

Manual de Usuario

Nuevo Firmware para Pantalla a Color
de 2.8/3/3.5 Pulgadas.

Acerca de este Manual

- No todos los dispositivos tienen la función con ★ El producto real prevalece.
- Las fotografías de este manual pueden ser diferentes al producto real. El producto real prevalece.

Aviso importante

Primero, gracias por adquirir la terminal híbrida facial y de huella dactilar, por favor lea este manual cuidadosamente para evitar daños innecesarios. La compañía le recuerda que el uso apropiado mejorará el uso y la velocidad de autenticación. .

Sin un escrito de nuestra compañía, ninguna unidad o individuo tiene permitido aceptar copiar el contenido de esta manual completo o en partes, tampoco difundir en cualquier forma.

El producto descrito en el manual puede incluir software con derechos de autor las licencias de nuestra compañía son compartidos, excepto para el permiso del soporte correspondiente, ninguna persona lo puede copiar, distribuir, revisar, modificar, extraer, descompilar, desmontar, des-criptar, arrendar, transferir, sub-licenciar el software, infracción de otros actos de derechos de autor, se excluyen limitaciones aplicadas a la ley.

i

Debido a la constante renovación de productos, la compañía no puede tomar el actual producto la consistencia del documento, también cualquier conflicto derivado por la diferencia entre los parámetros técnicos y la información en este documento. Cambios sin previo aviso.

1. Índice

CONTENIDO

1. Instrucciones de Uso.....	1
1.1 Colocación de Huella	1
1.2 Modos de Verificación.....	1
1.2.1 Verificación de Huella 1:N.....	1
1.2.2 Verificación de Huella 1:1.....	2
1.2.3 Verificación de Contraseña.....	2
1.2.4 Verificación de Tarjeta ID.....	3
1.3 Iconos de Estatus.....	4
2. Menú Principal.....	5
3. Administración de Usuarios.....	8
3.1 Agregar Usuario.....	8
3.1.1 Ingresar un ID de usuario.....	8
3.1.2 Ingresar Nombre.....	9
3.1.3 Modificar Rol de Usuario.....	9
3.1.4 Enrolar Huella.....	10
3.1.5 Enrolar Tarjeta ID.....	10
3.1.6 Enrolar Contraseña.....	11
3.1.7 Enrolar Foto.....	11
3.1.8 Rol de Control de Acceso	11
3.2 Consultar Usuarios.....	13
3.2.1 Consultar Usuario por ID y Nombre.....	14
3.2.2 Editar y Eliminar Usuario.....	14
3.3 Modo de Pantalla.....	15
4. Rol de Usuario.....	16
5. Ajustes de Comunicación.....	17
5.1 Ethernet.....	17
5.2 Comunicación Serial.....	18
5.3 Conexión a PC.....	18
5.4 Red de Datos Móviles.....	19
5.5 Red Inalámbrica.....	20
5.6 ADMS.....	21
5.7 Ajustes Wiegand.....	22
5.7.1 Entrada Wiegand.....	22
5.7.2 Salida Wiegand.....	23

CONTENIDO

6. Sistema.....	24
6.1 Fecha/Hora.....	24
6.2 Asistencia.....	26
6.3 Huella Digital.....	27
6.4 Reiniciar.....	28
6.5 Actualización USB.....	29
7. Personalización.....	29
7.1 Interfaz de Usuario.....	29
7.2 Voz	31
7.3 Horario de Timbre.....	31
7.4 Opciones de Estado.....	33
7.5 Teclas de Acceso Rápido.....	34
8 Administración de Datos.....	35
8.1 Eliminar Datos.....	35
8.2 Respaldo de Datos.....	36
8.3 Restaurar Datos	37
9. Ajustes de control de acceso.....	38
9.1 Opciones de Control de Acceso.....	38
9.2 Horario.....	39
9.3 Ajustes de Vacaciones.....	40
9.4 Grupos de Acceso.....	42
9.5 Multi-verificación.....	44
9.6 Anti-passback.....	45
9.7 Parámetros de Alarma de Amago.....	45
10 Administración de Tarjetas IC.....	46
10.1 Configurar ID.....	46
10.2 Enrolar Tarjeta de Huella Digital.....	47
10.3 Limpiar Información de Tarjeta.....	49
10.4 Copiar Información de Tarjeta.....	49
10.5 Configuración de Parámetros	50
11 Administración de USB.....	51
11.1 Descarga.....	51
11.2 Subir Datos	52
11.3 Opciones de Descarga.....	52
12 Búsqueda de Asistencia.....	53

CONTENIDO

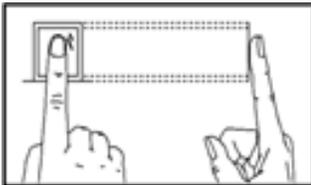
13 Impresión.....	54
13.1 Configuración de Datos.....	54
13.2 Opciones de Impresión.....	55
14 Mensaje Corto.....	55
14.1 Mensaje Corto.....	55
14.2 Mensajes Públicos y Personales.....	57
14.3 Opciones de Mensaje.....	57
14.4 Verificar Mensaje del Empleado.....	57
15 Código de Trabajo.....	58
15.1 Agregar Código de Trabajo.....	58
15.2 Todos los Códigos de Trabajo.....	59
15.3 Ajustes de Código de Trabajo.....	60
16 Prueba Automática.....	60
17 Información del Sistema.....	61
Apéndice	
Apéndice 1 Descripción de Operación para Entrada de Texto.....	62
Apéndice 2 Reglas para Cargar Imágenes.....	63
Apéndice 3 Funciones de Impresión.....	63
Apéndice 4 Anti-passback.....	65
Declaración de Privacidad y Derechos Humanos.....	68
Descripción de Uso Amigable con el Medio Ambiente.....	69

1. Instrucciones de Uso

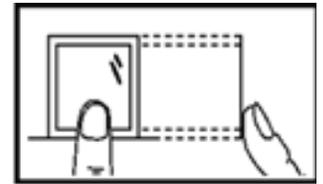
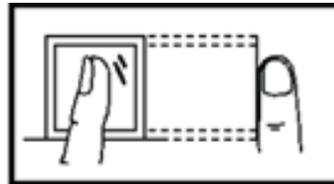
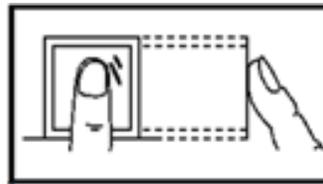
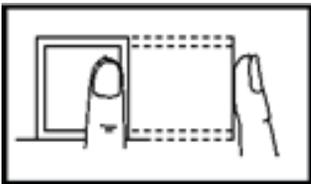
1.1 Colocación del Dedo

Dedos recomendados: El dedo índice, el dedo medio o el dedo anular; el pulgar y el dedo meñique no son recomendados (porque estos son generalmente difíciles de recolectar en la pantalla).

1) Colocación correcta del dedo: El dedo debe estar plano en la superficie y centrado.



2) Colocación correcta del dedo: No poner fuera del centro o inclinado.

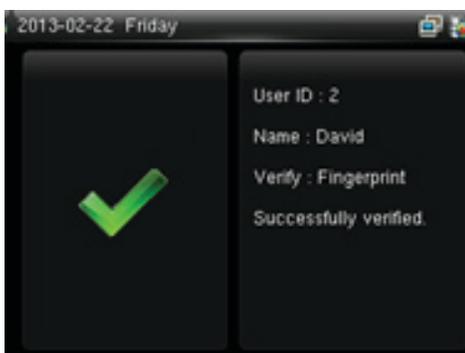


1.2 Modos de Verificación

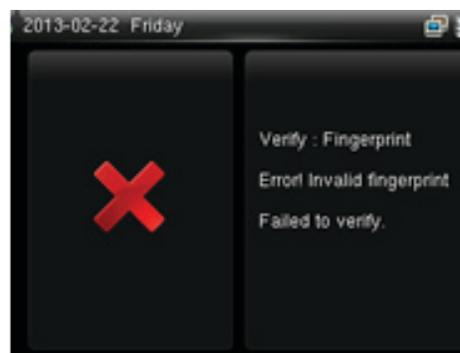
1.2.1 Verificación de Huella 1:N

La terminal compara la huella digital actual recolectada por el lector con todos los datos de las huellas de la terminal.

Presione su dedo sobre el lector de huella para adoptar la apropiada colocación del dedo. Para detalles, ver 1.1 (Colocación de Dedo)



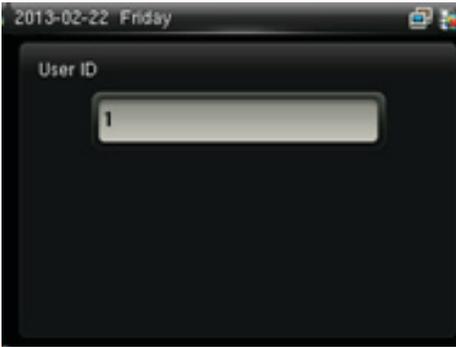
Cuando la verificación sea exitosa, se mostrará la interfaz anterior.



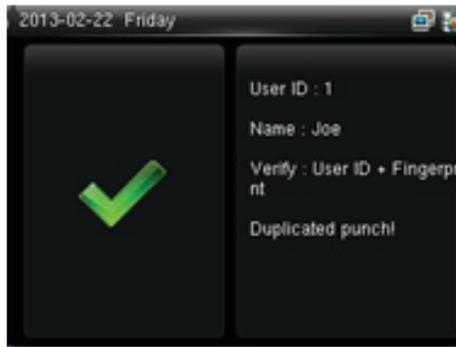
Cuando la verificación sea fallida, se mostrará la interfaz anterior.

1.2.2 Verificación de Huella 1:1

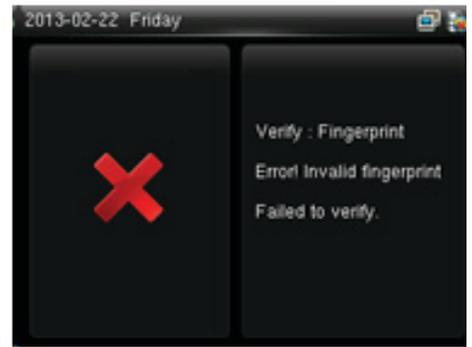
En el modo de verificación de contraseña, la terminal compara la contraseña ingresada con relación al ID del usuario.



Ingrese el ID de usuario usando el teclado en la interfaz inicial. Después presione OK. Coloque el dedo registrado correctamente en el sensor



Cuando la verificación sea fallida, se mostrará la interfaz anterior.



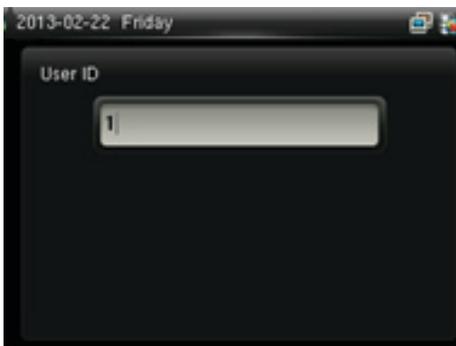
Cuando la verificación sea exitosa, se mostrará la interfaz anterior.

Nota:

1. Sí, el número de enrolamiento es erróneo, esto significa que no existe el número del empleado o la contraseña del empleado no está enrolada.
2. Si el dispositivo dice "Intente de nuevo, por favor", coloque de nuevo la huella en el sensor. Puede intentarlo 2 veces más por default. Los tiempos de repetición pueden ser ajustados en 6.3 Huella Dactilar. Si falla después de 2 veces, regrese al paso 1 para la segunda operación.

1.2.3 Verificación de Contraseña

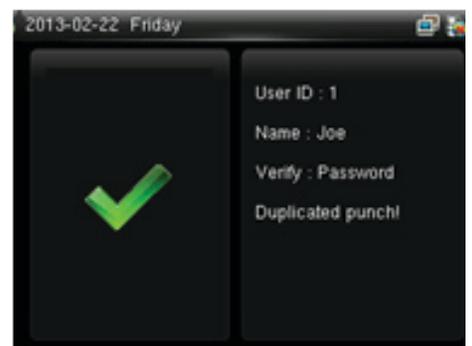
En el modo de verificación de contraseña, la terminal compara la contraseña ingresada con relación al ID del usuario.



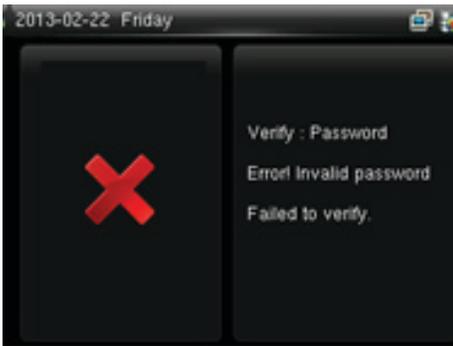
Ingrese el ID de usuario usando el teclado en la interfaz inicial. Después presione OK.



Ingrese la contraseña y presione OK.



Cuando la verificación sea exitosa, se mostrará la interfaz anterior.



Cuando la verificación sea fallida, se mostrará la interfaz anterior.

Nota:

Si el dispositivo dice "ID inválido", ingrese la contraseña de nuevo. Puede intentarlo en dos ocasiones por default. Las veces repetidas pueden ser ajustadas en 6.3 Huella Dactilar. Si falla después de las dos veces, regrese al paso 1 para la segunda operación.

1.2.4 Verificación de Tarjeta ID

Solo los productos con módulo de tarjeta ID incorporado soportan verificación de tarjetas ID. Los productos con módulo de tarjeta incorporado soportan los siguientes dos modos de verificación:

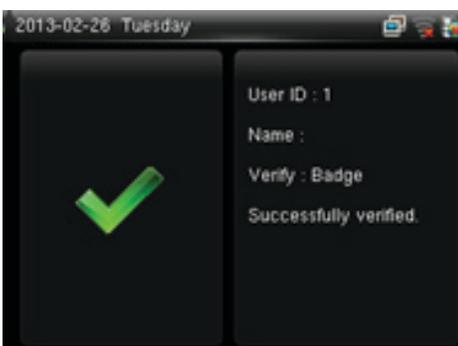
El módulo de tarjetas ID soporta los siguientes modos de verificación.

Tarjeta ID: Los usuarios solo necesitan deslizar su tarjeta de verificación.

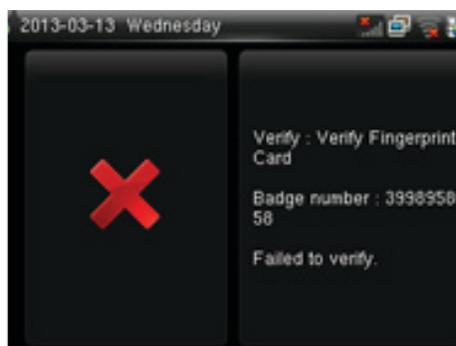
Tarjeta ID + Huella: Después de pasar la verificación de tarjeta, también puede realizar la verificación dactilar.

1. Tarjeta ID

- 1) Si tiene el número de tarjeta ID enrolada en el sistema, puede pasar la verificación deslizando su tarjeta ID en el área apropiada de tarjetas.

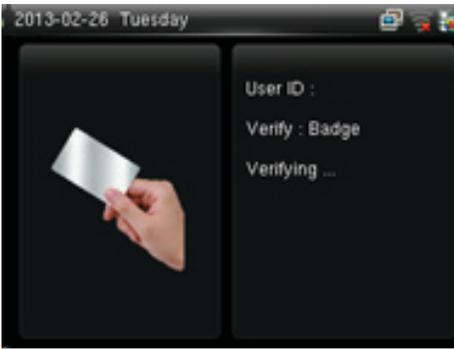


Cuando la verificación sea exitosa, se mostrará la interfaz anterior.



Cuando la verificación sea fallida, se mostrará la interfaz anterior.

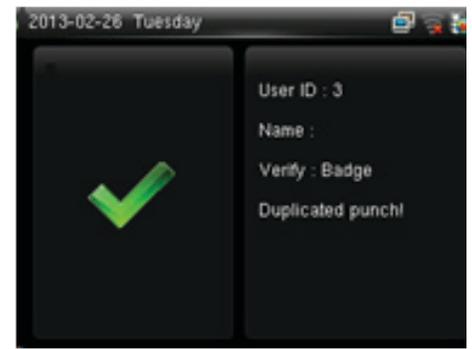
2. ID + Verificación Facial



Deslice su tarjeta ID apropiadamente para ingresar el modo de verificación facial 1:1



Coloque el dedo apropiadamente en el sensor de huella.



Cuando la verificación sea exitosa, se mostrará la interfaz anterior.

1.3 Iconos de Estatus

Iconos de Estatus	Nombre	Descripción
	Señal	El estatus de los iconos indican si se encuentra dentro de la cobertura de red móvil, con barras verdes que indican señal fuerte. G: Indica que la red móvil es una red GPRS, sobre el dispositivo el cual se accede a internet. E: Indica que el operador de red EDGE (GSM) está disponible, sobre el dispositivo el cual se accede a internet. W: Indica que la red móvil actual es WCDMA.
	Timbre	Indica que se ha establecido el timbre.
		Indica una alarma de desmontaje.
	Ethernet	Indica que la conexión a Ethernet ha sido establecida.
		Indica que el Ethernet esta desconectado.
	Servidor ADMS	La conexión entre el dispositivo y el servidor ADMS es exitosa.
		La conexión entre el dispositivo y el servidor ADMS es fallida.
		La comunicación de datos del ADMS son transmitidos.
	Mensajes cortos	Existen mensajes cortos.
	Señal Wi-Fi	La conexión Wi-fi es normal.
		La conexión Wi-fi es fallida.

2. Menú Principal

El menú principal tiene dos diferentes estilos, pero el sub menú es el mismo. Este manual solo explicará el estilo del menú principal de la imagen izquierda.



Cuando el dispositivo está en la interfaz inicial, presione **M/OK** para abrir el menú principal como se muestra debajo:



Administración de Usuarios: Puede buscar la información almacenada en el dispositivo, incluye el ID de usuario, nombre, usuario, fotografía, tarjeta, contraseña, foto de usuario, agregar, modificar o eliminar información del usuario.

Rol de Usuario: se utiliza para establecer los derechos del usuario y definir rol esto para derechos de menús.

Ajustes de comunicación: puede ajustar los parámetros relacionados para comunicación entre la terminal y la PC, incluyendo la dirección IP, puerto, Mascara sub-red, velocidad de transmisión,

Sistema: Puede ajustar los parámetros relacionados con el Sistema, incluyendo fecha y hora, asistencia, huella, cámara, reiniciar o actualizar mediante USB, para permitir que la terminal pueda satisfacer los requerimientos de los usuarios en la mayor medida de términos y visualización.

Personalización: utilizado para cumplir los requisitos en la mayor medida respecto a la pantalla, audio y definición del teclado.

Administración de Datos: puede realizar la administración de los datos almacenados en la terminal, por ejemplo: eliminar datos, respaldo de datos y restauración de datos.

Control de Acceso: puede ajustar los parámetros de las cerraduras eléctricas y relacionarlas con los dispositivos de control de acceso.

Tarjeta IC: Soporta tarjeta MIFARE no toque la tarjeta inteligente con trabajo de frecuencia 13.56MHZ. Integración de huella dactilar a otros sistemas y soporta modo de multi-verificación para satisfacer la demanda de diferentes personas.

Administración de USB: puede importar la información del usuario y datos de asistencia almacenados en una USB para relacionar software u otro equipo de reconocimiento dactilar.

Búsqueda de Asistencia: para consultar el registro guardado en el dispositivo, se proporciona la función de consulta de registros.

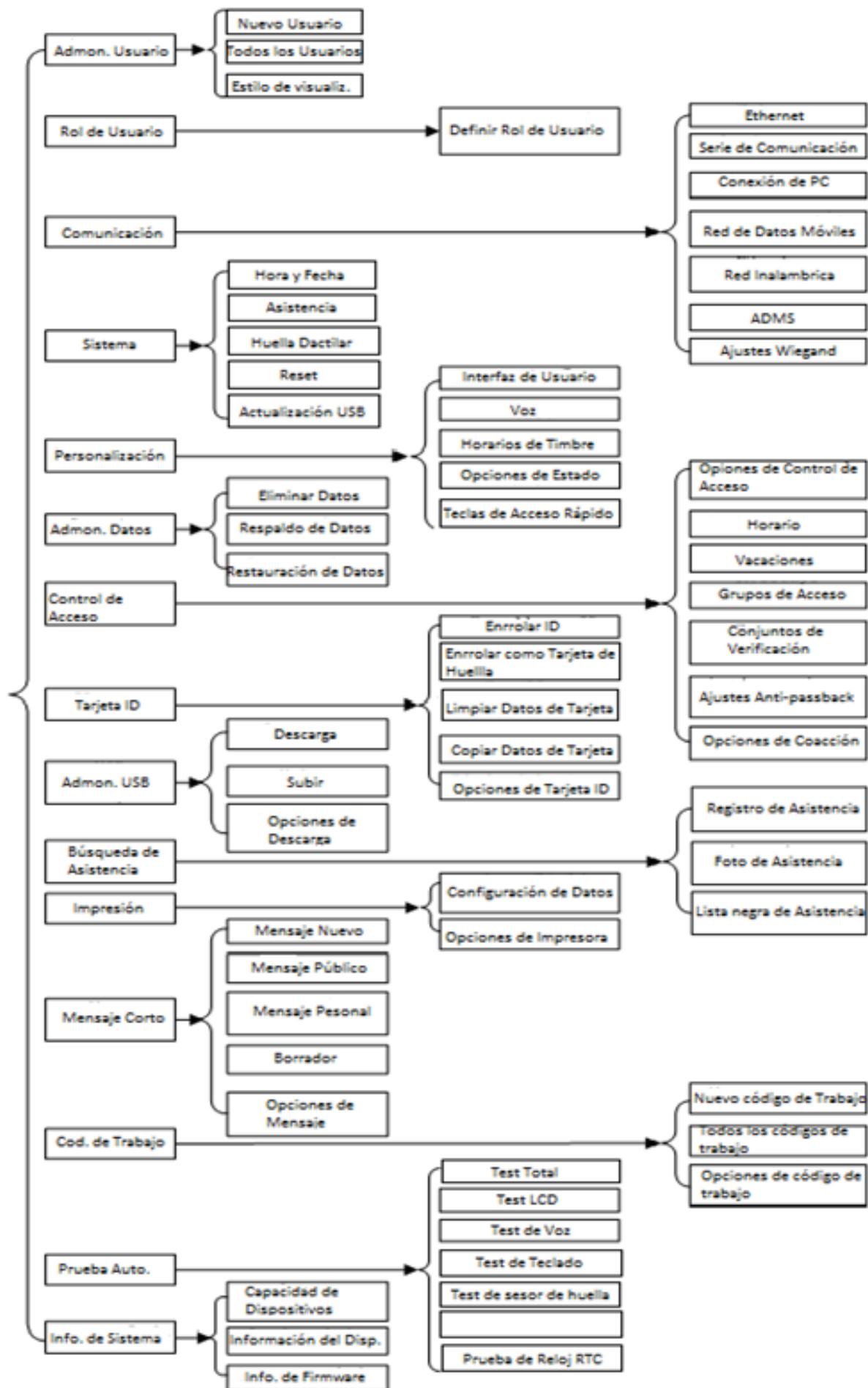
Impresión: Se utiliza para determinar si se deben imprimir los registros de asistencia de inmediato.

Mensaje Corto: se utiliza para establecer un mensaje público o privado. El mensaje corto se desplegará para una persona en específico después de registrar su asistencia, facilitando la transferencia de información.

Código de Trabajo: Se utiliza para identificar diferentes tipos de trabajo, facilitando el control de asistencia.

Prueba Automática: este sub-menú permite probar automáticamente las funciones son normales de varios módulos, incluyendo la pantalla, huella dactilar, voz, teclado y hora.

Información de Sistema: para verificar la capacidad actual del dispositivo, información del dispositivo e información del firmware.



