Manual de Usuario
F21

Control de Acceso con Tiempo y Asistencia

Versión: 1.0

Acerca de este manual

- Este manual introduce la operación de la interfaz y menú de usuario, las funciones del dispositivo F21 Control de Acceso con Tiempo y Asistencia.
- Las imágenes de este manual pueden no ser exactamente coherentes con los de su producto; por lo que el producto real prevalece.
- No todos los dispositivos tienen la función de ★, por lo que el producto real prevalece..

CONTENIDO

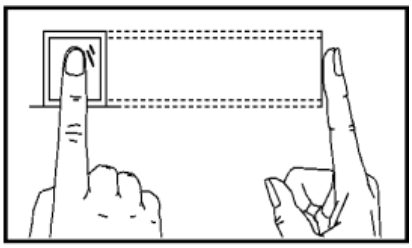
CONTENIDO

1. Notas de Guía

1.1 Colocación de la Huella Digital

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

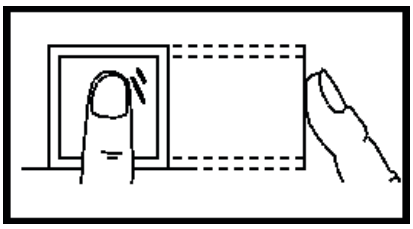
1. Forma correcta de colocar:



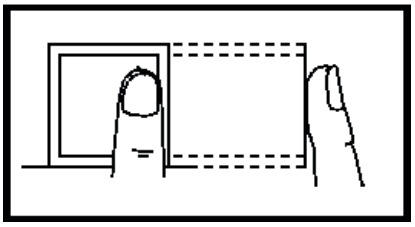
El dedo debe colocarse en una forma totalmente plana y centrado en el sensor.

1. Forma incorrecta de colocar:

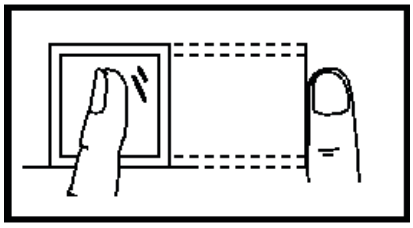
No plano



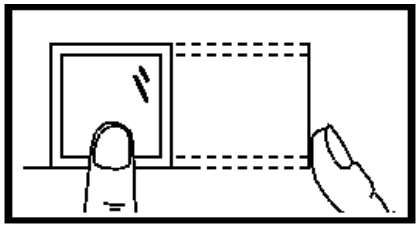
Fuera del centro



De lado



Fuera del centro

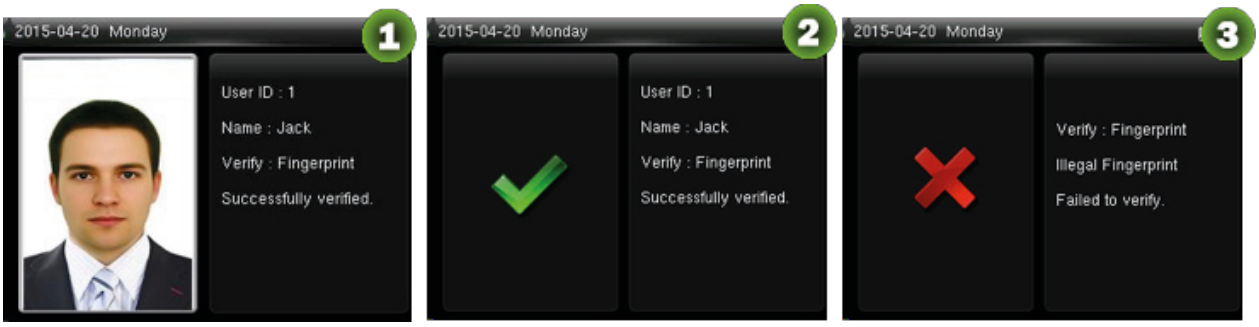


Nota: Utilice el método correcto de presionar para el registro y verificación de huellas digitales. Nuestra empresa no asume la responsabilidad por el rendimiento de la verificación baja causada por un funcionamiento incorrecto del usuario. Los derechos a la interpretación definitiva y enmienda son reservados

1.2 Modos de Verificación

1.2.1 Verificación de Huella Digital 1:N

Bajo este método de verificación de huella digital, la huella dactilar recolectada por el sensor se verifica con todas las huellas digitales almacenadas en el dispositivo.
Por favor use la manera correcta de colocar la huella digital en el sensor (para más detalles, por favor consulte 1.1 Colocación de la Huella Digital). <-Vinculo



Verificación Exitosa | Verificación Exitosa | Error de Verificación

Comentarios:

1. Cuando el dispositivo indique "por favor coloque su dedo de nuevo", coloque su dedo de nuevo en el sensor. Si la verificación falla después de 2 intentos más, saldrá a la interfaz inicial.
2. En los dispositivos que tienen la función Foto ID, la figura 1 será mostrada en pantalla después de una verificación exitosa, de lo contrario, la figura 2 será mostrada.

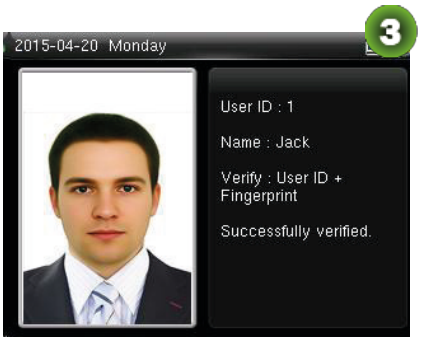
★ **Solo algunos productos cuentan con la función Foto ID.**

1.2.2 Verificación de Huella Digital 1:1

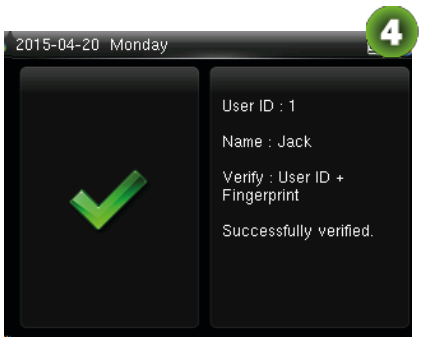
Bajo este método de verificación de huella digital, la huella dactilar recolectada por el sensor es verificada con la huella correspondiente al ID de usuario introducido. Utilice este método cuando tenga dificultad en la Verificación de Huella Digital 1:N.

Introduzca el ID de Usuario y presione **[M/OK]**

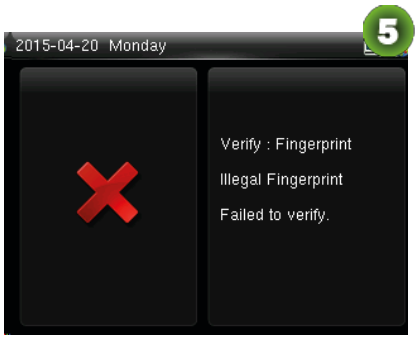
Presione Huella y después **[M/OK],** coloque el dedo después en el sensor.



Verificación Exitosa



Verificación Exitosa



Error de Verificación

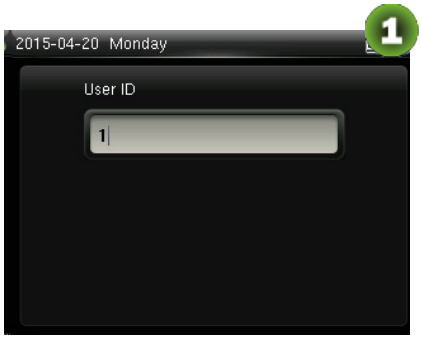
Comentarios:

1. Coloque el ID de usuario en la interfaz inicial y pulse [M/OK]. Si "ID de usuario incorrecto!" aparece, esto significa que el ID de usuario no existe.
2. Cuando el dispositivo muestra "Coloque su dedo de nuevo", pulse el dedo de nuevo en el sensor de huella. Si la verificación sigue fallando después de 2 intentos, saldrá a la interfaz inicial.
3. En los dispositivos que poseen la función Identificación con Foto (Photo ID), como se muestra en la figura 3, se visualiza en la pantalla tras el éxito de la verificación, de lo contrario, aparecerá la figura 4.

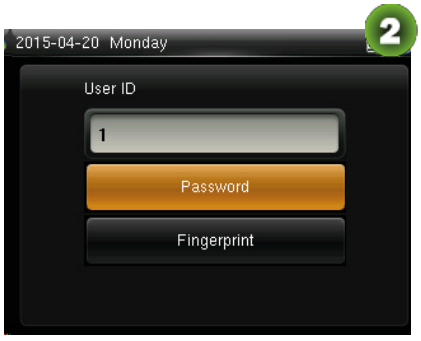
★ Solo algunos productos cuentan con la función Foto ID.

1.2.3 Verificación con Contraseña

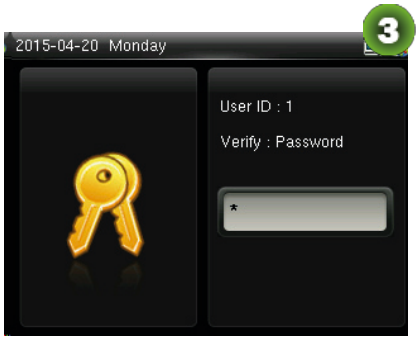
En este método de verificación, la contraseña introducida es verificada con la contraseña del ID de usuario introducido.



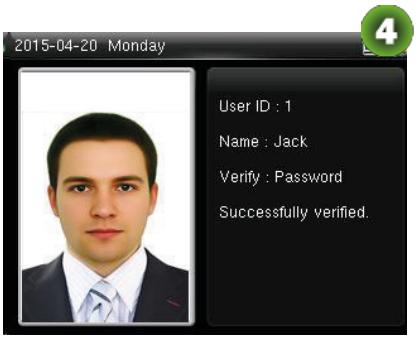
Introduzca el ID de Usuario y presione **[M/OK]**



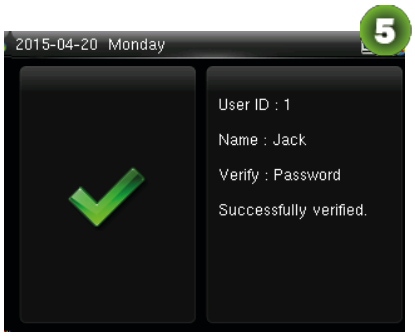
Presione "Contraseña" y después **[M/OK]**



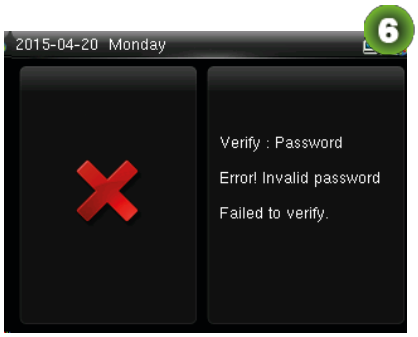
Coloque la contraseña



Verificación Exitosa



Verificación Exitosa



Error de Verificación

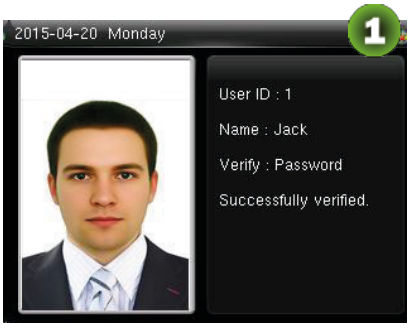
Comentarios:

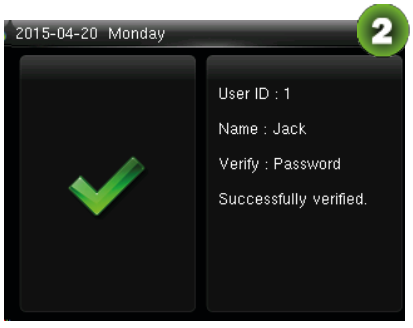
1. Si se muestra "Contraseña Incorrecta", coloque la contraseña de nuevo. Si la verificación sigue fallando después de 2 intentos, saldrá a la interfaz inicial.
2. En los dispositivos que poseen la función Photo ID, como se muestra en la figura 4, se visualiza en la pantalla tras el éxito de la verificación, de lo contrario, aparecerá la figura 5.

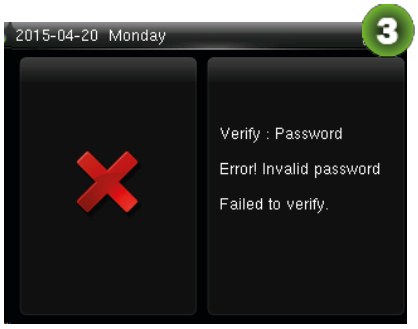
★ Solo algunos productos cuentan con la función Foto ID.

La función de Tarjeta es opcional, solamente algunos productos cuentan con el módulo para la lectura de tarjetas y la función activada. Contacte a soporte técnico si la requiere.

1. Pase la tarjeta por encima del lector de tarjetas (la tarjeta debe estar registrada).
2. Verificación exitosa.
3. Error de verificación.





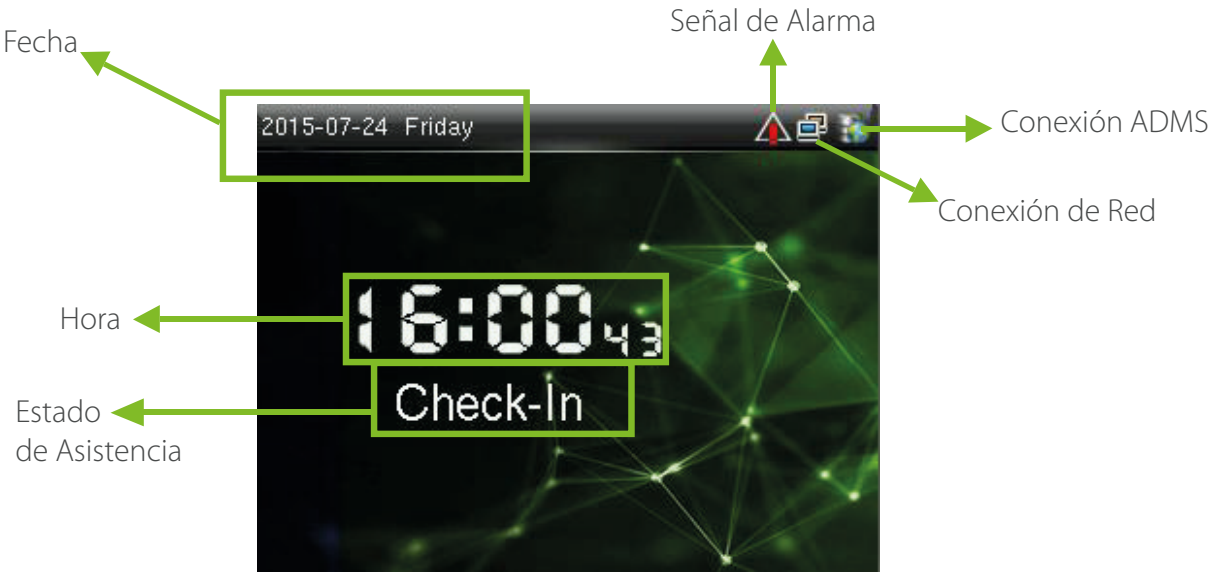


En los dispositivos que cuentan con la función Photo ID, la figura 1 se mostrará en pantalla después de una verificación exitosa, de lo contrario, se mostrará la figura 2.

★ Solo algunos productos cuentan con la función Foto ID.

1.3 Interfaz Inicial

Cuando el dispositivo está encendido, la interface inicial se muestra como sigue:



2. Menú principal

Cuando el dispositivo se encuentre en estado de reposo, presiona **[M/OK]** para abrir el menú principal.

Gest. Usuario: Información básica de usuarios registrados, incluyendo el ID de usuario, rol de usuario, huella digital. ★ (tarjeta ID y Mifare opcionales), contraseña, usuario foto ★ y papel de control de acceso.

Rol de Usuario: Establece los roles de usuario para acceder al menú y cambiar la configuración.

Comm.: Establece los parámetros relacionados de la comunicación entre el dispositivo y el PC, incluyendo Ethernet, parámetros tales como la dirección IP, etc., comunicaciones serie, conexión de PC, ADM ★ y Wiegand ajustes.

Sistema: Para configurar los parámetros relacionados con el sistema y la actualización del firmware, incluyendo el ajuste de fecha y hora; tiempo, asistencia y parámetros de huellas dactilares y restablecer los ajustes de fábrica.

Personalizar: Esto incluye la visualización de la interfaz de voz, timbre, punch claves de estado y las teclas de método abreviado del modo configuración.

Gestion Datos: Elimina los datos de asistencia, eliminar todos los datos, eliminar rol administrador y eliminar los protectores de pantalla, etc.

Control de Acceso: Esto incluye la configuración de los parámetros de la cerradura.

USB Manager: Para transferir datos, como los datos de usuario y los registros de asistencia desde el disco USB para el software compatible u otros dispositivos.

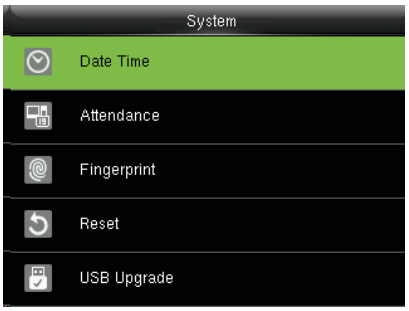
Búsqueda de Asistencia: Para buscar los registros almacenados en el dispositivo después de verificación satisfactoria.

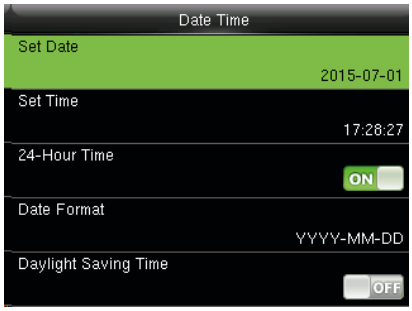
Imprimir: Para establecer la información de impresión y las funciones (si la impresora está conectada al dispositivo).

Auto prueba: Para probar automáticamente diferentes funciones del módulo, incluyendo el LCD, voz, teclado, lector de huella, cámara y prueba de RTC reloj.

Inf. Sistema: Para comprobar la capacidad del dispositivo y la información del firmware.

3 Ajustes de Fecha/Hora





En el interfaz inicial, pulse [M/OK] > Sistema > Fecha/Hora para introducir la fecha/hora de configuración de la interfaz. Incluye ajuste de fecha, hora, reloj de 24 horas, el formato de la fecha y el horario de verano.

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

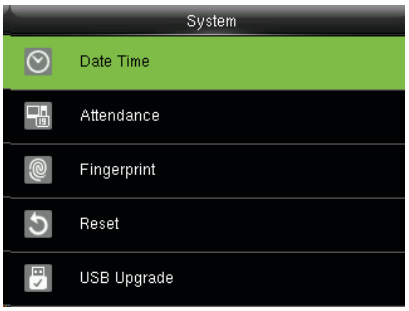
Comentarios:

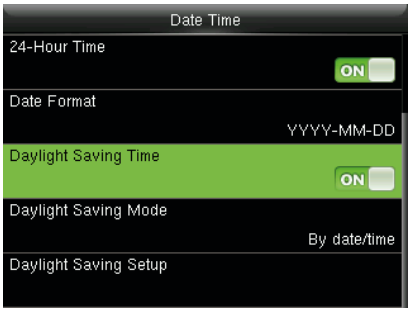
Cuando se restablecen los ajustes de fábrica, la fecha/hora del dispositivo no se restaurarán (si la fecha/hora está establecido a las 18:30 del 1 de enero de 2020, después de que se restablecen los ajustes de fecha/hora, la estancia será a las 18:30 del 1 de enero de 2020.

