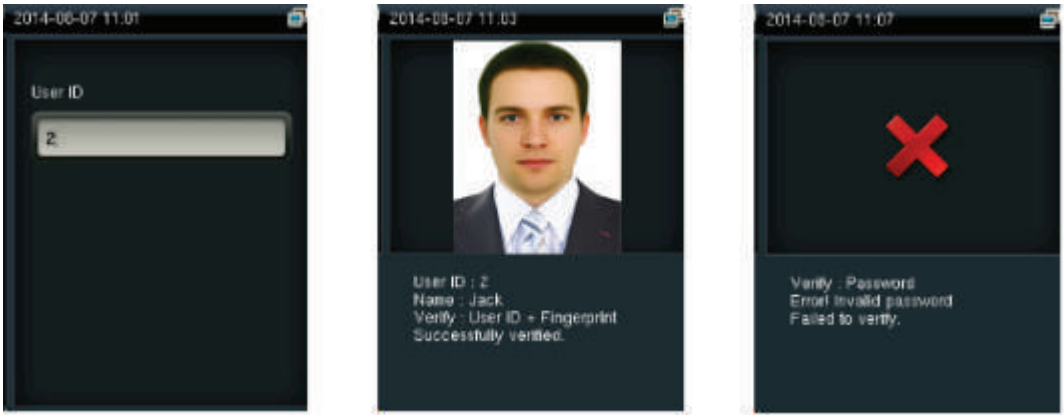
Tenemos dos mensajes después de la verificación: verificación exitosa y verificación fallida.





Verificación de huella 1:1: En este modo de verificación de huella, la terminal compara la huella digital tomada a través del lector actualmente con la que se introdujo al enrolar al usuario. Active esta función solo cuando sea difícil reconocer la huella digital.

Ingrese el número del usuario y coloque la huella, tenemos dos mensajes después de la verificación: verificación exitosa y verificación fallida.



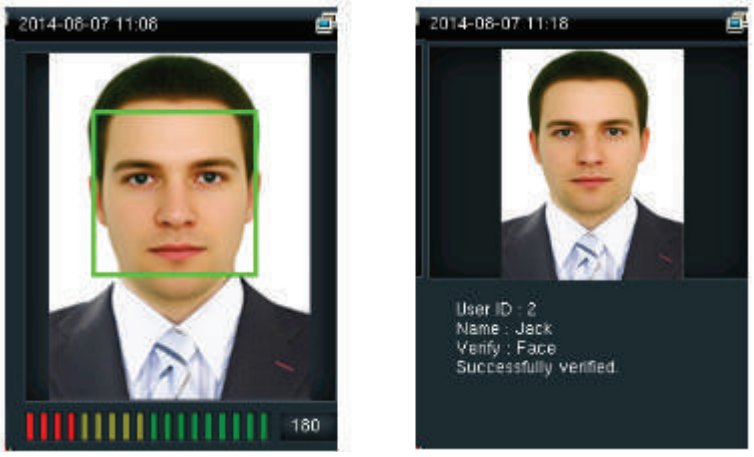
Notas:

• Si se muestra que el número ingresado es incorrecto, significa que no existe tal número.

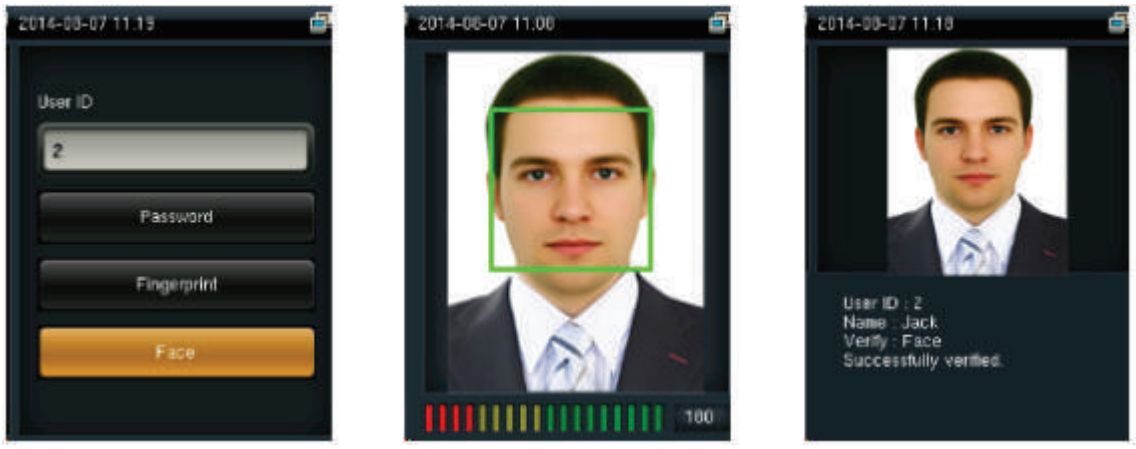
• Si el dispositivo muestra "Por favor, presione de nuevo", vuelva a colocar el dedo en el sensor de huellas. Puede probar otras 2 veces en la forma predeterminada. Si falla después de 3 intentos, regrese al menú anterior para intentar de nuevo.

1.3.2 Reconocimiento de Rostro

Verificación de rostro 1:N : La terminal compara el rostro actual con todos los almacenados en él. Utilice el método correcto de enrolamiento y verificación. Utilice la forma correcta con uno de los dedos recomendados para enrolar y verificar.

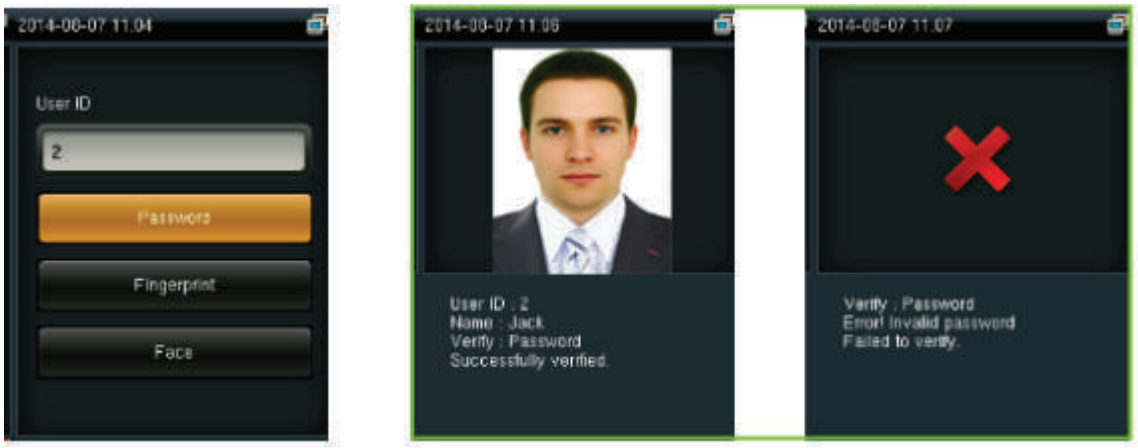


Verificación de rostro 1:1: En el modo de verificación de rostro, la terminal compara el rostro actual con la del número de empleado que se introdujo. Ingrese el número de usuario y presione rostro.



1.3.3 Verificación con contraseña

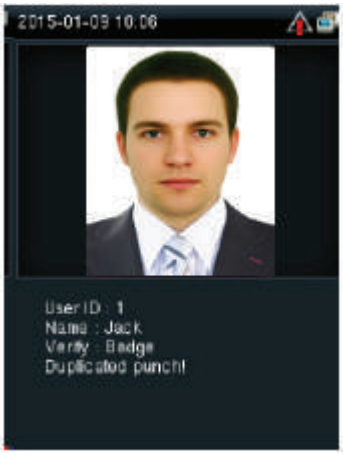
En la verificación con contraseña, la terminal compara la contraseña introducida con la del usuario registrado. Ingrese el número del usuario, presione "contraseña" e ingrésela. Tenemos dos mensajes después de la verificación:



Nota: El dispositivo dice "Contraseña inválida" cuando es fallida la verificación. Puede probar otras 2 veces de forma predeterminada. Si falla después de 3 veces, regrese al paso 1 para intentar de nuevo.

1.3.4 Verificación con Tarjeta

Acerque la tarjeta de proximidad en el área de la lectura cuando la terminal se encuentre en modo espera:



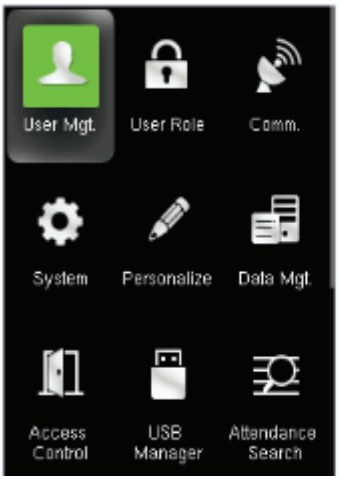
Notas:

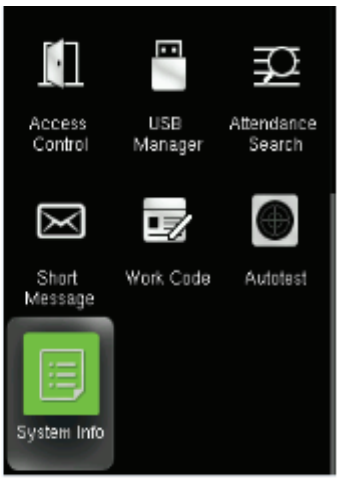
• El lector mostrará "Verificación Duplicada" cuando haya aproximado la tarjeta por segunda ocasión de forma exitosa.

• El dispositivo indicará un mensaje de error cuando la tarjeta no esté registrada.

2. Menú Principal

Presione M/OK para ingresar al menú principal. Presione la tecla para deslizarse en los iconos inferiores.





Introducción a las Funciones:

Gestión de Usuarios: Agregar, editar y borrar información de los usuarios, incluidos número de usuario, nombre, privilegio, huella, FC, contraseña, foto y parámetros de control de acceso.

Privilegio: Defina los permisos que asignará a un privilegio, es decir, el privilegio para operar los menús.

Comunicación: Configurar los parámetros de comunicación entre la PC y el dispositivo, como son la dirección IP, mascara de red, puerta de enlace, DNS, Puerto TCP, etc.

Sistema: Esta opción permite configurar parámetros como la fecha/hora, reportes de asistencia, parámetros de rostro y/o huella, resetear y actualizar via usb.

Personalizar: Esto incluye la visualización de la interfaz, el sonido, timbre, estado de asistencia y configuración de las teclas de función.

Gestión de Datos: Borra/Respaldar/Restaurar los datos almacenados en el dispositivo.

Control de Acceso: Para ajustar los parámetros de los dispositivos de control de acceso como horario, días de festivos, grupos de acceso, verificación multi-usuario, huella de amago y anti-passback.

Gestión USB: Para importar y exportar datos de usuario, registros de asistencia, código de trabajo, mensajes cortos etc. Con la USB puedes importar la información de asistencia del dispositivo al software o importar información entre dispositivos. Búsqueda de Asistencia: Esta opción permite a los empleados buscar sus registros de asistencia almacenados en el dispositivo.

Mensaje: Esta opción permite agregar, editar, borrar un mensaje público o personal.

Código de Trabajo: Permite agregar, editar, borrar códigos de trabajo. Si esta función está habilitada, debe seleccionar un código o ingresar uno después de la verificación.

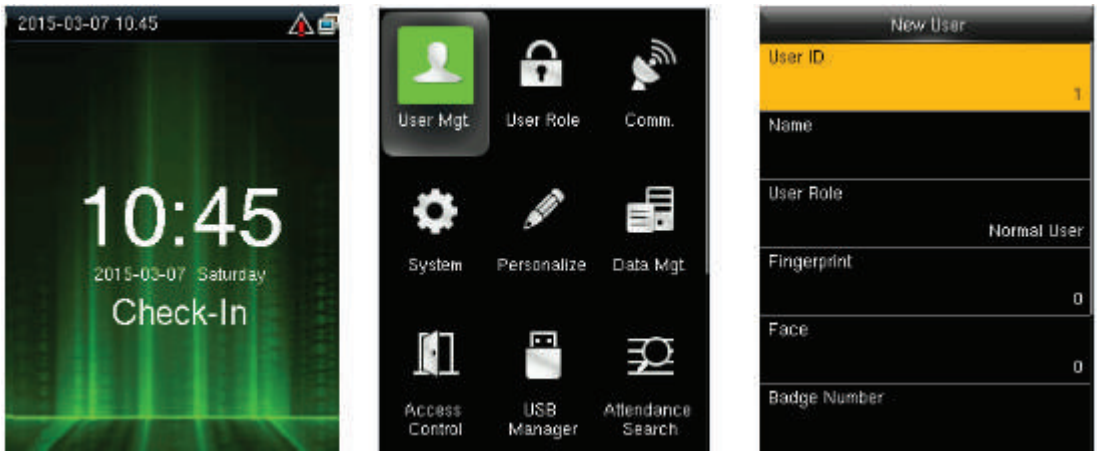
Pruebas: Para probar de forma automática funciones diferentes módulos, incluyendo la pantalla LCD, voz, teclado, sensor de huellas digitales, la cámara y el reloj de tiempo real.