3. Administración de Usuario

Mediante este sub-menú, puede buscar la información del usuario almacenada en la terminal, incluyendo el ID de usuario, rol de usuario, huella dactilar, tarjeta, contraseña, foto de usuario; agregar, modificar o eliminar información del usuario. .en la gestión de asistencia de la empresa, para el cambio de empleados, la información en el sensor también necesita modificación. Incluyendo operaciones “agregar, eliminar, verificar, modificar, etc.” Pueden ser en el sensor de huella.

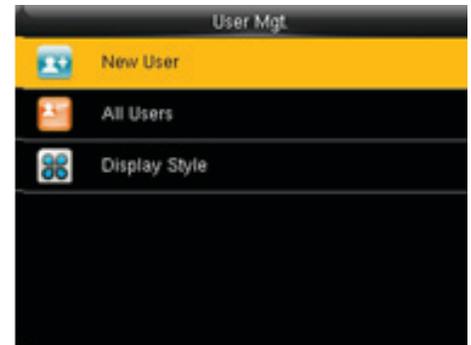
3.1 Agregar Usuario



Presione M/OK en la interfaz inicial.



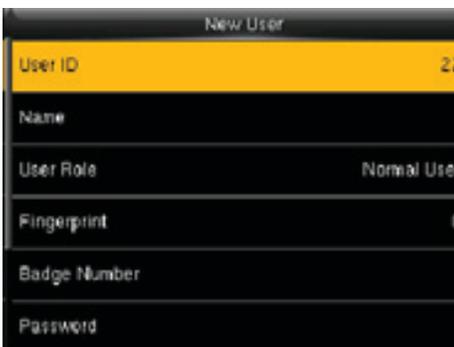
Seleccione usuarios y presione OK.



Seleccione usuarios y presione OK.

3.1.1 Ingresar un ID de Usuario

La terminal automáticamente asigna un ID inicial desde el primero por cada usuario en secuencia. Si utiliza el ID asignado por la terminal, puede omitir esta sección.



Seleccione el ID de usuario y presione OK.

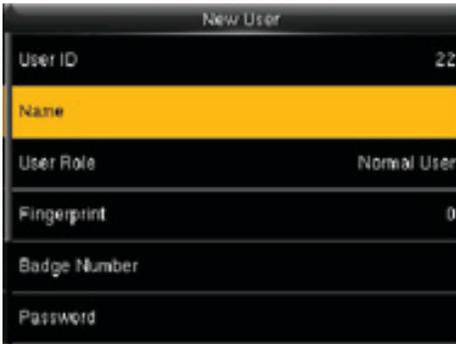


Ingrese el ID del usuario utilizando el teclado y presione OK

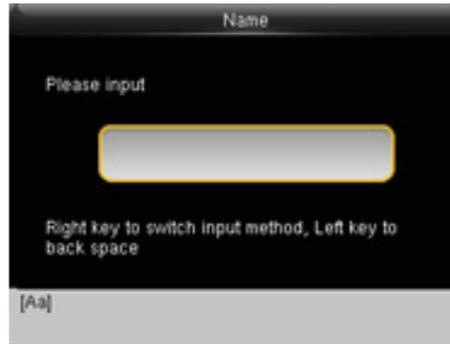
Tip: La terminal soporta 1 a 9 dígitos de ID de usuario por defecto.
Si se despliega el siguiente mensaje “El usuario ID ya existe” ingrese otro ID.

3.1.2 Ingresar Nombre

Ingresar un nombre de usuario mediante el teclado.



Presione ▼ para seleccionar nombre y presione OK.



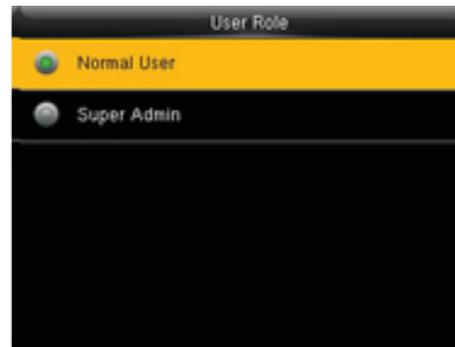
Presione * para cambiar método de entrada e ingrese el nombre, presione OK.

Tip: La terminal soporta de 1 a 23 caracteres por default. Para detalles de operación de la interfaz del teclado, vea **Apéndice 1** Instrucciones para ingresar texto.

3.1.3 Modificar Rol de Usuario



Presione ▼ para seleccionar Rol



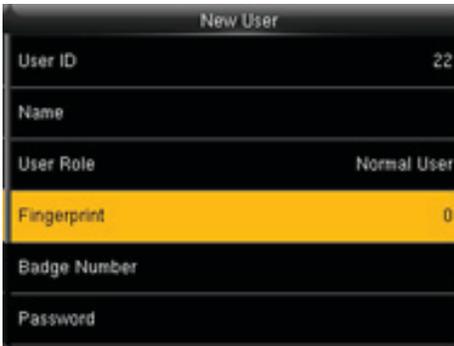
Seleccione el Rol.

Súper Administrador: El súper administrador tiene los derechos de operación de todas las funciones del menú.

Usuario Normal: Si el sistema tiene un administrador, un usuario normal solo tiene autenticación por su huella, contraseña o tarjeta. Si el sistema no tiene un administrador, un usuario normal tiene los derechos para operar todas las funciones del menú.

Definir Rol de Usuario: Al papel definido por el usuario se puede asignar otro menú de opciones en adición a las funciones disponibles para un usuario común. (Cuando ingrese como súper administrador, tiene los derechos para asignar funciones de menú a una función personalizada.

3.1.4 Enrolar Huella Digital



Presione ▼ para seleccionar huella y presione OK.



Coloque su dedo en el sensor apropiadamente.

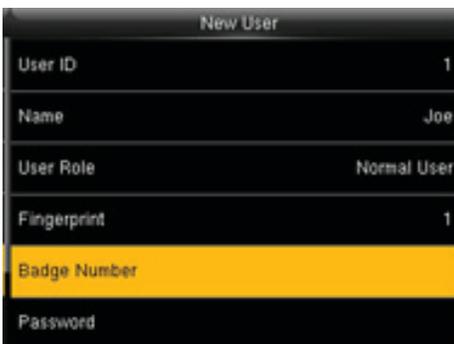


Coloque el mismo dedo en el sensor en tres ocasiones.

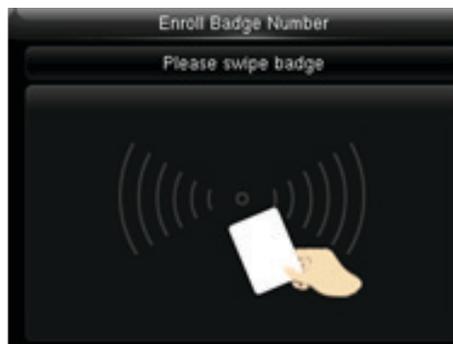


Enrolamiento exitoso. Si el enrolamiento falla, el sistema desplegará un mensaje, Regrese a la interfaz de (Enrolar Huella). En este caso, necesita repetir los pasos de operación 2.

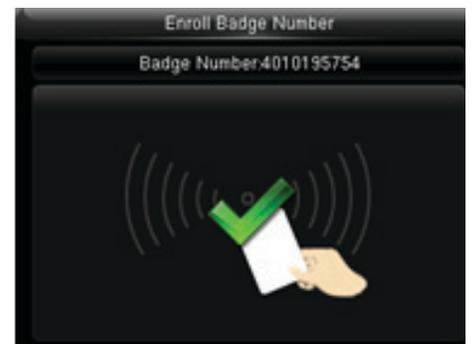
3.1.5 Enrolar Tarjeta ID



Presione ▼ para seleccionar numero de usuario.

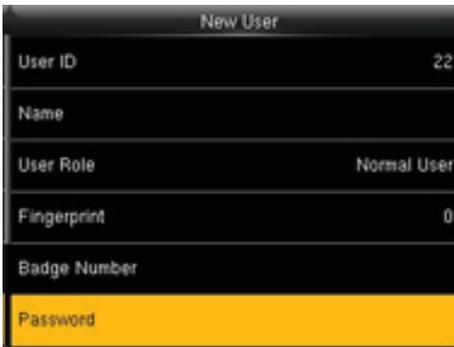


Deslice la tarjeta ID en el área apropiada.

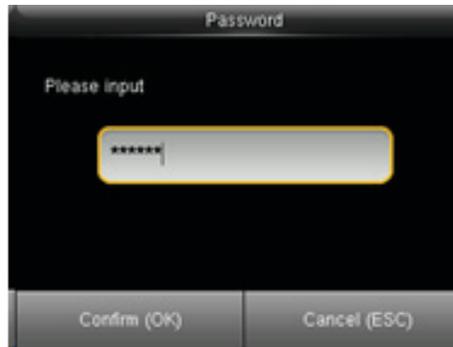


Leído correctamente

3.1.6 Configurar Contraseña



Presione ▼ para seleccionar contraseña y presione OK



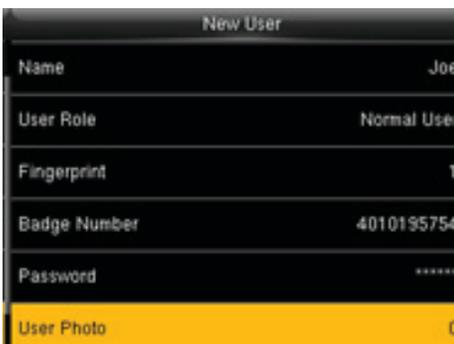
Ingrese una contraseña utilizando el teclado, después presione OK. La FRR de la terminal soporta de 1 a 8 dígitos por defecto



Re-ingrese la contraseña acorde al Sistema después presione OK.

3.1.7 Capturar Fotografía

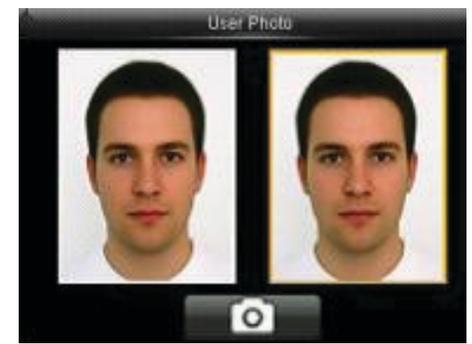
Si tiene enrolada una foto en el Sistema, el Sistema desplegará la foto enrolada junto con el ID y nombre después de pasar la verificación.



Presione ▼ para seleccionar foto de usuario y presione OK.



Mantenerse de forma natural enfrente de la pantalla. Presione OK.



Presione ESC para regresar directamente a la interfaz previa.

3.1.8 Rol de Control de Acceso

La opción de control de acceso de usuario es para ajustar el acceso para apertura de la puerta dirigido a todos los usuarios, incluyendo ajustes de subgrupo, modo de verificación, uso de zona horaria, administración de huella de amago.

Grupos de Acceso: Enrolar al usuario en diferentes grupos para la administración conveniente.

Modo de Verificación:

- 1) Tipo de verificación de grupo: si el usuario utiliza su tipo de verificación de grupo.
- 2) Tipo de verificación individual: Seleccione el tipo de verificación del usuario. Si el tipo de verificación por grupo no es utilizada, otros tipos de verificación no serán afectadas.

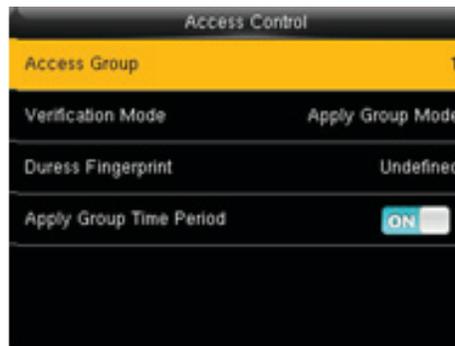
Huella de Amago: El usuario enrola una nueva huella o especifica una huella en el sensor como huella de amago. En cualquier momento y cualquier lugar, la alarma de amago se generará después de pasar la verificación dactilar.

Aplicar periodo de tiempo de grupo:

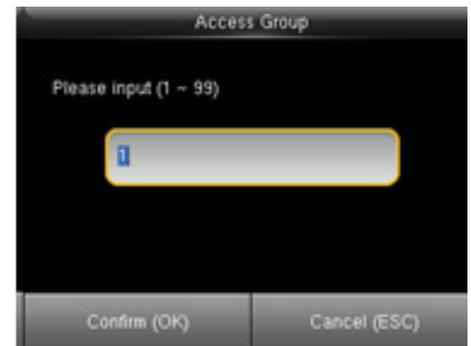
- 1) Seleccione "ON", zona horaria de grupo, el usuario utiliza sus grupos de zona horaria por default.
- 2) Seleccione "OFF", establecer hora de desbloqueo de usuario. Si la zona horaria de grupo no es utilizada, otros horarios de desbloques no serán afectados.



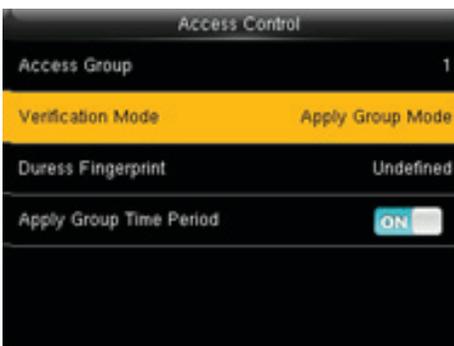
Presione ▼ para seleccionar Rol de Control de Acceso y Presione OK



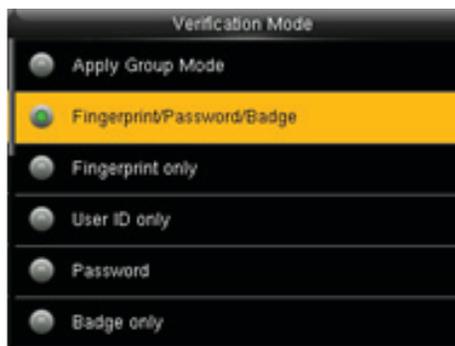
Presione OK para entrar a la interfaz de Grupos de acceso.



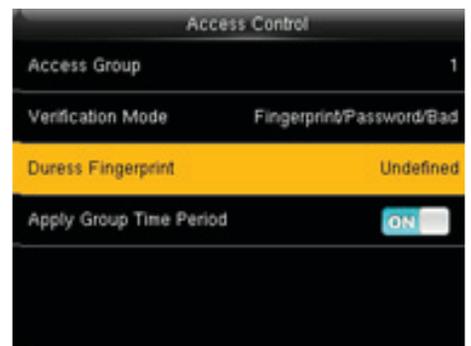
Ingrese el grupo del usuario utilizando el teclado, después presione OK para regresar



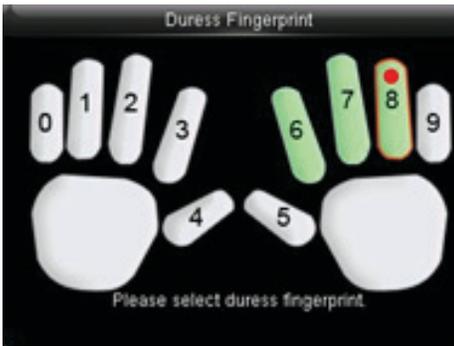
Presione ▼ para seleccionar el modo de verificación y presione OK



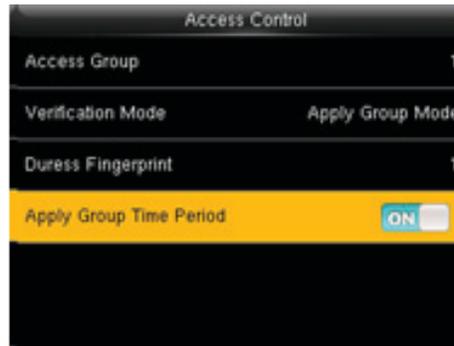
Presione ▼ para seleccionar el tipo de verificación y presione OK



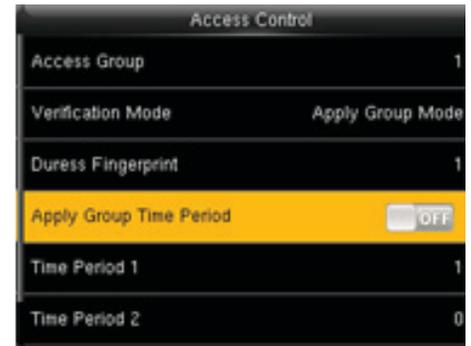
Presione ▼ para seleccionar alarma de amago y presione OK.



Presione ► para enrollar el dedo y después presione OK.



Presione ▼ para seleccionar aplicar periodo de tiempo de grupo, presione OK para seleccionar si el usuario utiliza su zona de tiempo de grupo por default.



Cuando seleccione "OFF", presione ▼ para seleccionar el periodo de tiempo 1.

3.2 Consultar Usuarios.

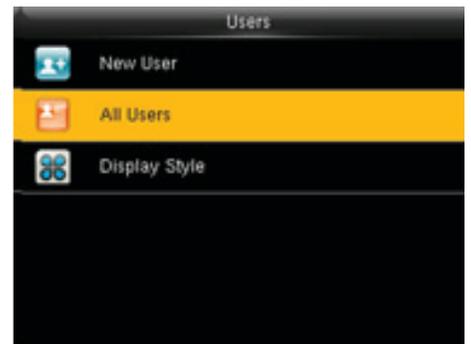
Para facilitar a los administradores localizar a los administradores de forma rápida a partir de un gran número de usuarios enrollados, la terminal FFR permite la consulta del usuario mediante "ID" y "Nombre". (Búsqueda de Ubicación)



Presione M/OK en la interfaz inicial.

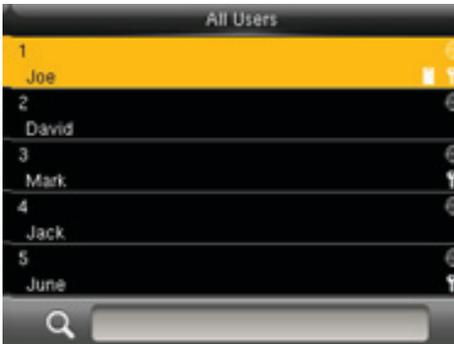


Seleccione usuario y presione OK.

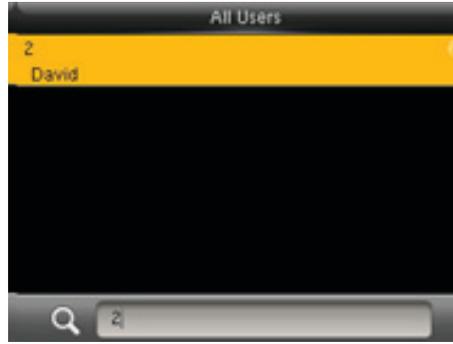


Presione ▼ para seleccionar todos los usuarios y presione

3.2.1 Consulta por ID de Usuario y Nombre



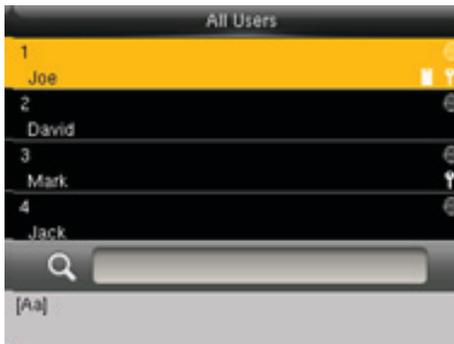
Ingrese el ID de usuario utilizando el teclado para consultar y ver todos los usuarios.



El cursor para que el usuario sea consultado.

Presione # en la interfaz de búsqueda para cambiar el método de entrada y presione las teclas del teclado numérico para búsqueda por nombre.

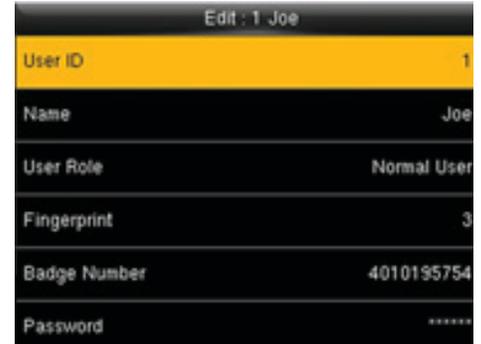
3.2.2 Editar y Eliminar un Usuario



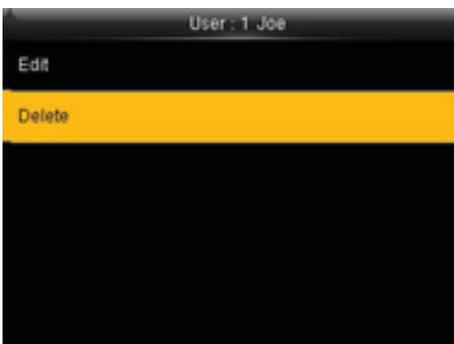
Presione ▼ para seleccionar un usuario y presione OK.



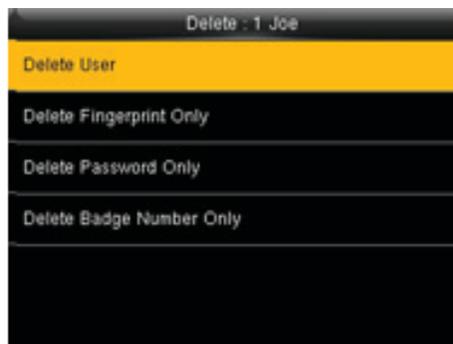
Presione OK para entrar a la interfaz de información del usuario.



El ID de usuario no puede ser modificado, otras operaciones son similares a las realizadas para añadir un usuario.



Presione ▼ para para eliminar y presione OK.



Presione ▼ para seleccionar un elemento que necesite eliminar y presione OK.

Otros usuarios definidos por el administrador se borran cuando se eliminan los derechos de usuarios.

3.3 Estilo de Pantalla



Presione M/OK en la interfaz inicial.



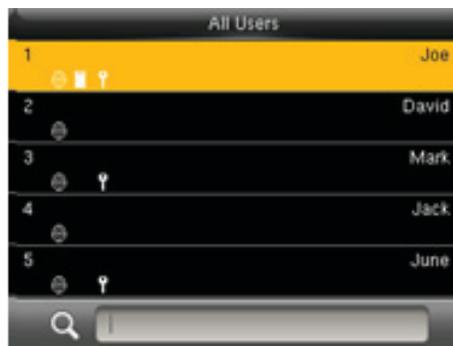
Seleccione usuarios y presione OK.



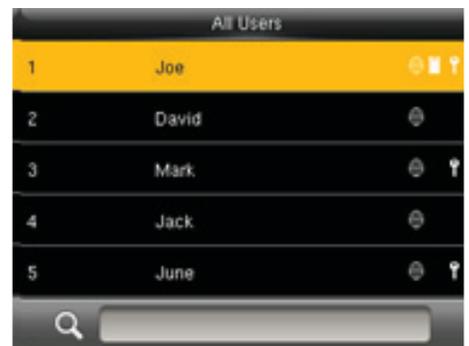
Presione ▼ para seleccionar estilo de pantalla y presione OK.



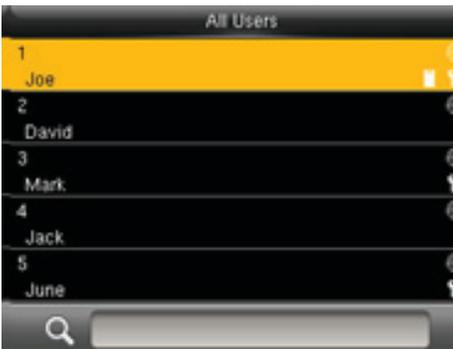
Presione ▼ para seleccionar estilo de pantalla y presione OK.



Línea Individual



Línea Múltiple



Línea Mezclada

4. Rol de Usuario

Establecer los derechos de un rol definido del usuario, es decir, derechos a los menús.