3.1 Hora de Verano

DST, que también se denomina horario de verano, es un sistema de ajuste de la hora local con el fin de ahorrar energía. El tiempo aprobada durante las fechas establecidas es llamado "horario de verano". Normalmente, el tiempo será una hora adelante en verano. Esto permite a los usuarios dormir o levantarse temprano, y también reducir la iluminación del dispositivo para ahorrar energía. En otoño, el tiempo se reanudará la hora estándar.

Las reglas son diferentes en distintos países. En la actualidad, casi 110 países adoptan el horario de verano. Para satisfacer la demanda de DST, la opción es especial, puede ser personalizado. Hacer que el tiempo avance una hora XX (hora) XX (día) XX (mes) y hacen que el tiempo retroceda una hora XX (hora) XX (día) XX (mes).



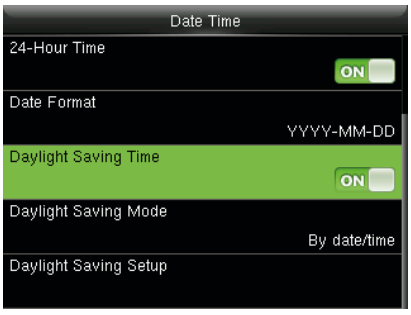


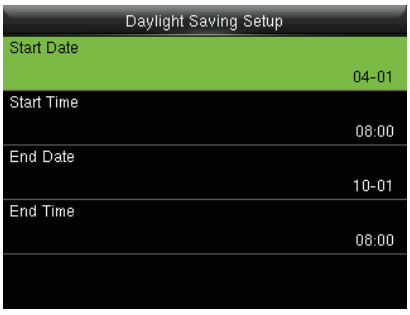
Pulse **[M/OK]>System>Fecha Hora>luz del día**, ahorrando tiempo y, a continuación, pulse [M/OK] para activar el horario de verano.
Modo de ahorro de luz diurna: Modo de horario de verano, por modo de fecha/hora y por semana/día modo de selección.
Daylight Saving Setup: Establecer fecha/hora o semana/día del Horario de Verano de acuerdo con la selección en el modo de ahorro de luz diurna.

¿Cómo configurar el horario de verano?

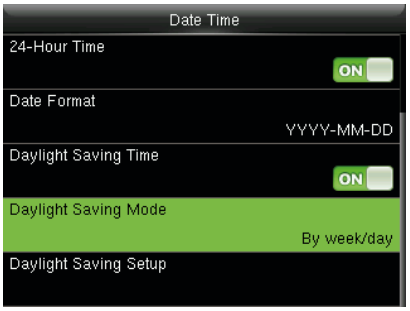
Por ejemplo, ajustar el reloj una hora adelante a las 08: 00 el 1 de abril y hacia atrás una hora a las 08: 00 el 1 de octubre (el sistema vuelve a la hora original).

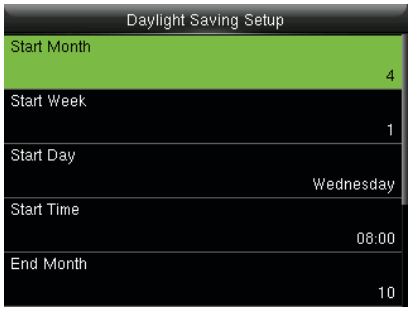
- Por modo de fecha/hora:

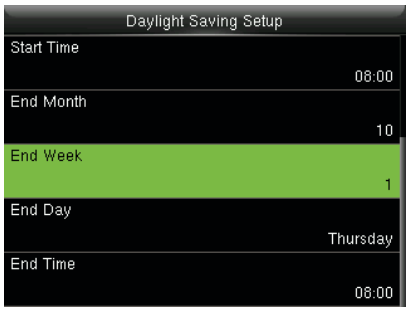




- Por semana/modo de fecha:







Comentarios:

1. Si el mes en que comienza el horario de verano es más tarde que cuando termina el horario de verano, el horario de verano abarca dos años diferentes. Por ejemplo, la hora de inicio del horario de verano es 2014-9-1 4:00 y la hora de fin del horario de verano es 2015-4-1 4:00.

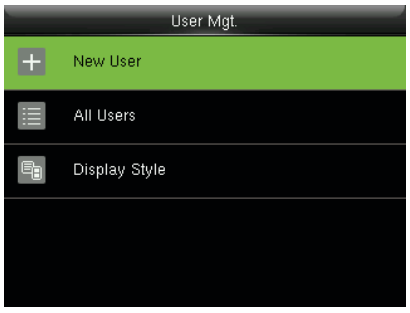
2. Asumir que la semana/día modo está seleccionada en modo **[Dayling Saving Mode]** y el DST empieza desde el domingo de la sexta semana de septiembre de 2013. Según el calendario, de septiembre de 2014 no tiene seis semanas pero tiene cinco semanas. En este caso, en 2014, el horario de verano comienza en el punto correspondiente a la hora del último domingo de septiembre.

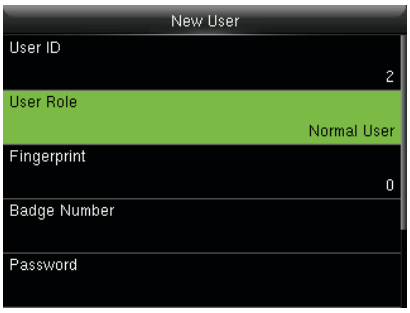
3. Asumir que el DST empieza desde el lunes de la primera semana de septiembre de 2014. Según el calendario, la primera semana de septiembre de 2015 no tiene el lunes. En este caso, el horario de verano comienza desde el primer lunes de septiembre de 2015.

4 Gestión de Usuarios

4.1 Agregar Usuario

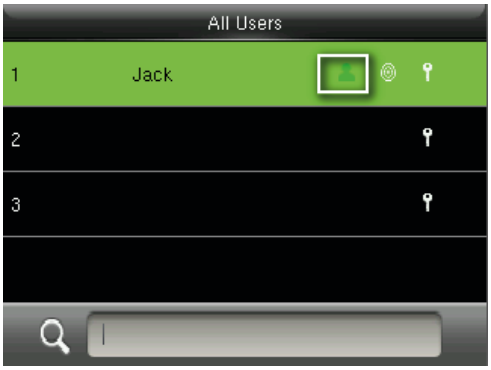
Incluyendo la adición de súper administrador y usuario normal.





En la interfaz inicial, pulse **[M/OK]>Usuario Mgt.>Nuevo Usuario** para ingresar a la interfaz de **Nuevo Usuario.** En ajustes se incluyen introducir el ID de usuario, elegir el rol de usuario, registro de huella y número de identificación ★ (ID y tarjeta Mifare son opcionales), establecer la contraseña, tomando fotos del usuario y configuración de Control de acceso de función.
Agregar un Super Admin: Elija "super administrador" en **[Rol de usuario]**, quién está autorizado para operar todas las funciones del menú.

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



Agregar un Usuario Normal: Elija "Usuario normal" en **[Rol de usuario].**
Cuando el Super Admin está configurado, los usuarios normales sólo pueden usar huella, contraseña o tarjeta de verificación; cuando el Super Admin aún no está establecido, los usuarios normales pueden controlar todas las funciones del menú.

Contraseña: de 1 a 8 dígitos de la contraseña es aceptada.

Comentarios:

1. El dispositivo automáticamente asigna el ID de usuario para usuarios en secuencia, pero el usuario puede definirlo manualmente.

2. El dispositivo es compatible con ID de usuario que varía de 1 a 9 dígitos.

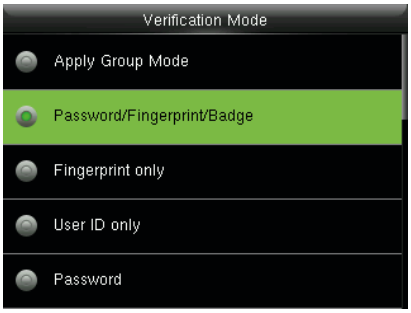
4.2 Ajustes del Control de Acceso

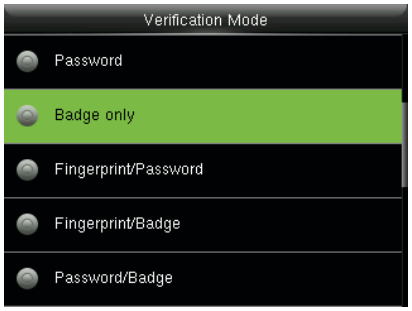
La opción del Control de acceso de usuario es configurar acceso de puertas abiertas dirigidas a todo el mundo, incluido el grupo de acceso, ajuste el modo de verificación, utilizando la zona horaria, la coacción de administración de huellas.

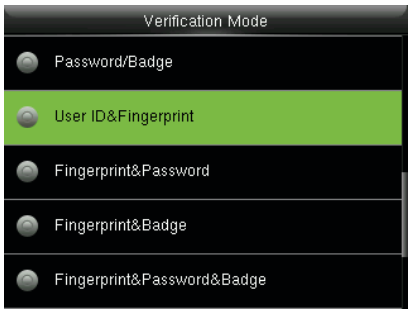
Grupo de Acceso: para asignar los usuarios a diferentes grupos de control de acceso para la gestión. Los usuarios nuevos pertenecen al grupo 1 en la configuración predeterminada, que pueden ser reasignados a otros grupos.

Modo de Verificación: el usuario puede elegir cualquier grupo o tipo de verificación. Si la verificación individual es escogido, el método de verificación utilizados por otros miembros del grupo no se verán afectados.

Tipo de Verificación Individual: Se incluye contraseña / huella digital / tarjeta, sólo huella digital, sólo ID de usuario, contraseña, tarjeta solamente, huella dactilar, huella digital / contraseña / tarjeta, tarjeta / contraseña, ID de usuario y huella dactilar, huella dactilar y contraseña, huella dactilar y tarjeta, huella dactilar y contraseña & tarjeta, contraseña & tarjeta, ID de usuario y contraseña y huella dactilar, huella dactilar y tarjeta y el ID de usuario.

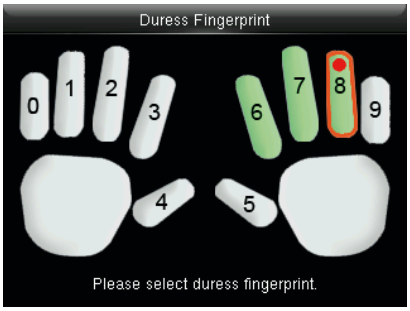






Comentarios:
La verificación individual prevalecerá sobre el grupo de verificación.

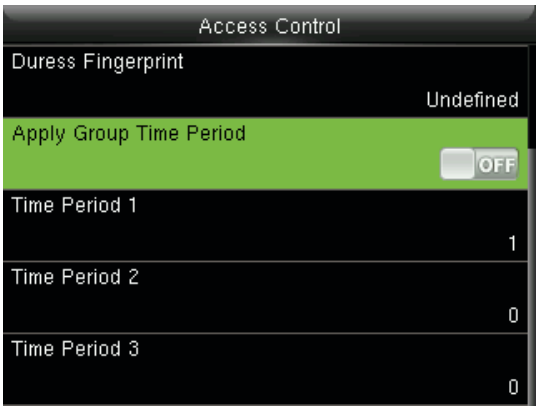
Huellas de coacción: el usuario puede elegir uno o más huella registrada(s) como huellas de coacción. Cuando esa huella es verificado, se activará la alarma de coacción.



Ejemplo: Entre las huellas dactilares registradas (6, 7, 8), seleccione la 8ª como la huella digital de huellas dactilares de coacción.

Utilice el Grupo Periodo de Tiempo:

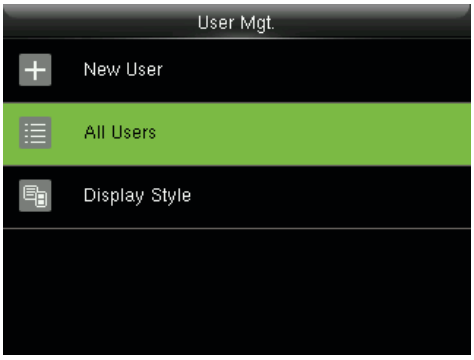
1. Cuando esta función está activada, el usuario utiliza la zona horaria predeterminada de su grupo.
2. Cuando esta función está desactivada, el usuario debe establecer una zona horaria personal (no con el grupo Zona horaria). Esto no afectará a la hora de acceso de zona de otros miembros del grupo.

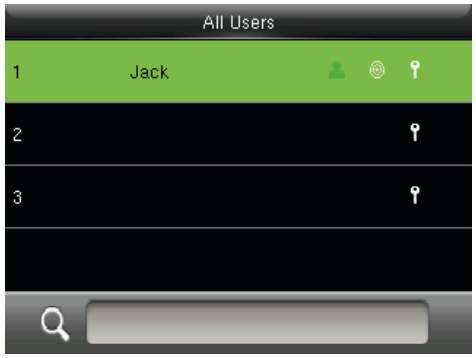


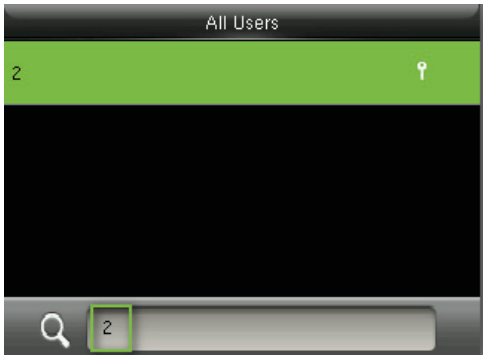
Comentarios:
Cada usuario puede establecer un máximo de 3 períodos de tiempo.

4.3 Búsqueda de Usuario

Introduzca el ID de usuario en la lista de usuarios para buscar un usuario.



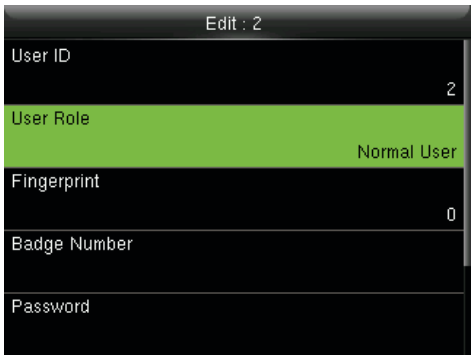




En el interfaz inicial, pulse **[M/OK]>Usuario Mgt.>**Para ingresar a la interfaz **Todos los usuarios.** En entrada "ID de usuario" , el usuario correspondiente será mostrado. Como se muestra en la figura anterior, busque el usuario con el ID de usuario "2".

4.4 Edición de Usuario

Después de que un usuario es elegido mediante 4.3 Buscar usuario, pulse **[M/OK]** y seleccione **[Editar]** para entrar en la interfaz de usuario de la edición.
O en el interfaz inicial pulse **[M/OK] > Usuario Mgt. > Usuarios > Buscar un usuario** > Pulse **[M/OK] > Edit** para entrar en la interfaz de usuario de la edición.
El método de operación de edición de usuario es el mismo con la adición de usuarios, pero el ID de usuario no se puede editar.

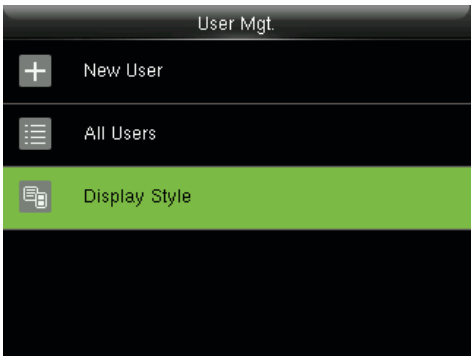


4.5 Eliminar un Usuario

Después de que un usuario es elegido mediante 4.3 Buscar usuario, pulse **[M/OK]** y seleccione **[Eliminar]** para acceder a la eliminación de la interfaz de usuario.
O en el interfaz inicial pulse [**M/OK] > Usuario Mgt. > Usuarios** > Buscar un usuario > **Pulse [M/OK] > Eliminar** para ingresar a la interfaz de eliminar usuario.

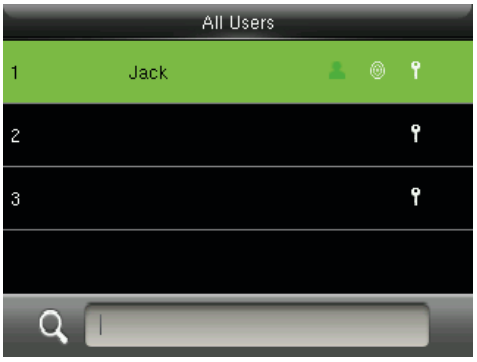
Nota: 1. Sólo cuando el usuario ha registrado las huellas dactilares, la contraseña, la tarjeta ★ y la foto del usuario★, será eliminado.
2. Sólo algunos dispositivos cuentan con la función de Photo ID.
3. La función de la tarjeta es opcional.

4.6 Estilo de la Visualización de Usuario

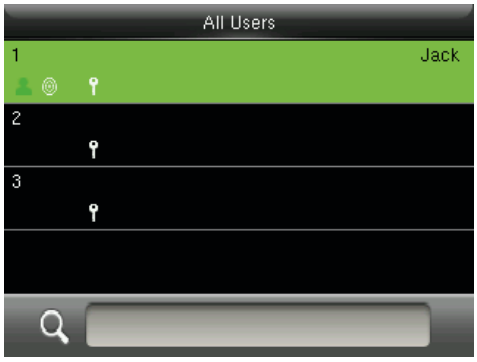


En la interfaz inicial, pulse **[M/OK] > Usuario Mgt. > Estilo de visualización** para entrar a la configuración de estilo de visualización de la interfaz.

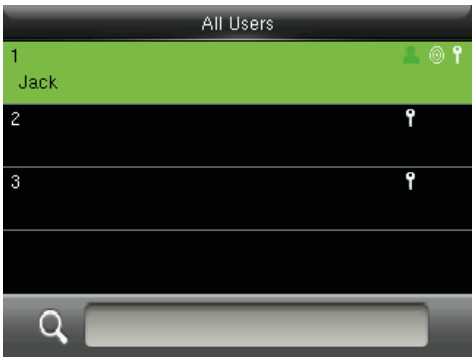
Se cuenta con varios estilos de visualización como se indica a continuación:



Estilo de línea única



Líneas múltiples



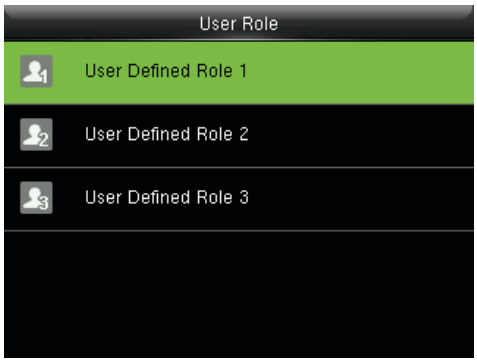
Línea mixta

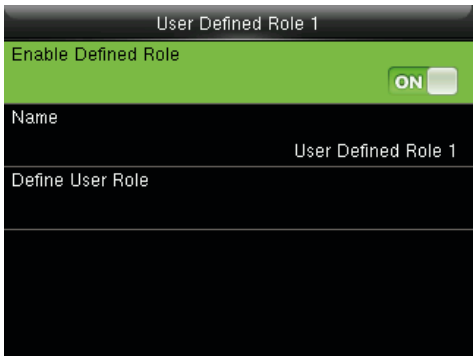
5 Función de Usuario

La configuración de derechos de usuario de manejo del menú (solo un máximo de 3 funciones pueden definirse). Cuando está activada la función de usuario, en [**Usuario Mgt.] > [Nuevo] > [Usuario]** Función de usuario, puede asignar el rol de usuario adecuado para cada usuario.