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

3. Gestión de Usuarios

3.1 Agregar usuario

Solo los usuarios registrados pueden realizar verificación en el dispositivo. En la interfaz inicial, pulse [M/OK] > Usuarios > Nuevo Usuario.



3.1.1 Ingresar nombre y número de usuario

Presione ▲/▼ para seleccionar "numero de usuario" o "nombre de usuario" en el menú agregar usuario, Presione [M/OK].

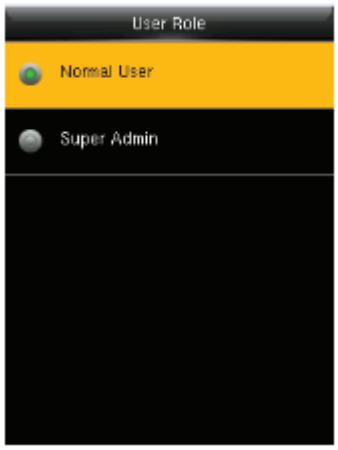


Notas: Puede ingresar el número o utilizar el consecutivo que proporciona la terminal.

Presione ◘▶ para cambiar los caracteres de entrada del teclado T9. Ingrese el nombre con el teclado T9. Para más información, consulte el "Apéndice 1: Teclado T9".

3.1.2 Seleccionar privilegios

Presione ▲/▼ para seleccionar "Privilegio" en el menú de Nuevo Usuario, presione [M/OK].



Administradores: A un administrador se le conceden los privilegios de operar todos los menús, incluido el registro de huellas digitales y contraseñas.

Usuarios Normales: Un usuario normal sólo puede registrar su asistencia, así como consultar sus registros de asistencia y mensajes.

Nota: Se recomienda enrolar un administrador para un mejor manejo de la información.

3.1.3 Enrolar una huella

Presione ▲/▼ para seleccionar "Huella Digital" en el menú de agregar usuario, presione [M/OK].





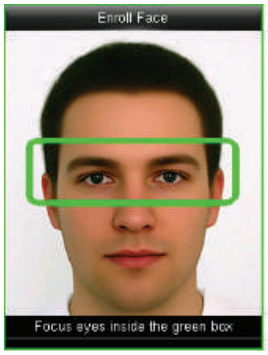
1. Presione el número de correspondiente al dedo que desea enrolar, Presione [M/OK].

2. Coloque 3 veces su dedo en el sensor cuando el lector lo indique.

Nota: Necesita volver a enrolar si el lector le indica "por favor intente de nuevo".

3.1.4 Agregar un rostro

Presione ▲/▼ para seleccionar Rostro en el menú de agregar usuario, Presione [M/OK].





Coloque sus ojos dentro del rectángulo verde, como lo indica el dispositivo.

Nota: Durante el enrolamiento una foto será tomada y guardada de forma automática en el dispositivo, esta foto se usará como "foto de usuario" a menos que se toma otra.

3.1.5 Enrolar una tarjeta

Presione ▲/▼ para seleccionar Número de Tarjeta en el menú de agregar usuario, presione [M/OK]:





Acerca tu tarjeta al lector de proximidad o alrededor del sensor de huella.

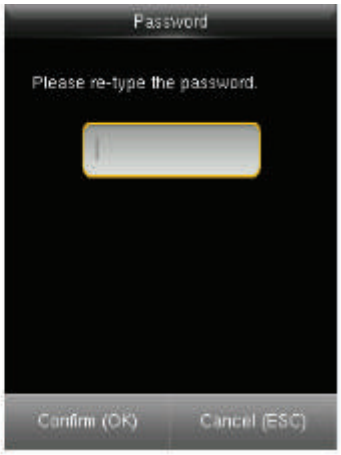
Nota: ¡Si el dispositivo muestra "¡Error! Tarjeta ya enrolada", probar con otra tarjeta.

La tarjeta debe ser de proximidad RFID.

3.1.6 Agregar una contraseña

Presione ▲/▼ para seleccionar "Contraseña" en el menú agregar usuario, Presione [M/OK].





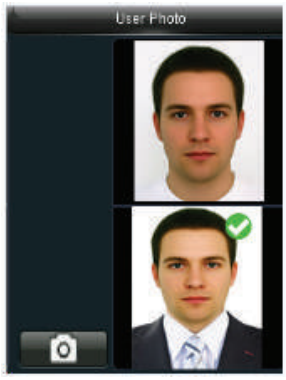
Acerca tu tarjeta al lector de proximidad o alrededor de sensor de huella.

Nota: ¡Si el dispositivo muestra "Error! Tarjeta ya enrolada" probar con otra tarjeta.

La tarjeta debe ser de proximidad.

3.1.7 Capturar foto

Presione ▲/▼ para seleccionar "Foto del usuario" en el menú de agregar usuario, Presione [M/OK].

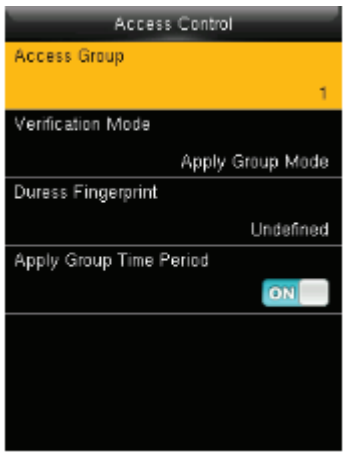


Presione [M/OK] para capturar la foto.

La foto se mostrará en la pantalla después de realizar una verificación exitosa.

3.1.8 Control de acceso

Presione ▲/▼ para seleccionar "control de acceso" en el menú agregar usuario, Presione [M/OK].



Grupo de acceso: Para asignar los usuarios a diferentes grupos de control de acceso.

Modo de Verificación: El usuario puede elegir entre el modo de verificación del grupo o uno individual.

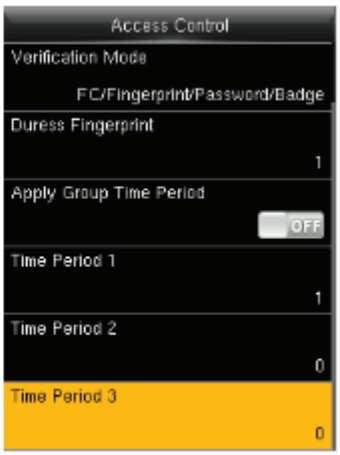
Usar horario de grupo: Si desea aplicar el horario de grupo a los nuevos usuarios. Seleccione un horario especifico para cada usuario si no.

Nota: para más detalles acerca de control de acceso, por favor consulte "9.- Control de Acceso."

Seleccionar grupo de acceso, huella de amago y horario de grupo:





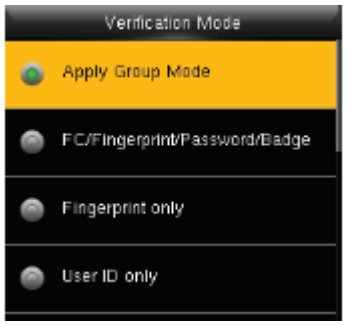


1.Número máximo de grupo es 99.

2.Seleccionar una o más de una huella para amago o coacción. La alarma del dispositivo se activará siempre que valide la huella de amago.

3.El número máximo para el horario es 50.

Seleccionar modo de verificación:



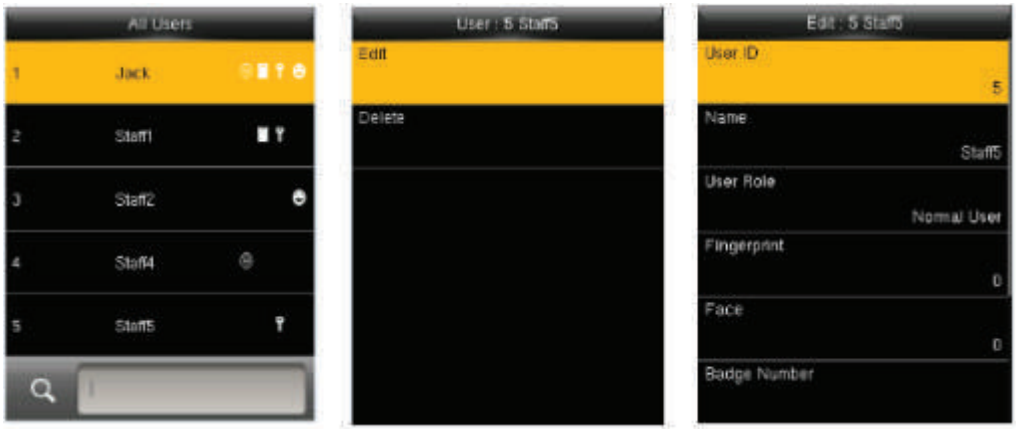
Aplicar modo grupo: El usuario utiliza el modo de verificación del grupo. Si no utiliza el modo grupo de validación, se tienen varias combinaciones: Rostro/Huella/Contraseña/Tarjeta, solo huella, solo número de usuario, contraseña, solo tarjeta, huella/contraseña, etc.

Cuando seleccione una de las opciones de combinación, necesitará verificar con todos los datos del modo de validación. Por ejemplo, si selecciona huella/contraseña necesita verificar con ambos, huella y contraseña para que la verificación sea exitosa.

3.2 Gestión de usuarios

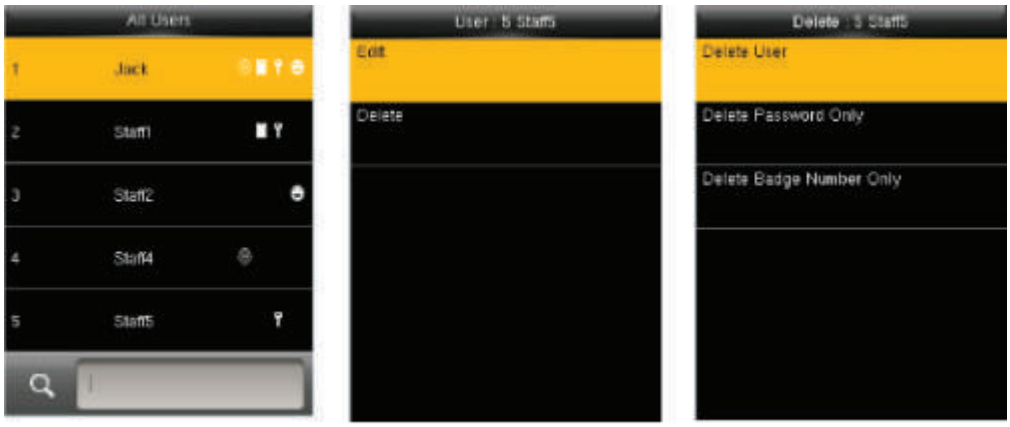
Ingresar al menú principal. Ingresar a "gestión de usuarios " → "Todos los usuarios".

Editar usuario
Presione ▲/▼ para seleccionar el usuario a editar y Presione [M/OK]. Ingresar a "Editar":

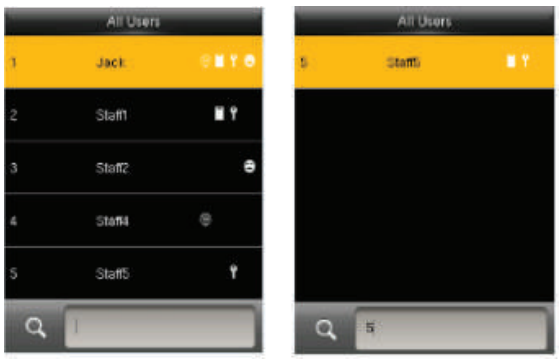


Se puede modificar toda la información excepto el número de usuario.

Borrar un usuario
Presione ▲/▼ para seleccionar el usuario a editar y Presione [M/OK]. Seleccionar "Borrar":



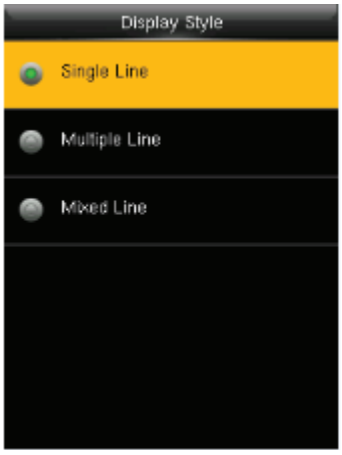
Puede seleccionar diferentes tipos de información del usuario a borrar.