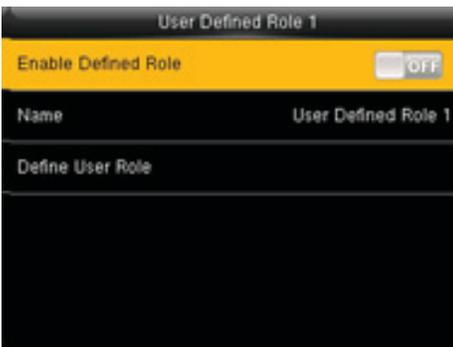
Presione M/OK en la interfaz inicial.



Presione ► para seleccionar Rol de Usuario y presione OK.



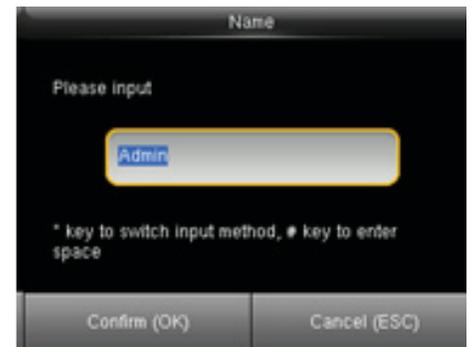
Presione ▼ para seleccionar definición de Rol de Usuario y presione OK.



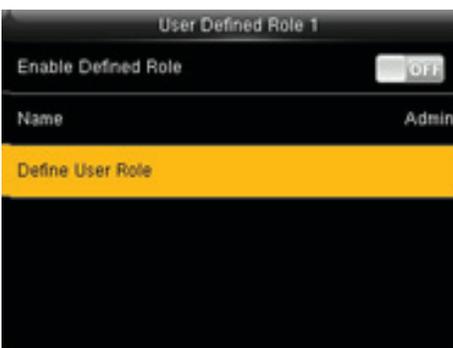
Presione OK para abrir.



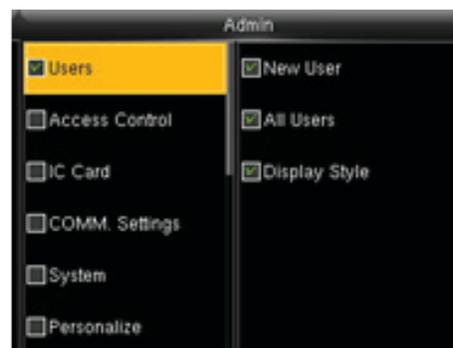
Presione ▼ para seleccionar Nombre y presione OK.



Presione * para cambiar el método de entrada e ingrese el Nombre, presione OK.



Presione ▼ para seleccionar Nombre y presione OK.



Presione ▼ y OK para seleccionar derechos. Presione ESC para salir.

5. Ajustes de Comunicación

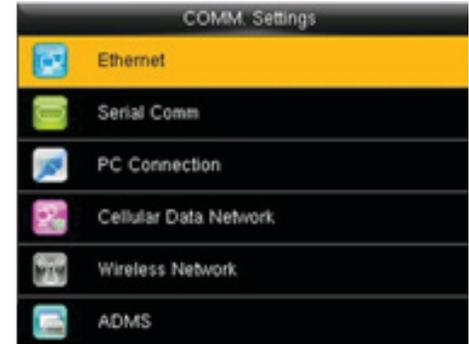
Establezca parámetros para la comunicación entre el dispositivo y una PC. Los parámetros incluyen la dirección IP, puerto, máscara sub-red, velocidad de transmisión y contraseña de inicio de sesión.



Presione M/OK en la interfaz inicial.



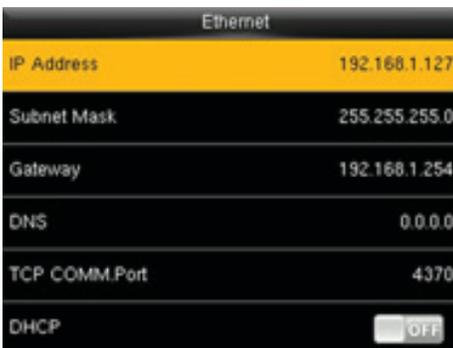
Presione ► para ajustes de comunicación y presione OK.



Seleccione Ethernet y presione OK.

5.1 Ethernet

Cuando el Ethernet es utilizado para comunicación del dispositivo y la PC, los siguientes ajustes necesitan ser verificados.



Dirección IP: La IP por default es 192.168.1.201. Puede modificarla si es necesario. Pero no puede ser la misma que la PC.

Máscara Sub-red: Por default es 255.255.255.0. Puede modificarla si es necesario.

Puerto: Por default es 0.0.0.0. si el dispositivo y la PC tienen diferente segmento de red, es necesario ajustar la dirección.

DNS: El servidor DNS por default es 0.0.0.0 y puede ser cambiado si lo requiere.

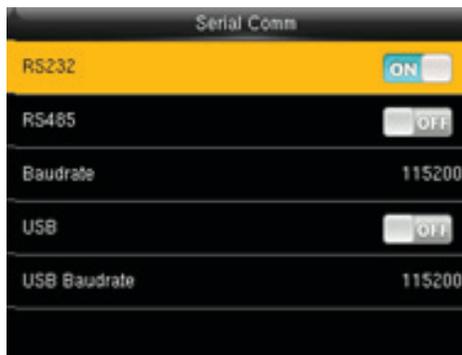
Comunicación de Puerto TCP: Por default es 4730. Lo puede modificar si es necesario.

DHCP: Configuración Dinámica de Host, es utilizado por un servidor para asignar direcciones IP dinámicas a los usuarios de una red.

Pantalla en barra de estado: utilizada para establecer los iconos de red en la barra de estatus del menú principal.

5.2 Comunicación Serial

Cuando el puerto serial (RS232/RS485) es usado para la comunicación del dispositivo y la PC, los siguientes ajustes necesitan ser verificados:



RS232: Si utiliza comunicación RS232. Seleccione “Si” si RS232 se va a utilizar.

RS485: Si utiliza comunicación RS485. Seleccione “Si” si RS485 se va a utilizar.

Velocidad de Transmisión: Usado para comunicación con PC. Existen cinco opciones: 9600, 19200, 38400, 57600 y 11520. Si la velocidad de comunicación es alta, se recomienda RS232. Si la velocidad de comunicación es baja se recomienda RS485.

USB: Si utiliza USB para comunicación. Seleccione “Si” si se va a utilizar USB.

Velocidad de Transmisión USB: Utilizando comunicación con PC. Existen cinco opciones; 9600, 19200, 38400, 57600, y 11520. Sí la velocidad de comunicación es alta.

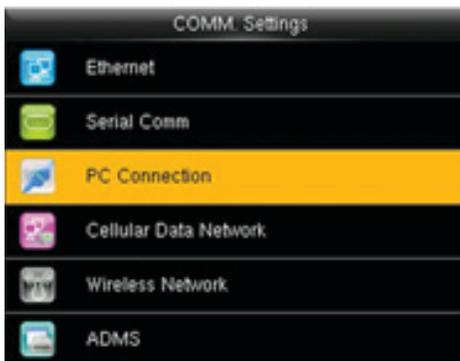
ID de Dispositivo: 1-254. Sí RS232/RS485, este ID necesita tener una entrada en la interfaz de comunicación del software.

5.3 Conexión a PC

Para mejorar la seguridad de datos de asistencia, la contraseña de conexión necesita ser ajustada aquí. La contraseña de conexión debe ser cuando el software se conecte con el dispositivo a la red de datos.

Clave de comunicación: La contraseña por default del sistema es 0. (Es decir, no hay ninguna contraseña) puede configurarse como otro valor. Después del ajuste la contraseña debe ingresarse si el software se comunica con el dispositivo. O la conexión fallará. La longitud de la contraseña es de 1 a 6 dígitos.

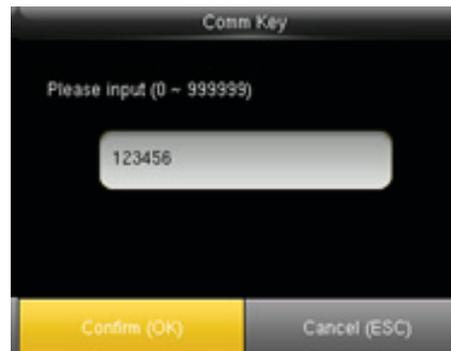
ID de Dispositivo: 1-254. Si se usa RS232/RS485, este ID necesita ser ingresado en el software en la interfaz de comunicación.



Presione ▼ para seleccionar conexión a PC y presione OK



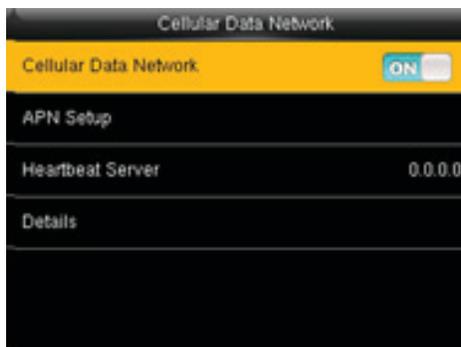
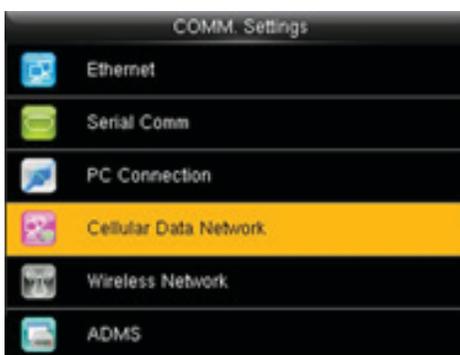
Presione OK.



Ingrese una contraseña, presione ▼ para seleccionar confirmar (OK) y presione OK.

5.4 Red de Datos Móviles

Cuando el equipo está en la red de acceso telefónico, asegúrese que el dispositivo este en cobertura GPRS o SEÑAL WCDMA, debe saber el tipo de modem utilizado, nombre el APN y el número de acceso.



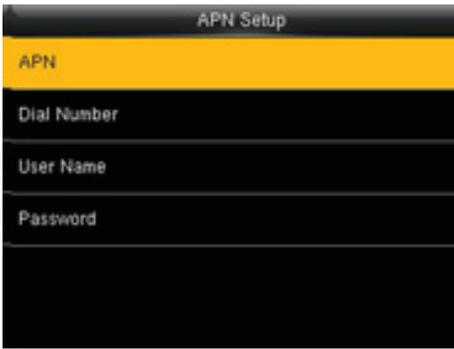
Red de Datos Móviles: Permitir el acceso a una Red de Datos Móviles.

Establecer APN: utilizado para ajustar información de APN, como el número de acceso, nombre de usuario, y contraseña.

Servidor: recolecta los registros de asistencia del dispositivo utilizando la conexión de datos con el software ofrecido por ZKTeco. Después de configurar correctamente la dirección IP del servidor para el dispositivo, el dispositivo enviará el registro de asistencia al servidor automáticamente.

Detalles: Incluye información acerca de la conexión de red móvil, como el modo de red, operador de telecomunicaciones, dirección IP, recepción y envío de datos.

Configuración de APN:



APN: Nombre del punto de acceso, utilizado para identificar tipos de GPRS/WCDMA.

Marcación de Número: El número de acceso de GPRS/WCDMA.

Nombre de Usuario y Contraseña: utilizado para verificar si un usuario tiene derechos para entrar a una red.

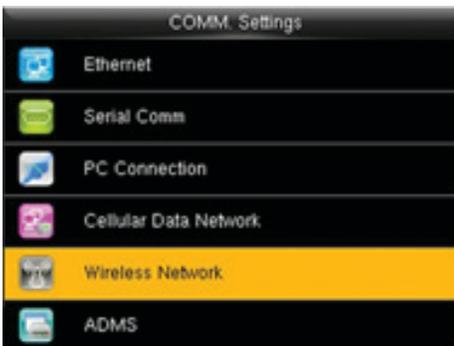
5.5 Red Inalámbrica

Wireless Fidelity (Wi-Fi) es también conocida como estándar 802.11b. La mayor ventaja de WIFI es la velocidad de transmisión arriba de 11Mbps. Wi-Fi también cuenta con larga distancia de trasmisión y excelente compatibilidad con varios dispositivos DSSS 802.11, IEEE 802.11b es el radio basado en variante de IEEE 802.11. el ancho de banda de IEEE 802.11b puede ser mayor a 11Mbps y ajustada automáticamente a 5.5 Mbps, 2Mbps y 1Mbps dependiendo la fuerza de la señal y el nivel de interfaz, garantizando la estabilidad y confiabilidad de la señal. Ventajas principales: Alta velocidad de transferencia y confiabilidad. La distancia de comunicación puede mayor de 305 mts en un área abierta y 76 mts a 122 mts en un área cerrada. Wi-Fi puede ser integrada convenientemente con la línea de Ethernet, haciendo más bajo el costo de la creación de redes.

Nuestra terminal tiene capacidad de Wi-Fi, soporta modulo interno externo de Wi-Fi para implementar datos inalámbricos de transmisión sobre Wi-Fi.

Presione OK para abrir o cerrar Wi-Fi.

Operación:



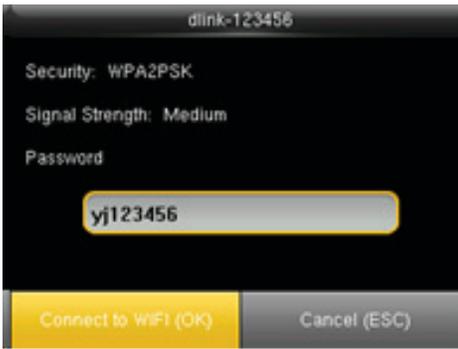
Presione ▼ para seleccionar red inalámbrica y presione OK.



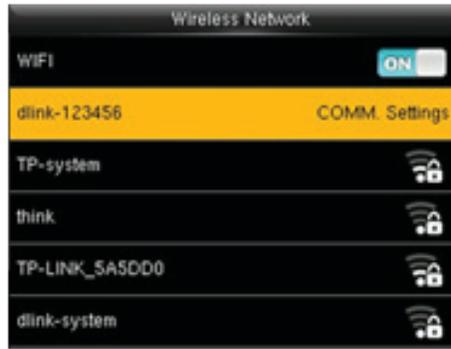
Presione WiFi para abrir o cerrar la función.



Presione ▼ para seleccionar "dlink-123"56" y presione OK.



Ingrese una contraseña, presione ▼OK.



Conecte, como se muestra en la figura.



Conecte, la interfaz inicial mostrada en la figura.

5.6 ADMS ★

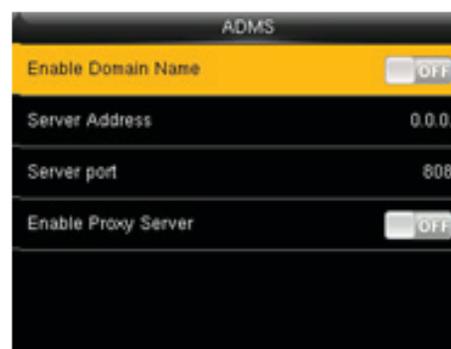
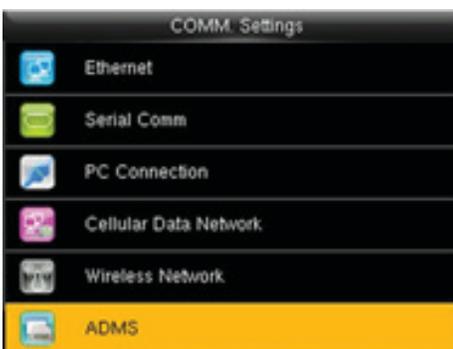
Este sub-menú es utilizado para conectar los ajustes relacionados con el servidor web, como dirección IP del servidor web, configuración de puerto y para ajustes de proxy.

Nombre del dominio disponible: Cuando el nombre del modo del dominio este habilitado, se accede a una página utilizando un nombre de dominio en el formato de http://; de otra manera debe ingresar una dirección IP para el acceso al sitio.

Dirección del servidor: dirección IP del servidor web.

Puerto del servidor: puerto utilizado por el servidor web.

Servidor Proxy habilitado: Cuando habilita la función proxy, establecer la dirección IP y número de puerto del servidor proxy. Esta opción indica si debe utilizar una dirección IP proxy. Puede seleccionar ingresar la dirección IP p la dirección del servidor para acceso a internet, cualquiera que desee.



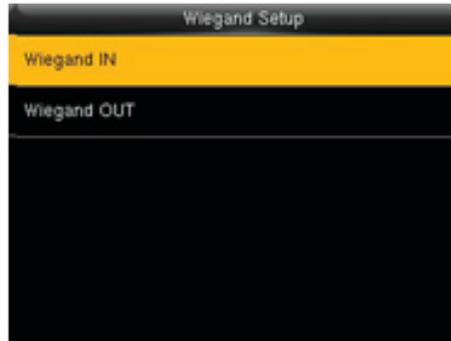
5.7 Ajustes Wiegand

5.7.1 Entrada Wiegand

Operación:



Presione ▼ para seleccionar configuración Wiegand y presione OK.



Presione OK.



Presione ▲/▼ y OK para seleccionar partida. Cuando los ajustes estén completados, presione OK para guardar la configuración y salir.

Formato Wiegand: El Sistema tiene dos formatos de entrada Wiegand 26-bits y 34-bits.

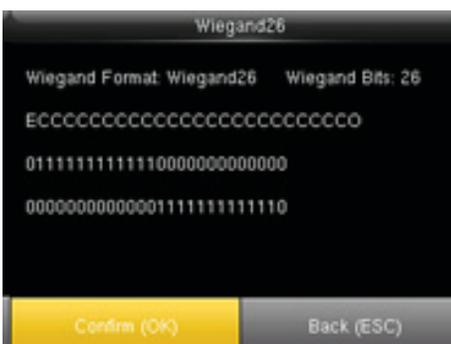
Bits Wiegand: Especifica el número de bits ocupados por el dato Wiegand

Ancho de pulso: El ancho de pulso por defecto son 100 microsegundos, puede ser ajustado de 20 a 100.

Intervalo de pulso: 100 microsegundos por defecto, pueden ser ajustados entre 200 y 2000.

Tipo de ID: Especifica el contenido de la señal de entrada wiegand, puede ser un ID de empleado o tarjeta ID, en base a su requerimiento.

Detalles de formato: Despliega la información definida por varios bits de la selección del formato Wiegand



Formato Wiegand 26

E: Paridad par
O: Paridad impar
C: Número de Tarjeta

5.7.2 Wiegand OUT

Formato Wiegand: el Sistema tiene dos formatos de entrada Wiegand de 26 bits y Wiegand de 34 bits.

ID Fallido: define el valor de salida de errores de autenticación del usuario. El formato de salida Wiegand es determinado por el formato Wiegand establecido. El rango de valor es de 0 a 65535.

Código del Sitio: Similar al ID del dispositivo. Pero el código es especificado por el usuario. Puede repetirse diferente dispositivo (con rango de 00-255)

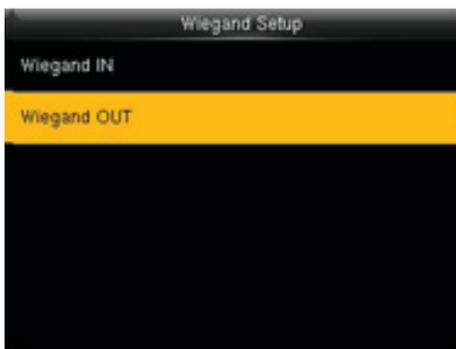
Ancho de Pulso: El ancho de pulso por default son 100 microsegundos, el cual se puede ajustar de 20 a 100.

Intervalo de Pulso: Son 100 microsegundos por default, se puede ajustar entre 200 y 2000.

Tipo de ID: Especifica el contenido de la salida par a la autenticación exitosa del usuario. Puede seleccionar el ID del empleado o la tarjeta ID.

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

Operación:



Presione OK.



Presione ▲▼ y O para seleccionar elemento. Cuando el ajuste este completado, presione OK para guardar la configuración y salga.

6. Sistema

Establezca los parámetros del Sistema para satisfacer la demanda de los usuarios. Incluye la fecha y hora, asistencia.



Presione M/OK en la interfaz inicial.

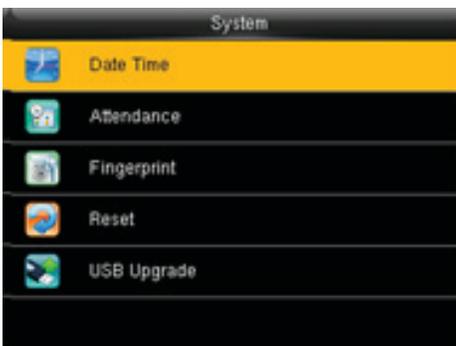


Seleccione sistema y presione OK.

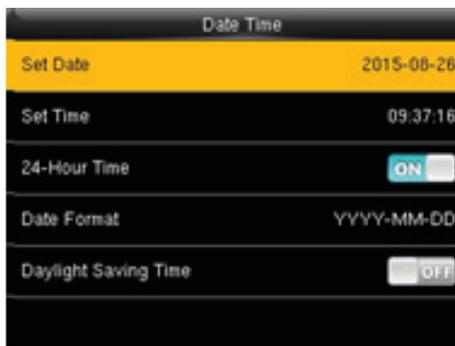


Seleccione Fecha y hora y presione OK.

6.1 Fecha /Hora



Seleccione Fecha/Hora y presione OK.



Presione ▲/▼ y OK para seleccionar elementos. Cuando los ajustes estén completos, presione OK para guardar configuraciones y salir.

Establezca Fecha/Hora: este parámetro es utilizado para establecer fecha y hora de la terminal FFR.

Horario DE 24 horas: Este parámetro es utilizado para establecer el modo de visualización de la interfaz inicial. Seleccione "ON" para adoptar el modo de 24 horas. Seleccione "OFF" para adoptar el modo de 12 horas.

Formato de Fecha: Este parámetro es utilizado para establecer el formato de fecha mostrado en la interfaz inicial de la terminal FFR.

Tipo de calendario: el dispositivo soporta tres tipos de calendario, gregoriano, gregoriano iraní e irán lunai. Puede modificarlo si es necesario.

Horario de verano

DST, también llamado horario de verano es un Sistema para percibir la hora local con el fin de ahorrar energía. El tiempo unificado adoptado durante la fecha del sistema es nombrado "DST". Usualmente, se adelanta una hora en verano. Esto puede hacer que las personas se duerman más temprano y despierten más temprano. Esta también reduce la iluminación para ahorrar energía. En otoño, el horario será recuperado. Las regulaciones son diferentes en diferentes países. Actualmente casi 110 países adoptan DST.

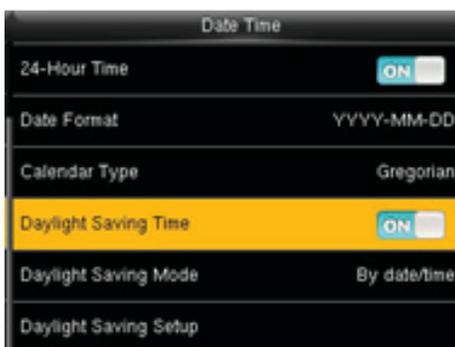
Para satisfacer la demanda del horario de verano, una opción especial puede ser personalizada en nuestra tarjeta de tiempo RF & en la grabadora de asistencia. Hacer que se adelante una hora a XX (minuto) XX(Hora) XX(día) XX (mes) y retrasar una hora a XX (minuto) XX (Hora) XX(día) XX (mes) si es necesario.

Operación:

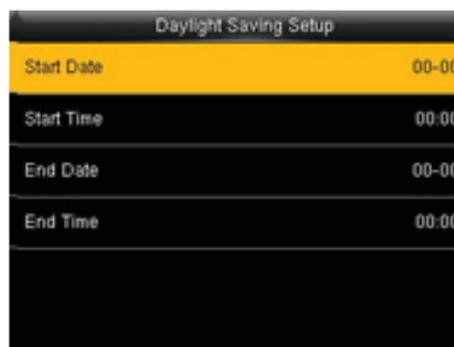
- 1) Establezca DST como "habilitado"
- 2) Entrada DST hora de inicio y hora final.