Rol: El súper usuario necesita asignar distintos derechos a los nuevos usuarios. Para evitar la configuración de derechos para cada usuario uno por uno, puede establecer roles de usuario para clasificar los diferentes niveles de permisos de administración de usuarios.

5.1 Habilitar Función de Usuario



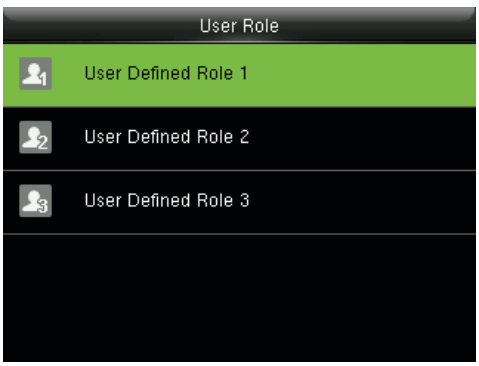


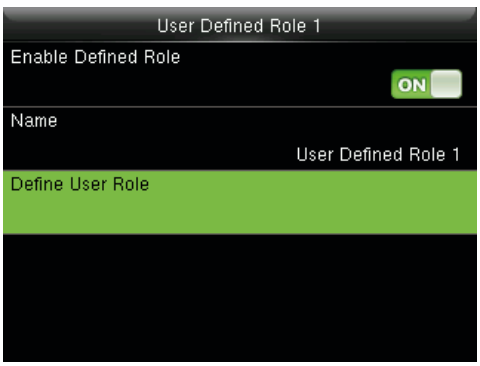
En la interfaz inicial, pulse **[M/OK] > Función de usuario > Función definida por el Usuario 1 (2 / 3)>Activar función definida**, pulse **[M/OK]** para habilitar la función definida.

Después de habilitar funciones definidas, puede comprobar el usuario habilitado funciones en **[Usuario Mgt.] > [Nuevo] > [Usuario]** la función de usuario.

Comentarios:
Al menos un administrador registrado es necesario para habilitar la función de usuario.

5.2 Asignación de Derechos

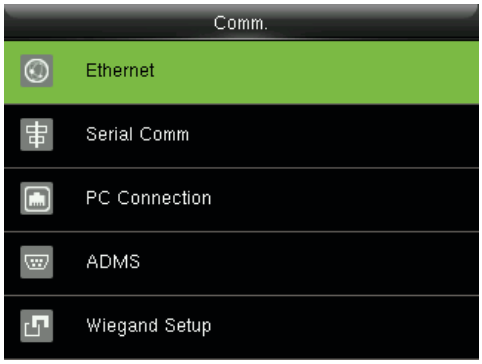


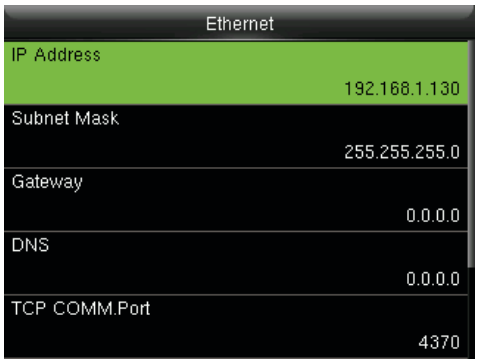


En la interfaz inicial, pulse **[M/OK] > Función de usuario > Función definida por el Usuario 1 (2 / 3) >** Definir rol de usuario para entrar a la función definida por el Usuario 1 (2 /3) derechos la asignación de interfaz. Pulse **[M/OK]** para seleccionar o cancelar el operando derecho de cada menú de función definida por el **Usuario 1 (2 /3).**

6 Ajustes de Comunicación

6.1 Ajustes de la Red Ethernet





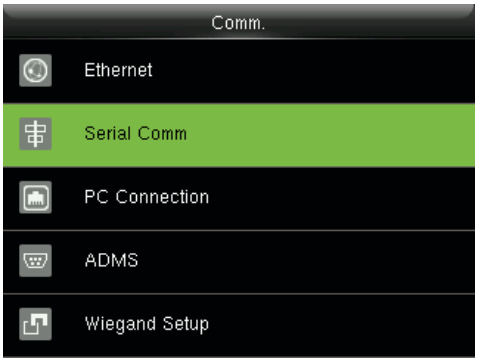
En la interfaz inicial, pulse **[M/OK] > Comm. > Ethernet** para entrar en la configuración de la interfaz Ethernet.

Los siguientes parámetros son los valores predeterminados de fábrica, Rogamos ajustarlos de acuerdo a la actual situación de la red.
Dirección IP: 192.168.1.201
Máscara de subred: 255.255.255.0
Gateway: 0.0.0.0
DNS: 0.0.0.0
TCP COMM. Puerto: 4370
DHCP: protocolo de configuración dinámica de host, que es para asignar dinámicamente las direcciones IP de los clientes a través del servidor. **Si el DHCP está activado, no se puede establecer la dirección IP manualmente.**
Mostrar en la Barra de Estado: para definir si desea mostrar el icono de red en la barra de estado.

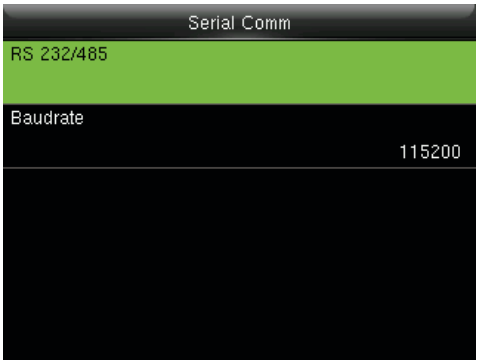
6.2 Ajustes de la Comunicación Serial

- Activar/Desactivar configuración RS485 Función

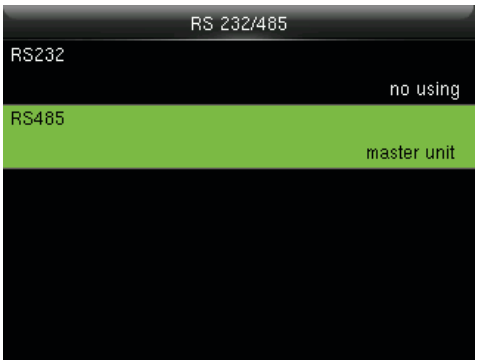
Pulse **[M/OK]** para entrar al menú principal y seleccione Comm.



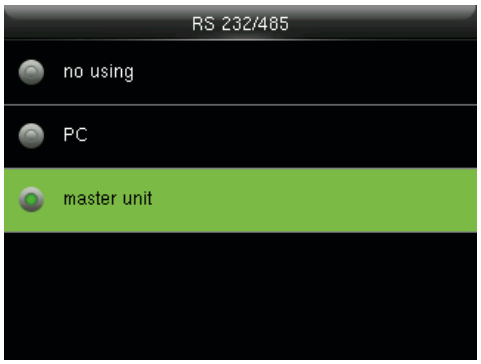
Pulse la tecla ▼para seleccionar **Serial Comm** y pulse **[M/OK]** para entrar.



Seleccione **RS232/485** y pulse **[OK]** para entrar.



Pulse la tecla ▼ para seleccionar **RS485** y pulse **[OK]** para entrar.



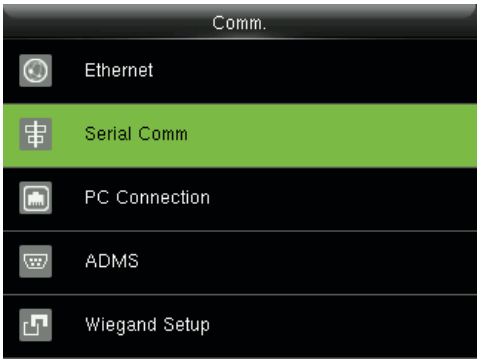
Pulse la tecla ▼ para seleccionar **RS485** como la función de PC o unidad maestra, o elija deshabilitar.

Comentarios:

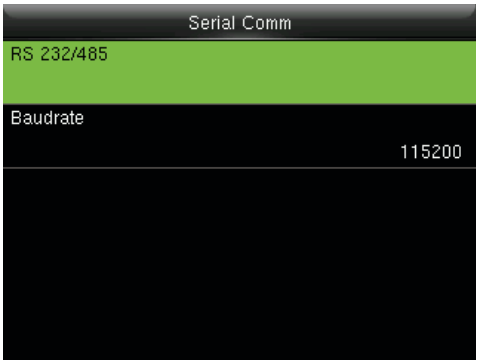
RS485 cuando se usa como la función de "maestro", la unidad puede ser conectada a un FR1200.

- Activación/Desactivación de RS232

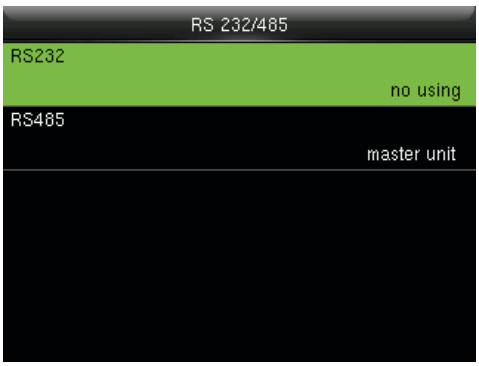
Pulse **[M/OK]** para entrar al menú principal y seleccione **Comm.**



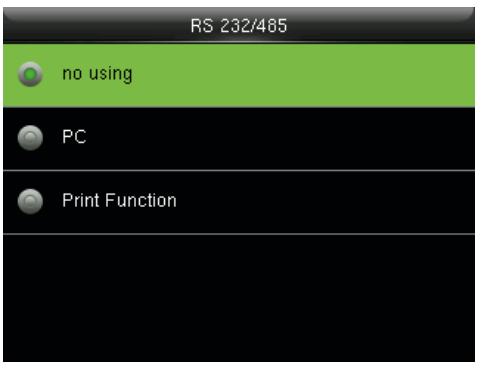
Pulse la tecla ▼ para seleccionar los **Serial Comm** y pulse **[OK]** para entrar.



Seleccione **RS232/485** y pulse **[OK]** para entrar.



Seleccione **RS232** y pulse **[OK]** para entrar.

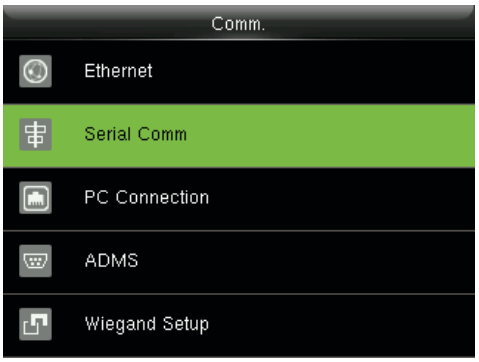


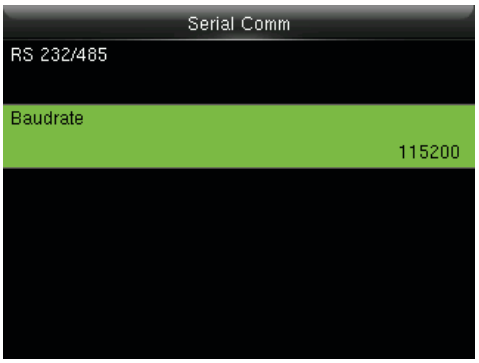
Pulse la tecla ▼ para elegir RS232 como la función de PC o de la función de impresión★ o para deshabilitar RS232.

Comentarios:

1. La comunicación RS485 y RS232 son funciones de comunicación no pueden utilizarse al mismo tiempo.
2. Cuando elige RS232 "función print" y se reinicia el dispositivo, impresión de información relacionada se pueden establecer en el submenú "Imprimir". Para más detalles acerca de la función de impresión, consulte 17.5 Función de impresión.

- Activación/Desactivación de RS232





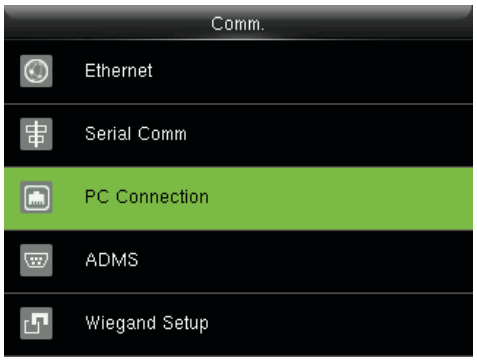
En la interfaz inicial, pulse **[M/OK] > Comm. > Serial Comm > Baudage** para entrar en la configuración de la interfaz de velocidad en baudios.

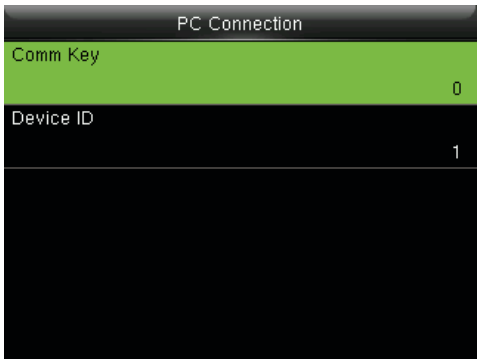
Baudage: La velocidad de la comunicación con el PC; hay 5 opciones de velocidad en baudios: 115200 (predeterminado), 57600, 38400, 19200 y 9600. Cuanto mayor sea la velocidad en baudios, la más rápida es la velocidad de comunicación, pero también la menos fiable. En general, una mayor tasa de baudios puede utilizarse cuando la distancia de comunicación es corto; cuando la comunicación es larga distancia, eligiendo una velocidad en baudios menor sería más fiable.

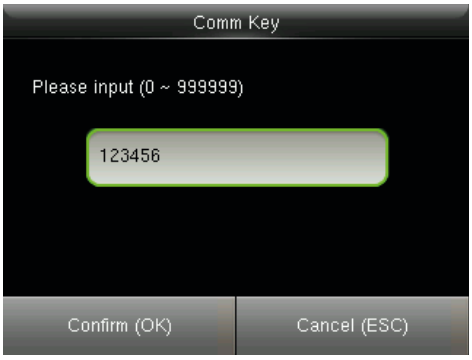
6.3 Conexión a PC

- Ajustes de la Clave de Comunicación

Para mejorar la seguridad de los datos, la clave para la comunicación entre el dispositivo y el PC debe ser configurado. Si una clave está configurado en el dispositivo, la conexión correcta se debe introducir la contraseña cuando el dispositivo está conectado a la PC, software, de modo que el dispositivo y el software pueden comunicarse.





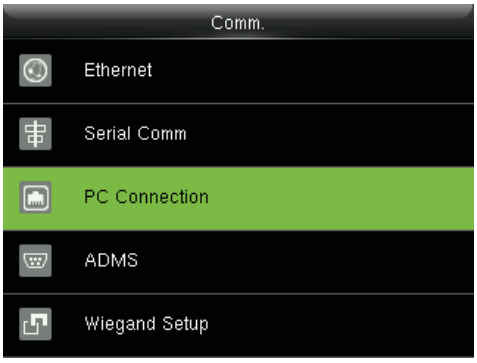


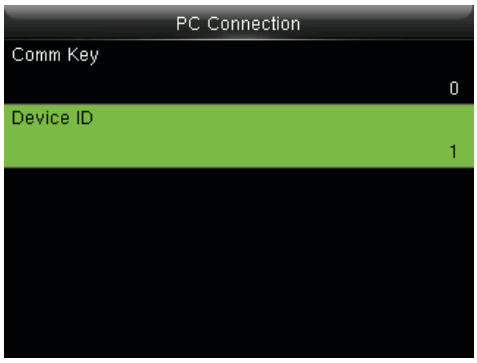
En el interfaz inicial, pulse **[M/OK] > Comm. > Conexión PC > Clave Comm** para entrar a la interfaz de configuración de clave.

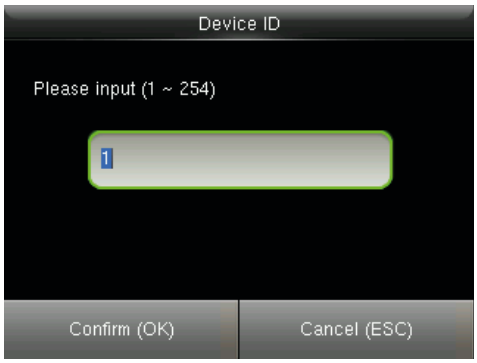
Clave de Comunicación: La contraseña predeterminada es 0 (sin contraseña). Comm clave puede ser 1~6 dígitos y oscila entre 0~999999.

- Configuración de ID de dispositivo

Si el método de comunicación es RS232/RS485, introducir este ID de dispositivo en la interfaz de comunicación del software es obligatorio.







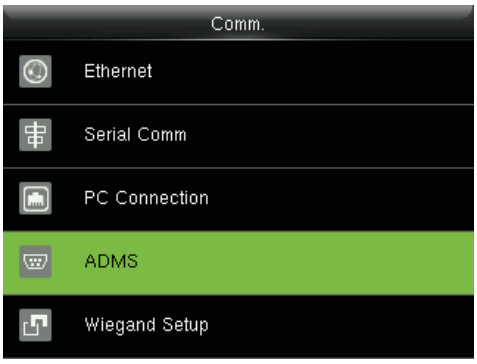
En el interfaz inicial, pulse **[M/OK] > Comm. > Conexión PC > ID Dispositivo** para entrar en la configuración del ID de dispositivo de interfaz.

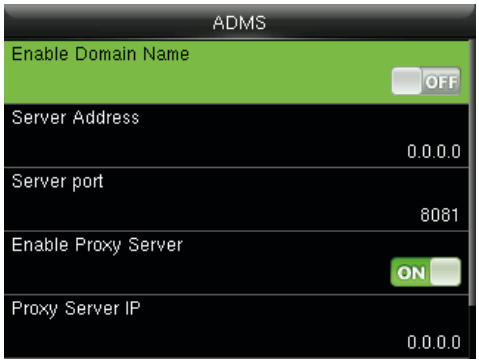
ID Dispositivo: Número de identificación del dispositivo, el cual oscila entre 1~254.

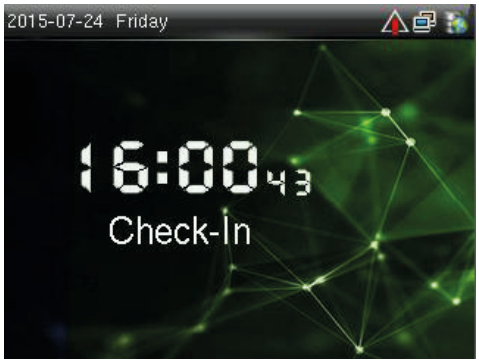
6.4 Ajustes de la función ADMS.★

Comentarios:
Sólo algunos dispositivos cuentan con la función de ajuste de ADMS.

Configuración utilizada para la conexión con el servidor de ADMS, tales como dirección IP y configuración de puerto, y si desea activar servidor proxy, etc.







En la interfaz inicial, pulse **[M/OK] > Comm. > ADMS** para entrar en la interfaz de configuración del servidor de ADMS. Cuando el servidor Web está conectado correctamente, la interfaz principal mostrará el logotipo.

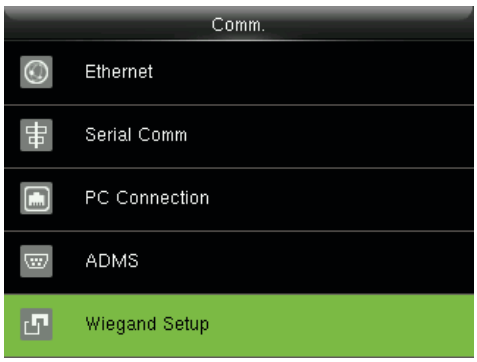
Activar el nombre de dominio: Cuando esta función está activada, el modo de nombre de dominio http://... será utilizada, tal como indica el nombre de dominio http://www.XXX.com. XXX cuando este modo está activado; cuando este modo está desactivado, introduzca la dirección IP en formato XXX.