Buscar un usuario
Colocar el número de usuario para realizar una búsqueda rápida, una vez localizado puede editar o eliminar.

3.3 Estilo de pantalla

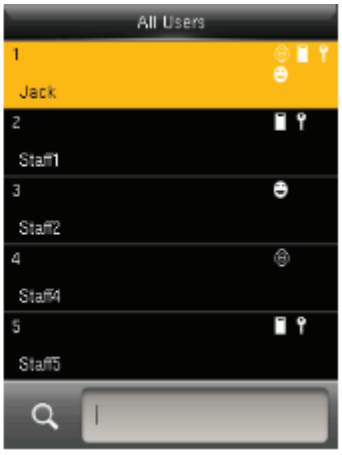
El estilo por defecto es "línea simple". Ingresar a usuario → estilo de pantalla:



Línea Simple



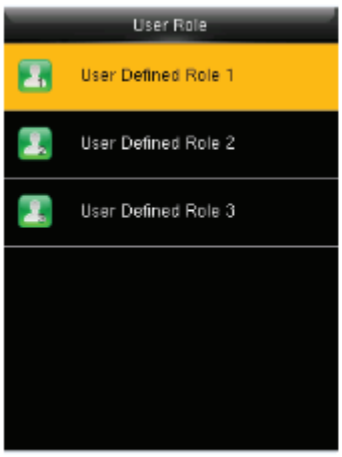
Línea Múltiple

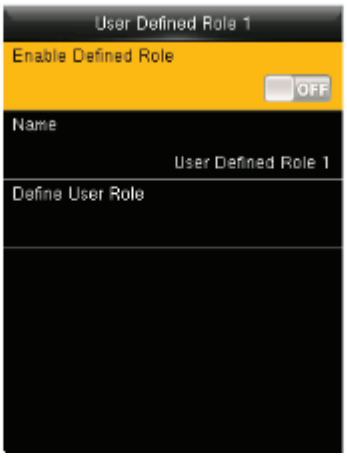


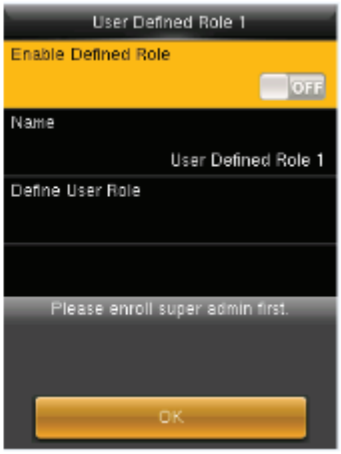
Línea

4. Privilegios del Usuario

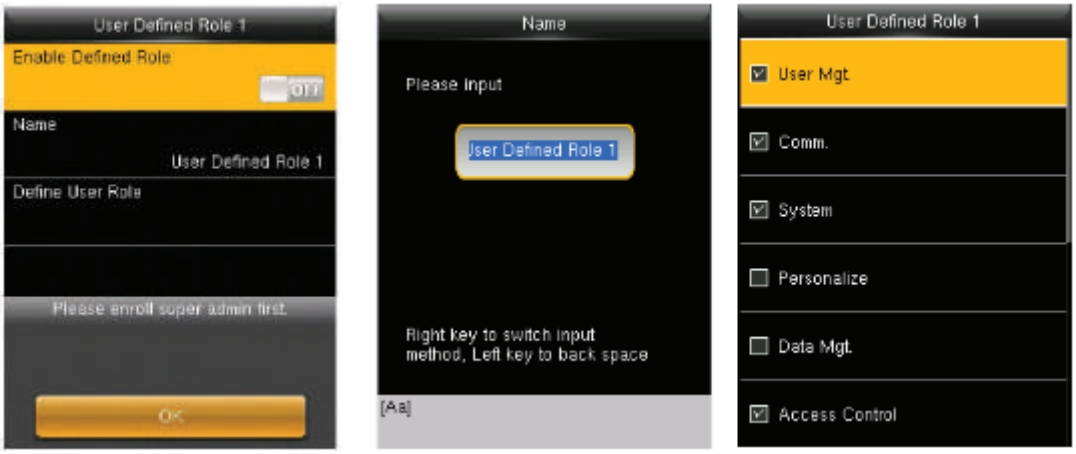
Se configuran los permisos de operación del menú que puede tener un usuario. Se cuenta con 3 perfiles de privilegios. Ingrese a "Privilegios" y seleccione el rol a editar:







Un usuario administrador debe ser definido antes de definir un nuevo privilegio, o este no podrá ser habilitado.

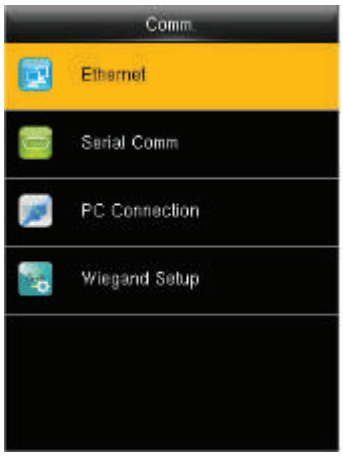


Definiendo nombre y funciones

1. Ingresar el nombre con el teclado.
2. Puede seleccionar más de un menú para un rol. Presione [M/OK] para seleccionarlo.

5. Ajustes de Comunicación

Para definir los parámetros de comunicación ingresar a comunicación:



Ethernet: El dispositivo de comunica vía red al pc configurando los parámetros correspondientes.

Comunicación serial: El dispositivo se comunica vía serial al pc configurando el puerto.

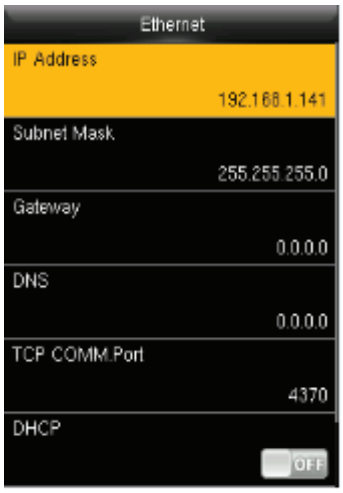
Conexión a PC: Definir contraseña y numero de dispositivo para realizar la conexión al software.

Ajustes Wiegand*: Definir los parámetros de salida wiegand. Para más detalles ir a "5.4 Ajustes Wiegand".

ADMS*: Configuraciones para el servidor ADMS.

5.1 Ethernet

Ingresar a Comunicación ⟶ "Ethernet"



Dirección IP: Modificar si es necesario. Esta no puede ser igual a la de la PC.

Máscara de Subred: Modificar si es necesario.

Puerta de enlace: Este parámetro es necesario si el dispositivo y la PC están en diferentes segmentos de red.

DNS: Configurar la dirección del servidor DNS.

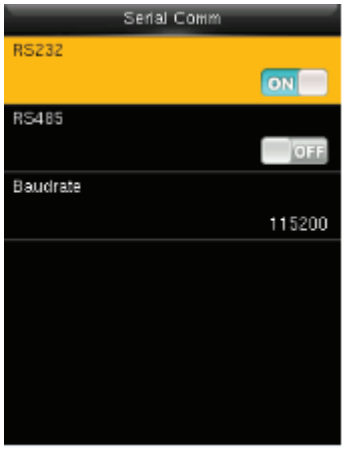
Puerto de comunicación: Configurar el puerto de comunicación TCP.

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.

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

5.2 Comunicación serial

Ingresar a Comunicación ⟶ "Comunicación Serial"



RS232: Si utiliza el puerto RS232 para la comunicación a la PC.

RS485: Si utiliza el puerto RS485 para la comunicación a la PC.

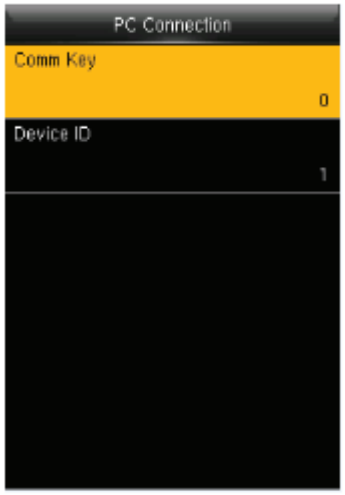
Velocidad de Baudios: Se configura para comunicar con la PC . solo para el puerto RS232 para rápida transferencia de datos es recomendado.

Nota: Tenemos 5 opciones de velocidades para el RS232: 9600, 19200, 38400, 57600, y 115200; "9600" no aplica para el RS485. Reiniciar el dispositivo para aplicar los cambios.

5.3 Conexión a PC

Para mejorar la seguridad de los datos, una Clave de Comunicación necesita ser establecida.

Ingresar al menú Comunicación ⟶ Conexión a PC

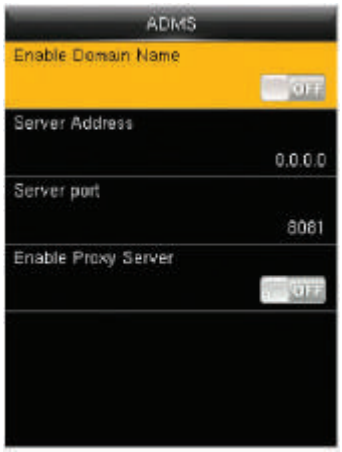


Clave de comunicación: Definir una contraseña de 1 a 6 dígitos, la contraseña debe ser colocada en el software al realizar la comunicación.

ID de Dispositivo: El rango del número de dispositivo debe ser de 1-254. Si el RSR232 o RS485 está habilitado el número de id debe ser colocado en el software para realizar la comunicación.

5.4 ADMS

(Solo aplicable para modelos KF160, 460 - MB10, 360, 460)



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

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

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

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

5.5 Ajustes Wiegand

La comunicación wiegand realiza la comunicación entre dispositivos del número de empleado y la tarjeta de proximidad. Cuando se realiza conexión maestro/esclavo, los datos verificados en el esclavo se mostrarán en el maestro. Esto significa que una vez que se realiza la verificación exitosa en el esclavo el maestro recibe la señal y liberar el acceso. Nuestro dispositivo solo puede ser utilizado como esclavo, por lo que la salida wiegand debe ser configurada.

Ingresar a Comunicación → Ajustes Wiegand → Salida Wiegand.



Formato Wiegand: El dispositivo cuenta con 5 formatos wiegand incorporados: Wiegand 26, Wiegand 34, Wiegand 36, Wiegand 37 and Wiegand 50. Cada formato tiene dos tipos de Wiegand x y Wiegand xa excepto Wiegand 50. Puede ser seleccionado más un formato Wiegand.

Bits de Salida Wiegand: Seleccionar los bits de wiegand en base al formato wiegand establecido. Si selecciono todos los formatos wiegand para ser utilizados, tendrá 5 opciones a elegir.

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. El valor predeterminado oscila de 0 a 256.

Amplitud de Pulso: La amplitud del pulso enviado por Wiegand. El valor puede ajustarse entre 20 a 100 microsegundos.

Intervalo de Pulso: El valor 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.

Definición de formato Wiegand

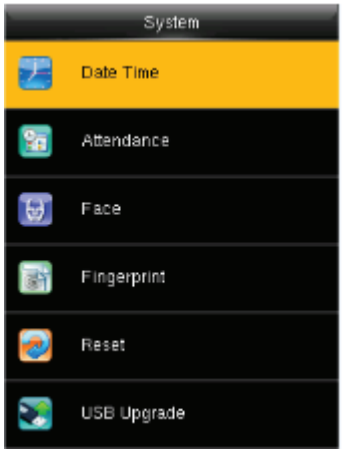
El formato wiegand consta de dos cadenas de caracteres: los bits de datos y los bits de paridad. La siguiente tabla es la definición de esos cinco formatos wiegand:

Formato Wiegand	Descripción
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.
Wiegand 34	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.

Wiegand 34a	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.
Wiegand 36	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.
Wiegand 36a	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.
Wiegand 37	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.
Wiegand 37a	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.
Wiegand 50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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. Configuración de Sistema

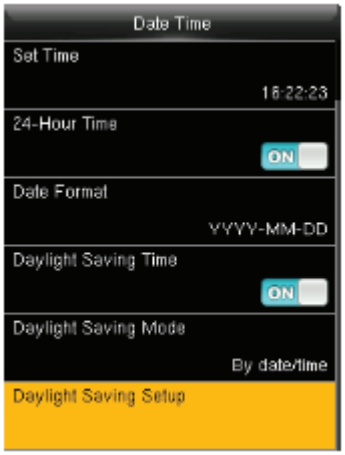
Configurar parámetros relacionados con el sistema. Ingresar a "Sistema":



El reseteo del dispositivo no borrara información de usuario y registros de checadas.