Por ejemplo, si 8:00, 1 de Abril es establecido, el dispositivo debe entrar en DST, y el horario se adelantara una hora. Si es 8:00, 1 de Agosto, el dispositivo se reiniciara al horario normal.

- 3) Presione OK para guardar configuración. Presione "ESC" para salir sin guardar.



Abra el horario de verano



Configure horario en fecha/hora



Configure la hora en semana/día

Modo de horario de verano: Puede seleccionar el modo de fecha (mes-día-hora) o modo de semana (mes- día laborable- hora). Por default el modo de fecha es utilizado.

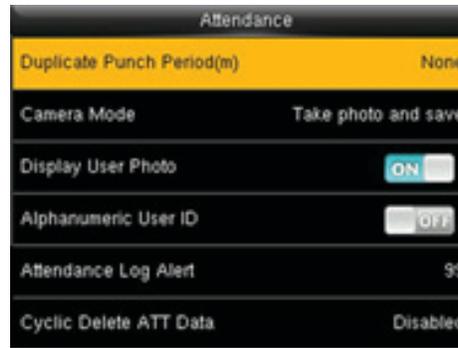
Configuración del horario de verano: Utilizado para ajustar el horario de inicio o final de DST.

Descripción del modo de fecha y modo de semana:

1. Si el mes en que inicia el horario de verano es posterior a cuando termina el horario de verano, el horario de verano se expandirá dos años diferentes. Por ejemplo, el inicio de horario de verano es 2012-9-1 4:00 y el final del horario de verano es 2013-4-1 4:00.

2. Asuma que el modo semanal es seleccionado y el horario de verano inicia el domingo de la sexta semana de Setiembre en 2012. Acorde al calendario, Septiembre de 2013 no tiene seis semanas pero tiene cinco semanas. En este caso, en 2013, el horario de verano inicia en el tiempo correspondiente al último domingo de Septiembre.
3. Asuma que el horario de verano inicie el lunes de la primera semana de Septiembre de 2012. Acorde al calendario, la primera semana de Septiembre 2012 no inicia con lunes. En este caso, el horario de verano inicia el primer lunes de Septiembre 2012.

6.2 Asistencia



Presione ▼ para seleccionar Asistencia y presione OK.

Presione ▲▼ y OK para seleccionar elementos. Cuando la configuración este completa, presione OK para guardar la configuración y salga.

Periodo duplicado (m): Si el registro de asistencia de un usuario ya existe y el usuario presiona de nuevo sin el periodo especificado (unidad: minuto), el segundo registro no será almacenado. (Valor de alcance: 1-60 minutos).
Modo de cámara: cuando el empleado está en el registro de asistencia, captar fotografías y guardarlas. Está dirigido a la configuración de todos los empleados.

Existen 5 modos:

Sin fotografía: No existe fotografía tomada durante el registro de asistencia.

Tomar la foto, sin guardarla: toma la fotografía pero no la guarda en el registro de asistencia.

Tomar foto y guardarla: Toma la fotografía y la guarda durante el registro de asistencia.

Verificación guardada exitosamente: cuando un empleado verifica la asistencia, una fotografía del empleado es tomada y guardada.

Guardar la verificación fallida: cuando un empleado falla la verificación de asistencia por tres veces consecutivas, se toma una fotografía del empleado y es guardada.

Mostrar foto de usuario: La fotografía del usuario es mostrada cuando el empleado realiza la verificación de asistencia.

ID Alfanumérico del usuario: El ID del empleado puede contener letras. El ID del empleado con letras ayuda a clasificar los empleados.

Alerta de registro de asistencia: Cuando el espacio habilitado es insuficiente para almacenar un número específico del registro de asistencia, la terminal FFR automáticamente generará una alarma (valor de alcance: 1-99).

Borrar datos cíclicos ATT: Especifica el número máximo de registro de asistencia que pueden ser eliminados en el momento en que el número de registros alcance el límite superior. Esta función puede ser deshabilitada de otra manera, el rango de valor es de 1 a 999.

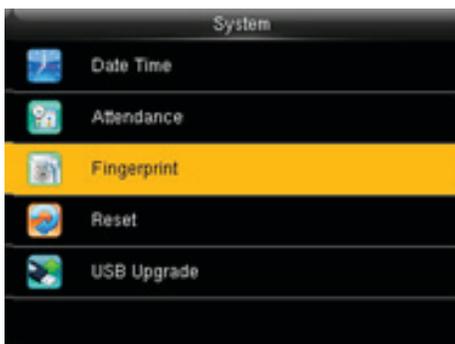
Borrar datos cíclicos de fotografías ATT: Especifica el número máximo de fotografías de asistencia que puede ser eliminadas una sola vez cuando el número de fotografías de asistencia alcance el límite superior, esta función puede ser deshabilitada; de otra manera, el rango de valor es de 1 a 99.

Confirmar retraso de pantalla: Especifica el tiempo de la visualización del resultado de la verificación. el rango de valor es de 1 a 9s.

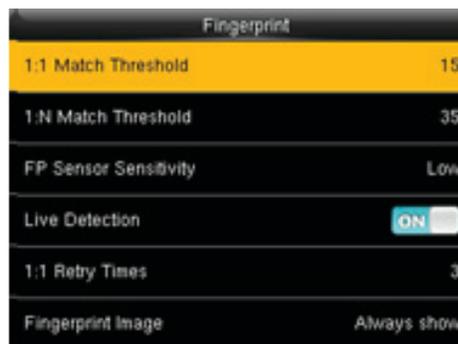
Guardar registro de verificación ilegal: Guarde el registro de verificación ilegal en una zona de tiempo y combinación ilegal o no la guarde cuando el control de acceso este habilitado.

Regla de expiración: Puede seleccionar una de las tres condiciones: retener información de usuario y no guardar registros de asistencia; retener información de usuario y guardar registros de asistencia; eliminar información de usuario.

6.3 Huella Digital



Presione ▼ para seleccionar huella digital y presione OK.



Presione ▲/▼ y OK para seleccionar elementos. Cuando las configuraciones estén completas, presione OK para guardar la configuración y salga.

Valores recomendados de verificación:

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

Sensibilidad del sensor de huella digital: utilizado para configurar la sensibilidad del sensor. El valor por default mediano es el recomendado. Puede ajustar la sensibilidad de la colección de huella digital Alto cuando la respuesta a la exploración del dedo se encuentra en un ambiente seco. Cuando se utiliza en un ambiente húmedo, puede configurar la sensibilidad de la huella digital Bajo si la huella es difícil de identificar.

Detección en tiempo real: Seleccione para abrir la función ID en tiempo real. Abra función ID en tiempo real, es decir abrir la función de huellas digitales falsas. Después de abrirlo, cuando se registre o verifique huellas digitales el dispositivo identificara la huella falsa, principalmente el registro fallido o si la verificación no paso.

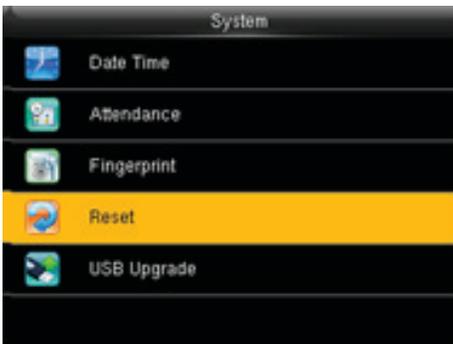
Reintentar verificación 1:1: Este parámetro es utilizado para configurar las veces de reintentar de verificación fallida 1:1 o verificación de contraseña debido a la ausencia de huellas enroladas o la inadecuada colocación de los dedos, para evitar operaciones repetitivas.

Algoritmo de huella dactilar: este parámetro es utilizado para seleccionar la versión de algoritmo de huella entre 9 y 10. Por favor seleccione la versión del algoritmo con precaución porque las plantillas de las huellas de estos dos algoritmos son incompatibles.

Imagen de huella: este parámetro es utilizado para establecer la visualización de la imagen de la huella en la pantalla durante el enrolamiento o comparación. Tiene dos valores visualización permanente y sin visualización.

6.4 Reiniciar

Opción de comunicación del dispositivo, opción del Sistema y así reiniciar al estado de fábrica.



Presione ▼ para seleccionar Reiniciar y presione OK.



Presione ▲▼ para seleccionar OK o Cancelar y presione OK.

6.5 Actualización USB

Puede actualizar el firmware de la terminal FFR utilizando la actualización del archivo de actualización en la USB mediante este parámetro.



Si necesita el archivo de actualización de firmware, por favor contacte a nuestro personal de soporte técnico. Generalmente la actualización del firmware no es recomendable.

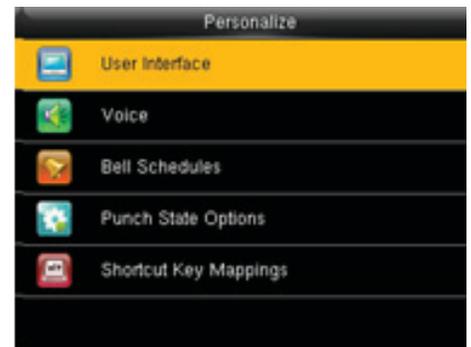
7. Personalizar



Presione M/OK en la interfaz inicial



Seleccione personalizar y presione OK.



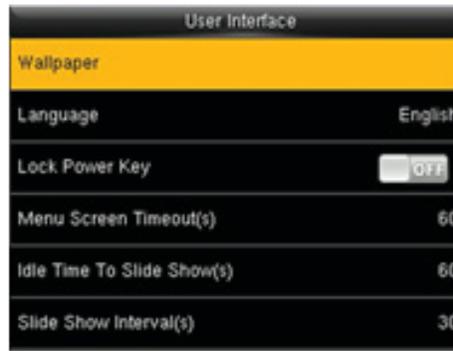
Seleccione interfaz de usuario y presione OK.

7.1 Interfaz de Usuario

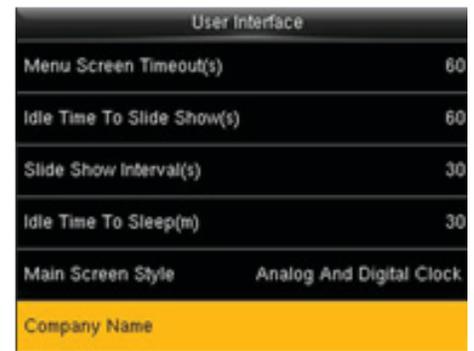
Acorde a las preferencias del personal puede configurar el estilo de la interfaz inicial.



Presione ▼ para seleccionar interfaz de usuario y presione OK.



Presione ▲/▼ y OK para seleccionar elementos. Cuando los ajustes estén completados, presione OK para guardar la configuración y salga.



Wallpaper: Los usuarios pueden seleccionar el wallpaper mostrado en la pantalla.

Lenguaje: Puede seleccionar un lenguaje para el dispositivo basado en sus requerimientos.

Tecla de encendido de bloqueo: para prevenir apagado hostil, seleccione para bloquear el apagado o no. "Deshabilitar": Se apagará después de tres segundos de presionar apagar. "Habilitar": no funcionara después de presionar apagar.

Tiempo de espera del menú en la pantalla: el dispositivo mostrará la interfaz principal automáticamente cuando ninguna operación es realizada en un menú sin el tiempo de espera del menú. (Esta función puede ser deshabilitada: de otra manera, el rango de valor es de 60s a 99999s)

Tiempo de inactividad de pantallas: La imagen de aviso se muestra cuando ninguna operación es realizada en la interfaz principal sin el tiempo de espera. (Esta función puede ser deshabilitada; de otra manera, el rango de valor es de 3s a 999s.)

Intervalo de pantalla: Este parámetro es utilizado para configurar el intervalo de imagen (alcance de valor: 0-99 segundos).

Tiempo de inactividad para reposo: Este parámetro es utilizado para especificar un periodo después que el dispositivo se ponga en modo de reposo sin ninguna operación en este periodo. Se puede reactivar el dispositivo presionando cualquier tecla o tocando la pantalla. Rango numérico de 1-30 minutos, el tiempo por defecto de fábrica son 3 minutos.

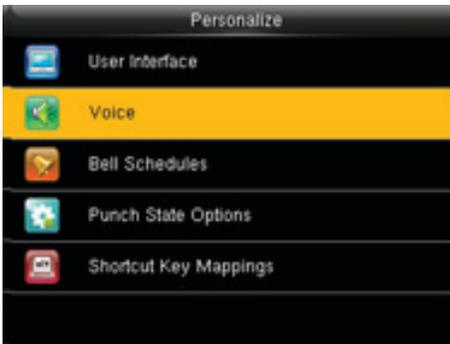
Estilo de pantalla principal: configure donde y como se muestra el reloj y el estatus en la pantalla de menú principal.

Nombre de la compañía: cuando un nombre de la compañía es especificado, puede seleccionar imprimir el nombre de la compañía en ajustes de impresión.

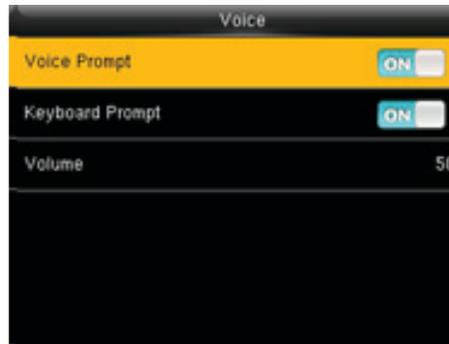
Nota:

El nombre de la compañía es solo en caso de abrir la función de impresión.

7.2 Voz



Presione ▼ para seleccionar Voz y presione OK.



Presione ▲▼ y OK para seleccionar elementos. Cuando las configuraciones estén completadas, presione OK para guardar los ajustes y salga.

Mensaje de voz: este parámetro es utilizado para configurar para reproducir indicaciones de voz durante la operación de la terminal FFR. Seleccione "ON" para habilitar mensaje de voz y seleccione "OFF" para silenciar.

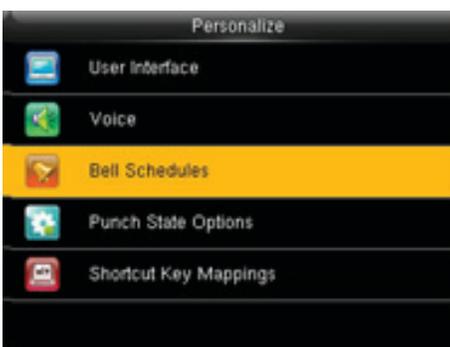
Sonido de teclado: este parámetro es utilizado para configurar la generación de un sonido bip en respuesta a la pulsación de teclado. Seleccione "ON" para habilitar sonido bip, y seleccione "OFF" para silenciar.

Volumen: Este parámetro es utilizado para ajustar el volumen del mensaje de voz.

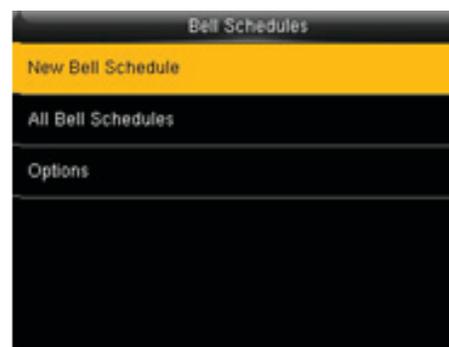
7.3 Timbres de Horarios

Muchas compañías necesitan timbres en servicio y fuera de servicio. Algunos utilizan el manual de timbres. Algunos utilizan timbres electrónicos. Para ahorrar costo y tener conveniencia para la administración, integramos funciones de timbre en el sensor de huellas. Puede configurar el tiempo para el timbre. Cuando sea un horario programado, el dispositivo reproducirá automáticamente el tono seleccionado y activar la señal del relé. El tono no se detiene hasta que haya transcurrido la duración del tono. Por default, el dispositivo ofrece 15 tonos.

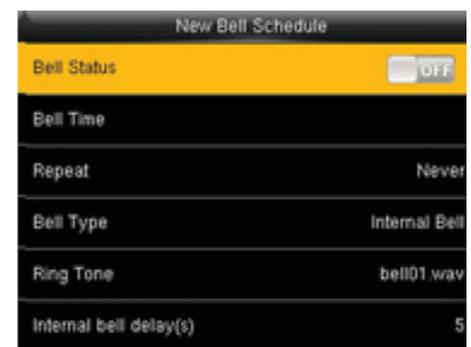
1. Agregar un timbre



Presione ▼ para seleccionar horarios de timbre y presione OK.



Presione ▼ para seleccionar nuevo horario de timbre y presione OK.



Presione ▲▼ y OK para seleccionar elementos, presione OK para guardar y salga.

Estatus de timbre: Si tiene habilitado el timbre.

Horario de timbre: Los tonos de timbre sonaran automáticamente cuando estén en el horario especificado.

Repetir: Especificar para repetir tono.

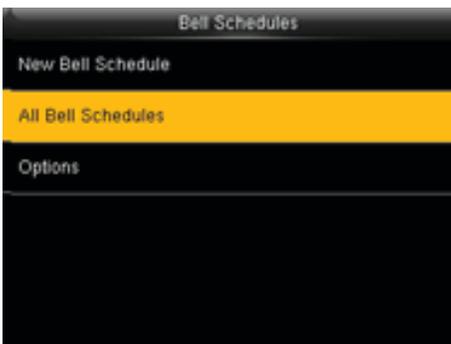
Tipo de Timbre: puede seleccionar entre el tono interno y el tono externo. Para el tono interno , el tono es reproducido por la bocina de la terminal. Para el tono externo, será reproducido por un timbre eléctrico externo que es conectado con la terminal.

Tono: Sonido de timbre.

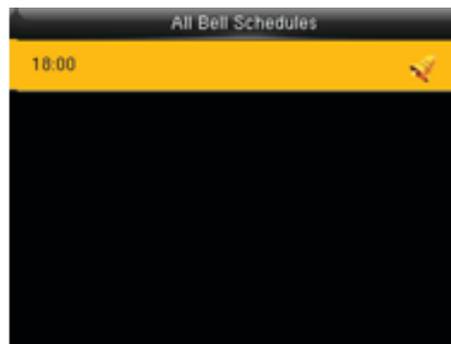
Retardo de timbre interno: especifica la duración de reproducción del tono. El rango de valor es de 1s a 999s.

Noticia: Solo algunos modelos tienen opción de timbre externo.

2. Editar y eliminar un timbre



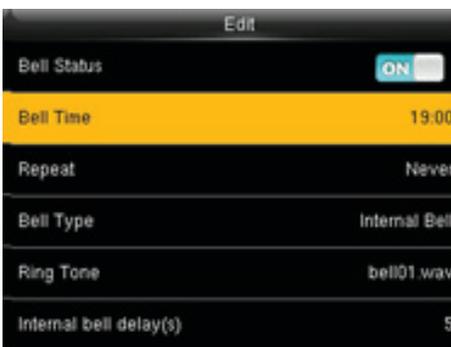
Presione ▼ para seleccionar horarios de timbre y presione OK.



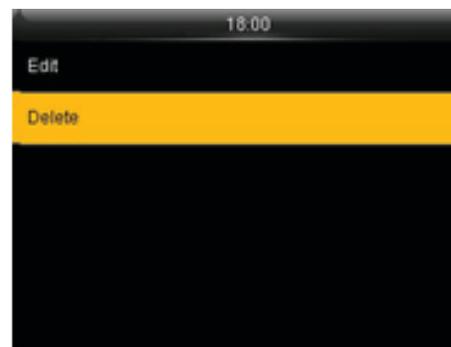
Seleccione nuevo horario de timbre y presione OK.



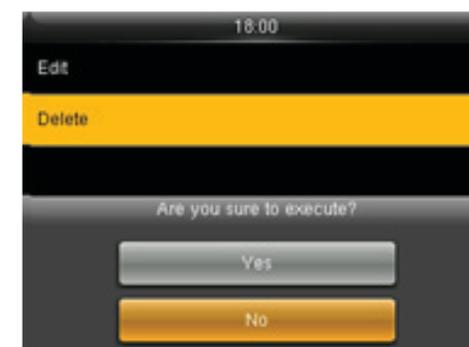
Seleccione editar y presione OK.



Seleccionar elemento.



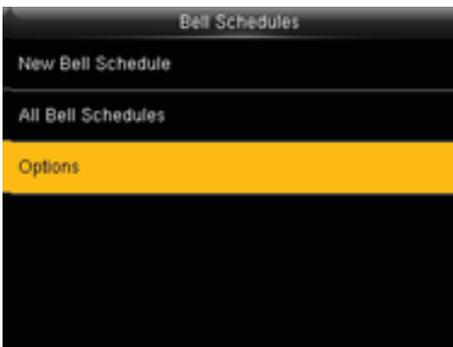
Presione ▼ para Eliminar y presione OK.



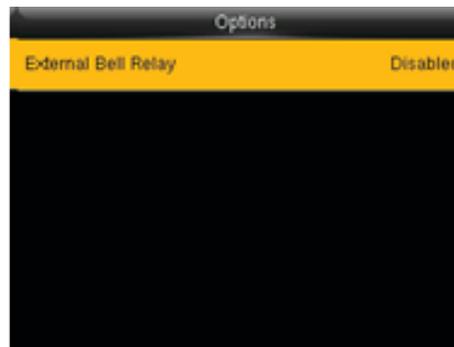
Presione ▼ para seleccionar "Si" o "No"

3. Opciones

Cuando la función de tono externo es utilizada, configure la salida de la terminal.



Presione ▼ para seleccionar Opciones y presione OK

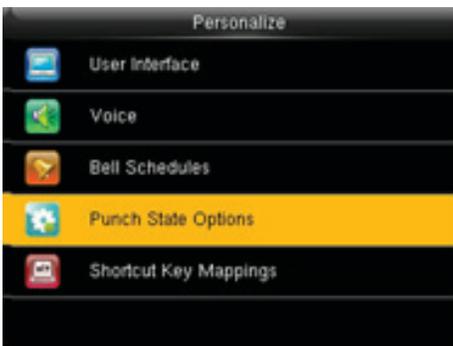


Presione OK.

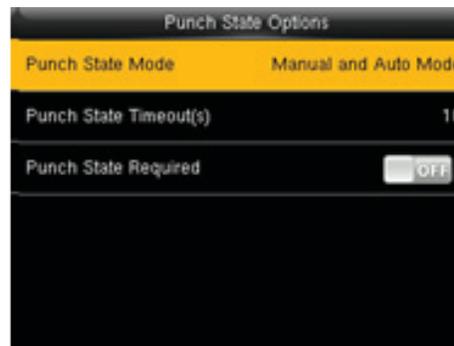


Presione ▼ para seleccionar, presione OK para guardar y regresar.

7.4 Opciones de Estado



Presione ▼ para seleccionar Opciones de estado y presione OK.



Presione ▲/▼ y OK para seleccionar elementos. Cuando las configuraciones estén completas, presione OK para guardar los ajustes y salga.

Modo de estado: Utilizado para seleccionar un estado de modo de tecla. Los siguientes modos están disponibles:

Apagado: El estatus de función de tecla no es utilizado. El estatus de las teclas definidas como teclas de acceso directo no está disponibles.

Modo Manual: Cambiar el estatus de teclas de forma manual y la tecla de estado actual desaparecerá cuando el tiempo haya transcurrido.

Modo Automático: Si una tecla de atajo de estatus es configurada debe ser cambiado después de un periodo de tiempo, la tecla de estatus es cambiada automáticamente cuando el periodo de tiempo haya transcurrido.