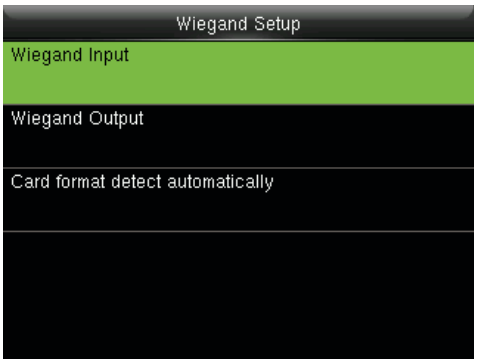
Dirección de servidor: dirección IP del servidor de ADMS.

Puerto del servidor: el puerto utilizado por el servidor de ADMS.

Activar Proxy Server: Método de activación proxy. Para habilitar el proxy, configure la dirección IP y número de puerto del servidor proxy. Introducir la dirección IP del servidor proxy y será el mismo.

6.5 Configuración Wiegand

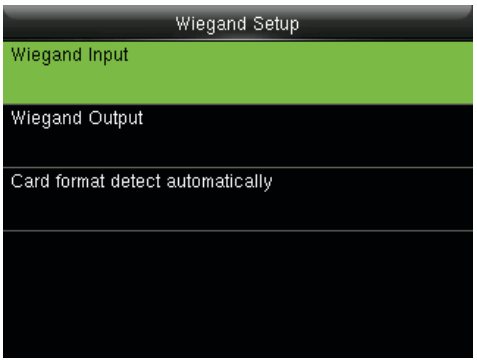




En el interfaz inicial, pulse **[M/OK] > Comm. > Configuración Wiegand** para entrar en la configuración de la interfaz Wiegand.

6.5.1 Entrada Wiegand

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



Formato Wiegand: el usuario puede elegir entre los siguientes formatos Wiegand incorporada: Wiegand 26, Wiegand 26A, Wiegand 34, Wiegand 34, Wiegand 36, Wiegand 36A, Wiegand 37, Wiegand 37a y Wiegand 50.

Anchura de pulso (US): La anchura de pulso enviado por Wiegand. El valor predeterminado es de 100 microsegundos, lo cual se puede ajustar dentro del rango de 20 a 100 microsegundos.

Intervalo de pulso (US): El valor predeterminado es 1000 microsegundos, lo cual puede ajustarse dentro del rango de 200 a 20000 microsegundos.

Tipo de ID: contenido de entrada incluido en la señal de entrada Wiegand. ID de usuario o el número de identificación puede ser elegida.

Definiciones de formatos Wiegand:

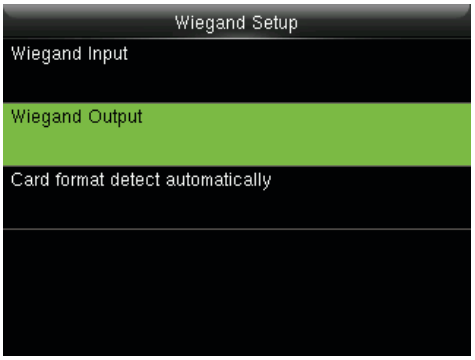
Formatos Wiegand	Definición
Wiegand 26	ECCCCCCCCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El bit 1 es el bit de paridad par del 2 al 13 de 26 bits, mientras que el bit es el bit de paridad impar del 14 al 25. La segunda a 25 bits son el número de la tarjeta.
Wiegand 26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El bit 1 es el bit de paridad par del 2 al 13 de 26 bits, mientras que el bit es el bit de paridad impar del 14 al 25. Del 2º al 9 bits son el código del sitio, mientras que los días 10 a 25 bits son el número de la tarjeta.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El bit 1 es el bit de paridad par del 2 al 17 bits, mientras que la 34bit es el bit de paridad impar de la 18 a 33 bits. La segunda a 25 bits son el número de la tarjeta.
Wiegand 34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Se compone de 34 bits de código binario. El bit 1 es el bit de paridad par del 2 al 17 bits, mientras que la 34bit es el bit de paridad impar de la 18a 33bits. Del 2º al 9 bits son el código del sitio, mientras que los días 10 a 25 bits son el número de la tarjeta.
Wiegand 36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El bit 1 es el bit de paridad impar de la 2ª a 18 bits, mientras que la 36bit es el bit de paridad par de la 19ª a 35bits. Del 2 al 17 bits son el código del dispositivo, la 18ª a 33 bits son el número de la tarjeta, y la 34ª a 35 bits son el código de fabricante.

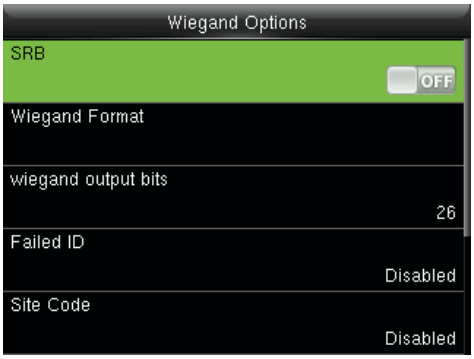
Wiegand 36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consta de 36 bits de código binario. El bit 1 es el bit de paridad par de 2a a 18 bits, mientras que la 36 bit es el bit de paridad impar de la 19ª a 35bits. Del 2º al 19 bits son el código del dispositivo, y la 20ª a 35 bits son el número de la tarjeta.
Wiegand 37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE Consta de 37 bits de código binario. El bit 1 es el bit de paridad impar de la 2ª a 18 bits, mientras que la 37 bit es el bit de paridad par de la 19ª a 36 bits. La 2ª a 4 bits son el código de fabricante, el 5º a 16 bits son el código del sitio, y la 21ª a 36 bits son el número de la tarjeta.
Wiegand 37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consta de 37 bits de código binario. El bit 1 es el bit de paridad par de 2a a 18 bits, mientras que la 37 bit es el bit de paridad impar de la 19ª a 35 bits. La 2ª a 4 bits son el código de fabricante, 5º a 14 bits son el código del dispositivo, de 15 y 20 bits son el código del sitio, y la 21ª a 36 bits son el número de la tarjeta.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 50 bits de código binario. El bit 1 es el bit de paridad par de 2a a 25 bits, mientras que la 50bit es el bit de paridad impar de la 26ª a 49 bits. Del 2 al 17 bits son el código del sitio, y 18ª a 49 bits son el número de la tarjeta.

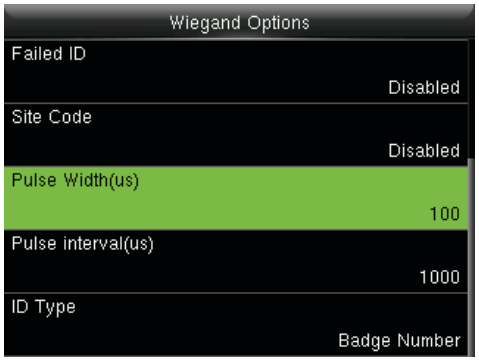
Nota: **C** denota el número de tarjeta, **E** indica número bit de paridad, **O** denota bit de paridad impar, **F** denota el código del dispositivo, **M** denota el código de fabricante, **P** denota el bit de paridad, y **S** indica el código del sitio.

6.5.2 Salida Wiegand

Salida Wiegand conector admite SRB, o conecta el dispositivo como un dispositivo esclavo en otro dispositivo (dispositivo maestro), formando un sistema maestro/esclavo.







BRS: Seleccione **[On]** para activar la función de SRB, mientras que la elección de **[OFF]** Puede desactivar la función.

Formato Wiegand: el usuario puede elegir entre los siguientes formatos Wiegand incorporada: Wiegand 26, Wiegand 26A, Wiegand 34, Wiegand 34, Wiegand 36, Wiegand 36A, Wiegand 37, Wiegand 37a y Wiegand 50. Múltiples opciones están disponibles, pero el formato Wiegand real dependerá de la opción **[Salida Wiegand bits].**

Por ejemplo: Si el 26-bit Wiengand 26, 34-bit Wiegand 34a, 36-bits Wiegand 36, 37-bit Wiegand 37a y el 50-bit Wiegand de 50 son elegidos en **[Formato Wiegand]** de 36 bits, pero es seleccionado en **[salida Wiegand bits]**, entonces el actual formato Wiegand para uso será Wiegand de 36 bits-36.

Salida Wiegand bits: Número de bits de datos Wiegand. Después de elegir [salida Wiegand bits], el dispositivo utilizará el número de bits para encontrar el adecuado formato Wiegand en **[Formato Wiegand].**

Error ID: Se define como el valor de la producción ha fallado la verificación del usuario. El formato de salida depende del formato **[Configuración Wiegand]**. El valor predeterminado varía de 0 a 65535.

Código de sitio: es similar a la ID de dispositivo excepto que puede ajustarse manualmente y repetible con diferentes dispositivos. El valor predeterminado varía de 0 a 256.

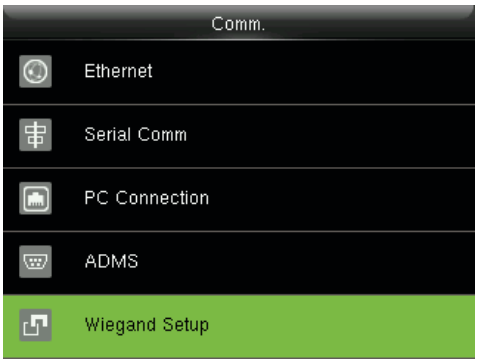
Anchura de pulso (US): La anchura de pulso enviado por Wiegand. El valor predeterminado es de 100 microsegundos, lo cual se puede ajustar dentro del rango de 20 a 100 microsegundos.

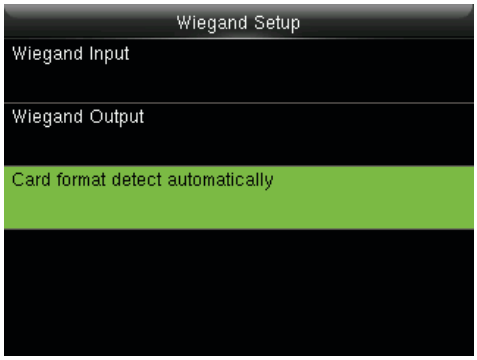
Intervalo de pulso (US): El valor predeterminado es 1000 microsegundos, lo cual puede ajustarse dentro del rango de 200 a 20000 microsegundos.

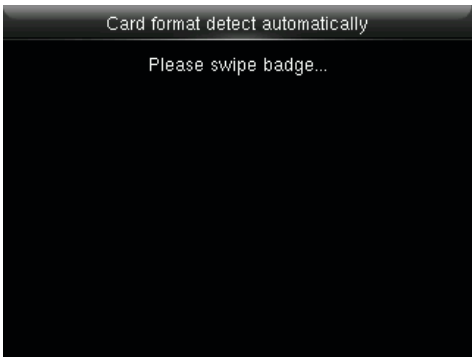
Tipo de ID: Contenido de salida tras el éxito de la verificación. ID de usuario o número de tarjeta puede ser elegida.

6.5.3 Detectar automáticamente el formato de la tarjeta

[Detectar automáticamente el formato de la tarjeta] pretende ayudar a los usuarios con rapidez a detectar el tipo de tarjeta y su correspondiente formato. Varios formatos de tarjeta están predefinidas en el dispositivo. Después de pasar la tarjeta, el sistema lo detectará como números de tarjeta diferentes según cada formato; sólo requiere que el usuario elija el elemento equivalente al número de tarjeta real y establecer el formato como el formato Wiegand para el dispositivo. Esta función también es aplicable a la función de lectura de tarjetas y lector Wiegand auxiliar.

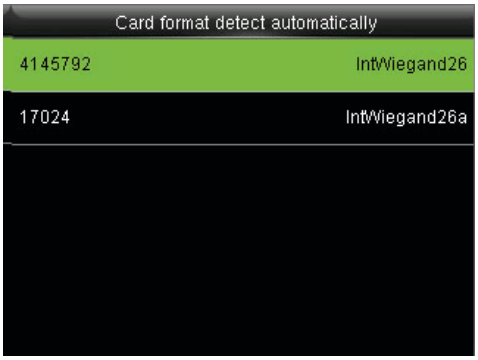




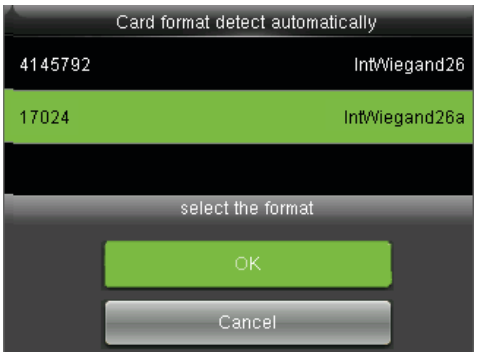


En la interfaz inicial, pulse **[M/OK] > Comm. > Configuración > Formato tarjeta Wiegand Detectar Automáticamente** al introducir el formato de la tarjeta de interfaz detecte automáticamente.

Procedimiento de funcionamiento:



1. Tras ingresar a la interfaz [Detectar Formato de Tarjeta Automáticamente] de un ID de dispositivo, pase la tarjeta de identificación del lector de tarjeta (anteriormente n el dispositivo local o lector de tarjeta auxiliar), la interfaz mostrará el formato Wiegand que detecta automáticamente y el análisis de los números de tarjetas.

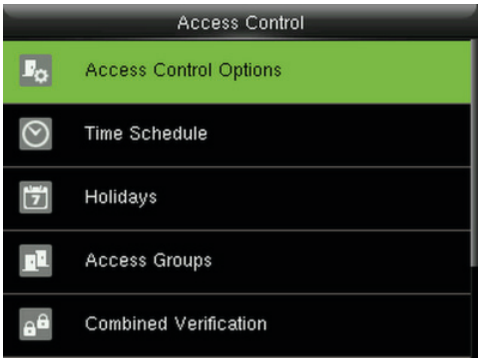


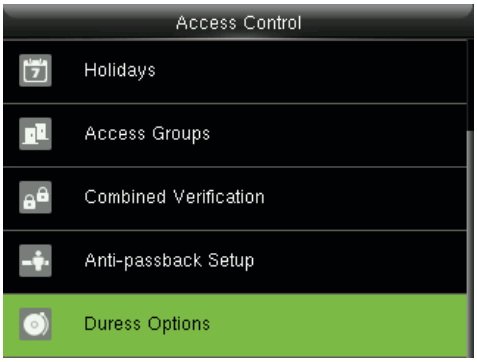
2. Elija el elemento correspondiente al número de tarjeta real del dispositivo [Formato Wiegand], que es el formato Wiegand para leer este tipo de tarjeta.

Comentarios:
En la interfaz [Detección de formato automática de Tarjeta] de un IC de dispositivo, el dispositivo no puede detectar el número de tarjeta o formato Wiegand sólo por pasar una tarjeta IC. Para detectar el formato Wiegand de tarjeta IC, es necesario conectar un lector de tarjetas IC con el dispositivo y pase una tarjeta IC encima del lector de tarjeta auxiliar, de modo que el dispositivo mostrará el número de la tarjeta y el formato Wiegand.

7 Control de Acceso

La opción de control de acceso se utiliza para establecer el horario, vacaciones, Grupos de Acceso, combinados, etc., la verificación de los parámetros relacionados con el dispositivo para controlar el bloqueo y otros dispositivos.





En la interfaz inicial, pulse **[M/OK] > Control de acceso** para entrar a la interfaz configuración de Control de acceso.

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

1. El tiempo de acceso del usuario cae dentro o personal del usuario, grupo o Zona horaria.

2. Grupo del usuario debe estar en el acceso combinado (cuando hay otros grupos en el mismo tipo de acceso, verificación de miembros de estos grupos son también necesarios para desbloquear la puerta).

En la configuración predeterminada, los nuevos usuarios son asignados en el primer grupo con el grupo predeterminado de zona horaria y tipo de acceso como "1", y en estado de desbloqueo.

7.1 Ajuste de las Opciones de Control de Acceso

En la interfaz inicial, pulse **[M/OK] > Control de Acceso > Opciones de Control de Acceso** para entrar en la configuración de la interfaz de Opciones de control de acceso.

Retraso de la cerradura de la puerta (s): El período de tiempo de desbloqueo (a partir de la apertura de la puerta para cerrar automáticamente) tras la cerradura electrónica recibe una señal abierta enviada desde el dispositivo (el valor varía de 0 a 10 segundos).

Sensor de puerta delay (s): Cuando se abre la puerta, el sensor de la puerta se comprobará después de un período de tiempo; si el estado del sensor de puerta es incompatible con el modo de sensor de la puerta, la alarma se activará. El periodo de tiempo es el **retardo del sensor de puerta** (valor varía de 0 a 255 segundos).

Tipo de sensor de puerta: No incluye, **normalmente abierto** y **normalmente cerrado. No** significa que el sensor de la puerta no está en uso; **normalmente abierto** significa abrir la puerta cuando la electricidad está encendida; **normalmente cerrado** significa que la puerta está cerrada cuando la electricidad está encendida.

Retardo de alarma de puerta (s): Cuando el estado del sensor de puerta es incompatible con este tipo de sensor de la puerta, la alarma se activará después de un período de tiempo; este período de tiempo es el r**etardo de la alarma** de la puerta (el valor varía de 1 a 999 segundos).

Tiempos de reintento de alarma: cuando el número de errores de verificación alcanza el valor establecido (el valor varía de 0 a 9 veces), se activa la alarma. Si el valor es 0, la alarma no se activará después de que falló la verificación.

NC Periodo de Tiempo: Período de tiempo para definir el período de tiempo para el modo normalmente cerrado, de forma que nadie pueda acceder durante este período.

NO Periodo de Tiempo: para definir el período de tiempo de normalmente abierto, de modo que la puerta siempre está desbloqueado durante este período.

Configuración de entrada auxiliar: Para establecer la **salida Aux/Bloquear tiempo abierto y tipo de salida Aux** para el dispositivo con conector auxiliar. Salida Aux tipo incluye ninguno, desencadenan la puerta abierta, disparador de alarma y disparo de alarma y puerta abierta.

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

Vacaciones: válido para establecer si NC Periodo o ninguna configuración del período de tiempo son válidas en tiempo de vacaciones. Seleccione [Sí] para permitir que el conjunto NC o ningún período de tiempo en vacaciones.

Alarma: Altavoz cuando [el altavoz] de alarma está activada, el altavoz provocará una alarma cuando el dispositivo está siendo desmantelada.

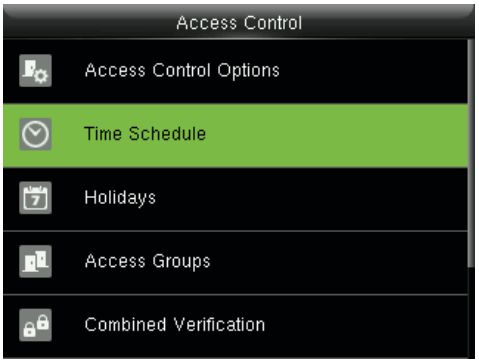
Restablecer la configuración de acceso: para restablecer los parámetros de retardo de la cerradura de la puerta, sensor de puerta, sensor de puerta tipo delay, retardo de alarma de puerta, tiempos de reintento para alarma, NC Periodo de tiempo, ningún plazo, configuración de entrada auxiliar, normalmente abrir / cerrar por vacaciones, altavoz, alarma anti-passback dirección, estado del dispositivo, función de alarma de coacción, en coincidencia 1:1, Alarma en 1: N PARTIDO, alarma en Contraseña y retardo de alarma. Sin embargo, el contenido de los datos de acceso, eliminación de datos [Mgt.] no se verán afectados.