6.1 Fecha y Hora

Configurar la fecha y hora del dispositivo. Ingresar a "Sistema" ⟶ "Fecha/Hora":



Fecha/Hora: Configurar la fecha y hora al dispositivo.

Formato de 24 Horas: Si utiliza el formato de 24 horas, en caso contrario el formato de 12 horas será el mostrado en pantalla.

Formato de fecha: Definir el formato de fecha: YY-MM-DD, YY/MM/DD, YY.MM.DD, DD-MM-YY, Etc.

Horario de verano

El Horario de Verano, que también llamado DST, es un sistema de ajuste de la hora local con el fin de ahorrar energía. El tiempo que se adopta durante las fechas establecidas se llama "Horario de Verano". Por lo general, se adelanta una hora en el verano. Esto permite reducir la iluminación del dispositivo para ahorrar energía. En otoño, el tiempo se reanudará el tiempo estándar. Las regulaciones son diferentes en distintos países.

El dispositivo cuenta con la opción DTS para ajustar el tiempo una hora a las XX (hora) XX (día) XX (mes), y retroceda el tiempo una hora a XX (hora) XX (día) XX (mes). Por ejemplo, Programar el dispositivo para que adelante una hora a las 8:00 el día 1 de abril y retrasar el dispositivo una hora a las 8:00 el día 1 de octubre.

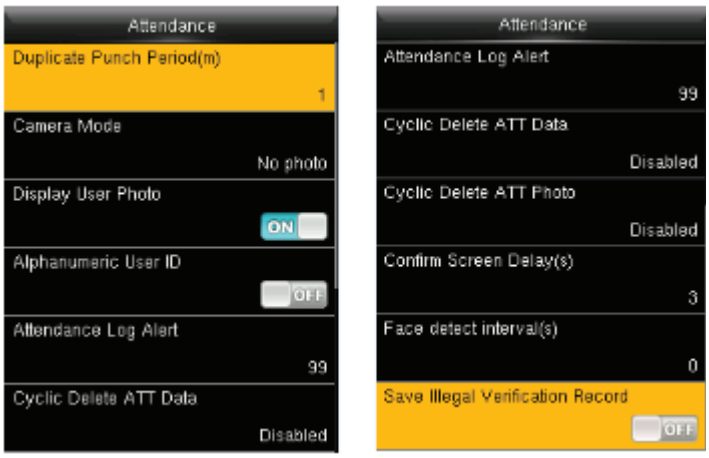
Modo de Horario de Verano: Puede elegir entre el modo por fecha o por semana.

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

Nota: La configuración del horario de verano no puede programarse para un año posterior, más específicamente, la fecha de fin del horario de verano debe ser posterior a la fecha de inicio, pero en el mismo año.

6.2 Ajustes de Asistencia

Configurar parámetros de asistencia. Ingresar a Sistema ⟶ "Asistencia".



Los Parámetros para la interfaz de Asistencia son los siguientes:

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

Modo de Cámara: Sirve para establecer si se tomarán y guardarán fotos durante la verificación.
• 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.

Numero de usuario Alfanumérico∗: Definir si el número de usuario puede ser alfanumérico. El número de usuario con caracteres alfanuméricos es conveniente para ordenar y administrar usuarios.

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 establecerse a un valor de entre 1 a 99.

Limpieza periódica de Eventos: La cantidad de registros de asistencia que serán eliminados cada vez que se llega a la máxima capacidad de almacenamiento. La función puede establecerse a un valor de entre 1 a 99.

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 establecerse a un valor de entre 1 a 99.

Limpieza periódica de fotos de la lista negra∗: Cuando se han almacenado más de 999 fotos en el dispositivo, el sistema borrara automáticamente esas fotos.

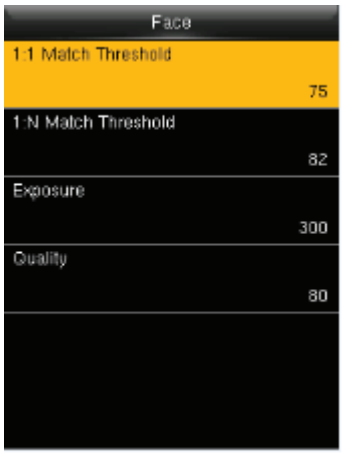
Duración de Pantalla de Confirmación (s): El tiempo que se muestra en la pantalla el resultado de las verificaciones. El valor oscila de 1 a 9 segundos.

Duración de pantalla de detección facial (s): El tiempo para la misma verificación de rostro, el valor puede establecerse de 0 a 9 segundos.

Regla de expiración: Una vez habilitado, se tienen tres opciones de la regla: Mantener usuario, no auditar futuras validaciones/ Mantener usuario y auditar futuras validaciones/ Borrar Usuario.

6.3 Parámetros para validación de rostro

Configurar parámetros de rostro. Ingresar al menú sistema → Rostro



Umbral de Verificación 1:1: Es la similitud entre el rostro verificar y el rostro registrado del usuario.

Umbral de Verificación 1:N: Es la similitud entre el rostro a verificar y todos los rostros registrados.

Exposición: Defina el valor de exposición de la cámara. El rango va de 40 a 1000.

Calidad: Defina el umbral de calidad para las imágenes obtenidas. La terminal acepta las imágenes faciales y las procesa adoptando el algoritmo facial cuando su calidad es mayor al umbral seleccionado; de lo contrario, las imágenes son filtradas. El valor oscila es 50-150.

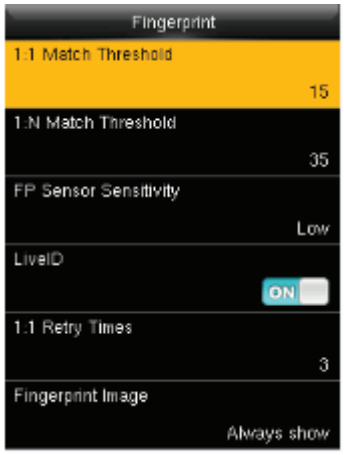
Nota: Realizar una configuración incorrecta de los valores de exposición y calidad, podrían provocar afectaciones severas al funcionamiento del equipo. Por favor realice estos ajustes bajo la supervisión de nuestro personal certificado.

Umbral de Verificación Recomendado:

FRR	FAR	Umbral de coincidencia	
		1:N	1:1
Alto	Bajo	85	80
Medio	Medio	82	75
Bajo	Alto	80	70

6.4 Ajustes de Huella

Configurar parámetros de huella. Ingresar al menú "Sistema" → "Huella Digital":



Umbral de Verificación 1:1: Es la similitud entre la huella digital a verificar y la huella registrada del usuario.

Umbral de Verificación 1:N: Es la similitud entre la huella digital a verificar y todas las huellas registradas.

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".

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.

Umbral de Verificación Recomendado:

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

6.5 Restablecer valores de fábrica

Reestablece información como ajustes de comunicación, configuraciones del sistema y configuraciones de personalización.

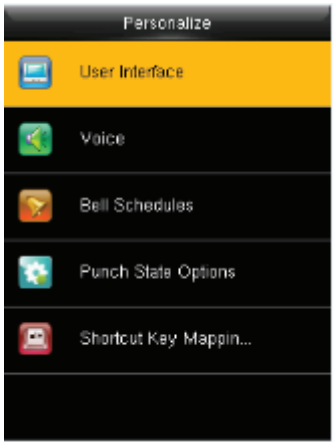


6.6 Actualización por USB

El firmware del dispositivo puede ser actualizado por medio de la USB. La actualización de Firmware no se recomienda bajo circunstancias normales. Si necesita un archivo de actualización, póngase en contacto con nuestro soporte técnico.

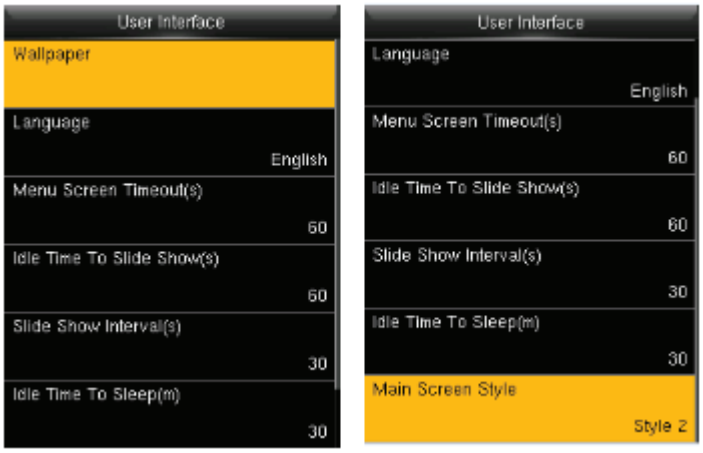
7. Configuración de Personalización

Configurar algunos parámetros usuales. Ingresar al menú "Personalizar".



7.1 Interfaz de Usuario

Configurar los parámetros mostrados. Ingresar al menú "Personalización" ⟶ "interfaz del usuario".



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

Idioma: Seleccione el idioma del dispositivo.

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

Tiempo de Espera para Diapositivas (s): Cuando no se haga ninguna operación en la interfaz inicial después del horario seleccionado, iniciará una presentación de diapositivas. El valor puede establecerse entre 3 a 999 segundos.

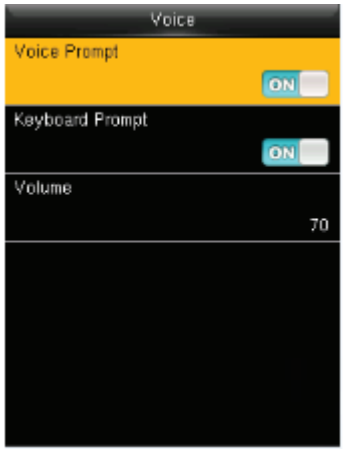
Intervalo de tiempo para Dispositivas (s): Se refiere al intervalo de tiempo entre dispositivas diferentes. El valor puede establecerse entre 3 a 999 segundos.

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.

Estilo de la Pantalla Principal: Seleccione el estilo de pantalla deseado (se cuenta con 3 estilos).

7.2 Ajustes de Voz

Configurar parámetros de voz. Ingresar al menú "Personalizar" → "Voz":

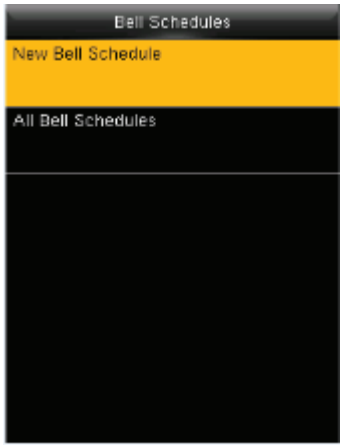


Sonido de Voz: Seleccione si desea activar los mensajes de voz durante la operación del dispositivo.

Sonido del Teclado: Seleccione si desea activar los mensajes de voz durante la operación del teclado.

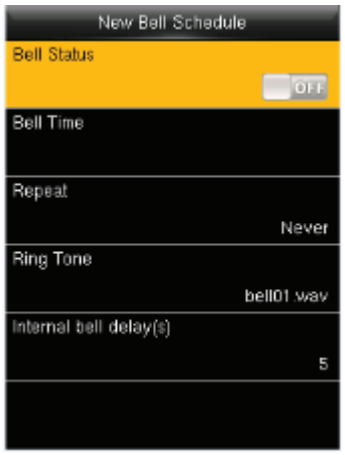
Volumen: Ajuste el volumen del dispositivo.

7.3 Ajustes de Timbres



Muchas empresas eligen utilizar un timbre para dar aviso del inicio/fin de la jornada laboral. Se pueden configurar más de un timbre por tono. Ingresar al menú "personalizar" → "Ajustes de Timbres":

Nuevo Timbre Programado
Ingresar al menú "personalizar" → "Ajustes de timbres" → "nuevo timbre programado":



Estatus de Timbre: Configurar si habilitara el timbre

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

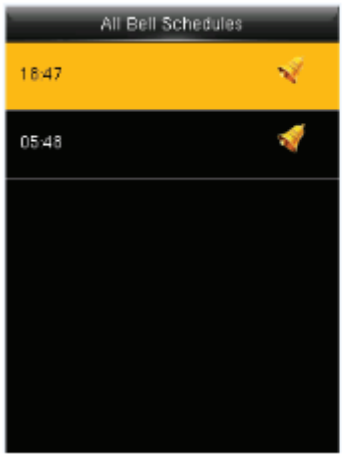
Repetir: Establecer si el timbre se repetira.

Tono de Timbre: El tono que suena como timbre.