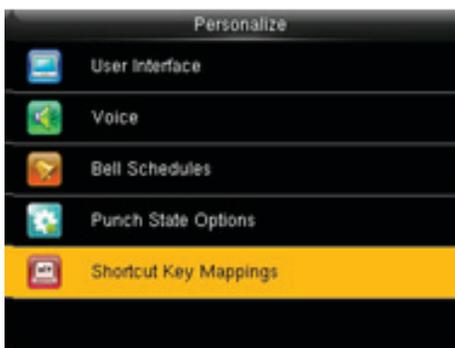
Modo Manual y Automático: La interfaz principal muestra las teclas de estatus que pueden ser cambiadas automáticamente, y también puede hacer el cambio de estatus de teclas manualmente. Una tecla de estatus seleccionada manualmente será cambiada acorde al plan de cambios después desaparecerá después del tiempo de espera.

Modo Manual Fijo: Después de que una tecla de estatus es cambiada, siempre será mostrada hasta después de ser cambiada de nuevo.

Modo Fijo: Un estatus de tecla siempre es mostrado y no puede ser cambiado.

Estado requerido: especifica si el estatus de verificación de asistencia debe ser seleccionado durante la autenticación.

7.5 Asignación de Teclas de Acceso Rápido



Presione ► para seleccionar tecla y presione OK.



Presione >> y OK para seleccionar elementos.



Cuando las configuraciones estén completadas.

Nota:

Cuando ajuste las teclas de acceso directo de estatus de asistencia, puede configurar también el parámetro "Cambio Automático". Cuando "Cambio Automático" este habilitado, la terminal FFR cambia automáticamente el estatus al horario especificado. Si una tecla de estatus es seleccionada, el dispositivo no utilizara ninguna tecla de estatus cuando la tecla de estatus este deshabilitada.

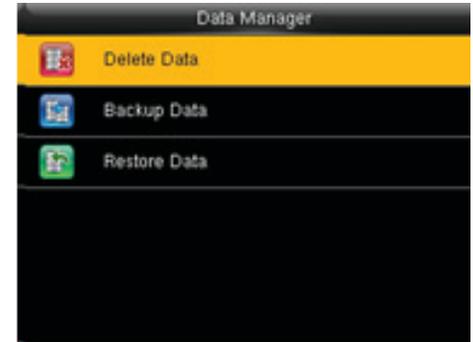
8. Administración de Datos



Presione la tecla M/OK en la interfaz inicial.



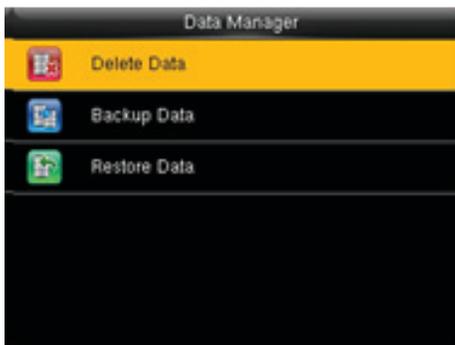
Seleccione administración de datos y presione OK.



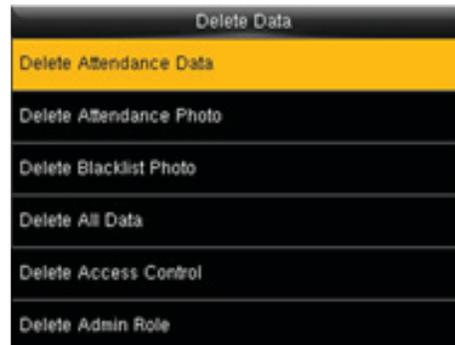
Seleccione Eliminar datos y presione OK.

8.1 Eliminar Datos

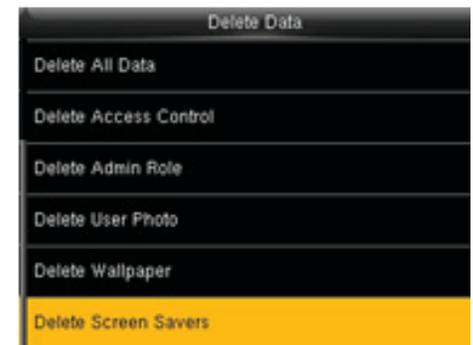
Mediante el menú (Administración de Datos), puede realizar administración de datos almacenados en la terminal FFR, por ejemplo, eliminar el registro de asistencia, todos los datos y fotografías, gestión de derechos y reinicie la terminal FFR a defectos de fábrica.



Seleccione Eliminar Datos y presione OK



Presione ▼ y OK para seleccionar elemento para ser eliminado.



Eliminar fecha de asistencia: eliminar todos los registros de asistencia.

Eliminar foto de asistencia: eliminar todas las fotos de los empleados.

Eliminar fotos de lista negra: eliminar las fotos guardadas quienes fallaron en verificar la asistencia.

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

Eliminar control de acceso: Eliminar registro de control de acceso.

Limpiar rol de administrador: Cambiar todos los administradores a usuarios ordinarios.

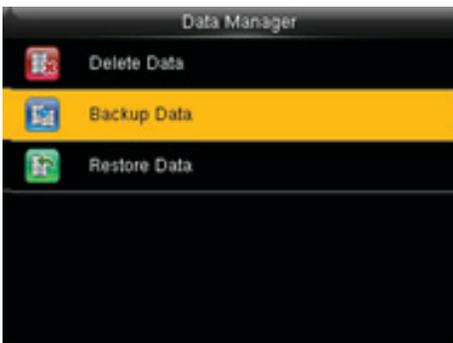
Eliminar foto de usuario: Eliminar todas las fotos del usuario.

Eliminar wallpaper: eliminar todos los wallpaper.

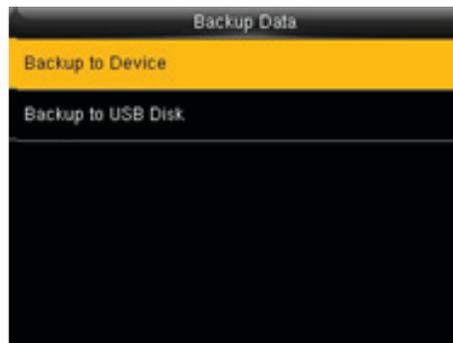
Eliminar protectores de pantalla: limpiar las imágenes cargadas de la USB a la terminal FFR. (Para detalles de cómo subir imágenes promocionales, vea "5.4 Cargar Imagen")

8.2 Respaldo de Datos

Respaldo de datos de servicio o configuración de datos del dispositivo al dispositivo o a una USB.



Presione ▼ para seleccionar Respaldo de Datos y presione OK



Presione ▼ para seleccionar Respaldo para el dispositivo y presione OK



Presione ▼ y OK para seleccionar elementos de configuración local para ser respaldados al dispositivo los elementos seleccionados.



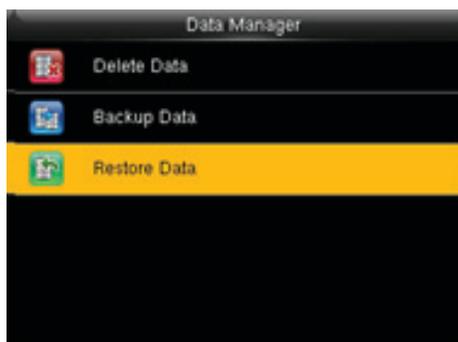
Presione ► para seleccionar inicio de respaldo y presione OK.

Nota:

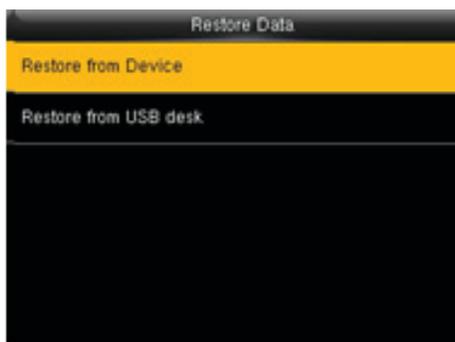
Respaldo a la USB, las operaciones son similares a las realizadas el respaldo del dispositivo.

8.3 Restaurar Datos

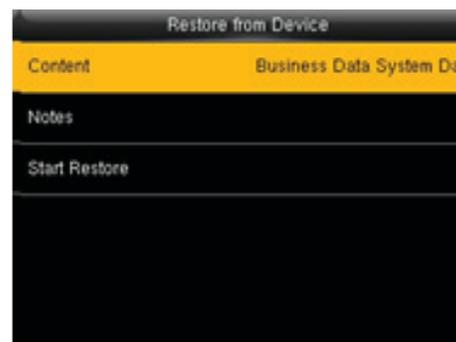
Restaurar datos almacenados en el dispositivo o en la USB.



Presione ▼ para seleccionar Restaurar datos y presione OK



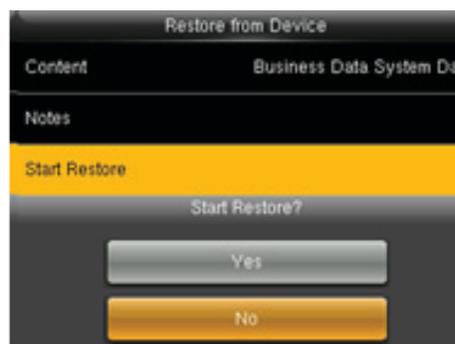
Presione ▼ para seleccionar Respaldo del dispositivo y presione OK.



Presione ▼ y OK para seleccionar elementos de la configuración local para ser restaurados y guardados.



Presione para seleccionar inicio de restauración y presione OK.



Presione ▼ para seleccionar "Si" o "No" y presione OK.

Nota:

Respaldo desde USB, las operaciones son similares a las realizadas en el respaldo desde el dispositivo.

9. Ajustes de Control de Acceso

La opción de control de acceso es para configurar a los usuarios la apertura de puertas de una zona horaria, controlar el bloqueo y parámetros relacionados con el dispositivo.



Presione M/OK en la interfaz inicial. Presione > para seleccionar control de acceso y presione OK. Presione > para seleccionar opciones de control de acceso y presione OK.

Para desbloquear al usuario enrolado debe ser acorde con las siguientes condiciones:

1. El tiempo de desbloqueo actual debe ser efectivo en el horario efectivo de la zona horaria del usuario zona de grupo.
2. El grupo donde el usuario debe estar en control de acceso (o in el mismo control de acceso con otro grupo, para abrir puertas juntos).

El sistema por default coloca a un nuevo usuario en el primer grupo, la zona horaria por default es 1, control de acceso como el primer grupo, y el nuevo usuario enrolado está en desbloqueo (si el usuario tiene modificado los ajustes relacionados de control de acceso, el sistema será cambiado con modificaciones de usuario).

9.1 Opciones de Control de Acceso.

Configure parámetros para control de cerraduras y dispositivos relacionados.

Retardo de cerradura de puerta: El dispositivo de cerradura electrónica está habilitada en tiempo (valor efectivo 1-10 segundos).

Retardo de sensor de puerta: Después de la apertura de la puerta, retrasar el tiempo para verificar el sensor de puerta. Si el estado del sensor de puerta es diferente al estado normal del modo del sensor de puerta, la alarma se emite. Este tiempo es llamado retraso de sensor de puerta. (Valor efectivo: 1-99 segundos)

Tipo de sensor de puerta: Incluye NONE, NC y NO, NONE significa que no tiene sensor de puerta. NO significa apertura de puerta normal. NC significa puerta cerrada normalmente.

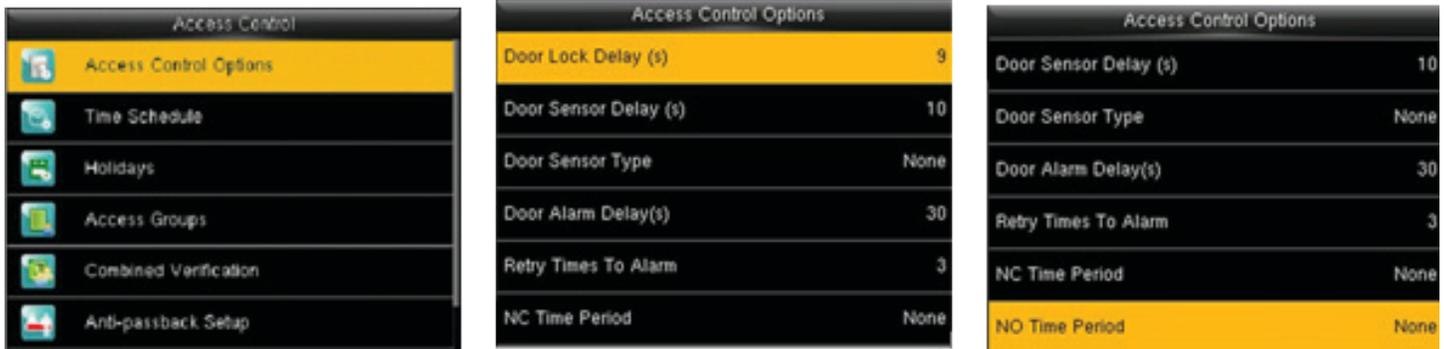
Retraso de alarma de puerta: Cuando un estado anormal del sensor de puerta es detectado, la alarma se emite después de cierto tiempo. El tiempo de la alarma del sensor de puerta. (Valor efectivo: 1-99 segundos)

Reintentar hora de alarma: cuando falle el horario de emisión configure los alcances de horario, salida de señal de alarma. (Valor efectivo: 1-9 veces)

Periodo de tiempo NC: Configure zona de tiempo para control de acceso NC. Nadie puede desbloquear durante esta zona de tiempo.

Periodo de tiempo NO: Configure zona horaria para control de acceso NO. El bloqueo siempre está habilitado durante esta zona horaria.

Operación:



Seleccione opciones de control de acceso y presione OK. Ingrese a opciones de control de acceso como se muestra en la figura.

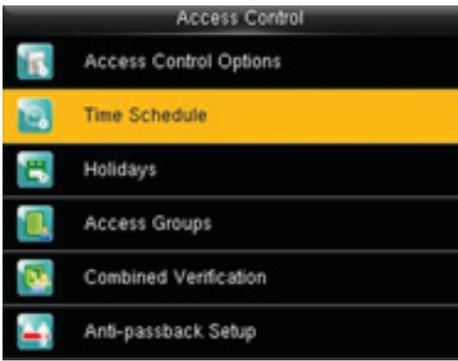
Presione >> para mover el cursor para el elemento que será configurado. Si esta en el cuadro de entrada, presione teclas numéricas en el teclado pequeño para ingresar un valor. Si esta en el cuadro de enrolar, presione >/> para cambiar los valores. Después de configurar, presione el menú directamente para regresar a la última interfaz. Presione "ESC" para cancelar configuración y regrese a la última interfaz.

Noticia

- 1) Cuando la zona horaria está configurada para NO o NC, por favor configure el modo de sensor de puerta como ninguno, o la señal de alarma puede salir durante la zona horaria NO o NC.
- 2) Si la zona horaria de NO o NC no está definida, el dispositivo le pedirá que la defina y agregue una definición en los ajustes de la zona horaria.

9.2 Horario

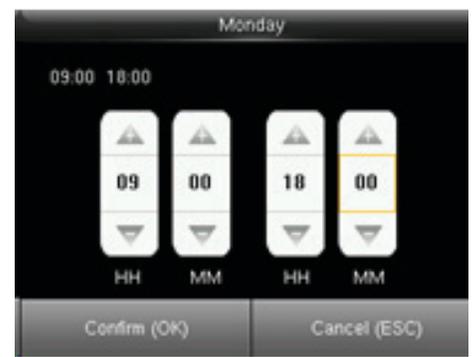
La zona horaria es el mínimo de opción de control de acceso. Todo el sistema puede definir 50 zonas horarias. Cada zona horaria define siete secciones de tiempo (es decir, una semana). Cada sección de tiempo es efectiva sin 24 horas todos los días. Cada usuario puede configurar 3 zonas horarias, o existir entre las tres zonas. Cada formato de sección de hora es HH:MM-HH:MM es decir, minutos precisos.



Presione > para seleccionar horario y presione OK.



Utilice teclas numéricas para un periodo de tiempo en el rango de 1 a 50. Presione > para seleccionar el elemento a configurar y presione OK.



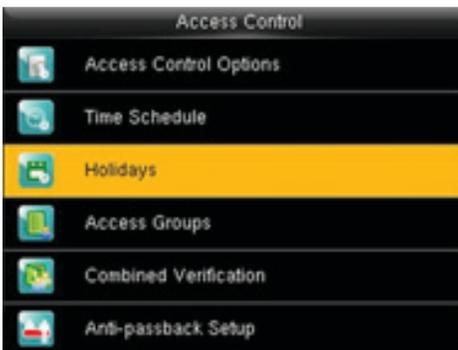
Presione >> para seleccionar una opción de hora y presione >> para configurar la hora. Después configure un periodo de tiempo, presione OK para guardar las configuraciones y salga.

Si la hora final es menor que la hora inicial (23:57-23:56), está prohibido todo el día. Si el horario final es mayor que el horario inicial (00:00- 23:59), es una sección efectiva. Zona horaria efectiva para desbloquear usuario: 00:00-23:59 u hora final mayor que la hora inicial.

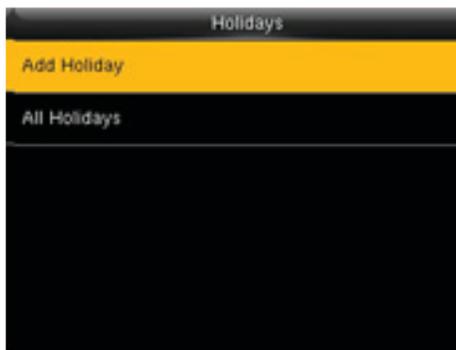
9.3 Configuración de Vacaciones

Se puede necesitar control de acceso especial durante las vacaciones. Es diferente para modificar el horario de control de acceso para todos. Entonces un acceso de control en vacaciones puede ser configurado, el cual es aplicado para todos los empleados.

Después de configurar el horario de control de acceso, los usuarios abrirán la puerta durante las vacaciones asignadas en la zona de tiempo.



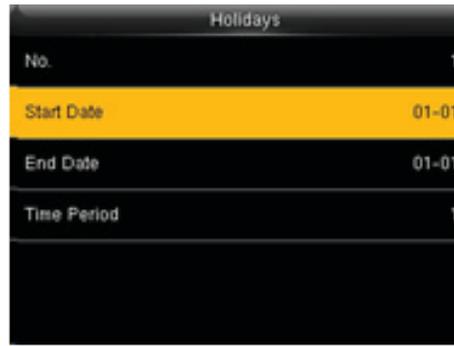
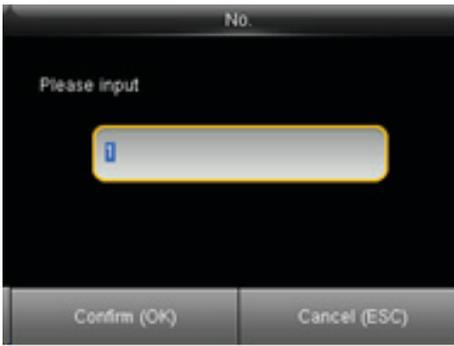
Presione > para seleccionar vacaciones y presione OK



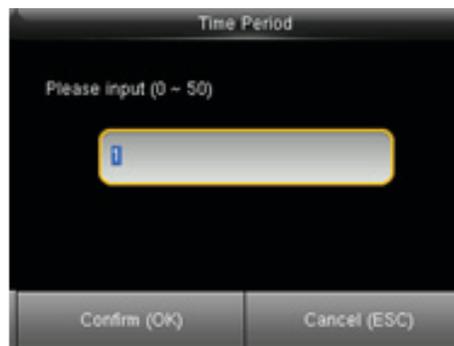
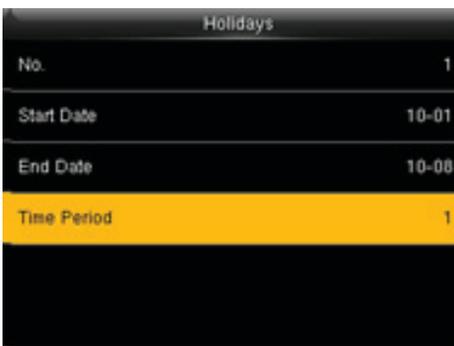
Presione OK para agregar Vacaciones.



Presione OK.



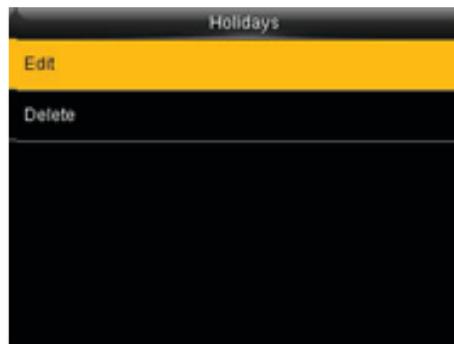
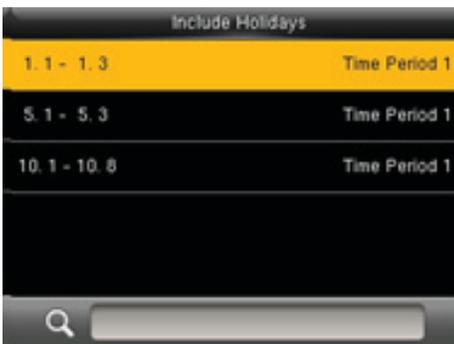
Ingrese el número de usando el teclado, presione OK. Presione > para seleccionar fecha de inicio y fecha final y presione OK. Presione >> para seleccionar una opción de horario y presione >> para configurar horario. Después de ajustar un periodo de tiempo, presión OK para guardar configuración y salga.



Presione > para seleccionar periodo de tiempo y presione OK.

Ingrese el periodo de tiempo usando el teclado, presione OK para regresar.

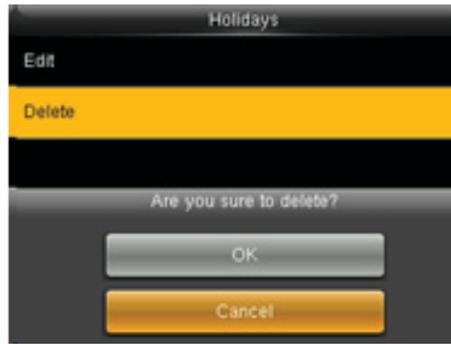
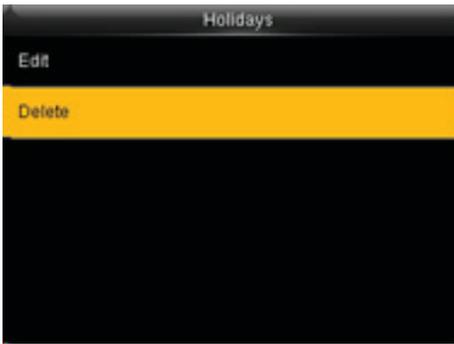
Presione > para seleccionar todas las vacaciones y presione OK.



Para verificar el periodo efectivo de un día festivo, ingrese números y puede ver la duración, presione OK

Presione OK para editar días feriados.

Edite días feriados las operaciones son similares a agregar días feriados.



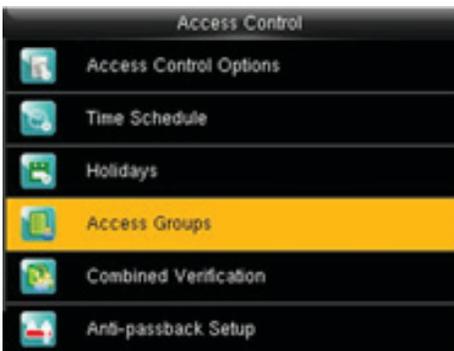
Presione > para seleccionar Eliminar y presione OK.