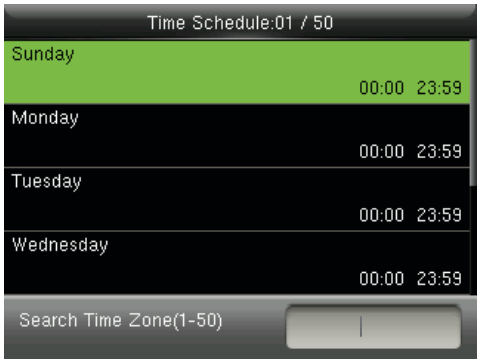
Parámetros de Acceso	Predeterminados de fábrica
Retardo de Puerta	10 s
Retardo Sensor de Puerta	10 s
Modo de sensor de puerta	No
Retardo Alarma de Puerta	30 s
Contador de Alarma	3 veces
Zona de Tiempo NC	No
Zona de Tiempo NO	No
Tiempo de Acceso de la Salida Auxiliar	255 s
Ajustes de Entrada Auxiliar	
Validez de Acceso en Vacaciones NO/NC	Apagado
Altavoz Alarma	Apagado
Dirección Anti-Passback	No Anti-Passback
Estatus del Dispositivo	Salida
Clave de Ayuda	Apagado
Alarma en Verificación 1:1	Apagado
Alarma en Verificación 1:N	Apagado
Alarma en Verificación por Contraseña	Apagado
Retardo de la Duración de Alarma	10 s

Comentarios:
Después de establecer el período de tiempo de NC, por favor, cierre bien la puerta así, de lo contrario, podría activarse la alarma durante el período de tiempo de NC.

7.2 Ajustes de Horario

Horario es la unidad mínima de tiempo de configuración de control de acceso; en la mayoría de los 50 horarios se pueden establecerse para el sistema. Cada horario consta de 7 secciones de tiempo (una semana), y cada sección es la hora válida en 24 hrs.



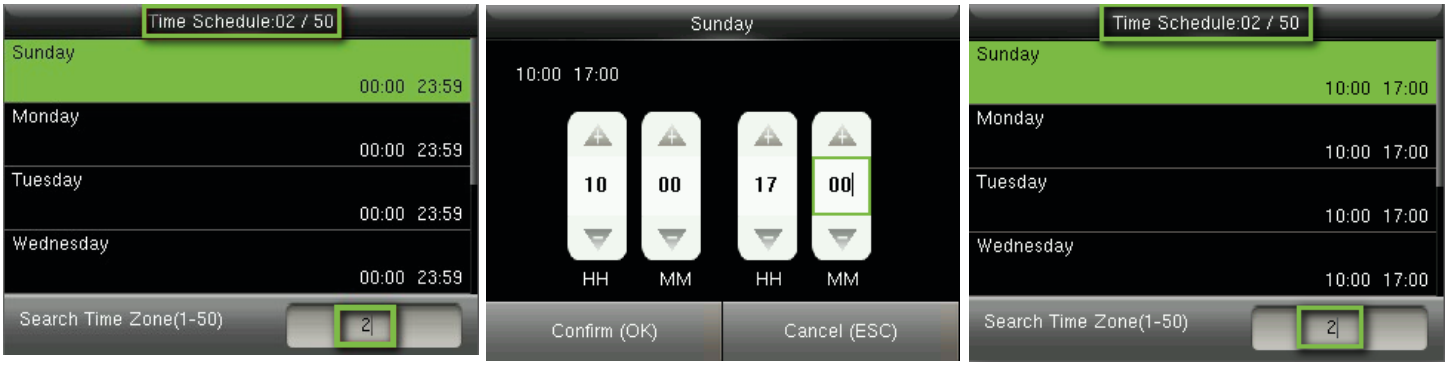


En la interfaz inicial, pulse **[M/OK] > Control de Acceso > Horario** para entrar en la interfaz de programación de tiempo. El horario predeterminado es el nº 1 (todo el día) válido, que puede editarse.

Válido Horario: 00:00 ~ 23:59 (todo el día) válida o cuando la hora de finalización es superior a la hora de inicio.

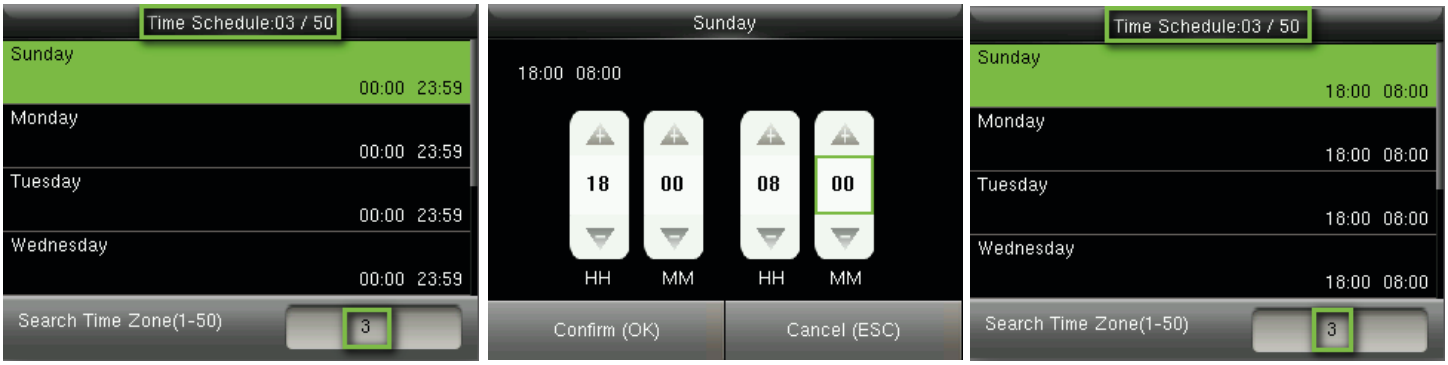
Horario no válido: cuando la hora final es menor que la hora de inicio.

Ejemplo 1: Ajuste horario 02 (Válido)



Establecerlo como 10:00 ~ 17:00, de domingo a sábado, desde la hora de finalización es superior a la hora de inicio, **Horario 2 es válido.**

Ejemplo 2: Ajuste horario 03 (no válido)



En **horario 3**, el diario el tiempo final es menor que la hora de inicio, así que el tiempo de la zona 3 no es válido.

Comentarios:
El horario no puede ajustarse en dos días, lo que significa que la hora de finalización debe ser mayor que la hora de inicio.

7.3 Ajustes de Días Festivos

El control de acceso para los días festivos, se puede ajustar el tiempo que es aplicable para todos los usuarios durante las vacaciones.

En el interfaz inicial, pulse **[M/OK] > Access Control > Días Festivos > Añadir** Vacaciones para entrar en la i nterfaz Añadir Festivo. La configuración incluye el número, la hora de inicio, hora de finalización y período de tiempo.

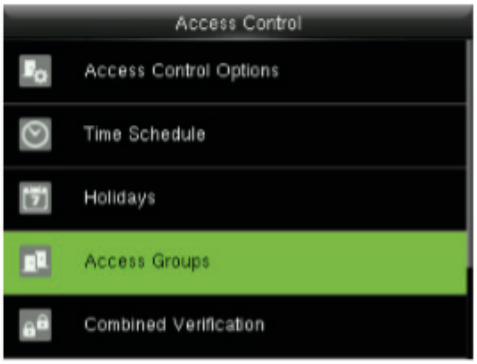
Comentarios:
Las fechas de inicio/finalización sólo se requiere establecer el mes (MM) y la fecha (DD), que es aplicable a todos los años. Como se muestra en la figura anterior: Vacaciones 2 comienza el 1 de mayo de cada año y finaliza el 3 de mayo de cada año, mientras que la adopción de período de tiempo 2 (10:00 ~ 17:00, de domingo a sábado).

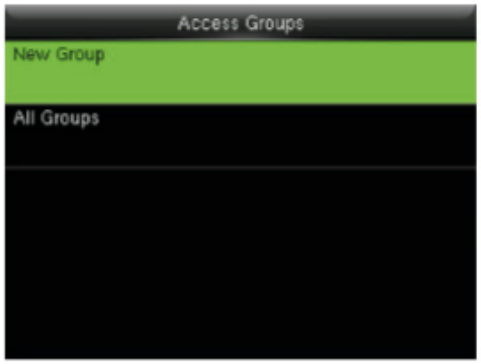
Para habilitar la función de días festivos:

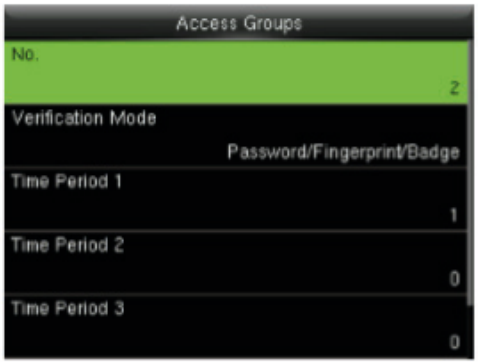
En la interfaz inicial, pulse [**M/OK] > Access Control > Grupos de Acceso > Todos los grupos >** seleccione un grupo de control de acceso>Editar>Incluir vacaciones, pulse **[M/OK]** para activar (ON) las vacaciones.
La activación/desactivación de la función de vacaciones es aplicable a todos los usuarios en el mismo grupo de acceso.

7.4 Ajustes de Grupos de Acceso

Agrupación es para administrar usuarios en grupos.
Los usuarios de grupo la zona horaria predeterminada es la zona horaria de grupo, mientras que los usuarios pueden establecer su propia zona horaria. Cada grupo puede definir 3 zonas horarias en la mayoría, siempre que uno de ellos es válido, el grupo puede ser verificado correctamente.
Por defecto, los nuevos matriculados usuario pertenece al Grupo de Acceso 1, y también puede ser asignado a otro grupo de acceso.

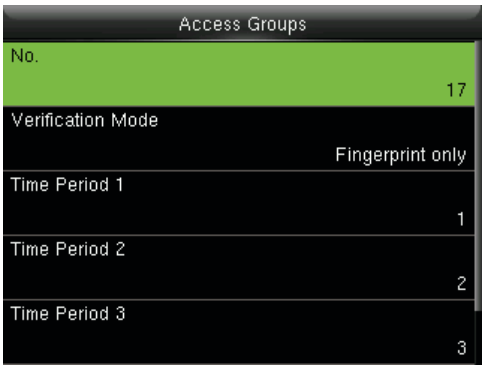


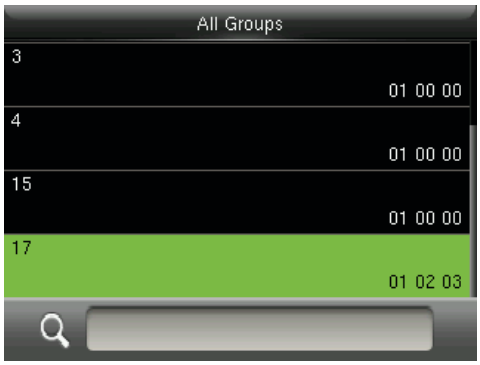




En la interfaz inicial, pulse **[M/OK] > Access Control > Grupos de Acceso > Nuevo Grupo** para introducir la nueva interfaz del grupo.

Tomando como ejemplo las ilustraciones siguientes:





Tal y como se muestra en las figuras anteriores, el **Modo de Verificación del Grupo de Acceso 17** es sólo de huellas dactilares; Zona Horaria 1, 2 y 3, mientras que la función de vacaciones está habilitado.

7.4.1 Establecer Vacaciones para Grupo de Acceso

Para habilitar la función de vacaciones:

Intervalo de tiempo configurado (incluido el acceso Calendario y horario de vacaciones) > Colocar vacaciones > Asignar usuarios a un grupo del acceso > Seleccione [incluir feriados] del grupo de acceso a [ON].

Comentarios:

1. Cuando la función de vacaciones está habilitado, sólo cuando los calendarios de grupo de acceso y las vacaciones se superponen los miembros pueden tener acceso.

2. Cuando la función de vacaciones está desactivado, el tiempo de acceso de los usuarios de un grupo de acceso no se verán afectados.

Por ejemplo:

Si el Grupo de Acceso 2 requiere para utilizar el tiempo de vacaciones en la Lista 2, Día Internacional del trabajador, lo que significa que permite a los usuarios acceder durante las 10:00 ~ 17:00 (Horario 2) del 1 al 3 de mayo.

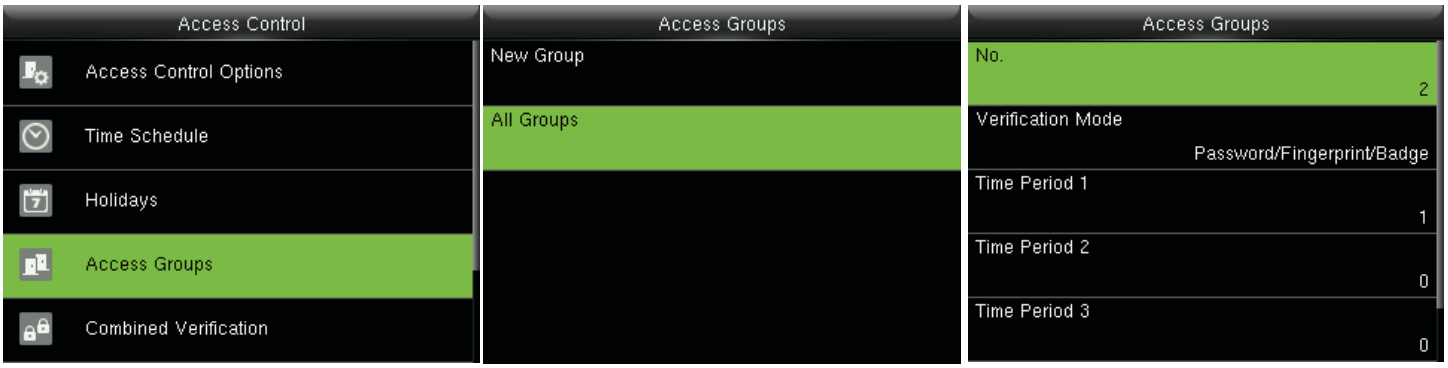
Método de funcionamiento:

1. Establezca Horario de 2 a 10:00 ~ 17:00, de domingo a sábado. Para el método de configuración, consulte el ejemplo de la configuración de la zona horaria 2 en 7.2 Ajustes de Horario.

2. Uso Horario 2 para pasar las vacaciones. Para el método de ajuste de vacaciones, por favor, consulte 7.3 Establecer días festivos.

3. Grupo de acceso de configuración, consulte 7.4 Configuración de los grupos de acceso para la instrucción.

4. **Habilitar la función de vacaciones.** En el interfaz inicial, pulse **[M/OK] > Access Control > Grupos de Acceso > Todos los grupos > 2 >** Pulse **[M/OK] > Editar > Incluir vacaciones,** pulse **[M/OK]** a la [incluir feriados] en **[ON]** (activado).



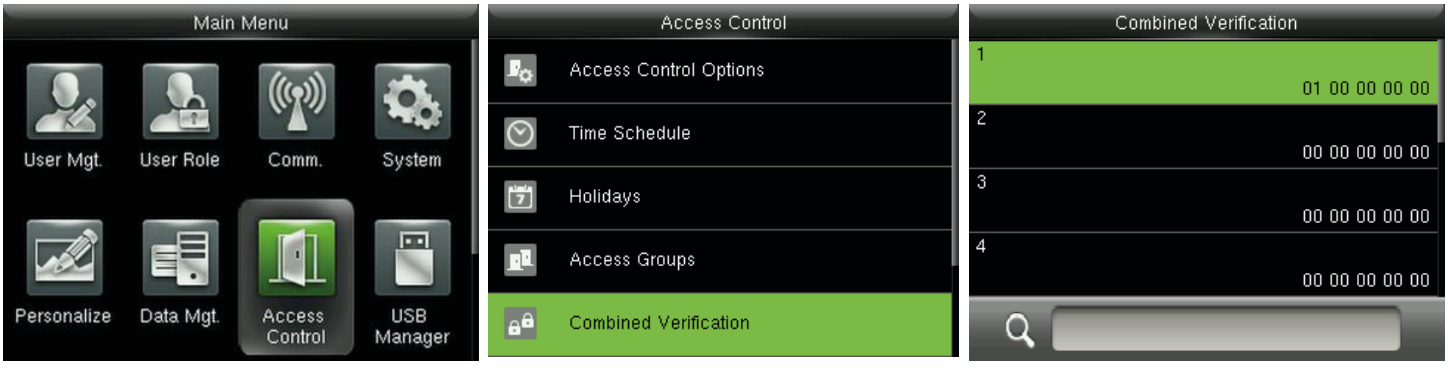
5. Los usuarios del grupo de acceso 2 compruebe para acceder, la configuración es correcta.

Comentarios:
Si un feriado debe ser válida para todos los usuarios, asignar a todos los usuarios del mismo grupo o activar el botón [incluir feriados] para todos los grupos de acceso.

7.5 Ajuste de Verificación Combinada

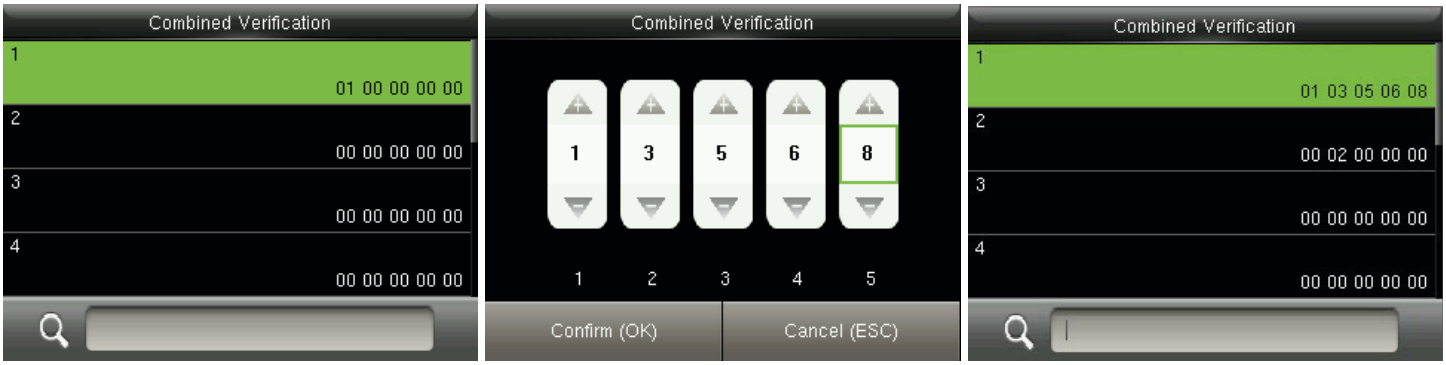
Combinar dos o más miembros para lograr multi-Verificación y mejorar la seguridad.
En una combinación de la verificación, el rango de número de usuario es: 0 <= N <= 5; los usuarios pueden pertenecer a un solo grupo, o pertenecen a 5 grupos diferentes a la mayoría.

Comentarios:
Sólo el No. de Grupo en la interfaz de grupo de acceso, puede seleccionar la opción de verificación de la combinada.