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

Editar timbre

Ingresar al menú "personalizar" → "timbre programado" → "Todos los timbres programados":





1. Seleccionar timbre a editar.

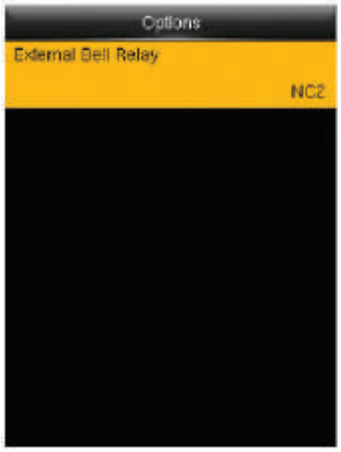
2. Presione "Editar" para modificar la información.

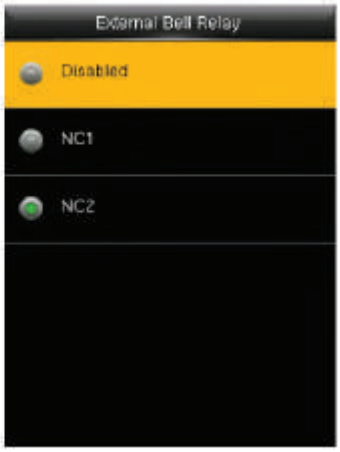
Borrar timbre

Ingresar al menú "Personalizar" → "Todos los timbres programados", Seleccionar el timbre a eliminar.

Opciones

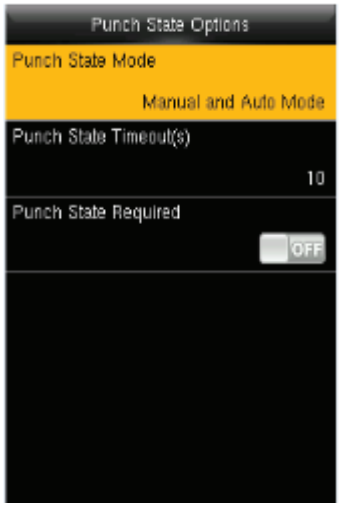
Cuando se usa la función de timbre externo, configure la salida del dispositivo para timbre externo.





7.4 Ajustes de Estados de Asistencia →

Para configurar las teclas con las que selecciona un Estado de Asistencia. Ingresar al menú "Personalizar" "Opciones de Estados de Asistencia".



Modo de Estado de Asistencia: Apagado: Deshabilita la opción teclas de Estado de Asistencia.

Modo Manual: Los usuarios seleccionaran la tecla de asistencia de forma directa presionando la tecla deseada.

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

Modo Manual & Automático: Un Estado de Asistencia que usted seleccione manualmente cambiará automáticamente cuando pase el tiempo de espera configurado.

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

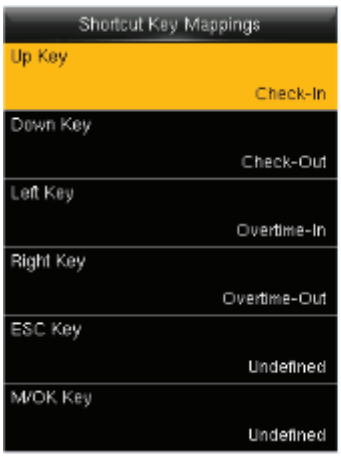
Modo Fijo: Un Estado de Asistencia es siempre mostrado y no puede ser cambiado.

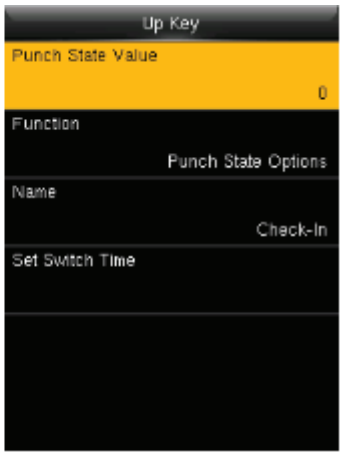
Tiempo de Espera del Estado de Asistencia (s): Especificar el tiempo que se muestra el Estado de Asistencia seleccionado. El valor varía de 5 a 999 segundos.

Estado de Asistencia Requerido: Especificar si el Estado de Asistencia debe ser seleccionado durante la verificación.
Nota: Hay 4 Estados de Asistencia: Entrada, Salida, Entrada a Tiempo Extra y Salida de Tiempo Extra.

7.5 Asignación de Teclas de Atajo

Usted puede definir las teclas ▲, ▼ /, [ESC], [M/OK] que sirvan de atajo hacia un Estado de Asistencia o hacia funciones del menú. Cuando el dispositivo se encuentre en la interfaz principal, oprima la Tecla de Atajo correspondiente para mostrar un Estado de Asistencia o para acceder a la interfaz de un menú de operaciones de forma rápida. Ingresar al menú "Personalizar" ⟶ "Asignación de teclas de atajo" y seleccionar la tecla a configurar.





Nota: Solo cuando se selecciona estado de asistencia como función, aparecerán las opciones: valor de estado de asistencia, nombre y configurar hora de cambio en el menú. El estado de asistencia se puede configurar como cambio automático. El estado de asistencia cambiará automáticamente una vez que se cumpla el tiempo configurado para dicho cambio.

Cuando se presione una tecla de estado de asistencia, el dispositivo no activará el estado de asistencia si el Modo de Estado de Asistencia se estableció en Desactivado (OFF).

Valor de estado de asistencia: El dispositivo tiene 4 valores diferentes que corresponden a cuatro estados predeterminados. Valor 0 corresponde a estado de asistencia Entrada, 1 para Salida, 4 Entrada de tiempo extra, 5 Salida de tiempo extra. El rango varia de 0 a 250.

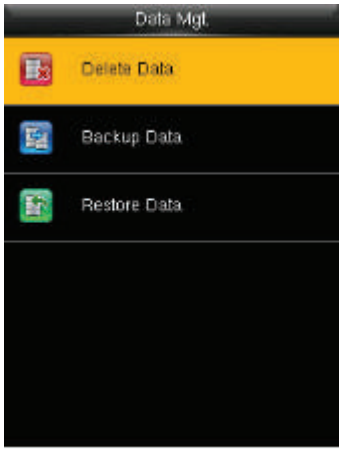
Función: Seleccione opciones de estado de asistencia o funciones de menú.

Nombre: Ingresar el nombre del estado de asistencia.

Configurar hora de cambio: Definir la hora en que se realizará el cambio del estado de asistencia.

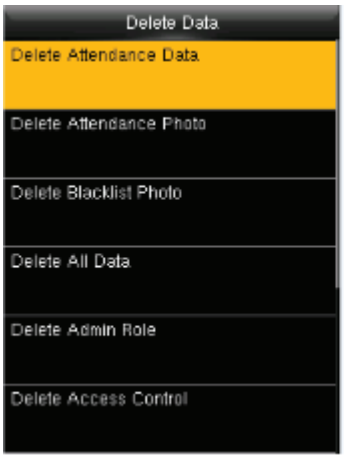
8. Gestión de Datos

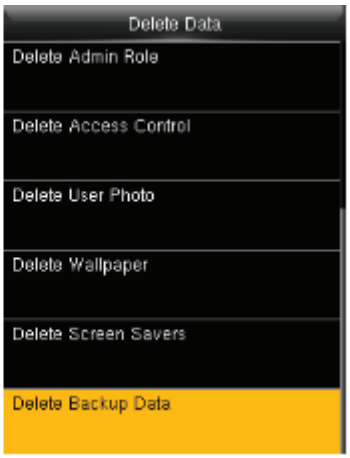
Administrar la información guardada en el dispositivo. Ingresar al menú "Datos":



8.1 Eliminar Datos

Ingresar al menú "Datos" → "Eliminar Datos":





Borrar Registros de Asistencia: Eliminar todos los registros de asistencia.

Borrar Registros de Fotos: Eliminar todos los registros de fotos de asistencia de los usuarios.

Borrar Fotos de la Lista Negra: Elimina las fotos guardadas de las verificaciones fallidas.

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

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

Borrar Foto del usuario: Borrar todas las fotos de los usuarios.

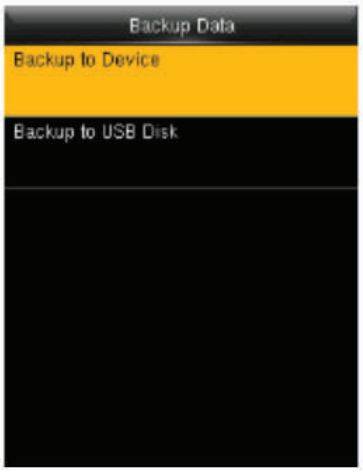
Borrar Fondo de Pantalla: Eliminar todos los fondos de pantalla en el dispositivo.

Borrar Protectores de Pantalla: Eliminar protectores de pantalla seleccionados o todos los protectores de pantalla en el dispositivo. (Para más detalles sobre cargar protectores de pantalla, favor de consultar Anexo 2 Procedimiento para Cargar Imágenes)

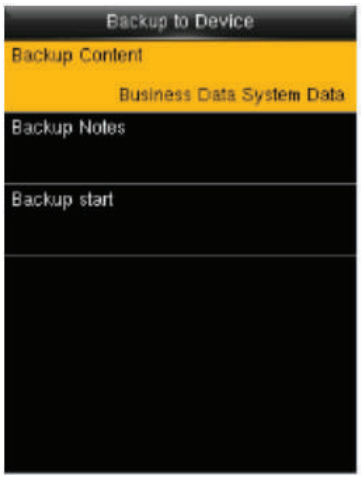
Borrar Datos de Respaldo: Eliminar los datos pertenecientes a la copia de seguridad.

8.2 Respaldar Datos

Para respaldar los datos de la empresa o de configuración en una unidad USB. Ingresar al menú "Datos" → "Respaldar Datos":



Seleccionar ruta



Seleccionar el tipo de contenido

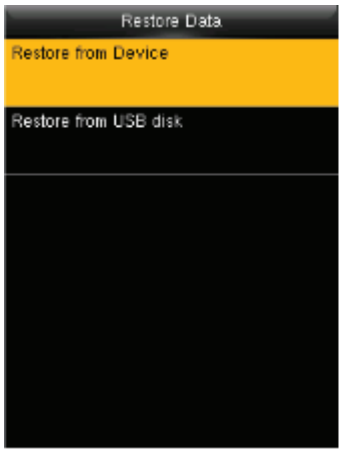


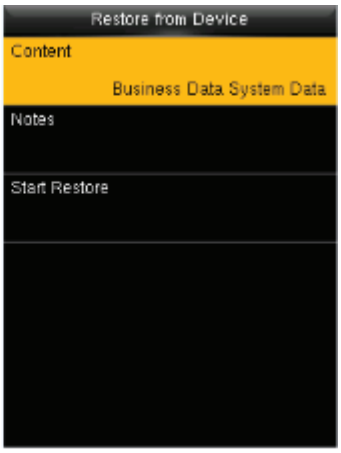
Escribir notas del respaldo

Nota: Cuando realice un respaldo de los datos a una unidad USB, primero debe insertar la unidad USB y después Presione [M/OK] para respaldar los datos a la unidad USB.

8.3 Restaurar Datos

Para restaurar los datos al dispositivo. Ingresar al menú "Datos" ⟶ "Restaurar Datos":





1. Seleccionar la ruta.

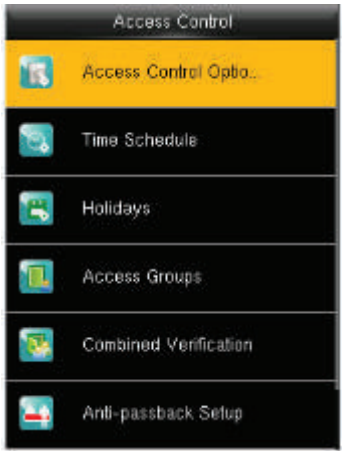
2. Seleccionar el tipo de contenido.

3. Iniciar restauración.

Nota: Cuando restaure los datos desde la unidad USB necesita, insertar la unidad USB en el dispositivo que contiene el respaldo.

9. Control de Acceso

Configuración de parámetros de control de acceso a los usuarios. Ingresar al menú "Control de Acceso".



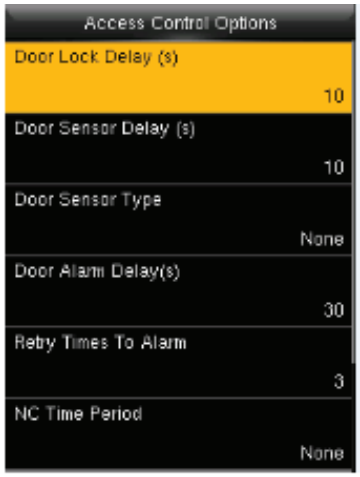
Para poder acceder, el usuario registrado debe cumplir las siguientes condiciones:

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). Un nuevo usuario se asigna al grupo 1 y la zona de tiempo 1 de forma predeterminada.