9.4 Grupos de Acceso

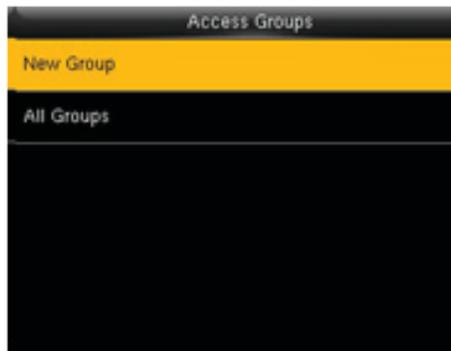
Agrupamiento es para administrar a los usuarios en grupos. El empleado en el grupo usa la zona de tiempo del grupo por default. Los miembros del grupo pueden configurar la zona horaria del usuario. Cada grupo puede contener las zonas horarias. Un nuevo usuario enrolado pertenece al grupo 1 por default. Puede estar localizado en otros grupos.

Operación

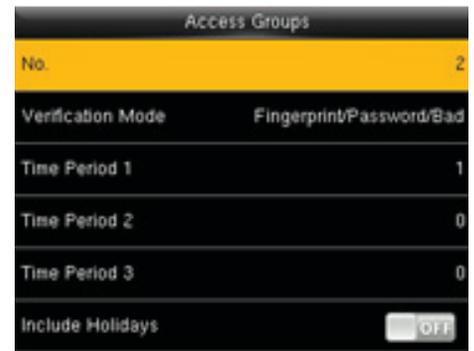
1) Agregar zona horaria de grupo



Presione ▼ para seleccionar Grupos de Acceso y presione



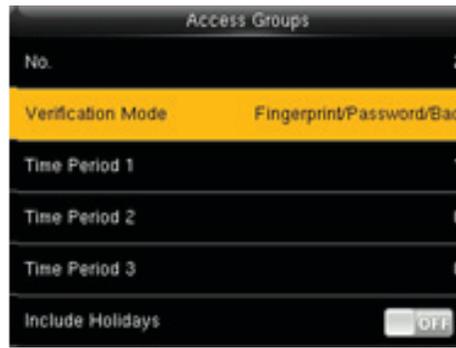
Presione OK para agregar un Nuevo grupo



Presione OK.



Ingrese el número usando el teclado y presione OK.



Presione ▼ para seleccionar modo de verificación y presione OK



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



Presione ▼ para seleccionar periodo de tiempo 1 y presione OK.



Ingrese el número usando el teclado y presione OK.

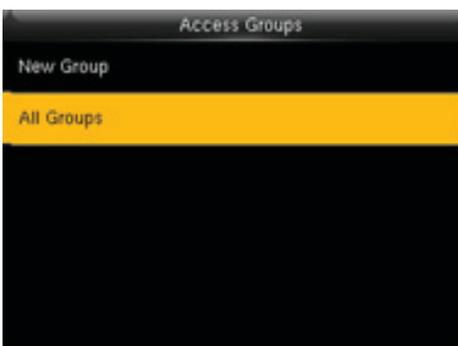


Presione ▼ para seleccionar días festivos incluidos, presione OK para habilitar elemento.

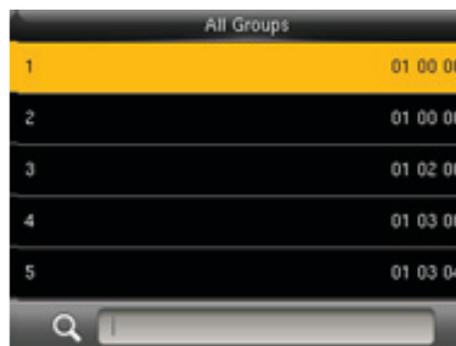
Nota:

1. Si el día feriado es efectivo, solo cuando exista intersección entre la zona de grupo y zona de tiempo de días a feriado el miembro del grupo abre la puerta.
2. Si el día feriado es ineficaz, el horario de control de acceso del miembro del grupo no se verá afectado por días feriados.

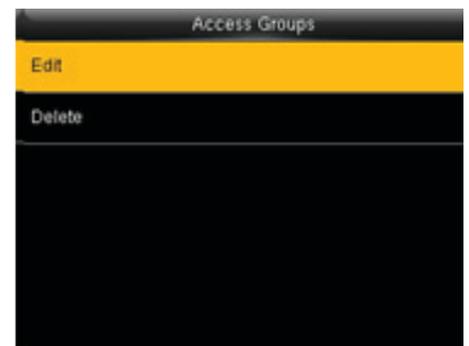
2) Edite y elimine zona horaria de grupo



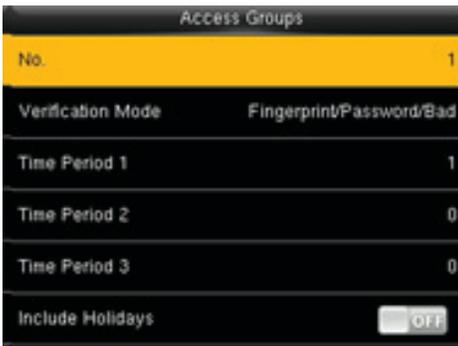
Presione ▼ para seleccionar periodo de tiempo 1 y presione OK.



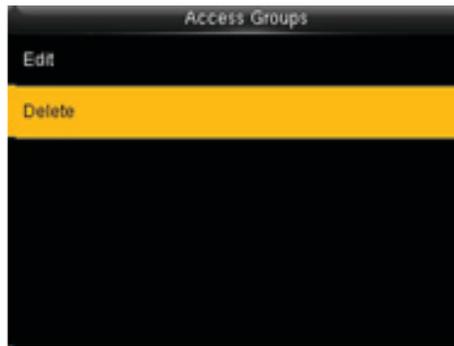
Presione ▼ para seleccionar uno de todos los grupos y presione OK.



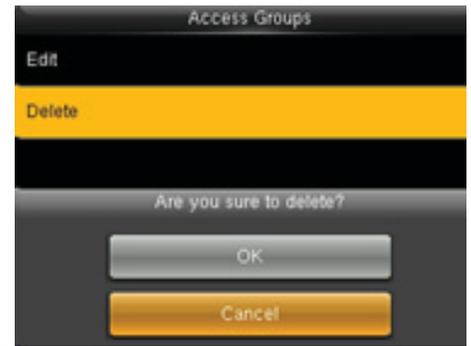
Presione ▼ para seleccionar Editar y presione OK



El número no puede ser modificado, y otras operaciones son similares a agregar nuevos grupos. Presione ESC para regresar.



Presione ▼ para seleccionar Eliminar y presione OK.



Presione ▲/▼ para seleccionar OK y eliminar los grupos de acceso.

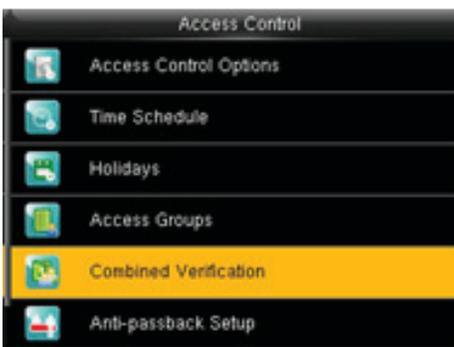
9.5 Multi-verificación

Haga varios grupos de acceso dentro de los diferentes controles de acceso para lograr multi-verificación y mejorar la seguridad. Un control de acceso puede componerse de 5 grupos como máximo.

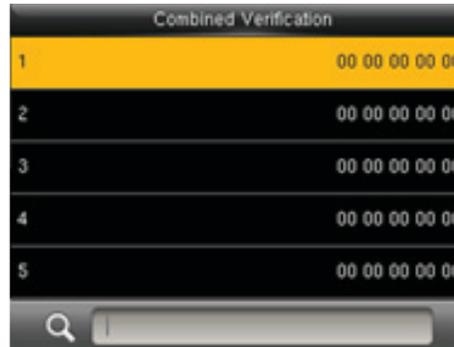
Operación

1) Agregar Verificación combinada

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



Presione ▼ para seleccionar verificación combinada y presione OK.



Presione OK para agregar una nueva verificación combinada.



Ingrese el Numero usando el teclado y presione OK.

2) Eliminar y Editar verificación combinada



Presione > para seleccionar la línea para editar, presione OK. Ingrese el número usando el teclado y presione OK. Cuando la configuración sea exitosa, una interfaz como la de arriba se mostrará

Nota:

Para eliminar una combinación de desbloqueo, configure el ID de grupo a 0s.

9.6 Anti-passback

Algunas veces, personas ilegales siguen al empleado dentro de la puerta, quienes pueden causar problemas de seguridad, para prevenir este riesgo, la función es habilitada. El registro de entrada debe ser comparado con el de salida, o la puerta no se abrirá. Esta función necesita dos máquinas para trabajar juntas. Referirse al Apéndice 4 anti-passback (para configuraciones de anti-passback).

9.7 Parámetro de Alarma de Amago

Existe un parámetro de coacción de alarma configurada en el dispositivo. Cuando el empleado cruza, seleccione modo de alarma de coacción, el dispositivo abrirá la puerta. Pero la señal de alarma será enviada.

Función de coacción: Si seleccione "Si", presione ayuda después presione la huella en los próximos 3 segundos o presione el número de ID y la alarma de coacción saldrá después de la verificación exitosa. Si selecciona "NO" no funcionara para ayuda. (Ayuda puede configurarse en definición del teclado)

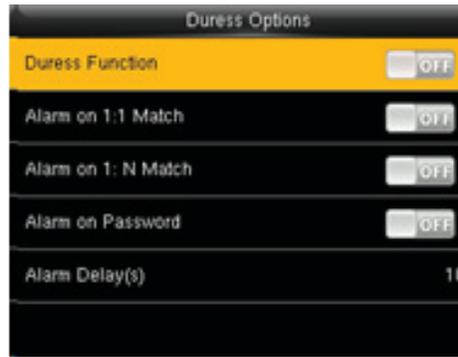
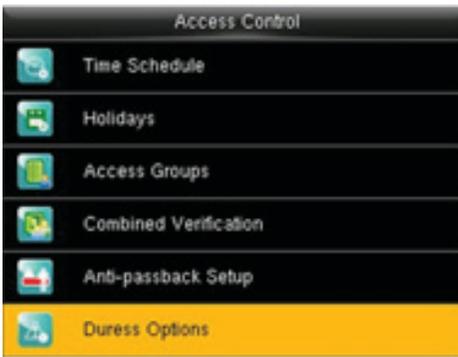
Alarma en verificación 1:1: Si selecciona "Si", cuando el usuario utiliza modo de verificación 1:1 la señal de alarma saldrá. O no existe señal de alarma.

Alarma en verificación 1:N: Si selecciona "Si", cuando el usuario utilice modo de verificación 1:N, la señal de alarma saldrá. O no existe señal de alarma.

Alarma en contraseña: Si selecciona "Si", cuando el usuario utilice modo de verificación por contraseña, la señal de alarma saldrá. O no existe señal de alarma.

Retraso de alarma: Después de que inicie la alarma de coacción, la señal de alarma no tiene salida directa. Pero puede ser definida. Después de algún tiempo, la señal de alarma se generara automáticamente.

Operación:



Presione ▼ para seleccionar Opciones de coacción y presione OK.

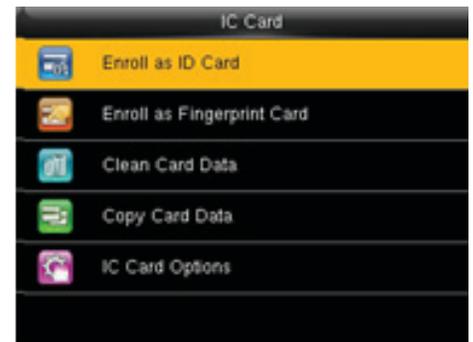
Ingrese a Opciones de control de acceso como se muestra en la figura:

Presione >> para mover el cursor al elemento a configurar. Si está en el cuadro de entrada, presione teclas numéricas en el teclado para ingresar el valor. Si está el cuadro de enrolamiento presione >> para cambiar los valores. Después de la configuración, presione menú para regresar directamente a la última interfaz. Presione ESC para cancelar ajustes y regrese a la interfaz inicial.

10. Administración de Tarjeta IC

Soporta Mifare con frecuencia de 13.56MHZ. Integración de huella de asistencia para otros sistemas y soporta modo multi-verificación para satisfacer las demandas de personas diferentes.

Operación:



Presione M/OK en la interfaz inicial.

Presione ► para seleccionar usuario, presione OK.

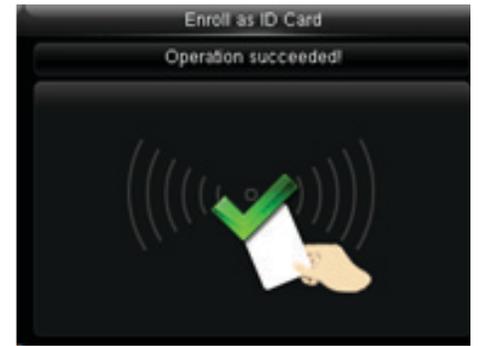
Seleccione Enrolamiento por tarjeta y presione OK.

10.1 Enrolar Tarjeta ID

Utilice tarjeta Mifare como tarjeta ID. Solo se necesita enrolar el número de la tarjeta.

Operación:

1. Enrolamiento

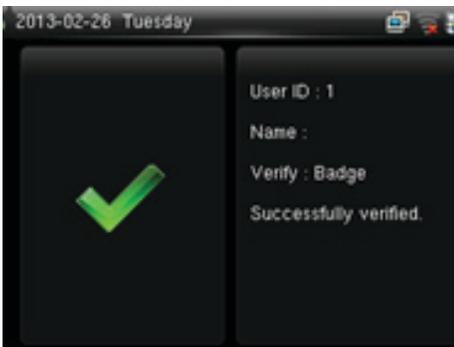


Ingrese el ID de usuario utilizando el teclado después presione OK. Deslice su tarjeta ID apropiadamente en el área designada. Operación exitosa

Observaciones: si el numero ya existe en el dispositivo, se mostrara un mensaje preguntándole si desea replicar la información en la tarjeta.

2. Verificación

Deslice la tarjeta ID apropiadamente en el área correspondiente. Cuando la verificación sea exitosa, el dispositivo lo mostrara de inmediato.



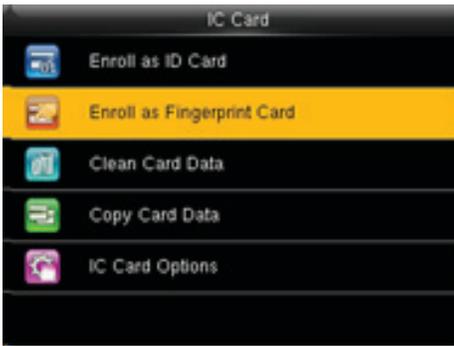
Por favor ingrese a las opciones de control de acceso del usuario para modificar el modo de verificación como RF, o la verificación no será exitosa.

10.2 Enrolar Tarjeta de Huella Digital

Enrolar huella y escribir plantilla de huella en la tarjeta.

Operación:

1. Enrolar



Presione ▼ para seleccionar enrolar como tarjeta de huella y Presione OK.



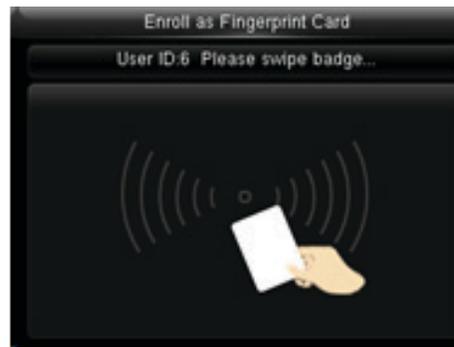
Ingrese el ID de usuario utilizando el teclado y presione OK.



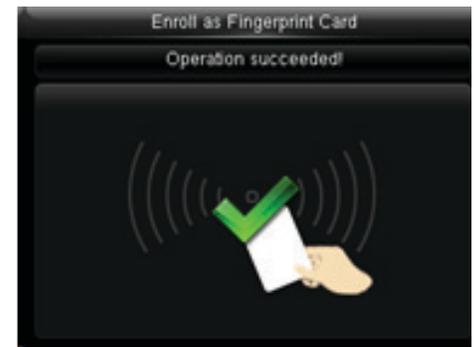
Presione ▼ para seleccionar un dedo y presione OK.



Coloque el mismo dedo en el colector de huellas por tres ocasiones consecutivamente. Para detalles, ver 1.1 Colocación de dedo.

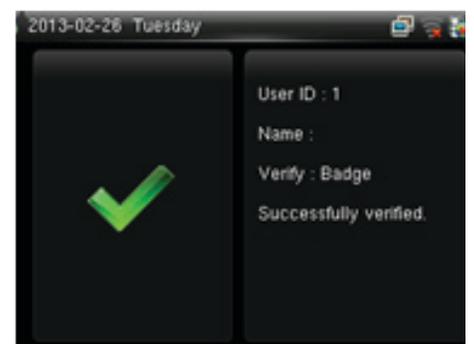
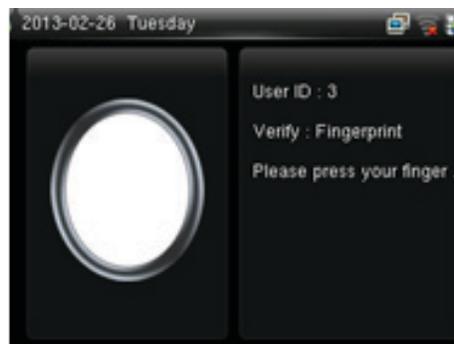
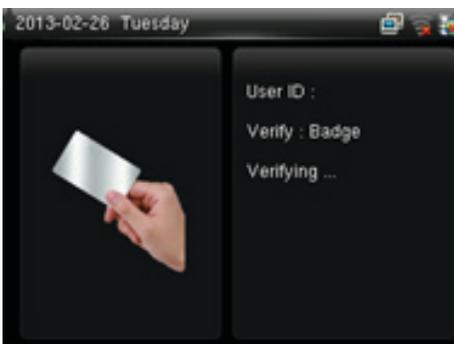


Enrolar exitosamente. Deslice la tarjeta ID apropiadamente en el área correspondiente.



Operación exitosa.

2. Verificación



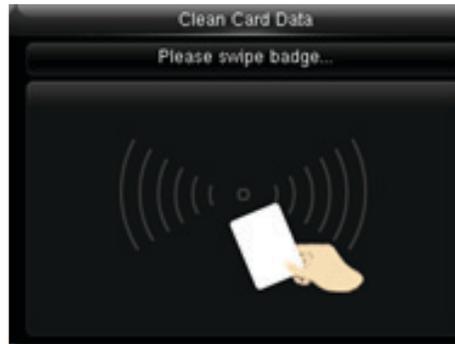
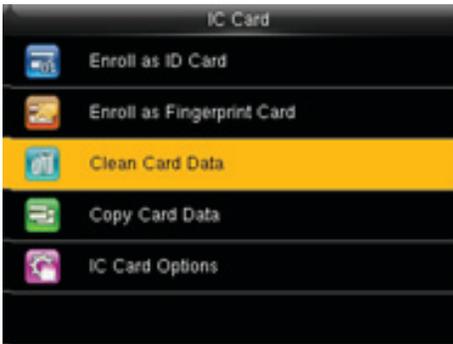
Deslice su tarjeta ID apropiadamente en el área correspondiente. Operación Exitosa!. "Por favor coloque su dedo". Coloque su dedo en el sensor de huellas apropiadamente. Verificación exitosa. Como se muestra en la figura.

Nota:

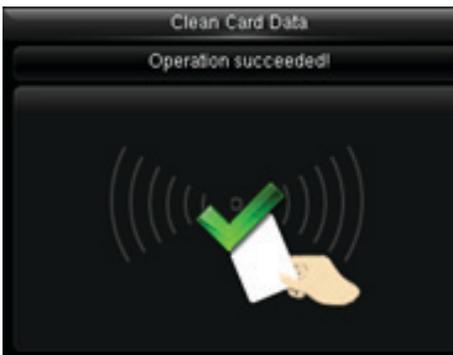
Si la huella colocada es diferente a la almacenada en la tarjeta, la verificación será fallida.

10.3 Limpiar Información de Tarjeta

Elimine toda la información en la tarjeta operada en la actualidad.
Operación:



Presione > para seleccionar Limpiar Datos de Tarjeta y presione OK. Deslice su tarjeta ID apropiadamente en la area correspondiente. Eliminar.

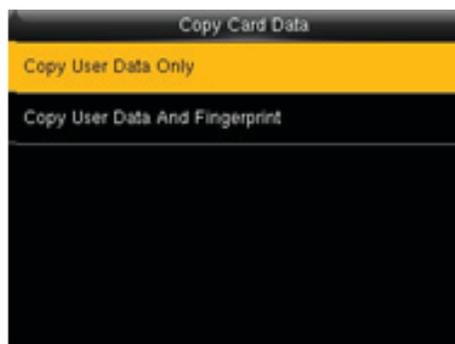
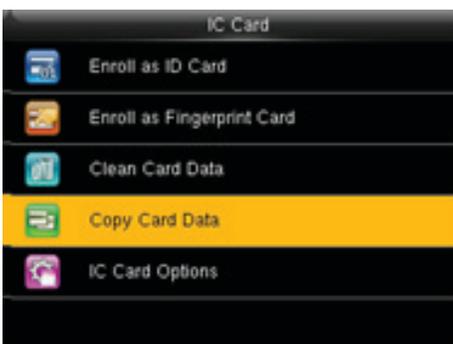


Ponga la tarjeta en el área de inducción, espere a que el dispositivo elimine toda la información en la tarjeta. Si los datos de la tarjeta están almacenados en el dispositivo, el dispositivo le avisará si desea eliminar la información contenida en el dispositivo o no. "Si" es para eliminar la huella e información del usuario en el dispositivo. "NO" es para mantener la información.

10.4 Copiar Información de Tarjeta

Copiar información de tarjeta al dispositivo (después de copiar, la huella se encuentra en la tarjeta), después coloque su huella directamente en el dispositivo, no necesitará utilizar tarjeta Mifare.

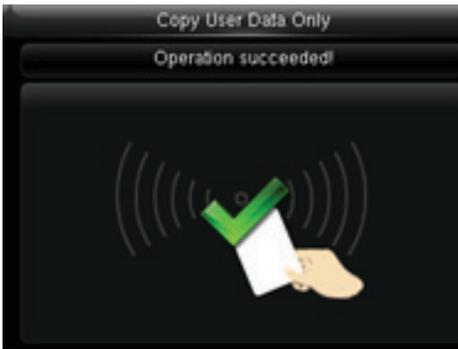
Operación



Presione ▼ para seleccionar copiar datos de tarjeta y presione OK.

Seleccione copiar datos de usuario y presione OK.

Deslice la tarjeta ID apropiadamente en el área correspondiente.



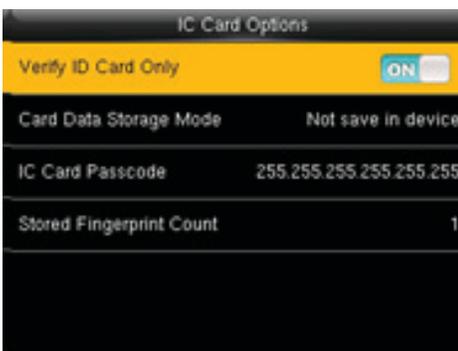
Operación exitosa

Copiar datos de usuario y huella:

Presione > para seleccionar Copiar datos de usuario y huella las operaciones son similares a las realizadas para Copiar Datos de Tarjeta

10.5 Configuración de Parámetros de Tarjeta

Configure contraseña de tarjeta Mifare y decida si la información se debe guardar o no.



Verificar tarjeta ID: si este parámetro es configurado a "Si", su verificación pasa solo después de la verificación de la tarjeta. Si este parámetro es configurado a "NO", tendrá que verificar la contraseña o huella después de la verificación de la tarjeta.

Modo de almacenaje de datos en tarjeta: Decida guarda la información enrolada al dispositivo cuando enrole la tarjeta o huella de tarjeta. Si selecciona "No guardar", la información del usuario solo se guarda en la tarjeta. Si selecciona "Solo usuario", el ID del empleado y el número de tarjeta son guardados en el dispositivo. Si selecciona "Usuario+huella", el ID del empleado, número de tarjeta, y huella son guardados en el dispositivo. En los dos últimos modos los datos se guardan en la tarjeta y el dispositivo.