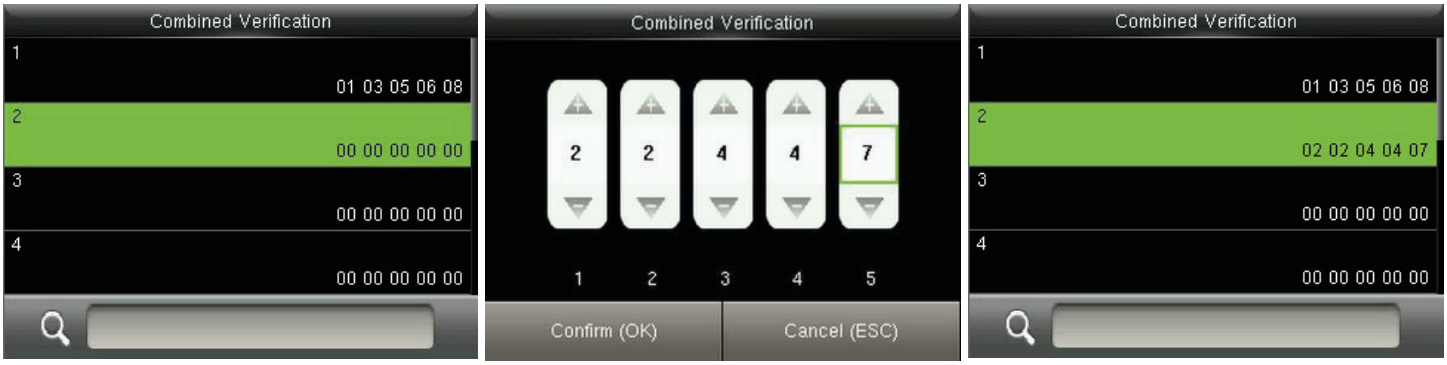


En el interfaz inicial, pulse [**M/OK] > Control de Acceso > Verificación combinado >** 1 para introducir la primera combinación de verificación Configuración de la interfaz.

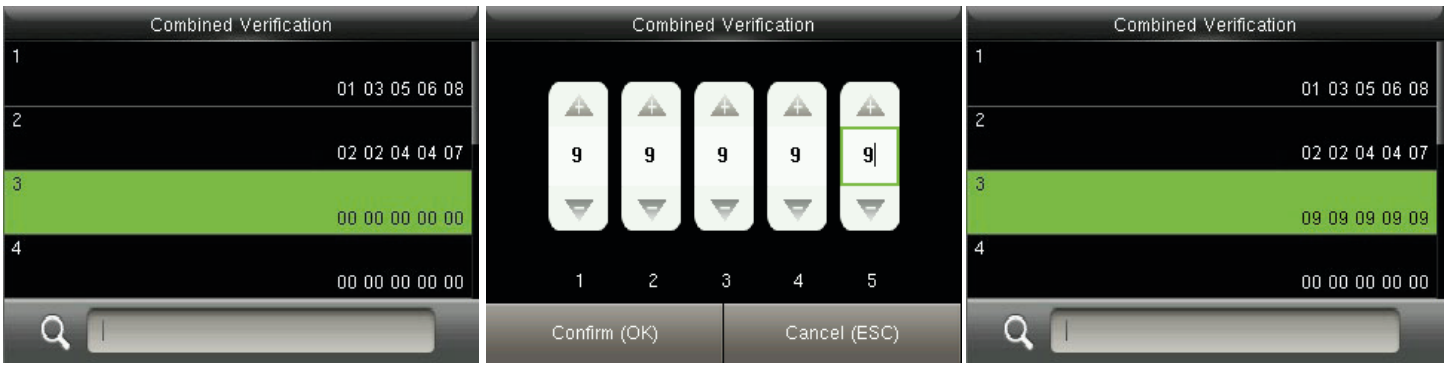
Por ejemplo (los siguientes grupos de acceso que se han definido en el grupo de acceso interface):



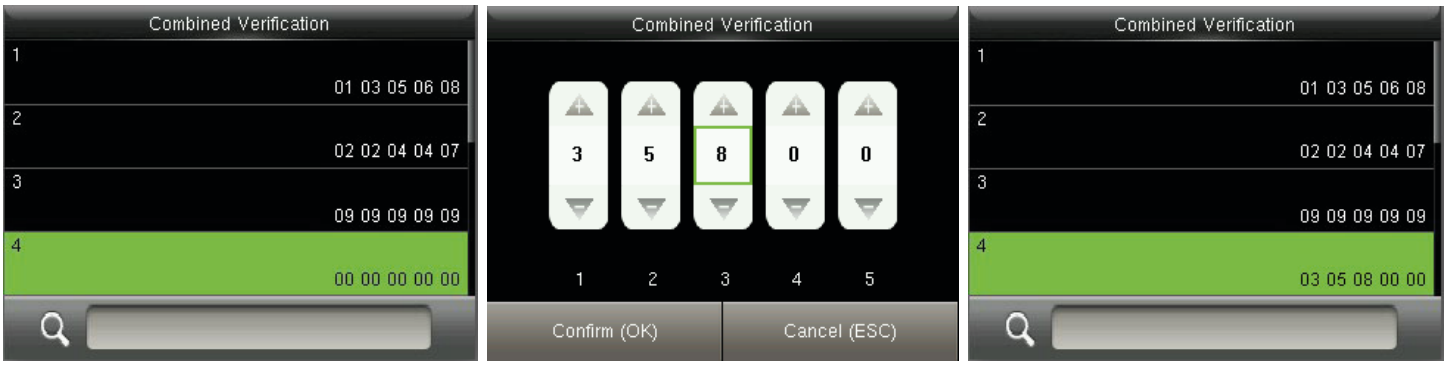
Como la figura anterior, Combinación de Verificación 1 está formado por cinco miembros procedentes de cinco grupos diferentes---grupo de acceso 1/3/5/6/8, respectivamente.



En la figura anterior, combinado la verificación 2 está formado por cinco miembros procedentes de tres grupos diferentes: dos miembros del Grupo de Acceso 2, dos del grupo 4, y uno del grupo 7.



En la figura anterior, combinado la verificación 3 está compuesto de cinco miembros, y todos ellos provienen del Grupo de Acceso 9.

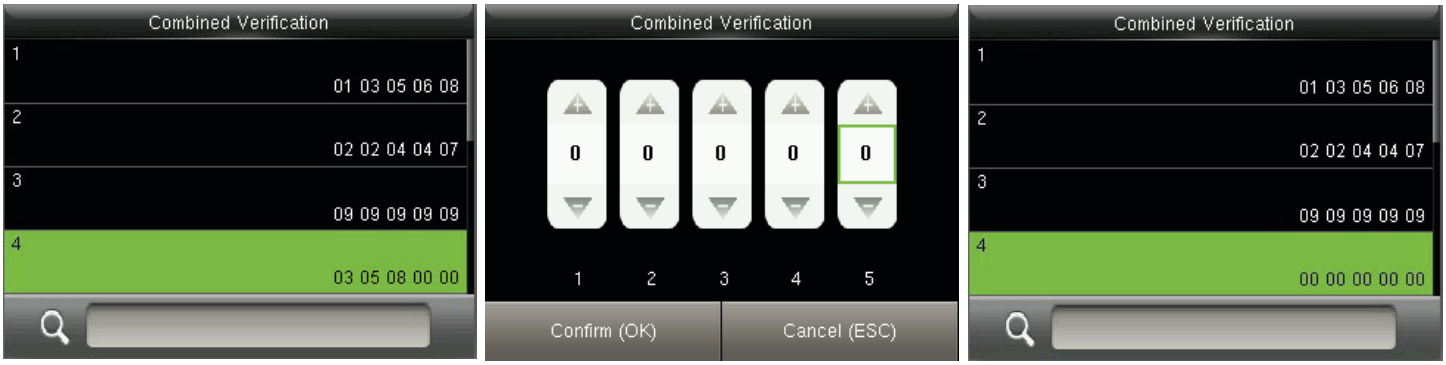


En la figura anterior, combinado verificación 4 se compone de tres miembros procedentes de tres grupos diferentes -- Grupo de Acceso 3, 5, 8 respectivamente.

Eliminación de una Verificación Combinada

Para eliminar una combinación de verificación, coloque el acceso de todos los integrantes del grupo en 0.

Por ejemplo, para eliminar la verificación combinado 4, por favor consulte las siguientes figuras:



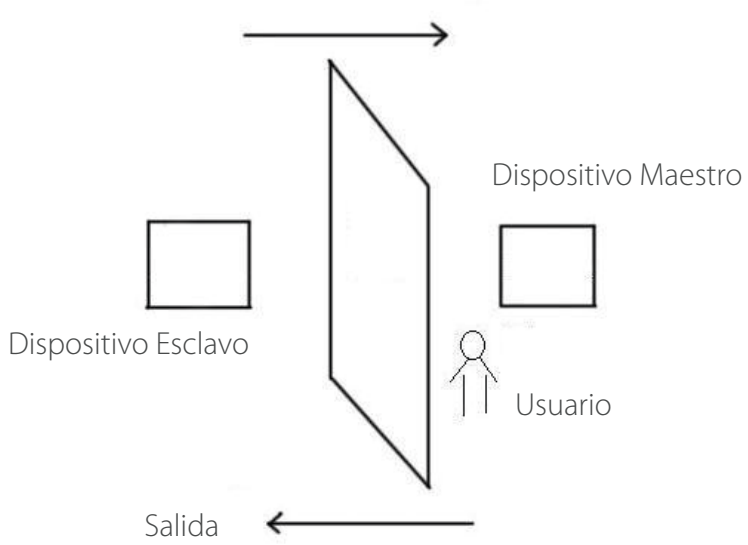
Si todos los números del grupo en una combinación de verificación 4 se establecen en 0, se eliminará.

7.6 Ajuste de Anti-Passback

Para evitar que algunas personas los siguientes usuarios para entrar en la puerta sin verificación, resultando en problemas de seguridad, los usuarios pueden activar la función Anti-Passback. El registro check-in debe coincidir con el registro de check-out para abrir la puerta.

Esta función requiere dos dispositivos para trabajar juntos: uno está instalado en el interior de la puerta (dispositivo maestro), el otro está instalado en el exterior de la puerta (dispositivo esclavo). Los dos dispositivos que se comunican a través de la señal Wiegand.

El formato y el tipo de salida Wiegand (ID de usuario/número de identificación), aprobado por el dispositivo maestro y esclavo dispositivo debe ser coherente.



En la interfaz inicial, pulse [M/OK] > Control de Acceso > Ajustes de Anti-Passback para introducir a la interfaz de configuración de Anti-Passback. Seleccione Anti-Passback dirección y estado del dispositivo.

- Dirección Anti-Passback

Sin Anti-Passback: Anti-Passback función está desactivada, lo que significa pasar la verificación de dispositivo maestro o esclavo dispositivo puede desbloquear la puerta. Estado de asistencia no está reservado.

Salida Anti-Passback: Después de que un usuario desprotege, sólo si el último registro es un Registro de check-in puede el usuario check-out de nuevo; de lo contrario, se disparará la alarma. Sin embargo, el usuario puede controlar libremente.

Entrada Anti-Passback: Después de que un usuario comprueba, sólo si el último registro es un Registro de check-out el usuario puede comprobar de nuevo; de lo contrario, se disparará la alarma. Sin embargo, el usuario puede controlar libremente.

Entrada/Salida Anti-Passback: Después de que un usuario comprueba entrada/salida, sólo si el último registro es un Registro de check-out el usuario puede comprobar de nuevo o un Registro de check-in, el usuario puede comprobar de nuevo; de lo contrario, se disparará la alarma.

Nulo y Guardar: Anti-Passback función está desactivada, pero la asistencia estatal está reservado.

- Estatus del Dispositivo

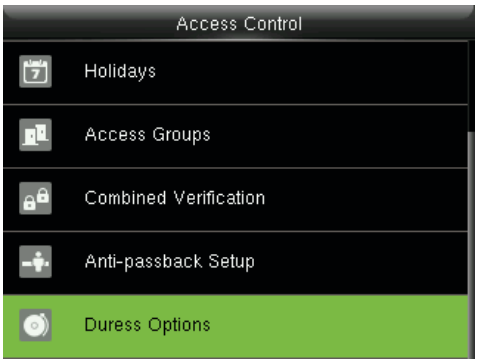
Ninguno: el estado del dispositivo para desactivar la función Anti-Passback.

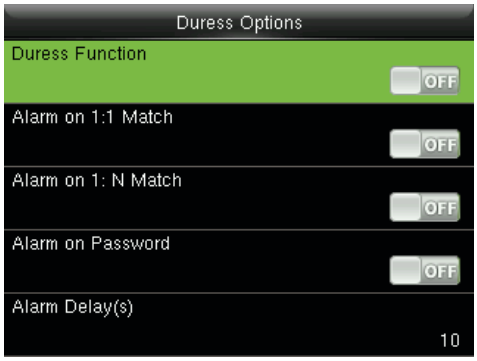
Salida: Todos los registros del dispositivo se registran en el check-out.

Entrada: Todos los registros en el dispositivo son registrados en check-in

7.7 Ajuste de Opciones de Coacción

Cuando los usuarios llegan a través de la coacción, seleccione el modo de alarma de coacción, el dispositivo se encargará de abrir la puerta como de costumbre y enviar la señal de alarma





En la interfaz inicial, pulse **[M/OK] > Control de Acceso > Opciones de Coacción** para entrar en la interfaz de configuración de opciones de coacción.

Comentarios:

Los cuatro tipos de métodos de activación de alarma de coacción (Función de alarma de coacción, en coincidencia 1:1, Alarma en 1:N y alarma en contraseña) están activados **[OFF]** en la configuración predeterminada.

Función Coacción: coacción en estado **[ON],** pulse la tecla "coacción" y, a continuación, presione cualquier huella registrada (en 10 segundos), la alarma de coacción será desencadenada tras el éxito de la verificación. En estado **[OFF]**, pulsando "coacción" clave no activará la alarma.

Alarma en 1:1: que coinciden en estado **[ON]**, cuando un usuario utiliza 1:1 Método de verificación para verificar cualquier huella registrada, la alarma se activará. En **[OFF]** Estado, ninguna señal de alarma se activará.

Alarma en 1:N: coincidencia en estado **[ON]**, cuando un usuario utiliza un método de verificación 1:N para verificar cualquier huella registrada, la alarma se activará. En estado **[OFF]**, ninguna señal de alarma se activará.

Alarma en Contraseña: En estado **[ON]**, cuando un usuario utiliza el método de verificación de la contraseña, la alarma se activará. En estado [OFF], ninguna señal de alarma se activará.

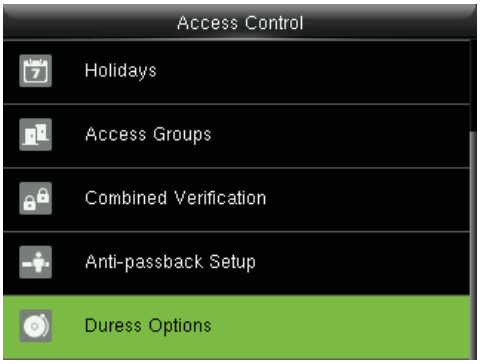
Retardo de alarma (s): Cuando se activa la alarma de coacción, el dispositivo enviará una señal de alarma después de 10 segundos (por defecto); el tiempo de retardo de la alarma puede modificarse (el valor varía de 0 a 999 segundos).

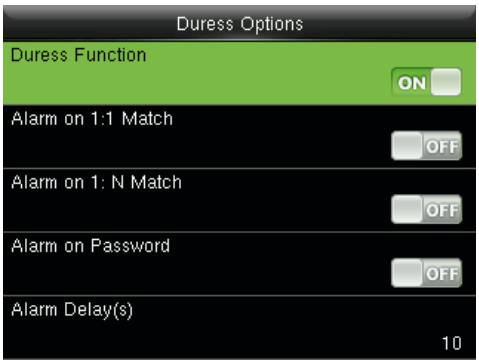
7.7.1 Ajuste de la Clave de Coacción

Función Coacción: en estado **[ON],** pulse la tecla "coacción" y, a continuación, presione cualquier huella registrada (en 10 segundos), la alarma de coacción será desencadenada tras el éxito de la verificación. En estado **[OFF]**, pulsando "coacción" clave no activará la alarma.

Para establecer M/OK como coacción clave

1. **Activar la función de coacción:** En la interfaz inicial, pulse **[M/OK] > Control de Acceso> Opciones > Función de coacción**, pulse **[M/OK]** para activar la función de coacción **[ON]**.



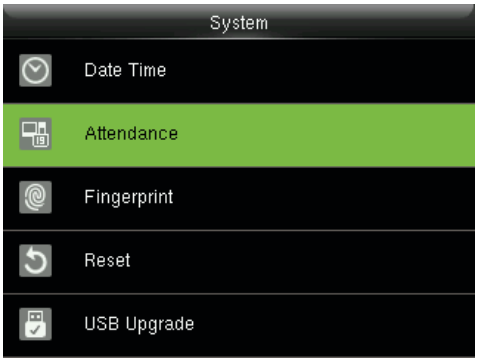


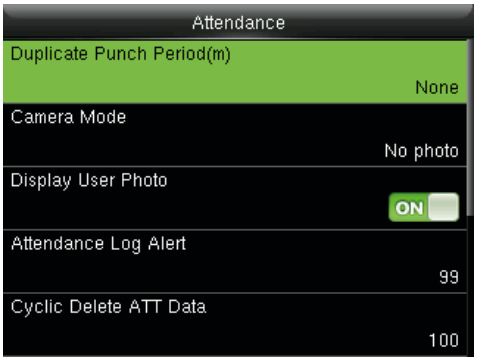
2. **Configuración de clave de coacción:** En la interfaz inicial, pulse **[M/OK] > Personalizar > Asignaciones de teclas de método abreviado >** seleccione **[M/OK]** > pulse **[M/OK] > Función** > Seleccione la opción "**Clave de coacción".** (La clave de coacción menú se mostrará después de la coacción, la función está activada).

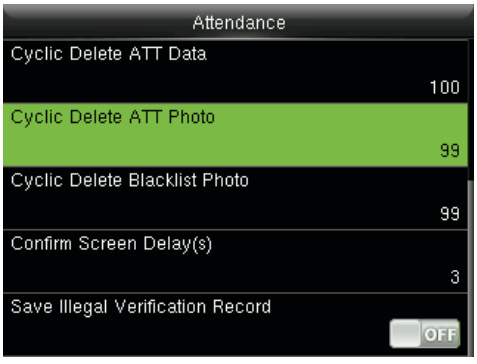
Comentarios:
Teclas de dirección o ESC también se pueden establecer como clave de coacción.

8 Ajuste del Sistema

8.1 Parámetros de Asistencia







En la interfaz inicial, pulse **[M/OK] > Sistema > Asistencia** para entrar en configuración de la interfaz.

Duplicar Punch Período (m): Dentro de un período determinado de tiempo (minutos), la presencia de registros duplicados no se reservan (valor oscila entre 1 y 999999 minutos).

Modo de cámara: Para definir si desea tomar y guardar fotos de verificación; aplicables a todos los usuarios. Los cinco modos siguientes se incluyen:

1. **No hay foto:** Ninguna foto es tomada en la verificación del usuario.
2. **Tomar foto, sin guardar:** tomar la foto pero no se guarda en la verificación.
3. **Tomar foto y guardar:** foto y se guarda en la verificación.
4. **Guardar en verificación satisfactoria:** foto y se guarda en una verificación efectiva.
5. **Guardar en falló la verificación:** foto es tomada y guardado en falló la verificación.

Mostrar el usuario Foto ★: establecer el usuario foto para que aparezca cuando un usuario pasa la verificación. Gírela [EN] para mostrar el usuario foto y [OFF] para desactivarla.

Registro de asistencia Alerta: cuando el resto de almacenamiento es menor que el valor establecido, el dispositivo de alerta automáticamente a los usuarios a la información de almacenamiento restante. Puede ser desactivado o configurado en un valor varió de 1 a 9999.

Eliminar datos cíclicos ATT: El número de registros de asistencia pueden ser eliminados en un tiempo cuando el almacenamiento máximo es alcanzado. Puede ser desactivado o configurado en un valor varió de 1 a 999.

Eliminar cíclica ATT Foto ★: El número de asistentes fotos permitidas para ser eliminado en un tiempo cuando el almacenamiento máximo es alcanzado. Puede ser desactivado o configurado en un valor varió de 1 a 99.