9.1 Opciones de control de acceso

Ingresar al menú "Control de Acceso" ⟶ "Opciones de control de acceso"



Retardo de la cerradura (s): Tiempo en que la cerradura electrónica permanece abierta. El valor oscila entre 0 a 10 segundos.

Retardo de sensor de puerta (s): El sensor de la puerta se activará luego de un horario. El valor oscila entre 0 a 255 segundos.

Tipo de Sensor de la Puerta: Incluye Ninguno (sin sensor de puerta), Normalmente Abierto (NO) y Normalmente Cerrado (NC).

Retardo de Alarma de Puerta(s): Cuando el estado del sensor de puerta no coincide con el tipo de sensor de puerta, se activará la alarma luego de este horario (el rango varía de 1 a 999 segundos)

Reintentos para Activar Alarma: Cuando el número de verificaciones fallidas llega al valor establecido (el rango varía de 0 a 9 intentos), la alarma se activará. Si el valor es 0, la alarma no se activará después de verificaciones fallidas.

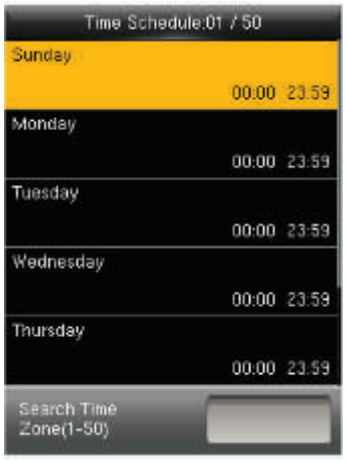
Horario NC: Establece el horario para el modo Normalmente Cerrado, de forma que nadie pueda acceder durante este periodo.

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

Nota: Cuando la zona de tiempo se configura para NO ó NC configurar sensor de puerta en modo ninguno, o la señal de alarma se activará durante la zona horaria de NC ó NO.

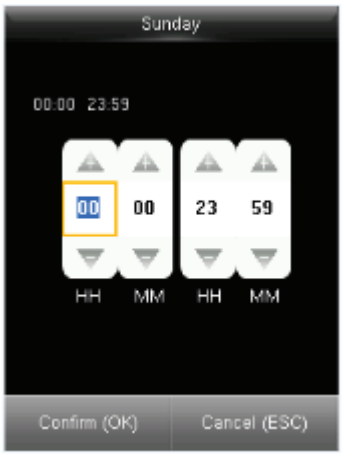
9.2 Configuración de Horarios

Configuración de horarios para la apertura de la puerta. "Control de acceso" → "Configuración de Horario":



El horario es la unidad de tiempo mínima de los ajustes de control de acceso; se pueden establecer un máximo de 50 horarios en el sistema. Cada Horario consiste de 7 secciones de tiempo (una semana) y 3 secciones de días festivos, y cada sección de tiempo es el tiempo válido dentro de 24 horas. A cada usuario se le pueden asignar un máximo de 3 horarios. El horario será válido siempre y cuando la hora de verificación caiga dentro de alguno de los horarios. El formato de cada intervalo de tiempo dentro de un horario es HH:MM – HH:MM, es decir, precisión de un minuto.

Cada zona de tiempo puede ser editada o puede realizar una búsqueda por el número de la zona de tiempo en el cuadro de búsqueda de forma rápida.

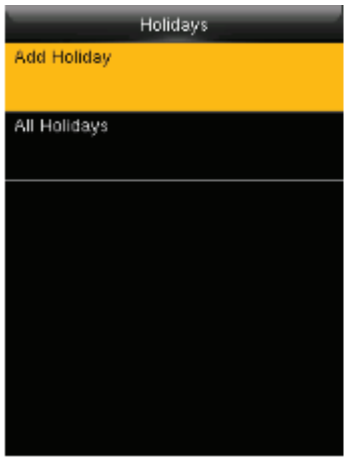


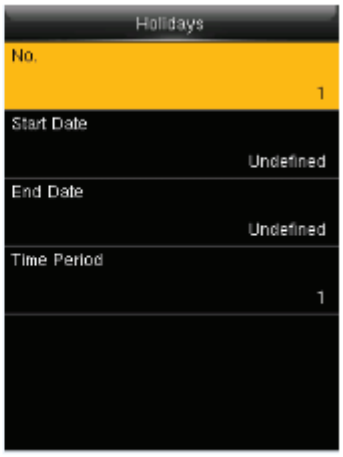
Cuando la hora final es antes de la hora inicial (por ejemplo, 23:57 – 23:56), significa que la puerta se mantiene cerrada todo el día. Cuando la hora final es después de la inicial (por ejemplo, 00:00 – 23:59), significa que el horario es válido. Horario Válido: 00:00 – 23:59 (Válido todo el día) o cuando la hora final sea después de la hora inicial.

Nota: Por defecto, el horario número 1 del dispositivo está configurado para permitir el acceso todo el día (de forma que los usuarios nuevos puedan abrir la puerta).

9.3 Ajustes de días festivos

En los días festivos se puede requerir de un control de acceso especial. Después de configurar el horario de tiempo para acceso en días festivos, la zona de tiempo para acceso del usuario esta. Ingresar al menú "Control de Acceso" → "Día Festivo".

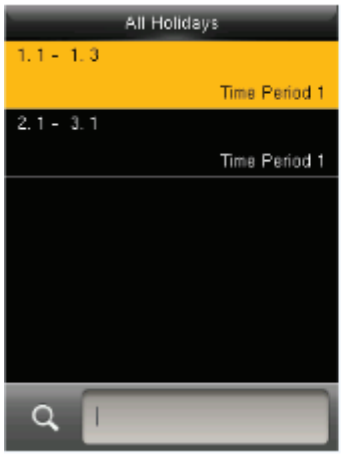


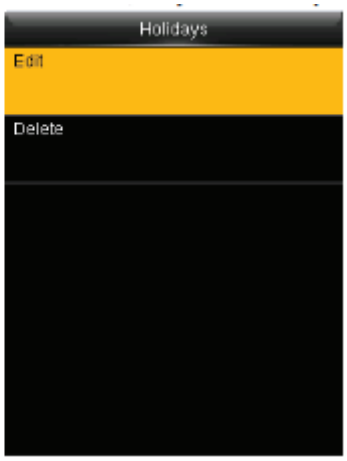


1. Presione "Agregar día festivo".

2. Editar las opciones.

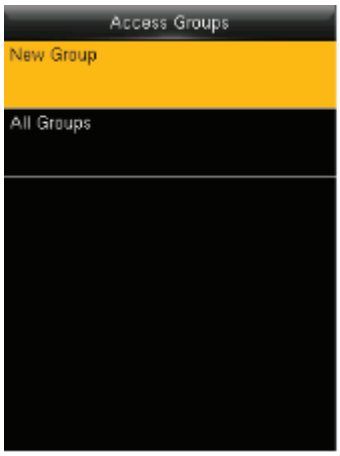
Se puede elegir para editar o borrar, o puede ingresar un número de día festivo a configurar.

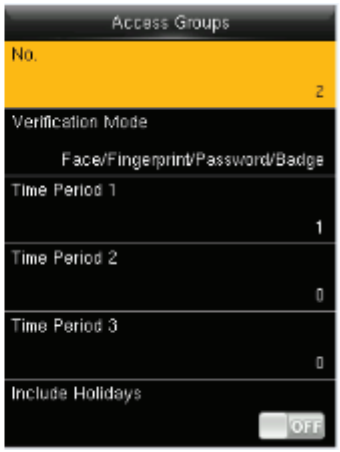




9.4 Grupos de Acceso

Los grupos son para administrar usuarios en grupos. Por defecto, los usuarios nuevos pertenecen al Grupo de Acceso 1, pero pueden ser asignados a otro grupo de acceso. Ingresar al menú "Control de Acceso" ⟶ "Grupos de Acceso":



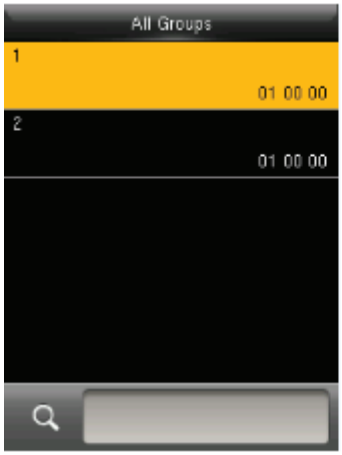


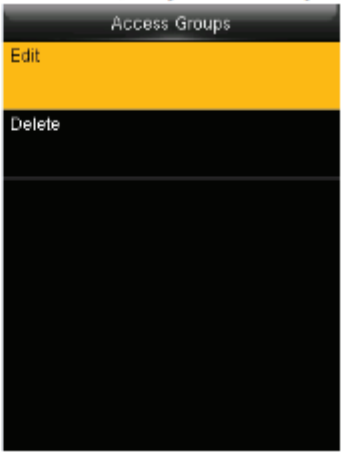
1. Presione "Nuevo Grupo".

2. Editar las opciones.

Nota: Solo cuando hay intersección entre la zona del grupo y la zona de tiempo para días festivos los miembros del grupo tendrán acceso si está habilitada la opción de días festivos o si los horarios de control de acceso de los miembros del grupo no son afectados por los días festivos.

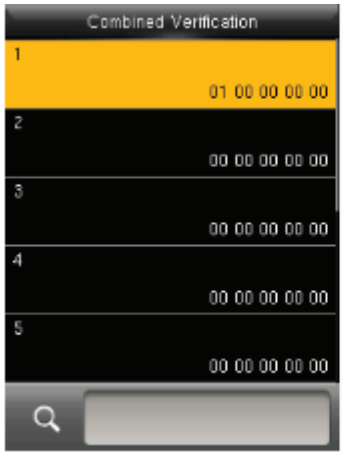
Puede seleccionarlos para editar o para eliminarlos o puede realizar búsqueda por número de grupo.

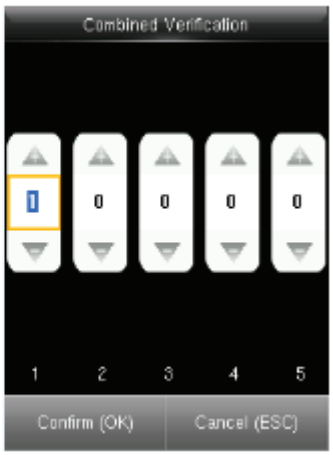




9.5 Ajustes de Verificación Multi-usuario

Combine varios grupos en diferentes controles de acceso para lograr una multi-verificación y así aumentar la seguridad. En la verificación Multi-Usuario, se pueden combinar hasta 5 usuarios. Ingresar al menú "control de acceso" ⟶ "Verificación Multi-usuario":





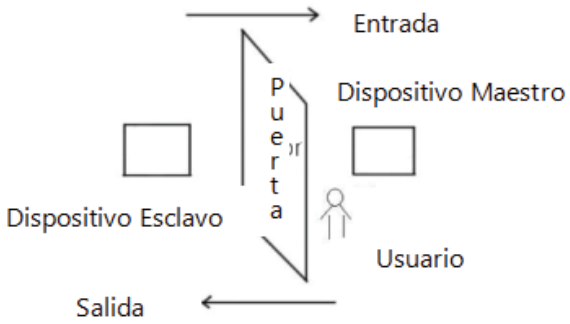
1 Seleccionar para editar.

2 Ingresar el número de grupo.

Nota: Puede seleccionarlo para editar o eliminar o puede colocar el número de grupo para posicionarse en el. Para deshabilitar la verificación multi-usuario configurar todos los grupos en 0.

9.6 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.



Principio de Funcionamiento

Esta función requiere de un dispositivo de entrada y otro para la salida, ambos por medio wiegand. Se conecta la salida de esclavo a la entrada wiegand del maestro. El numero enviado del lector esclavo debe encontrarse en el lector maestro.

Función

Valide si se trata de un anti-passback en base a los registros recientes de entrada-salida de los usuarios, el registro de entrada y salida deben coincidir. El dispositivo soporta anti-passback de salida-entrada o entrada-salida (Ingresar al menú → Configuraciones del sistema → Configuración avanzada → Anti-passback).