Código de acceso Tarjeta IC: después de que se establece la contraseña, el dispositivo escribirá la contraseña dentro de la tarjeta de huella enrolada. Después la tarjeta de huella puede ser utilizada solo en el dispositivo.

Numero de Huellas Almacenadas: utilizado para configurar el número de huellas guardadas en una tarjeta. Se pueden guardar hasta 10 huellas.

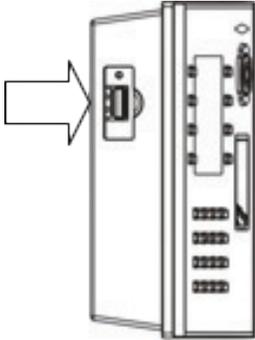
Nota:

Cuando la maquina se utiliza como función de control de acceso de alto nivel, la información del usuario debes ser guardada en el dispositivo para propósitos de autenticación. Para detalles, ver 9 Ajustes de Control de Acceso.

11. Administración de USB

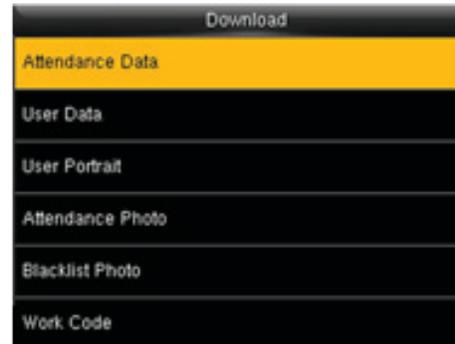
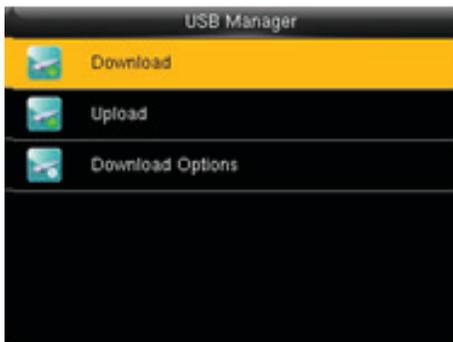
Importar información de usuario, plantilla de huella, datos de asistencia, etc. en el dispositivo al software de asistencia o importar la información del usuario y huella a otros dispositivos mediante USB.

Antes de cargar /descargar datos de una USB, inserte la USB en el dispositivo.



Inserte la USB en el espacio del sensor de huella mediante un cable mini USB. Presione M/OK en la interfaz inicial. Presione > para seleccionar administración de USB y presione OK.

11.1 Descarga



Seleccione descarga y presione OK

Presione ▼ y OK para seleccionar el elemento para descarga.

Descarga datos de asistencia: importe todos los datos de asistencia de la terminal FFR a una USB.

Descarga datos de usuario: importar toda la información del usuario, huella e imágenes faciales de la terminal FFR a una USB.

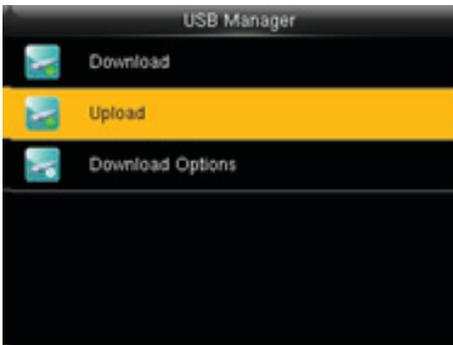
Descarga de foto del usuario: importe las fotos de los empleados de la terminal a la USB.

Descarga de foto de asistencia: descargue fotos de asistencia guardadas en el dispositivo a una USB. El formato de la foto es JPG.

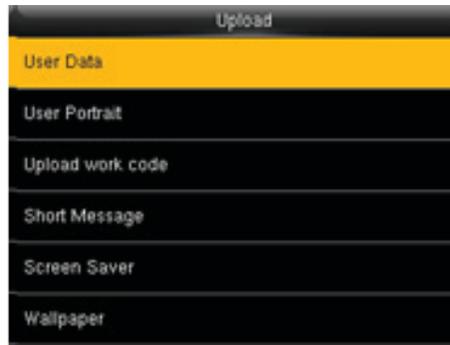
Descarga de fotos de lista negra: Descargue fotos de lista negra guardadas en el dispositivo a la USB.

Descarga código de trabajo: Utilizado para guardar IDs en el dispositivo a una USB.

11.2 Carga



Presione ▼ para seleccionar descarga y presione OK.



Presione ▼ y OK para seleccionar el elemento para ser cargado.

Carga de datos de usuario: Cargue el mensaje almacenado en una USB a la terminal.

Carga de foto del usuario: Cargue los documentos en JPG que son nombrados después de almacenar el ID de usuario en una USB a la terminal, las fotos de serán mostradas después de la verificación del empleado.

Cargar el código de trabajo: utilizado para cargar IDs de trabajo en una USB al dispositivo.

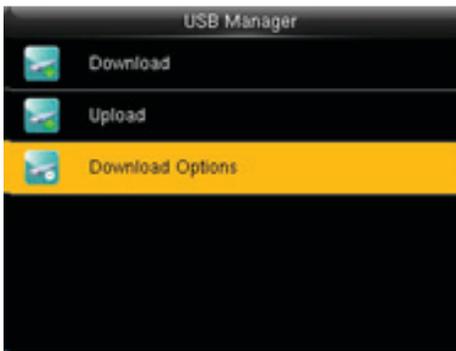
Cargar mensaje corto: utilizado para cargar mensaje corto en una USB al dispositivo.

Cargar fondo de pantalla: cargue los documentos JPG con "ad_" como letras iniciales del nombre del documento almacenado en una USB a la terminal. Después de cargar, estas imágenes pueden ser mostradas en la interfaz inicial de la terminal. (Para detalles de especificaciones de imagen, vea Apéndice 2 Reglas de Carga de Imágenes.

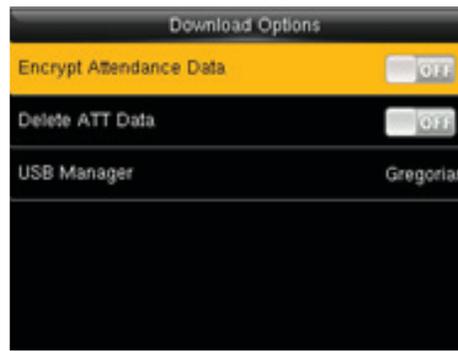
Carga de wallpaper: cargue los documentos JPG con "1-10.jpg" como letras iniciales del documento almacenado en una USB a la terminal. Después de cargarlos, estas imágenes pueden ser mostradas en la interfaz inicial de la terminal. (Para detalles de las especificaciones de imagen, vea Apéndice 2 Reglas de Carga de Imágenes.

11.3 Opciones de Descarga

Puede encriptar los datos en una USB y configure para eliminar los datos después de iniciar la descarga. Cuando descargue los registros de asistencia, puede configurar el tipo de calendario mostrado en el horario de asistencia. El dispositivo soporta tres tipo de calendarios puede ser Gregoriano, Irán gregoriano, Irán lunar.



Presione ▼ para seleccionar opciones de descarga y presione OK.



Presione ▼ y OK para seleccionar elementos. Cuando los ajustes estén completos, presione OK para guardar la configuración y salga.

12. Búsqueda de Asistencia

Los registros de asistencia serán guardados en el dispositivo. Para consulta conveniente, la función de consulta de registro está incluida.

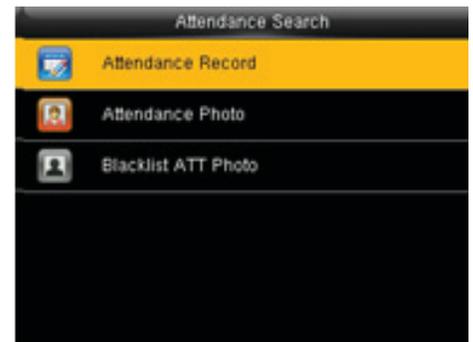
1. Registro de asistencia.



Presione M/OK en la interfaz inicial.



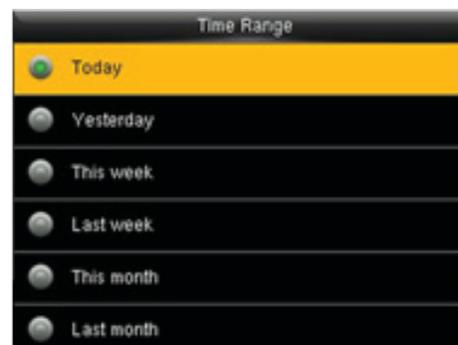
Presione > para seleccionar Búsqueda de Asistencia y presione OK.



Presione > para seleccionar registros de asistencia y presione OK.



Ingrese el ID de usuario y presione OK



Presione > para seleccionar Hora y presione OK.



Los registros se muestran acorde con las condiciones:

Id de usuario: Ingrese el ID de usuario del empleado para consulta. Si el campo se deja en blanco, puede consultar los registros de asistencia de todos los empleados. Si ingresa un usuario ID, puede consultar el registro de asistencia de todos los empleados. Si ingresa un ID de usuario, puede consultar el registro de asistencia del empleado con el ID de usuario.

Rango de hora: seleccione periodo de hora para consulta, incluyendo el periodo de hora personalizado, ayer, esta semana, la semana pasada, este mes, el último mes y todos los periodos de tiempo.

2. Foto de asistencia y foto de lista negra ATT.

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

13. Impresión

Puede conectar el dispositivo a una impresora, los registros de asistencia pueden ser impresos.



Presione M/OK en la interfaz inicial.

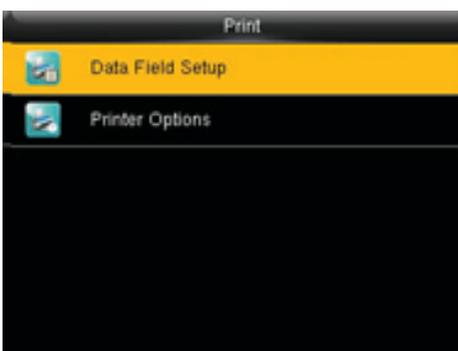


Presione > para seleccionar impresora, presione OK.

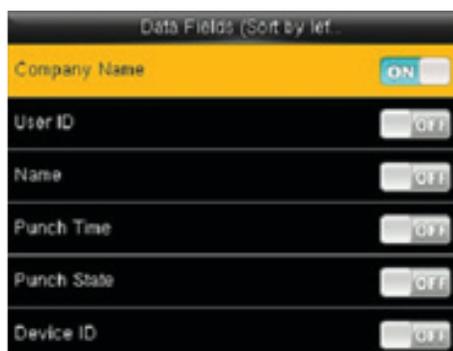


Presione > para seleccionar configuración del campo de datos y presione OK.

13.1 Configuración de Datos



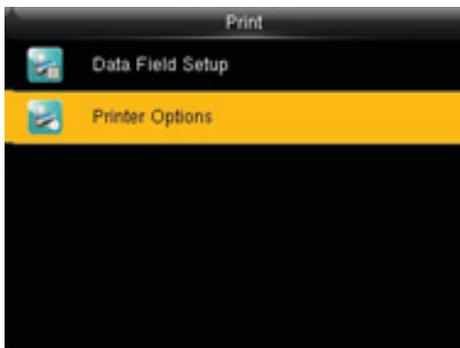
Presione > para seleccionar configuración de datos y presione OK.



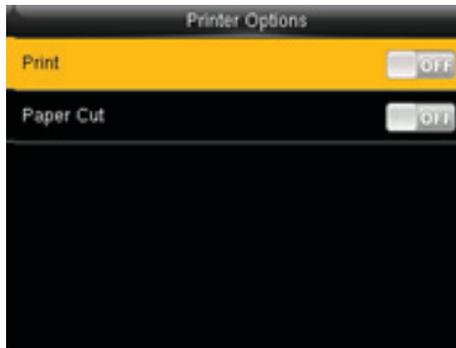
Presione > para seleccionar elemento para ser configurado y presione OK para habilitar o deshabilitar el elemento seleccionado.



13.2 Opciones de Impresión



Presione > para seleccionar Opciones de Impresión y presione OK



Presione > para seleccionar el elemento a configurar y presione OK para habilitar o deshabilitar el elemento

Nota:

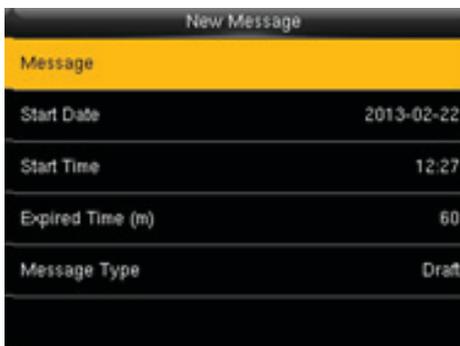
Para habilitar la función de corte de papel, conecte el dispositivo equipado con la función de impresión. Corte de papel es implementado automáticamente durante la impresión basada en la selección de información de impresión.

14. Mensaje Corto

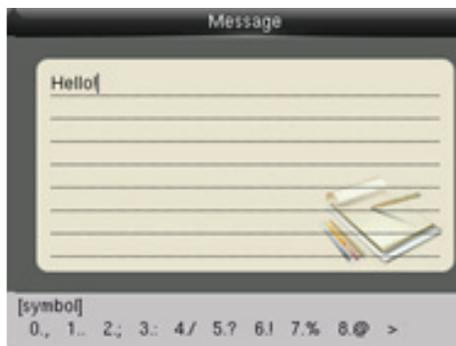
SMS es similar a una noticia. El operador puede editar el contenido de la noticia en avanzado y realizar la visualización del SMS en la pantalla. SMS incluye SMS común y SMS individual, si se configura un SMS COMUN, el mensaje se mostrara en una columna de información en la parte superior de espera especificado en el horario. Si un SMS individual es configurado, el empleado quien recibirá el SMS puede ver el mensaje después de la verificación exitosa de asistencia.

14.1 Mensaje Corto

1. Ingrese el mensaje en teclado



Seleccione Mensaje y presione OK.

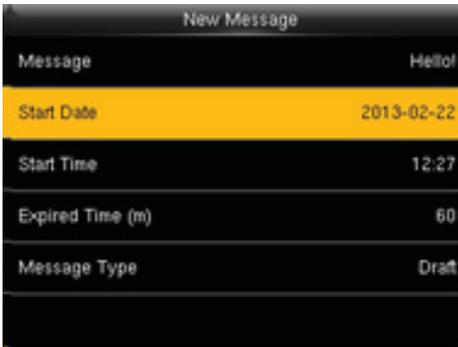


Presione * para cambiar el método de entrada e ingrese el mensaje, después presione OK.

Para detalles de ingresar nombre, ver Apéndice

1 Descripción de Texto Operación de entrada.

2. Configure el horario cuando el SMS entre en vigor.



Seleccione inicio de Fecha

Ingrese la fecha o presione ▲/▼ para seleccionarla fecha después presione OK.

3. Configure horario de expiración (m) SMS aparece en el horario efectivo. Después el horario efectivo, no aparecerá.

Nota:

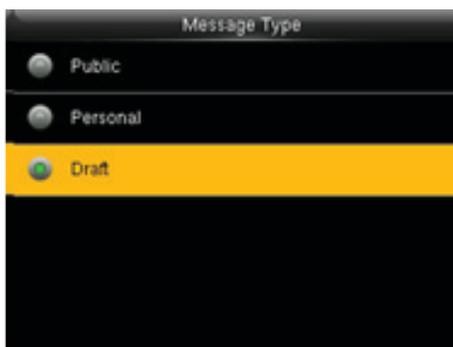
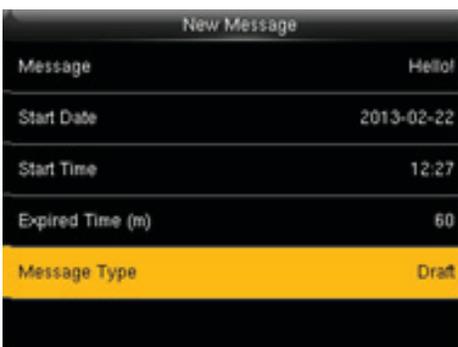
Para mensajes públicos, el periodo efectivo es también el periodo de visualización. Para mensajes privados, necesita configurar el periodo de visualización después configure un horario efectivo. El periodo de visualización de un mensaje privado puede ser visto cuando dentro y afuera durante el periodo efectivo del mensaje.

4. Configure tipo de mensaje:

Publico: SMS capaz de ser visto por todos los usuarios.

Personal: SMS dirigida a un solo individuo.

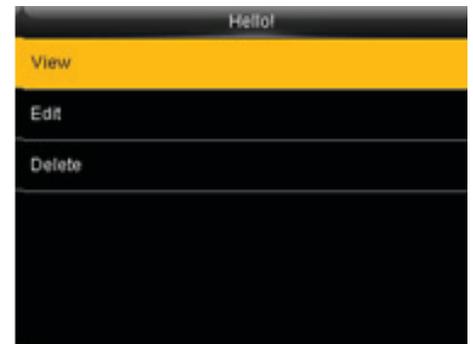
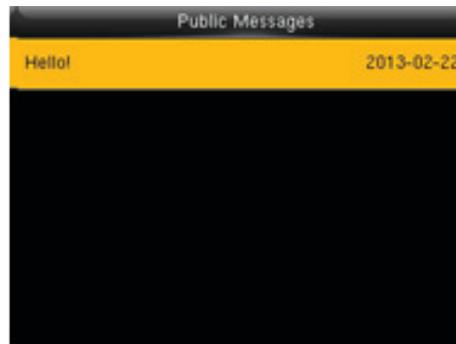
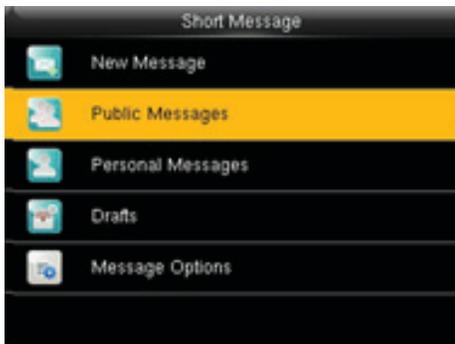
Borrador: Presione SMS, no hay diferencia de SMS individual o SMS común.



Seleccione Tipo de mensaje y presione OK.

Presione ▲/▼ para seleccionar el tipo de mensaje después presione OK.

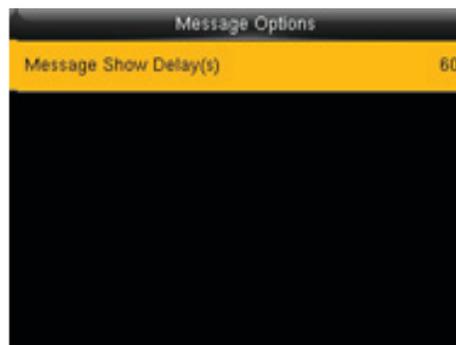
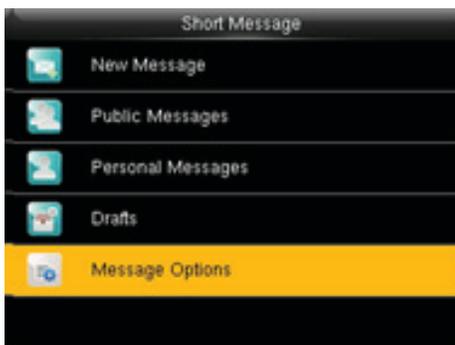
14.2 Lista de Mensajes Pública y Personal



Presione > para seleccionar la lista de mensaje después presione OK. Puede ver, editar o eliminar el que ha seleccionado. Cuando edita el mensaje, las operaciones son similares a las realizadas a agregar un SMS.

14.3 Opciones de Mensaje

Configure el mensaje personal de retardo de muestra en la interfaz inicial.



Presione > para seleccionar
Presione OK.Opciones de mensaje y
presione OK.

Presione OK.

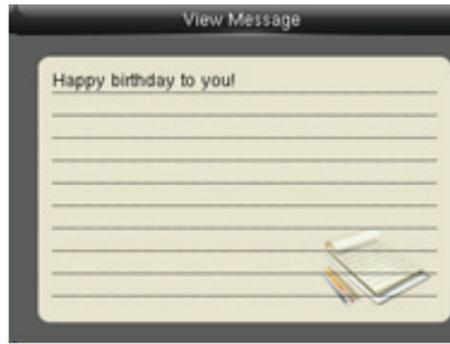
Presione >para seleccionar el hora-
rio y presione OK.

14.4 Verificación de SMS del Empleado

Después de la configuración de un mensaje corto, sin especificar el periodo de tiempo, la interfaz principal mostrara el icono de mensaje en la esquina superior derecha y muestra el contenido del mensaje público en el modo de desplazamiento en la parte inferior entonces el empleado podrá ver la información. El contenido del mensaje privado para un usuario muestra cuando el usuario es autenticado.



Mensaje Publico



La autenticación del usuario es exitosa después visualizará sus mensajes.

15. Código de Trabajo

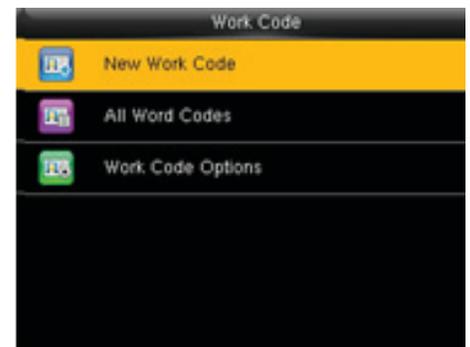
El salario de los empleados está en el registro de asistencia. Los empleados pueden estar en diferentes tipos de trabajo que pueden contener variaciones con horarios de tiempo. Considerando el salario y variaciones con otros tipos de trabajo, la terminal FFR ofrece un parámetro para indicar el tipo de trabajo correspondiente para cada registro de asistencia para facilitar y entender diferentes situaciones de asistencia durante los datos de asistencia.



Presione M/OK en la interfaz inicial



Presione > para seleccionar código de trabajo y presione OK.



Presione ▼ para seleccionar nuevo código de trabajo y presione OK.

15.1 Agregar un Código de Trabajo

ID: Un código digital del código de trabajo. Nombre: El significado del código de trabajo.

1. Ingrese el ID.



Seleccione ID y presione OK.



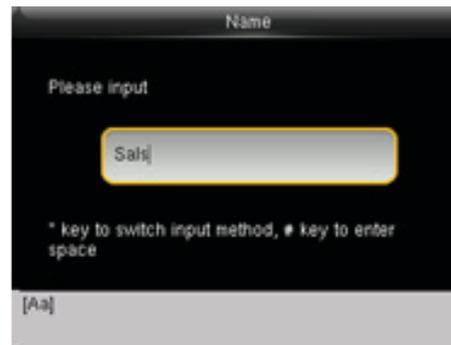
Ingrese el ID de usuario utilizando el teclado, presione OK.

Tip: La terminal soporta de 1 a 99999999 dígitos de ID por default. Si un mensaje rápido "El ID del empleado existe" se muestra, ingrese otro ID.

2 Ingrese el nombre



Seleccione Nombre y presione OK.

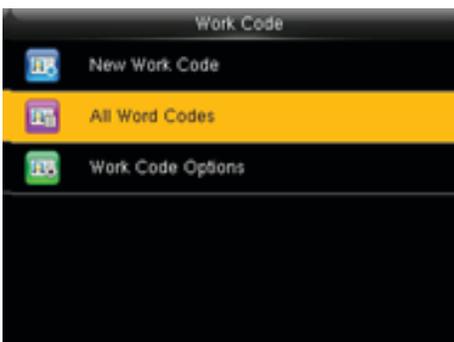


Ingrese el Nombre después presione OK.