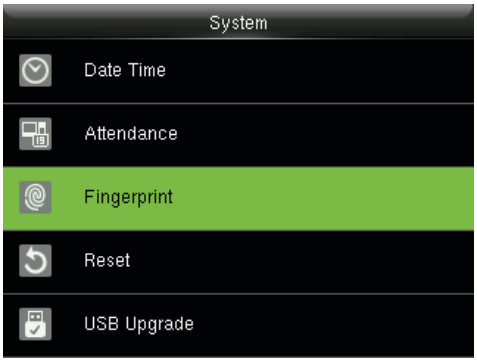
Eliminar cíclica lista negra Foto: El número de lista negra fotos permitidas para ser eliminado en un tiempo cuando el almacenamiento máximo es alcanzado. Puede ser desactivado o configurado en un valor varió de 1 a 99.

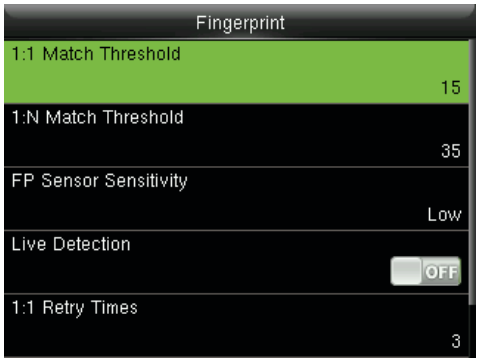
Pantalla de confirmación Delay(s): La visualización de la información de verificación interfaz después de la verificación. El valor varía entre 1 a 9 segundos.

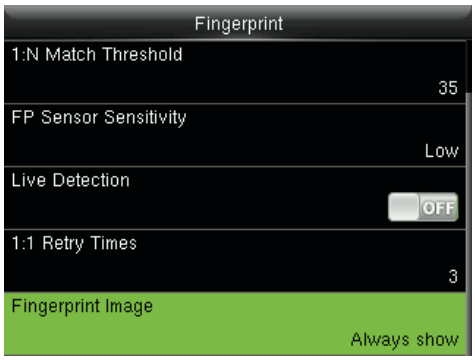
Por ejemplo, si la pantalla Confirmar Delay(s) está ajustado a 5s, tras el éxito de la verificación, la información de verificación interfaz será cerrada después de 5s.

Guardar registro de verificación ilegales: Para establecer si han fallado las verificaciones, tales como aquellos causados por el acceso en horarios no válido o ilegal verificación combinado, se guardará cuando la función de control de acceso avanzado está activado.

8.2 Parámetros de la Huella Digital







En la interfaz inicial, pulse **[M/OK] > System > Huellas Digitales** para entrar en la configuración de la interfaz.

Coincidencia Umbral 1:1: Por debajo del Método de verificación 1:1, sólo cuando la similitud entre la verificación de las huellas dactilares y las huellas dactilares registradas del usuario es mayor que este valor puede tener éxito la verificación.

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

Umbral de coincidencia recomendado:

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

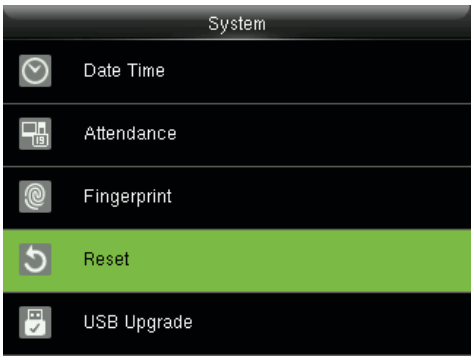
FP Alta Baja sensibilidad del sensor: Para ajustar la sensibilidad de la colección de huellas dactilares. Se recomienda utilizar el nivel predeterminado "medio". Cuando el ambiente está seco, resultando en la detección de huellas dactilares lento, puede establecer el nivel de "Alto" para aumentar la sensibilidad; cuando el ambiente es húmedo, con lo que resulta difícil identificar las huellas dactilares, puede establecer el nivel a "Bajo".

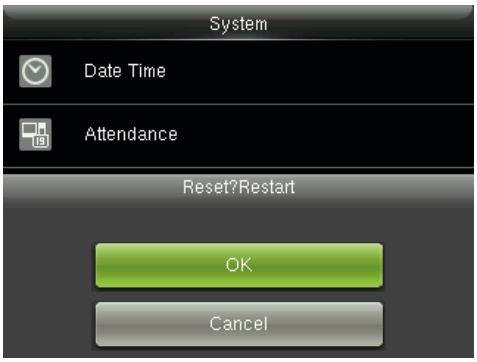
1:1 veces Reintentar: En 1:1, la verificación o la verificación de la contraseña, los usuarios podrían olvidar la huella registrada o contraseña, o pulse el dedo inadecuadamente. Para reducir el proceso de re-introducir el ID de usuario, reintento es permitido; el número de reintentos pueden estar dentro de 1~9.

Imagen de la huella: Para definir si desea mostrar la imagen de la huella en la pantalla de registro o de verificación. Cuatro opciones disponibles: show para inscribirse, show para coincidir, mostrar siempre, ninguno.

8.3 Ajuste del Reinicio a Valores de Fábrica

Restablecer datos como comunicación ajustes y configuraciones del sistema a los ajustes de fábrica.





En el interfaz inicial, pulse **[M/OK] > System > Reiniciar > OK** para finalizar el ajuste.

Restablecer los parámetros incluyen opciones de Control de acceso, opciones de coacción, Anti-Passback instalación, ajuste de comunicación (es decir, la configuración de Ethernet, Serial Comm., conexión para PC, ADMS ★ y Ajustes Wiegand), Personalizar (como mensaje de voz, indicador de teclado, el volumen y el tiempo de inactividad para dormir), cierre punch estado, etc.

Parámetros	Por defecto
Opciones de Control de Acceso	Retardo de puerta: 10 seg
	Retardo del sensor de puerta: 10 seg
	Tipo de sensor de puerta: Ninguno
	Retardo de alarma de puerta: 30 seg
	Tiempos de reintento de alarma: 3 veces
	Periodo de Tiempo NC: Ninguno
	Periodo de Tiempo NO: Ninguno
	Tiempo de la apertura auxiliar de la puerta: 225 seg
	Ajustes del Tipo de Salida auxiliar: puerta abierta trigle.
	Altavoz de la alarma: Apagado
Opciones de Amago	Función de Amago: Apagado
	Alarma de Verificación 1:1: Apagado
	Alarma de Verificación 1:N: Apagado
	Alarma de Contraseña: Apagado
	Retardo de Alarma: 10 seg
Anti-Passback	No Anti-passback
Ethernet	Sub-máscara de Red: 255. 255. 255.0
	Gateway: 0.0.0.0

Conexión PC	Clave de Comunicación:
	ID de Dispositivo: 1
ADMS ★	Nombre de Dominio Habilitado: Apagado
	Dirección de Servidor: 0.0.0.0
	Puerto del Servidor: 8081
	Habilitar Servidor Proxy: Encendido
	IP Servidor de Proxy: 0.0.0.0
	Puerto del Servidor Proxy: 0
Ajustes Wiegand	Ancho de pulso: 100 us
	Intervalo de pulso: 1000 us
Tiempo de muestra barra lateral	30 segundos
Tiempo de reposo	30 minutos
Menú en pantalla	30 segundos
Teclado	Encendido
Voz Altavoz	Encendido
Volumen	70

Comentarios:
Cuando se restablecen los ajustes de fábrica, la fecha y la hora no se verán afectados. Por ejemplo, si la fecha y la hora del dispositivo se establecen en 18:30 el 1 de enero de 2020, la fecha y la hora se mantienen inalterados después de restablecer los ajustes de fábrica.

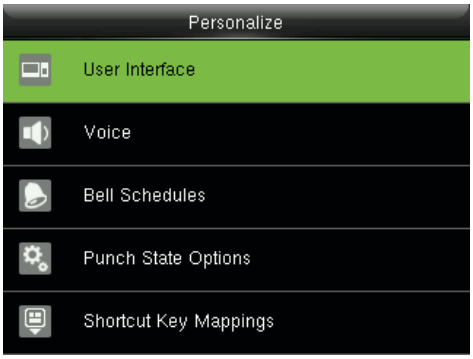
8.4 Actualización por USB

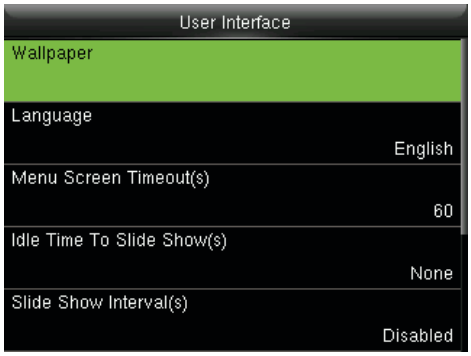
Inserte el disco con el archivo de actualización en el puerto USB del dispositivo, y en la interfaz inicial, pulse **[M/OK] > Sistema > Actualización USB** para completar la operación de actualización de firmware.

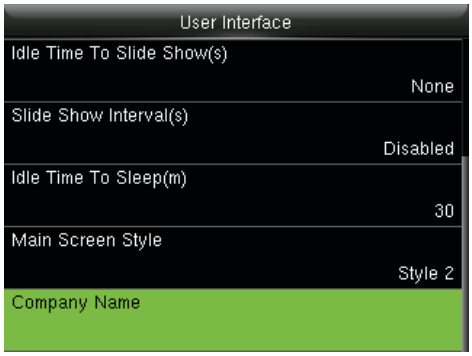
Nota: Si el archivo de actualización es necesaria, póngase en contacto con soporte técnico. Actualización de firmware no se ha retomado en circunstancias normales.

9 Personalizar Ajustes

9.1 Ajuste de la Interfaz de Usuario







En la interfaz inicial, pulse **[M/OK] > Personalizar > Interfaz de usuario** para la configuración de la interfaz de usuario.

Tapiz: Seleccione el papel tapiz de la pantalla principal como se requiere, puede encontrar fondos de pantalla de varios estilos en el dispositivo.

Idioma: Seleccione el idioma del dispositivo, según sea necesario.

Tiempo de espera de la pantalla de menú (s): Cuando no hay ninguna operación en la interfaz de menú y el tiempo supera el valor establecido, el dispositivo automáticamente saldrá a la interfaz inicial. Puede desactivar o ajustar el valor de 60~99999 segundos.

Comentarios:
Si se elige **[Desactivado],** el sistema no va a salir de la interfaz de menú incluso cuando no hay ninguna operación. **La desactivación de esta función no es recomendable debido a la gran potencia utilizada y la inseguridad.**

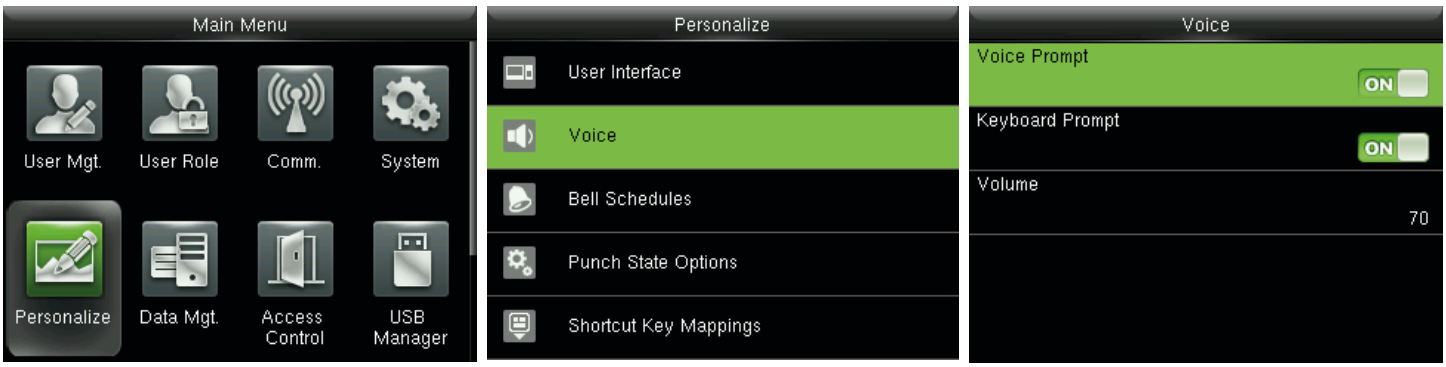
El tiempo de inactividad para presentación de diapositivas (s): Cuando no hay ninguna operación en la interfaz inicial y el tiempo supera el valor establecido, una presentación de diapositivas será mostrado. Puede ser desactivado (en **"None")** o establecer en 3~999 segundos.

Intervalo entre diapositivas (s): se refiere al intervalo entre la visualización de diferentes imágenes de presentación. Puede ser desactivado o configurado en 3~999 s.

El tiempo de inactividad para dormir (m): Cuando no hay ninguna operación en el dispositivo y el tiempo de reposo es alcanzado, el dispositivo entrará en modo de espera. Pulse cualquier tecla o el dedo para cancelar el modo de espera. Puede desactivar esta función, o establecer el valor de 1~999 minutos. Si esta función está activada a [Desactivado], el dispositivo no podrá entrar en modo de espera.

Comentarios:
La desactivación de esta función no es recomendable debido a la gran potencia utilizada.
Pantalla principal: Elegir el estilo y las formas de posición el reloj y el estado clave.
Nombre de la empresa: Introducir el nombre de la empresa de software relacionado

9.2 Ajuste de Voz



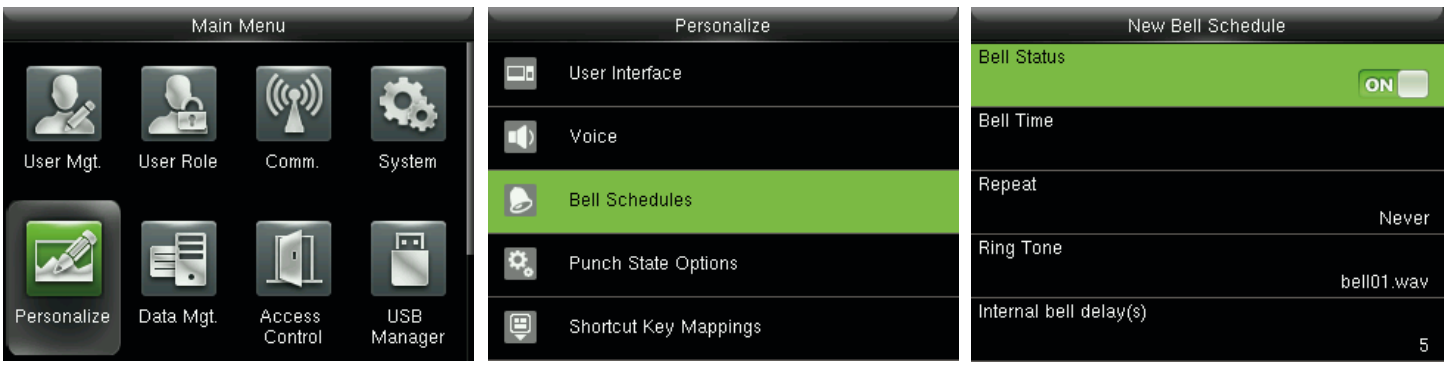
En la interfaz inicial, pulse **[M/OK] > Personalizar > Voz** para entrar en la interfaz de configuración de voz.

Mensaje de voz: Seleccione si desea activar mensajes de voz durante la operación, pulse [M/OK] para activarlo.
Indicador de teclado: seleccione si desea activar el sonido de teclado mientras presiona el teclado, presione **[M/OK]** para activarlo.

Volumen: Ajuste el volumen del dispositivo. Pulse ► clave para aumentar el volumen, pulse la tecla ◄ para disminuir el volumen.

9.3 Ajuste de Timbre

Muchas empresas optan por usar el timbre para significar en servicio y fuera de servicio. Cuando se alcanza la hora programada para el timbre, el dispositivo reproducirá el tono seleccionado automáticamente hasta que la llamada se pasa de duración.



En la interfaz inicial, pulse **[M/OK] > Personalizar > Horarios Timbre > Ajuste Nuevo Timbre** para introducir el horario del timbre agregando interfaz.

Estado de Timbre: [ON] es para activar el timbre, mientras que **[OFF]** es para desactivarlo.

Tiempo de Timbre: El timbre suena automáticamente cuando se alcanza el tiempo especificado.

Repetir: Para definir si desea repetir el timbre.

Tono: Permite seleccionar diferente timbre.

Intervalo de retardo del timbre (s): Para ajustar la longitud de la llamada. El valor varía de 1 a 999 segundos.

9.4 Ajustes de Estado de Marcaje

En la interfaz inicial, pulse **[M/OK] > Personalizar > Opciones de Estado de Marcaje** para entrar en la interfaz de configuración de opciones de estado de perforación.

Modo de estado de marcaje: Para elegir el modo de estado de perforación, que incluye los siguientes modos:

1. **Apagado** Para desactivar la función **Estado de Marcaje.** El marcaje de estado esta dentro clave bajo el menú Asignaciones de teclas de método abreviado no será válido.
2. **Modo manual:** para cambiar el estado de marcaje clave manualmente, y el estado de marcaje clave desaparecerá después del marcaje de estado de tiempo de espera.
3. **Modo automático:** Cuando es elegida, establezca el tiempo de conmutación de la clave del estado de marcaje en asignaciones de teclas de método abreviado; cuando el tiempo de conmutación es alcanzado, el conjunto de clave del estado de marcaje se desactivará automáticamente.
4. **Modo manual y automático:** En este modo, la interfaz principal mostrará el marcaje de conmutación automática de las claves de estado, por su parte admite la conmutación manual de la clave del estado de marcaje. Tras el tiempo de espera, la conmutación manual de marcaje será clave la conmutación automática de la clave del estado de marcaje.
5. **Modo fijo manual:** Después de la clave del estado de marcaje es conmutada manualmente, la clave del estado de marcaje permanecerá invariable hasta ser conmutada manualmente la próxima vez.
6. **Modo fijo:** Sólo el marcaje fijo de estado de clave será mostrado y no puede cambiarse.

Tiempo de espera de estado de marcaje (s): El tiempo de espera de la pantalla de estado de perforación. El valor oscila entre 5~999 segundos.

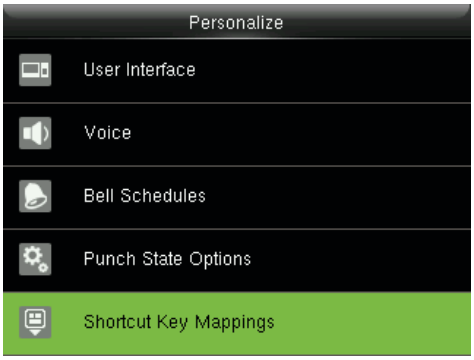
Estado de marcaje requerido: si es necesario elegir el estado de asistencia en la verificación.
Encendido la elección de estado de asistencia es necesaria después de la verificación.

Apagado: elegir la asistencia estatal no es necesario después de la verificación.

Comentarios:
Existen cuatro estados de marcaje: Entrada, Salida, Salida descanso y Entrada descanso.

9.5 Ajuste de la Teclas de Acceso Directo

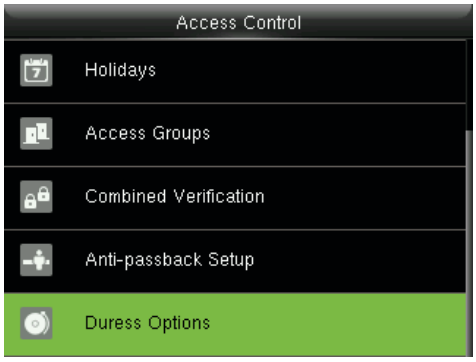
Teclas de método abreviado pueden definirse como claves del estado de marcaje o tecla de función menú. Cuando el dispositivo está en la interfaz principal, pulsa la tecla de acceso directo se mostrará el estado de asistencia o entrar en el menú de la interfaz de operación.