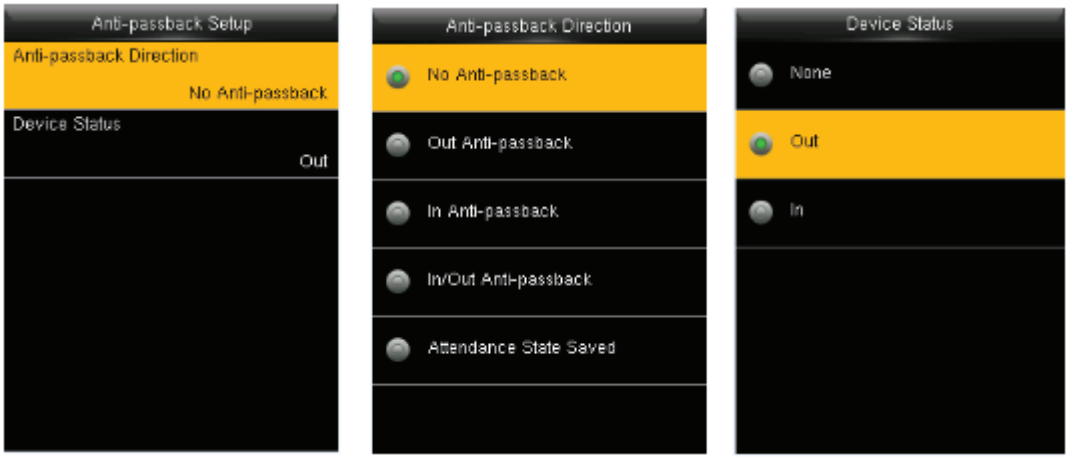
Cuando el dispositivo maestro está configurado como "Anti-passback de salida", si el usuario desea entrar y salir de forma normal, su registro actual debe ser de entrada o no podrá salir, cualquier registro de salida será rechazado por la regla de anti-pass back. Por ejemplo, el último registro de un usuario es "entrada" su segundo registro puede ser "salida" o "entrada" y el tercero se basará en el segundo, El registro de salida y de entrada deben coincidir, deben completarse en pares. Si el usuario no tiene un registro previo podrá ingresar, pero no podrá salir.

Cuando el dispositivo maestro está configurado como "Anti-passback de entrada", si el usuario desea entrar y salir de forma normal, su registro actual debe ser "salida" o no podrá salir, cualquier registro de "salida" será rechazado por la regla de anti-passback. (Nota: Si el usuario no tiene un registro previo, podrá salir, pero no podrá ingresar).

Cuando el dispositivo maestro es configurado como anti-passback "salida-entrada", si el usuario desea entrar y salir de forma normal, si su registro actual es "salida" y "entrada", su siguiente registro debe ser "entrada" y "salida".

Operaciones

Ingresar al menú "Control de Acceso" ⟶ "Ajustes de Anti-passback":



Dirección del 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.

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.

Estado del dispositivo

Entrada: El dispositivo es utilizado para controlar entradas, el dispositivo solo guarda registros de entrada

Salida: El dispositivo es utilizado para controlar salidas, El dispositivo solo guarda registros de salida.

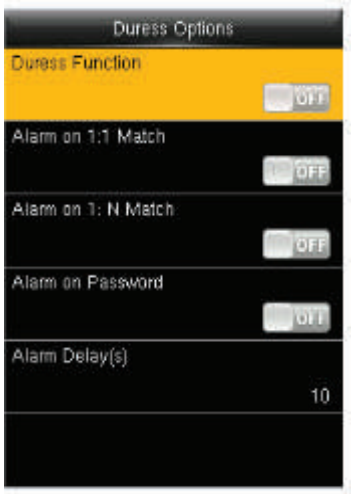
Ninguno: El dispositivo está configurado en ninguno, la función anti-passback esta deshabilitada en el dispositivo.

Nota: La comunicación wiegand está adaptada para maestro y esclavo. En referencia la siguiente conexión:

Maestro	Esclavo
IND0	⟶ WD0
IND1	⟶ WD1
GND	⟶ GND

9.7 Ajustes de Opciones de Coacción

Cuando los usuarios se encuentran en una situación de amenaza o coacción, el dispositivo se encargará de abrir la puerta como de costumbre y enviará la señal de alarma discreta. Ingresar al menú "Control de Acceso" ⟶ "Opciones de Coacción"



Función de Coacción: Si está activado, presione "Clave de coacción" y, a continuación, presione cualquier huella registrada (en 10 segundos), la alarma de coacción será enviada al verificar con la huella de coacción.

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

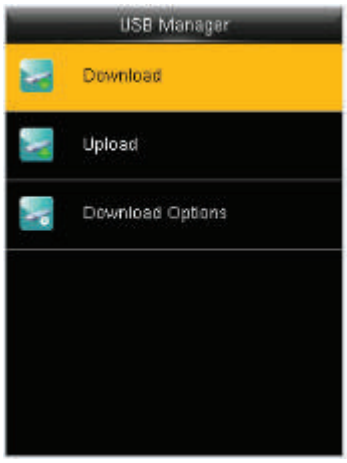
Alarma en 1:N: Si está activada, cuando un usuario utilice el método de verificación 1:N, la alarma se activará. Si está desactivada, no se activará ninguna señal de alarma.

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

Retardo de alarma (s): Cuando se activa la alarma de coacción, la señal de alarma no se emite directamente, pero puede configurarse. La señal de alarma se genera unos segundos después de forma automática.

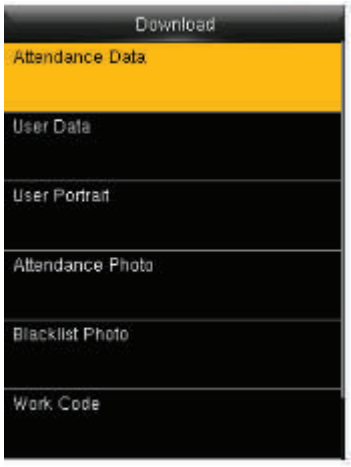
10. Gestión USB

Usted puede descargar información de usuario y datos de asistencia en una USB. Por lo que podemos cargar la información de usuarios desde otros dispositivos a este. Antes de cargar/descargar datos, inserte la unidad en el puerto USB del dispositivo. Ingresar al menú "Gestión USB":



10.1 Descarga

Ingresar al menú "Gestión USB" → "Descarga":



Descargar registros de asistencia: Descargar registros de asistencia en la unidad USB.

Datos de Usuario: Descargar toda la información de usuarios en la unidad USB.

Fotos de Usuario: Descargar todas las fotos de usuario del dispositivo en la unidad USB.

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

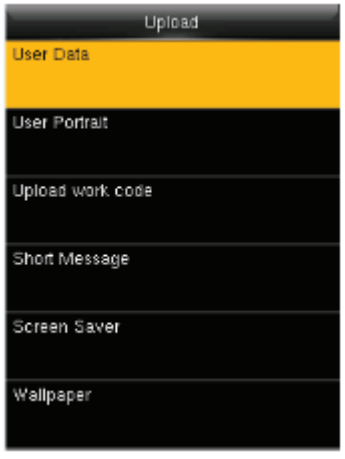
Fotos de Lista Negra: Descargar las fotos de lista negra, el formato es en jpg.

Código de Trabajo: Descarga todos los códigos de trabajo a la USB.

Mensajes: Descarga todos los mensajes cortos a la USB.

10.2 Carga desde USB

Ingresar al menú "Gestión USB" → "Cargar"



Datos de Usuario: Cargar toda la información de usuario guardada en la unidad USB al dispositivo.

Fotos de Usuario: Carga los archivos de fotos JPG al dispositivo.

Códigos de Trabajo: Carga todos los códigos de trabajo respaldados.

Mensajes: Carga todos los mensajes respaldados en la USB.

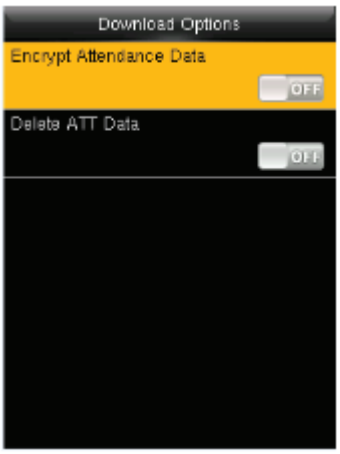
Protector de Pantalla: Carga todos los protectores respaldados en la USB.

Fondo de Pantalla: Carga los fondos de pantalla respaldados en la USB.

Sobre el formato de protector de pantalla, por favor revise "Apéndice 2. Reglas para carga de imagen".

10.3 Opciones de Descarga

Ingresar al menú "Gestión USB" → "Opciones de Descarga":

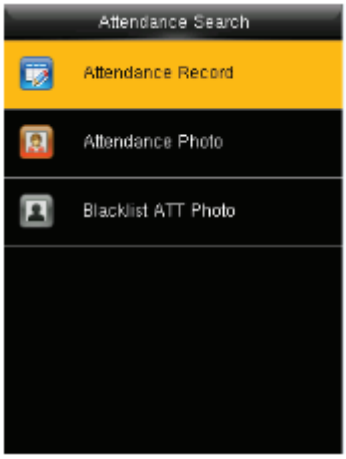


Para encriptar los datos de asistencia en la unidad USB y configurar si los datos se borran después de la descarga. Cuando descargue los registros de asistencia también puede configurar el tipo de calendario que mostrara en el horario de asistencia.

El dispositivo soporta tres tipos de calendario que son: Gregoriano, Irán gregoriano, Irán Lunar.

11. Búsqueda de Registros

Cuando los usuarios verifican exitosamente, se guarda un registro en el sistema. Esta función permite a los usuarios ver sus registros de asistencia. Ingresar al menú "Búsqueda de Registros":

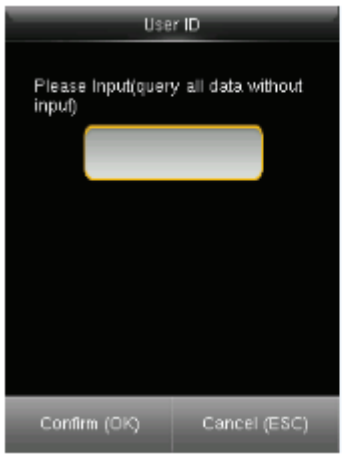


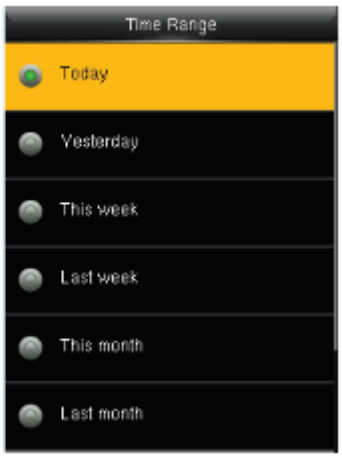
Registro de Asistencia: Buscar los registros de asistencia en el dispositivo. Cuando se realiza la validación en el dispositivo el registro es salvado.

Foto de Asistencia: Buscar lo registros de fotos de asistencia en el dispositivo. Cuando se hace validación, la cámara del dispositivo toma una foto y la guardada en el dispositivo.

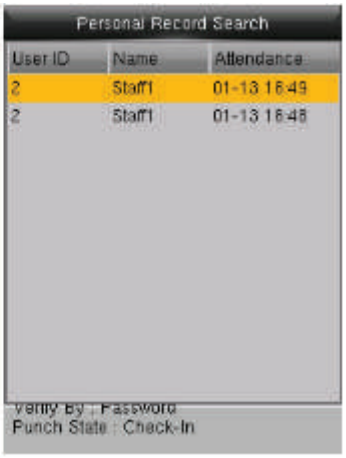
Fotos de Lista Negra: Cuando la verificación falla, la cámara del dispositivo puede tomar una foto y salvarla en la lista negra del dispositivo.

Tomé "Buscar registros de asistencia" como ejemplo, los otros dos menús son iguales en configuración como este. Ingresar al menú "Búsqueda de registros":









1. Ingrese el número de usuario a buscar.

2. Seleccione el horario para los registros que desee.

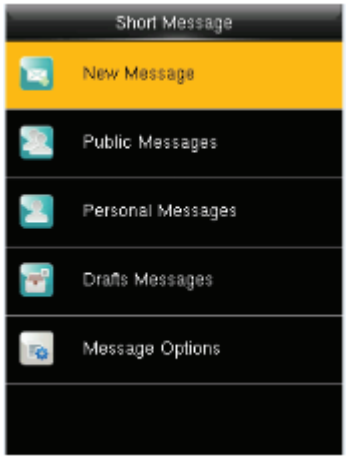
Nota: Puede dejar vacío el campo de búsqueda para que le muestre los registros de asistencia de todos los usuarios.

3. Se mostrará una lista con los registros.

4. Seleccione el deseado para visualizar detalles.

12. Mensajes

Ingresar al menú "Mensajes":



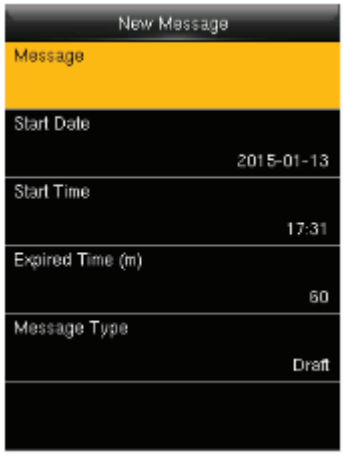
Es posible crear, editar, eliminar y enviar mensajes públicos o personales. Puede guardar los mensajes en borradores. A la hora asignada, un mensaje público se mostrará a todos los usuarios en el fondo de la pantalla principal, mientras que un mensaje personal se le mostrará al usuario específico después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

Puede revisar los mensajes públicos, personales o borradores en el menú.