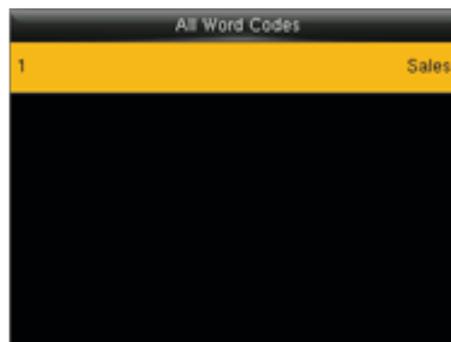
La terminal soporta de 1 a 23 caracteres por default. Para detalles de ingresar nombre, ver Apéndice 1 Instrucciones de entrada de texto.

15.2 Todos los Códigos de Trabajo

Puede ver, editar o eliminar la lista de código de trabajo. El ID no puede ser modificado y otras operaciones son similares a las realizadas en un código de trabajo. Cuando edite.



Presione > para seleccionar todos los códigos de trabajo y presione OK.



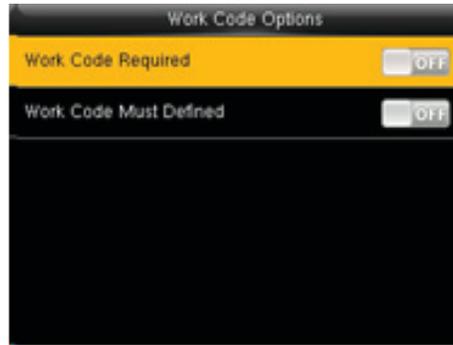
Ver todos los códigos de trabajo.



Presione > para seleccionar el que usted quiera editar o eliminar.

15.3 Configuración del Código de Trabajo

Configure verificación para ingresar el código de trabajo.



Presione > para seleccionar Opciones de Código de Trabajo y presione OK

Presione OK para abrir o cerrar

16. Prueba Automática

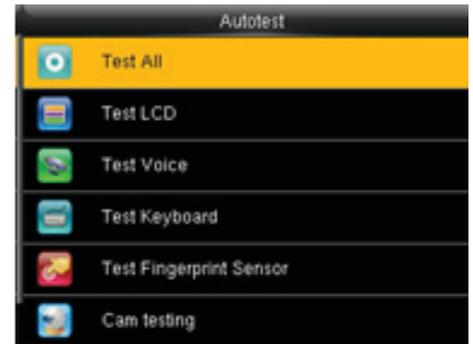
La prueba automática permite realizar una prueba del sistema para ver si las funciones de varios módulos son normales, incluyendo LCD, voz, sensor, teclado y pruebas de reloj.



Presione M/OK en la interfaz inicial.



Presione > para seleccionar el diagnóstico y presione OK.



Presione > para seleccionar el que desea visualizar y presione OK.

Prueba de todo: La terminal automáticamente realiza la prueba de LCD, voz, teclado y voz, presione (ok) para continuar y presione (ESC) para salir.

Prueba LCD: La terminal automáticamente realiza la prueba para el efecto de color de la pantalla TFT mostrando todo el color, puro blanco y puro negro comprueban si aparece la pantalla correctamente. Puede continuar la prueba tocando la pantalla o saliendo y presionando (ESC).

Prueba de voz: la terminal automáticamente prueba si los archivos de voz están completos, si la calidad de voz es buena reproduciendo los archivos almacenados en la terminal. Puede continuar la prueba tocando la pantalla o saliendo y presionando (ESC).

Prueba de teclado: La terminal realiza la prueba para identificar que cada tecla esté funcionando normalmente. Presione cualquier tecla en la (Interfaz de prueba de teclado) para verificar la tecla presionada coincide con lo que aparece en la pantalla. Las teclas son grises antes de pulsarlas y regresan a azul después de presionarlas. Presione (ESC) para salir de la prueba.

Prueba del sensor de huella: La terminal realiza automáticamente la prueba si el colector de huellas funciona apropiadamente la verificación de huellas son claras y aceptables. Cuando el usuario coloque su dedo en la guía de dedos, el colector de huellas es mostrado en la pantalla en tiempo real. Presione (ESC) para salir de la prueba.

Prueba de cámara: el dispositivo realiza automáticamente la prueba de la cámara si funciona correctamente verificando si colecta imágenes claras y aceptables. Presione (ESC) para salir de la prueba.

Prueba de reloj RTC: la terminal realiza la prueba si el reloj funciona apropiadamente verificando el cronógrafo del reloj. Toque la pantalla para iniciar y continuar, toque de nuevo para detener la verificación y si el recuento es exacto. Presione (ESC) para salir de la prueba

17. Información del Sistema

Puede verificar el estatus de almacenamiento así como la información del firmware de la terminal mediante la opción (Información del sistema).



Presione M/OK en la interfaz inicial.



Presione > para seleccionar información del sistema y presione OK.



Presione ▼ para seleccionar el que desee ver y presione OK.

Capacidad del dispositivo: El número de usuarios enrolados, administradores, contraseñas, el total de huellas almacenadas y capacidad de ocupación. . Tarjetas ID y capacidad de asistencia son mostrados respectivamente.

Información del dispositivo: nombre del dispositivo, número de serie, dirección MAC, algoritmo de huella fecha de fabricación son mostrados en la interfaz del si la interfaz del dispositivo.

Información de Firmware: La versión firmware, Bio servicio, servicio Push, servicio standalone y servicio Dev. Son mostrados en la interfaz de información de firmware.

Device Capacity	
User (used/max)	1/10000
Admin User	0
Password	0
Fingerprint (used/max)	2/8000
Badge (used/max)	0/10000
ATT Record (used/max)	7/300000

Capacidad del Dispositivo

Device Info	
Device Name	New-Archi
Serial Number	201301301745
MAC Address	00:17:61:7f:26:ca
Fingerprint Algorithm	ZKFinger VX10.0
Manufacturer	ZKTeco Inc.
Manufacture Date	

Información del dispositivo

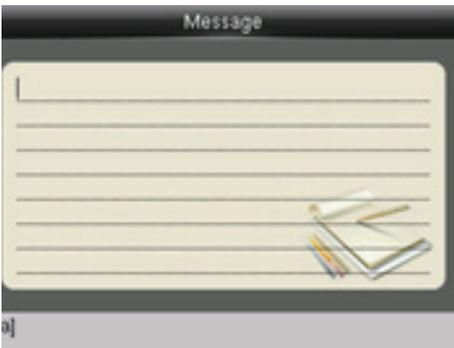
Firmware Info	
Firmware Version	Ver 7.0.2.100-20130218
Bio Service	Ver 1.2.100-20130218
Push Service	Ver 1.0.0-20130218
Standalone Service	Ver 1.0.0-20130218
Dev Service	Ver 1.0.100-20130218

Información del firmware

Apéndice

Apéndice 1 Descripción de la operación de entrada de texto

El dispositivo puede reconocer palabras en inglés, símbolos y números. Presione * para mostrar el método de entrada y presione * nuevamente para cambiar el método de entrada. Presione # para ingresar un espacio. Presione ESC para salir del método de entrada.



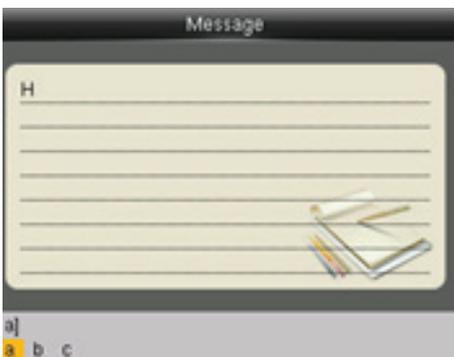
Presione * para mostrar el método de entrada.



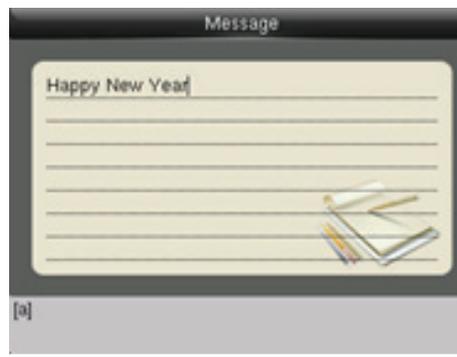
Presione * nuevamente para cambiar el método de entrada. Seleccione Aa, a, o A para utilizar mayúsculas y minúsculas basados en sus requerimientos.



Si es necesario, puede presionar 4 dos veces en sucesión para seleccionar H.



Presione 2 para seleccionar uno. Finalice la entrada del texto en el mismo lugar.



Presione # para ingresar un espacio si es necesario.



Presione * para cambiar el simbolo de entrada y presione 6. Cuando sea completada la entrada, presione ESC para salir.

Apéndice 2 Reglas para Subir Imágenes

Foto de usuario: Crear un nuevo directorio llamado "Fotografía" directamente en la raíz de la USB y coloque las fotos de usuarios en el directorio. Un máximo de 8,000 fotos pueden ser almacenadas, el tamaño de cada foto no puede exceder 15KB. El nombre de la imagen es X.jpg (X es el ID de usuario, el cual no tiene límites en el número de dígitos). Las imágenes deben estar en formato .jpg.

Imagen publicada: Crear un nuevo directorio llamado "Anunciado" en la raíz de la USB y coloque las imágenes dentro del directorio. Un máximo de 20 imágenes pueden ser almacenadas y el tamaño de cada imagen no puede exceder 30KB. No existen restricciones en el nombre de la imagen y tipo.

Wallpaper: Crear un Nuevo directorio llamado "Wallpaper" en la raíz de la USB y coloque los wallpapers en el directorio. Un máximo de 20 wallpapers puede ser almacenados el tamaño de cada wallpaper no puede exceder 30KB. No existen restricciones en el nombre de la imagen.

Nota:

Si el tamaño de la foto de un usuario o foto de asistencia es 10KB o menos, un total de 10,000 fotografías pueden ser almacenadas.

Apéndice 3 Función de Impresión

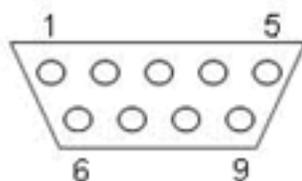
• Impresora externa

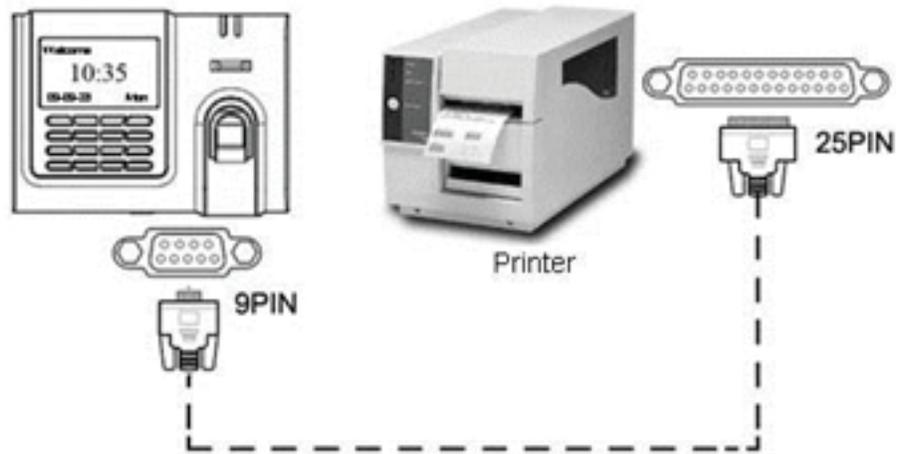
Explicación

Esta función está diseñada para un puerto serial únicamente, para impresoras paralelas no está disponible. La salida de la impresora es vía RS232. Después un usuario es verificado, el resultado será enviar mediante el puerto serial. Si el dispositivo conectado con la impresora el resultado puede imprimirse directamente, puede utilizar la Super Terminal para ver el contenido.

Dispositivo conectado con la impresora	Dispositivo		Impresora
	2TXD	<----->	3 RXD
	3 RXD	<----->	3 RXD
	5GND	<----->	7 FG

Ordenador Pin-line
RS232





Instrucciones

1. En el menú del dispositivo, presione Menú> Comunicación> RS232/485 y seleccione velocidad de transmisión como 19200.
2. En el menú del dispositivo, entre a Menú>Comunicación>Seguridad y seleccione el modo de impresión . existen 7 modos de impresión para seleccionar.

Nota:

1. Se imprimirá la información ilegible o no se podrá cuando no se seleccione 119200.
2. Cuando seleccione el modo 5, verificación de asistencia seleccione para imprimir.

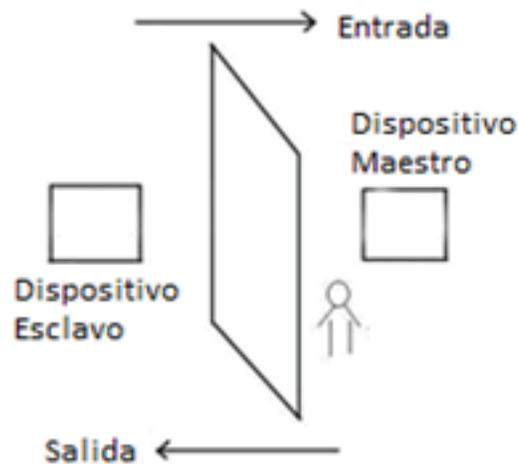
Por ejemplo: Coloque la tarjeta a las 13:24:55 de Septiembre 1, 2009, existen diferentes formatos de impresión para seleccionar, como se muestra a continuación:

<p>Versión 1 00001 San 09/09/01 55I</p>	<p>Versión 5: 00001 09.09.01 13 55Registro de entrada</p>
<p>Versión 2 Número de Usuario: Fecha/Hora Registro de entrada 09/09/01 13 55</p>	<p>Versión 6 00001 Fecha Registro de entrada 09.09.01 13 55</p>
<p>Versión 3 San 00001 09/09/01 13 55</p>	<p>Versión 7 Id de Usuario: Registro de Entrada: 09.09.01 13 55</p>
<p>Versión 4 Descanso: :24 01/09/2009 00001</p>	<p>Nota: Asegúrese que el equipo de huellas y la impresora (Súper Terminal) tengan la misma velocidad de transmisión. 2. Si el formato por default no satisface sus requerimientos, puede contactar a nuestra compañía para presentar otro formato personalizado.</p>

Apéndice 4 Anti-passback

Algunas ocasiones, personas ilegales siguen al empleado a la puerta, lo cual puede ocasionar problemas de seguridad. Para prevenir este riesgo, la función es habilitada. El registro de entrada debe coincidir con el registro de salida o la puerta no se abrirá.

Esta función necesita dos equipos funcionando juntos. Uno es instalado dentro de la puerta y el otro instalado fuera de la puerta. La comunicación Wiegand es adoptada entre los dos dispositivos.



Principio de funcionamiento

El dispositivo maestro tiene entrada Wiegand y el dispositivo esclavo tiene salida Wiegand. Conecte la salida Wiegand del dispositivo esclavo en la entrada Wiegand del dispositivo maestro. El número enviado al dispositivo maestro del dispositivo esclavo debe ser buscado en el dispositivo maestro.

Función

Juzgue el anti-passback acorde con el registro de entrada y salida de los usuarios. El registro de entrada y el de salida deben tener coincidencia. Este dispositivo soporta anti-passback entrada, salida o salida-entrada (ingrese al menú del dispositivo—Ajustes—Sistema—Configuración—Configuración avanzada—Anti-passback

Cuando el dispositivo maestro es configurado como "salida anti-passback", si el usuario quiere entrar y salir normalmente, el registro reciente debe ser de "Entrada" o no podrá salir. Cualquier registro de "Salida" será "anti-passback denegado". Por ejemplo, el registro de un usuario es "Entrada", su segundo registro debe ser "Salida" o "Entrada". Su tercer registro es basado en su segundo registro. El registro de salida y de entrada debe tener coincidencia. (Si el usuario no tiene un registro anterior, el podrá entrar pero no podrá salir).

Cuando el dispositivo maestro este configurado como "entrada anti-passback", si el usuario quiere entrar y salir normalmente, su registro más reciente debe ser "Salida", o no podrá salir. Cualquier registro de "Salida" será "Anti-passback rechazado" por el sistema. (Noticia: si el usuario no tiene un registro anterior, después podrá salir pero no podrá entrar).

Cuando el dispositivo maestro sea configurado como "salida-entrada anti-passback", si el usuario quiere entrar y salir normalmente, si su registro es "Salida" y "Entrada", su siguiente registro debe ser "Entrada" y "Salida".

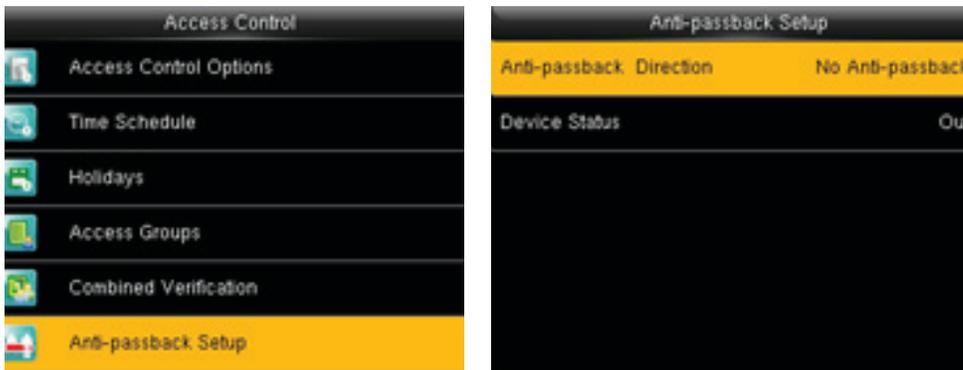
Operación

1) Seleccione Modelo

Dispositivo Maestro: Dispositivo con función Wiegand en funcionamiento, excepto para lector F10.

Dispositivo esclavo: Dispositivo con función Wiegand de salida.

2) Ajustes de Menú



Presione > para seleccionar configuración Anti-passback y presione OK.

Ingrese para configurar la interfaz de Anti-passback.

Anti-passback

Salida anti-passback: Si el dispositivo no almacena los registros de una persona, la persona puede verificar su salida después de la primera comparación. En caso de que el registro de una persona este almacenado en el dispositivo, una alarma activada cuando la persona verifique la salida sin el registro de entrada correspondiente en el dispositivo. Si únicamente la salida anti-passback es habilitada, es permitido acceder en cualquier momento.

Entrada anti-passback: si el dispositivo no almacena el registro de una persona, la persona puede verificar la entrada después de la primera comparación. En caso que el registro de una persona sea almacenado en el dispositivo, una alarma se activara cuando la persona verifique la entrada o salida correspondientes en el dispositivo.

Entrada/Salida Anti-passback: si el dispositivo no almacena el registro de una persona, la persona puede verificar la entrada después de la primera comparación. En caso que el registro de una persona este almacenado en el dispositivo, una alarma será activada cuando la persona verifica entrada o salida correspondientes en el dispositivo.

No Anti-passback: la persona se abrirá solo cuando una persona es autenticada por el host maestro.

Estatus del Dispositivo

Control de entrada: cuando un dispositivo es utilizada como control de entrada, el dispositivo guarda solo los registros de entrada.

Control de salida: cuando un dispositivo es utilizado para control de salida, el dispositivo solo guarda los registros de salida.

Ninguno: Cuando el estatus de un dispositivo sea configurado a ninguno, la función anti-passback del dispositivo es deshabilitada.

3) Modificar formato de salida Wiegand del dispositivo

Cuando dos dispositivos se comunican, solo las señales Wiegand sin el ID del dispositivo son recibidas. Ingrese al menú del dispositivo opción de comunicación → Opción Wiegand o ingrese al software → ajustes básicos → Administración del dispositivo → Wiegand, para modificar el "Formato definido" como "Wiegand 26 sin el ID del Dispositivo"

4) Enrolar usuario

El usuario debe estar en el dispositivo maestro y en el dispositivo esclavo al mismo tiempo, y el PIN del usuario debe ser el mismo.

Por lo tanto, es necesario enrolar a los usuarios en el dispositivo maestro y en el dispositivo esclavo.

5) Instrucciones de conexión

Comunicación Wiegand es adoptada por el dispositivo maestro y el dispositivo esclavo. Referirse a lo siguiente para la conexión:

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

Declaración de Privacidad y Derechos Humanos

Estimado Cliente:

Gracias por elegir los productos biométricos híbridos diseñados y fabricados por nosotros. Como una empresa reconocida mundialmente de tecnología biométrica y servicios, ponemos mucha atención a la conformidad con las leyes de derechos humanos y privacidad en cada país mientras constantemente realizamos investigación y desarrollo.

Por la presente hacemos las siguientes declaraciones:

1. Todos nuestros dispositivos de reconocimiento dactilar para uso civil únicamente recopilan puntos característicos de la huella en lugar de las imágenes dactilares, por tanto no hay problemas de privacidad involucrados.
2. Los puntos característicos colectados por nuestros productos no se pueden utilizar para restaurar las imágenes de huellas dactilares originales, por tanto no hay problemas de privacidad involucrados.
3. Nosotros, como proveedor de equipos, no somos responsables de ninguna de las consecuencias directa o indirectamente debido a la utilización de nuestros productos.
4. Para cualquier conflicto relacionado con privacidad y derechos humanos del uso de nuestros productos, por favor póngase en contacto directo con su empresa.

Otros equipos de huella dactilar o herramientas de desarrollo proporcionarían la función de recolectar la imagen original de los usuarios. En cuanto a si la recolección de huellas dactilares constituye una violación de su privacidad, por favor contacte al gobierno o al proveedor del equipo. Como somos los fabricantes del equipo original, no podrá ser legalmente responsables de cualquier infracción.

Nota: La ley de las personas de la República de China tienen las siguientes regulaciones con respecto a la libertad personal.

1. La detención ilegal, detención o búsqueda de las personas de República de China está prohibido; se prohíbe la violación de la privacidad individual.
2. La dignidad personal de las personas de República de China es inviolable.
3. El hogar de los ciudadanos de la República de China es inviolable.
4. La libertad y privacidad de la correspondencia de los ciudadanos de la República de China está prohibida y protegida por la ley.

Por último destacamos que la biometría, como una tecnología avanzada de reconocimiento, puede ser aplicada en varios sectores incluyendo el comercio electrónico, bancario, seguros, asuntos legales. Cada año las personas alrededor del mundo sufren grandes pérdidas debido a la inseguridad de contraseñas. El reconocimiento de huellas dactilares actualmente provee una protección adecuada para su identidad hasta un ambiente de alta seguridad.

Descripción de uso Favorable al medio ambiente.



El periodo de uso Favorable al Medio Ambiente (EFUP) señalado en este producto se refiere al periodo de tiempo de seguridad en el que el producto sea utilizado bajo las condiciones especificadas en las instrucciones, sin fuga de sustancias nocivas.

El EFUP de este producto no cubre las partes consumibles que necesitan ser reemplazadas como baterías. El EFUP de las baterías es de 5 años.

Nombres, concentración de tóxicos y elementos de sustancias peligrosas

Números de Parte	Sustancias o elementos toxicos peligrosos					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Resistencia del Chip	x	o	o	o	o	o
Capacidad de Chip	x	o	o	o	o	o
Inductor de Chip	x	o	o	o	o	o
Diodo de Chip	x	o	o	o	o	o
Componentes ESD	x	o	o	o	o	o
Timbre	x	o	o	o	o	o
Adaptador	x	o	o	o	o	o
Tornillos	o	o	o	x	o	o

o: Indica que la sustancia toxica contenida en los materiales homogéneos de esta parte del equipo se encuentra por debajo de los limites SJ/T11363-2006.

x: Indica que la sustancia toxica contenida en al menos una de los materiales homogéneos de esta parte está por encima del límite SJ/T11363-2006.

Nota: 80% de las partes de este equipo está fabricada con materiales no peligrosos y con materiales favorables al medio ambiente.

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



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

Derechos de Autor © 2016, ZKTeco, Inc. 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 Inc.