El mensaje público se mostrará en la parte inferior de la pantalla principal el tiempo programado. El mensaje personal aparecerá después de que el usuario haya verificado con éxito el tiempo programado.

12.1 Agregar y visualizar nuevo mensaje

Agregar un mensaje personal
Ingrese al menú "mensajes" ⟶ "Nuevo mensaje"



Mensaje: Escriba el mensaje.

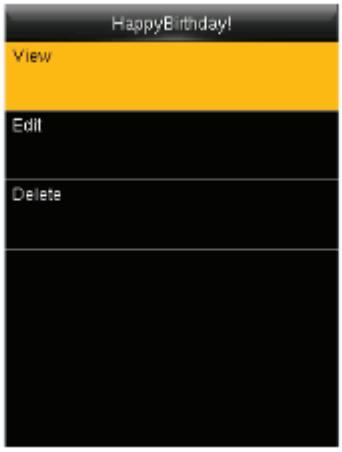
Fecha/Hora de Inicio: Establezca la fecha y hora en que desea se muestre el mensaje.

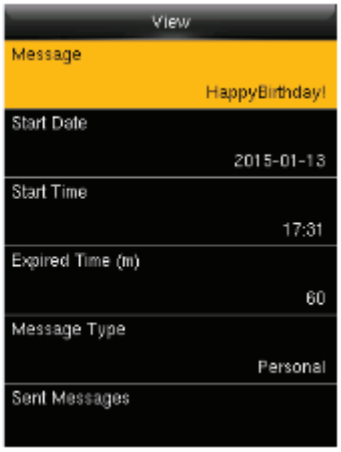
Tiempo de Duración: El tiempo en minutos antes de que desaparezca el mensaje, calculado a partir de la hora de inicio.

Tipo de Mensaje: Público, Personal y Borrador.

Visualizar mensaje personal
Ingresar al menú "Mensajes" ⟶ "Mensaje Personal", seleccionar "Visualizar":

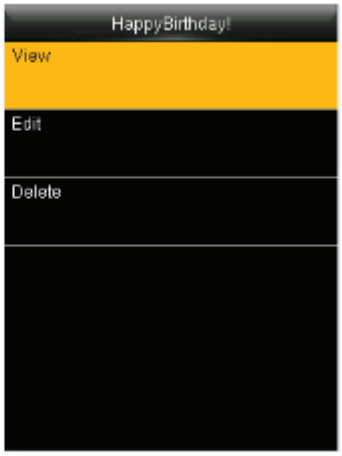






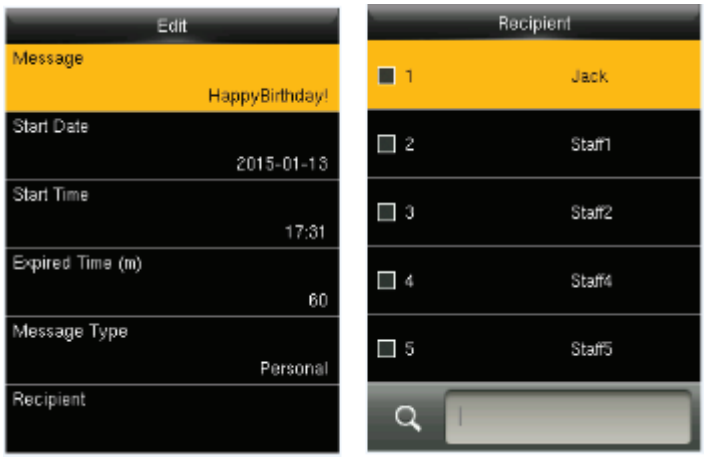
Ingresar al menú "Mensajes" ⟶ "Mensaje personal", seleccionar un mensaje:





Se pueden editar o borrar los mensajes seleccionados.

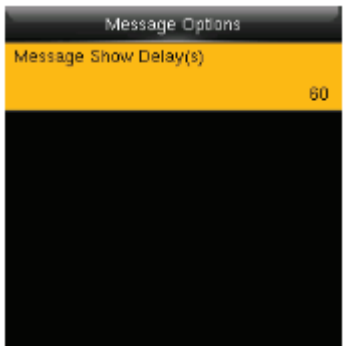
Seleccionar al receptor del mensaje: ingresar a "Editar" ⟶ "Receptor":



Se pueden seleccionar más un usuario para que le aparezca el mensaje. Presione [ESC] para salvar y salir.

12.2 Opciones de Mensaje

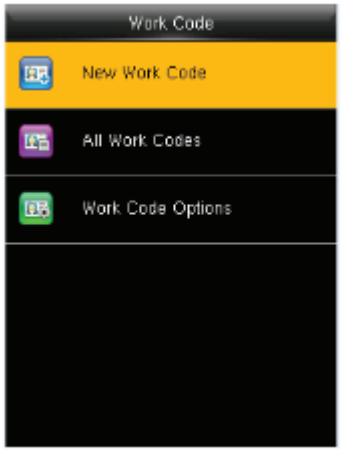
Ingresar al menú "Mensajes" ⟶ "Opciones de Mensaje":



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

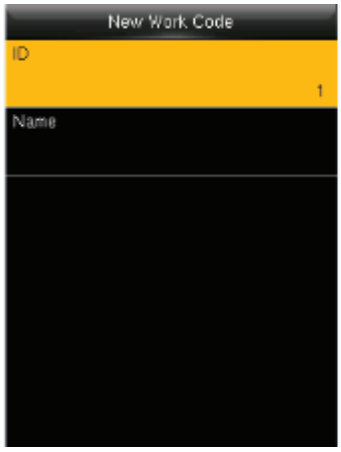
13. Código de Trabajo

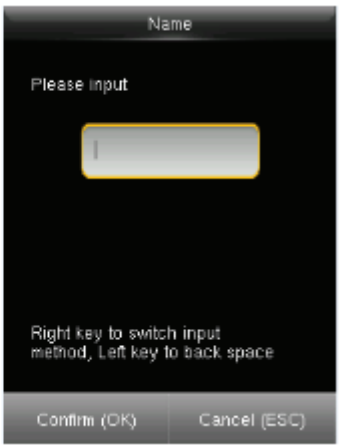
Ingresar al menú "Código de Trabajo":



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

13.1 Agregar código de trabajo





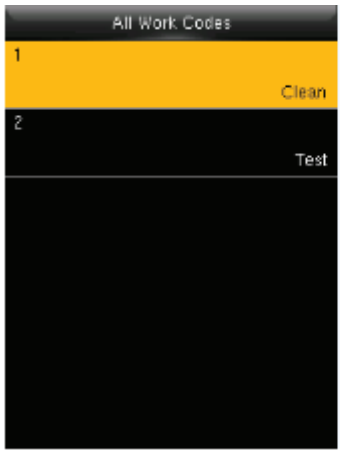
ID: Es el número asignado al código de trabajo. El rango es 1-99999999.

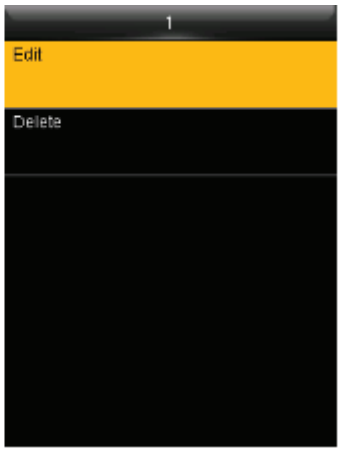
Nombre: Introduzca un nombre para el código de trabajo. El límite son 23 caracteres.

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

13.2 Editar y Borrar un código de trabajo

Ingresar al menú "Código de Trabajo " ⟶ " Todos los Códigos"



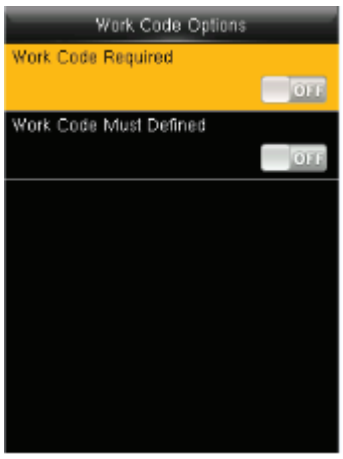


1. Seleccionar código de trabajo.

2. Presione "Editar" para modificar el nombre. Presione "Borrar" para eliminar.

13.3 Opciones de Código de Trabajo

Ingresar al menú "Código de Trabajo " ⟶ "Opciones de código de trabajo"

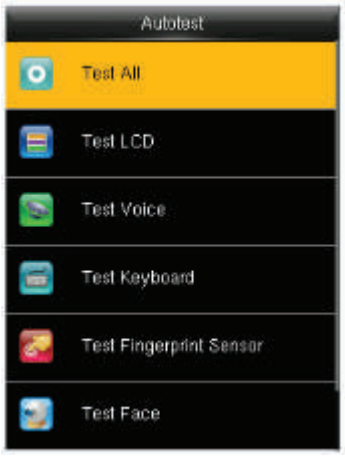


Código de Trabajo Requerido: Se debe introducir un Código de Trabajo durante la verificación. Seleccione si desea activar esta función.

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

14. Autopruebas

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



Probar Todo: Prueba todos los módulos del dispositivo.

Probar LCD: Probar la pantalla LCD.

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

Probar Teclado: Probar si todas las teclas funcionan correctamente.

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

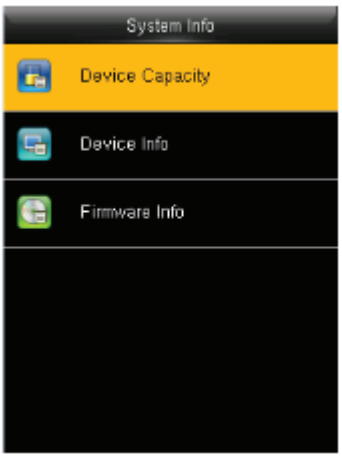
Probar Lector de Rostro: Probar si la cámara funciona normalmente.

Probar Reloj RTC: Probar el Reloj en Tiempo Real.

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

15. Información del Sistema

Para revisar el sistema y la información del dispositivo. Ingresar al menú "Información del sistema":



Seleccione una opción para revisar los parámetros:

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

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

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

Ya información solo puede ser consultada pero no editada.

16. Apéndice

Apéndice 1

Entrada de Teclado T9

El teclado T9 (entrada inteligente) es rápido y altamente eficiente. Cada tecla numérica (2-9) tiene asignada 3 o 4 letras, por ejemplo, A, B, C están en la tecla 2. Presione la Tecla correspondiente una vez, y el programa generará la ortografía adecuada.



Ingresar a "Nuevo Mensaje"



Presione [4] para colocar la H



Coloque "appy" con el mismo método





Presione > hasta encontrar "3". Presione 3 para espacio en blanco.



Coloque "New Year" presionando > a tipo numérico.





1. Coloque 2015, Presione la tecla >

2. Presione "6" para colocar la entrada "!"

Apéndice 2

Reglas para carga de 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 8000 imágenes, que no excedan los 15Kb cada una. El nombre de la imagen es x.jpg (x siendo el número de ID del usuario, máximo 9 dígitos). El formato de la foto debe ser JPG.

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 en total.

Declaración Sobre el Derecho a la 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 violen la privacidad de los usuarios.

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

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

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

Nuestros 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 del Componente	Sustancia / elemento peligroso / tóxico					
	Plomo (Pb)	Mercurio (Hg)	Cadmio (Cd)	Cromo hexavalente (Cr6 +)	Bifenilos polibromados (PBB)	Éteres de difenilo polibromados (PBDE)
Resistencia	×	o	o	o	o	o
Condensador	×	o	o	o	o	o
Inductor	×	o	o	o	o	o
Diodo	×	o	o	o	o	o
Componente ESD	×	o	o	o	o	o
Buzzer/Bocina	×	o	o	o	o	o
Adaptador	×	o	o	o	o	o
Tornillos	o	o	o	×	o	o

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

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

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



www.zkteco.com

www.zktecolatinoamerica.com

Derechos de Autor © 2022, ZKTeco CO., LTD. Todos los derechos reservados.
ZKTeco puede, en cualquier momento y sin previo aviso, realizar cambios o mejoras en los productos y servicios o detener su producción o comercialización.
El logo ZKTeco y la marca son propiedad de ZKTeco CO., LTD.