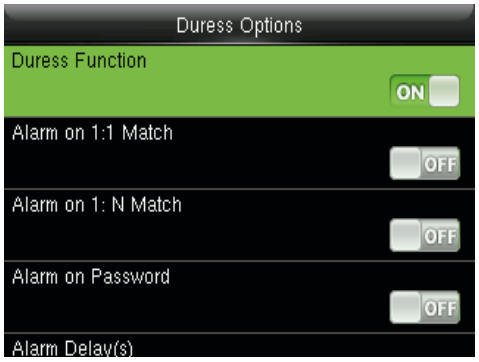


En el interfaz inicial, pulse **[M/OK] > Personalizar > Asignaciones de teclas de método abreviado** para entrar en la interfaz de configuración de las asignaciones de teclas de método abreviado.

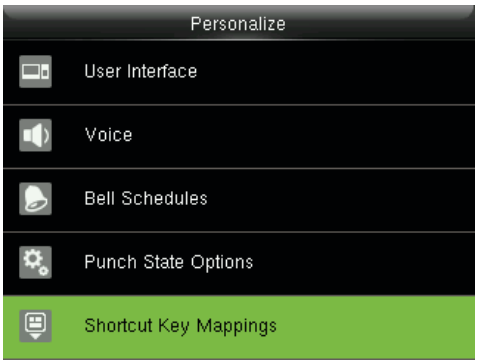
Para establecer **M/OK** como clave de coacción.

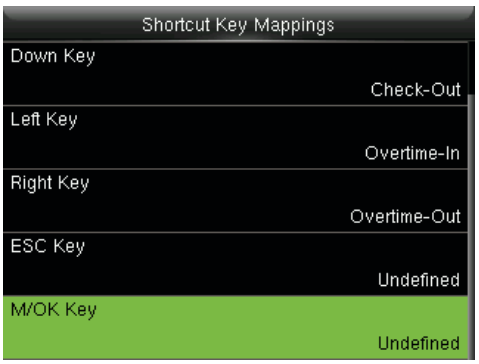
1. **Activar la función de coacción:** En la interfaz inicial, pulse **[M/OK] > Control de Acceso > Opciones > Función de coacción,** pulse **[M/OK]** para activar la función de coacción **Activar.**

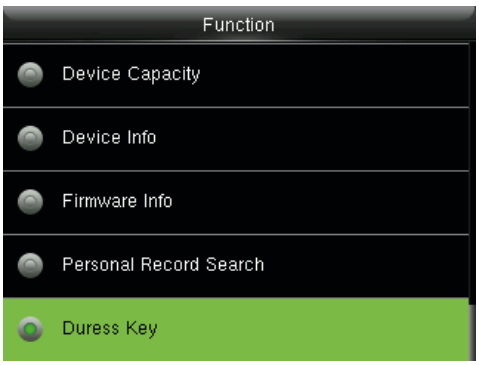




2. **Configuración de clave de coacción:** En la interfaz inicial, pulse **[M/OK] > Personalizar > Asignaciones de teclas de método abreviado** > seleccione **[M/OK]** > pulse **[M/OK] > Función** > Seleccione la opción **"Clave de coacción"**. (La clave de coacción menú se mostrará después de la coacción, la función está activada).





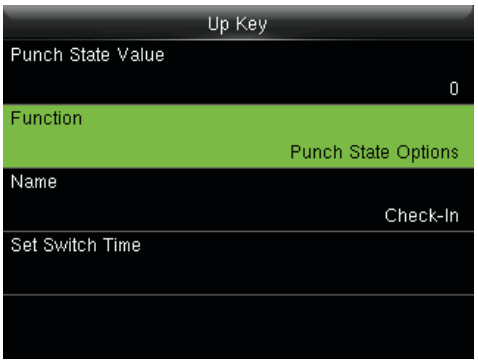


Comentarios:

Las teclas de dirección o ESC también se pueden establecer como clave de coacción.

Para establecer el tiempo de conmutación automática: Elige cualquier tecla de acceso directo y seleccione **[Opciones de Estado de Marcaje]** en **[Función]**, de modo que el tiempo de conmutación automática se puede ajustar.

Interruptor automático: Cuando se alcanza la hora fijada, el dispositivo cambiará la asistencia en estado automáticamente.

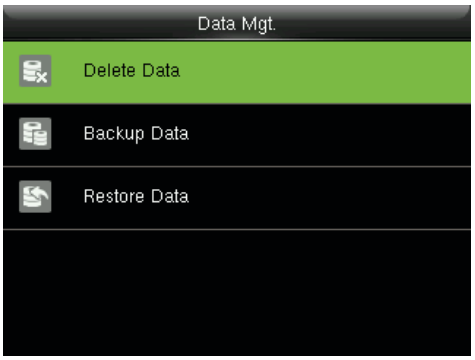


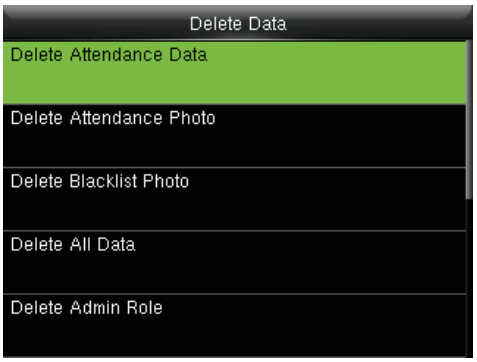
Cuando se establece la tecla de método abreviado para estado de marcaje, pero **[Desactivado]** está seleccionada en el modo **[Modo Estado de Marcaje] (Personalizar > Opciones > Modo Estado de Marcaje** > seleccione **Desactivado**) y, a continuación, la tecla de método abreviado no estará habilitado.

10 Gestión de Datos

10.1 Eliminación de Datos

Para administrar los datos en el dispositivo, el cual incluye eliminar los datos de asistencia, eliminar todos los datos, eliminar el rol del administrador y eliminar los protectores de pantalla, etc.





En la interfaz inicial, pulse **[M/OK] > Gestion de Datos > Eliminar Datos** para ingresar a la interfaz de configuración de eliminar datos.

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

Eliminar foto: Asistencia para eliminar a todos los usuarios de la asistencia de las fotos en el dispositivo.

Eliminar Lista Negra Foto: Para borrar todas las fotos en el dispositivo en la lista negra, lo que significa que las fotos tomadas tras haber fracasado las verificaciones.

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

Eliminar rol de admin: hacer que todos los administradores se convierten en usuarios normales.

Eliminar el control de acceso: Para borrar todos los datos de acceso.

Eliminar el usuario Foto: Para borrar todas las fotos de usuario en el dispositivo.

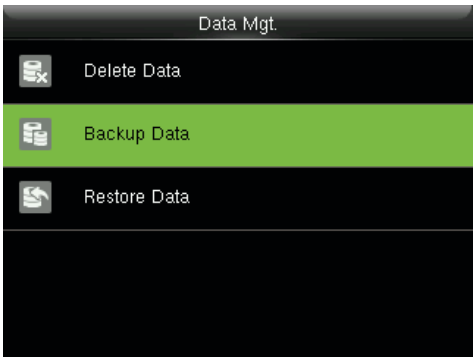
Fondo: Eliminar para eliminar todos los fondos de pantalla en el dispositivo.

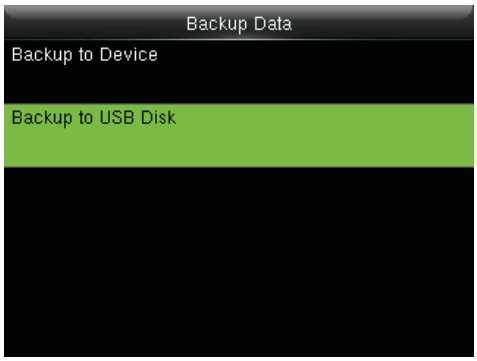
Eliminar protectores de pantalla: eliminar todos los protectores de pantalla en el dispositivo. (Para obtener información detallada de la carga de los protectores de pantalla, consulte 17.4 Cargar imagen regla.)

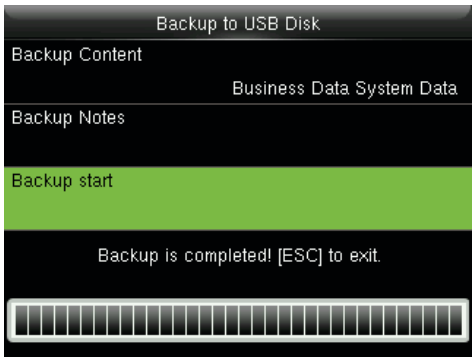
Borrar datos de copia de seguridad: Para borrar todos los datos de copia de seguridad.

10.2 Respaldo de Datos

Copia de seguridad de los datos empresariales, o los datos de configuración del dispositivo o USB.
Respaldo a disco USB







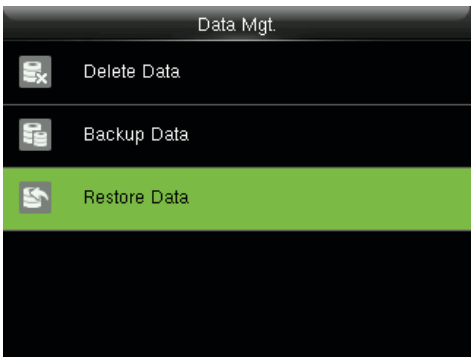
Inserte el disco USB. En el interfaz inicial, pulse **[M/OK] > Gestion de Datos > Copia de seguridad > Respaldo a USB > Respaldo de Datos** > Elegir contenido para ser respaldados (datos de empresa/datos del sistema) > Copia de seguridad de inicio para iniciar la copia de seguridad. Reiniciar el dispositivo no se necesita después de la copia de seguridad se ha completado.

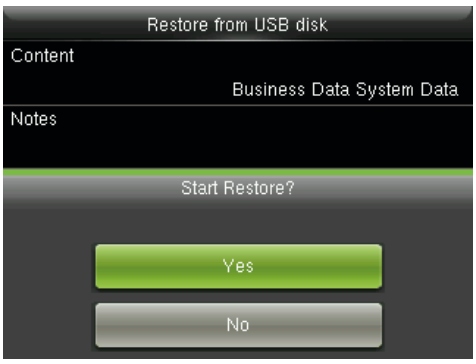
Comentarios:
Las operaciones de copia de seguridad de dispositivo son las mismas que las de copia de seguridad en disco USB.

10.3 Restauración de Datos

Para restaurar los datos en el dispositivo o disco USB para el dispositivo.

Restaurar desde un disco USB





Inserte el disco USB. En el interfaz inicial, pulse **[M/OK] > Gestion de Datos > Restaurar Datos > Restaurar a disco USB > Datos** > Elegir contenido para ser restaurado (Datos de empresa/datos del sistema) > I**niciar restauración** > Seleccione Sí para iniciar la restauración. Después de la restauración completa, haga clic en **[Aceptar]** para reiniciar automáticamente el dispositivo.

Comentarios:
Las operaciones de restauración del dispositivo son las mismas que las de restauración desde el disco USB.

11 Gestión USB

Carga o descarga de datos entre el dispositivo y el software correspondiente al disco USB.
Antes de cargar/descargar datos a/desde el disco USB, inserte el disco USB en la ranura USB.

11.1 Descargar por USB

En la interfaz inicial, pulse **[M/OK] > Gestion USB > Descargar** para entrar a la interfaz USB de descarga.
Período de tiempo está obligado a escoger sólo descargar datos de asistencia.

Datos de asistencia: Para descargar los datos de asistencia en el período de tiempo especificado en el disco USB.

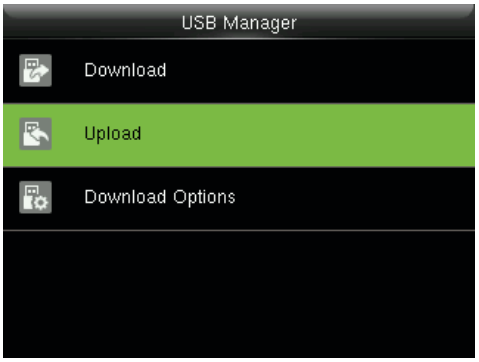
Datos de Usuario: Para descargar toda la información del usuario y las huellas del dispositivo en el disco USB.

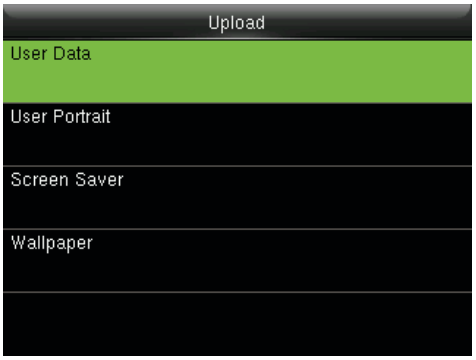
Foto de Usuario ★: Para descargar todas las fotos del usuario desde el dispositivo en un disco USB.

Foto de asistencia ★: asistencia para descargar todas las fotos del dispositivo USB en el disco.

Fotos de lista negra ★: Para descargar todas las fotos en la lista negra (fotos tomadas después de fracasado verificaciones) desde el dispositivo USB en el disco.

11.2 Carga por USB





En la interfaz inicial, pulse **[M/OK] > Gestion USB > Subir** para entrar en la interfaz de carga USB.

Datos de usuario: para cargar toda la información del usuario y las huellas dactilares del disco USB en el dispositivo.

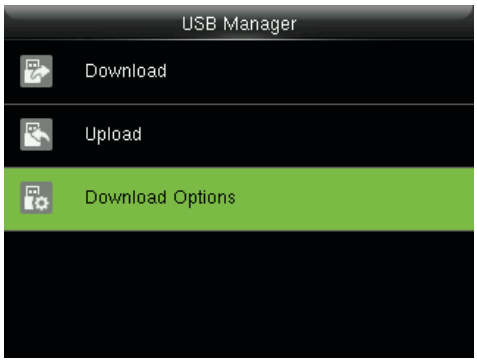
Foto de usuario ★: usuario cargar todas las fotos desde el disco USB en el dispositivo (para detalles de cargar imágenes de usuario, consulte 17.4 Regla para Subir Imagen).

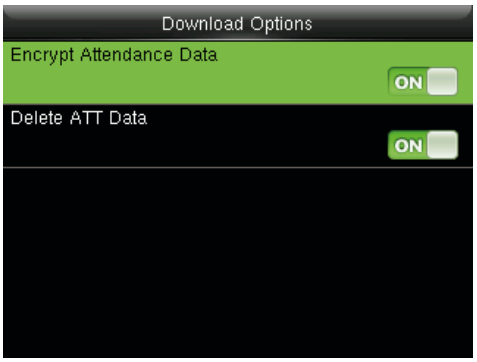
Protector de pantalla: para cargar todos los protectores de pantalla desde el disco USB en el dispositivo. Puede elegir imagen seleccionada **[Subir]** o **[Cargar]** todas las imágenes. Las imágenes se mostrarán en la interfaz principal del dispositivo después de cargar (para obtener las especificaciones de los protectores de pantalla, consulte 17.4 Regla para Subir Imagen).

Fondo de Pantalla: Para cargar todas las imágenes desde el disco USB en el dispositivo. Puede elegir imagen seleccionada **[Subir]** o **[Cargar]** todas las imágenes. Las imágenes se mostrarán en la pantalla después de cargar (para obtener las especificaciones de fondo de pantalla, consulte 17.4 Regla para Subir Imagen).

11.3 Ajuste de Opciones de Descarga

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





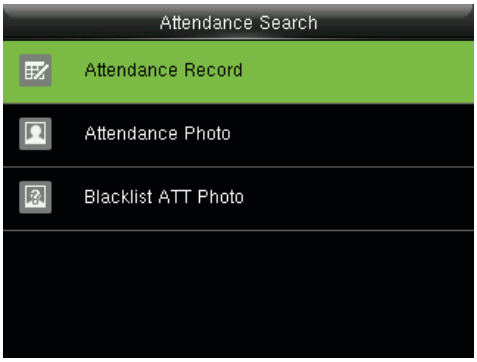
En el interfaz inicial, pulse **[M/OK] > Gestion USB > Opciones de descarga** para entrar en la interfaz de configuración de opciones de descarga.
Pulse **[M/OK]** para activar o desactivar opciones de **[Encriptar Datos] y [Eliminar Datos].**

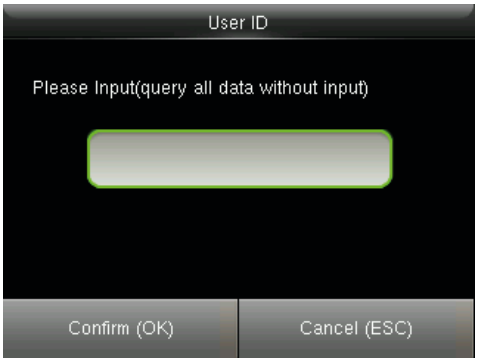
Comentarios:
El cifrar los datos de asistencia sólo pueden importarse en el software de ZKTime.Net 3.0.

12 Búsqueda de Asistencia

Cuando los usuarios comprueban correctamente, registros de asistencia son guardados en el dispositivo. Esta función permite a los usuarios comprobar los registros de asistencia, foto de asistencia ★y foto en la lista negra.★

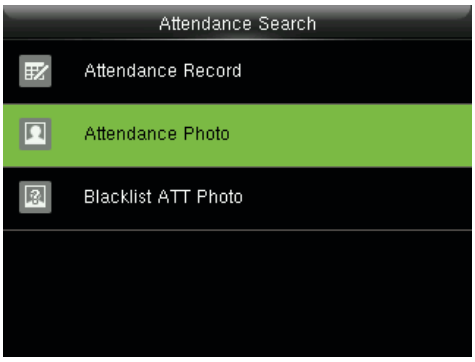
12.1 Búsqueda de Registro de Asistencia

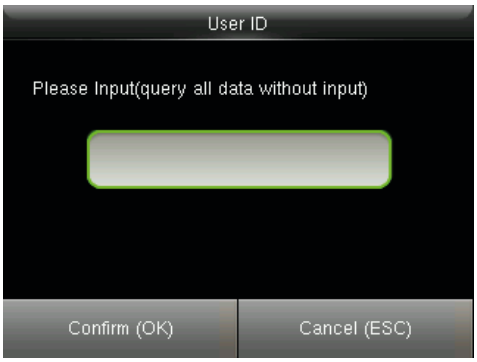




En la interfaz inicial, pulse **[M/OK] > Buscar > Asistencia Registro de asistencia** > Introduzca el ID de usuario (si no se introduce un código, todos los registros de usuario serán buscados) > seleccione el Rango de Tiempo > pulse **[M/OK]**, los correspondientes registros de asistencia será mostrada.

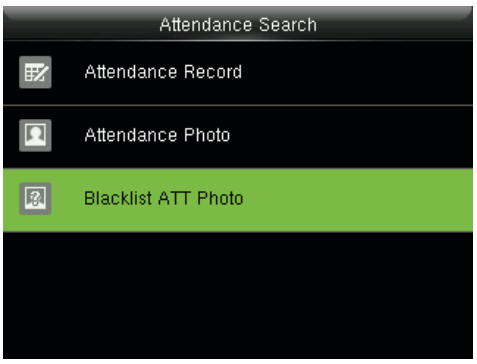
12.2 Búsqueda de Foto de Asistencia.★





En la interfaz inicial, pulse [**M/OK] > Búsqueda de Asistencia > Asistencia > Fotos** búsqueda introduzca el ID de usuario (si no se introduce un código, todos los asistentes fotos serán buscados) > seleccione el **Rango de Tiempo** > pulse **[M/OK]**, la correspondiente asistencia fotos será mostrada.

12.3 Búsqueda de Foto de Asistencia en Lista Negra. ★



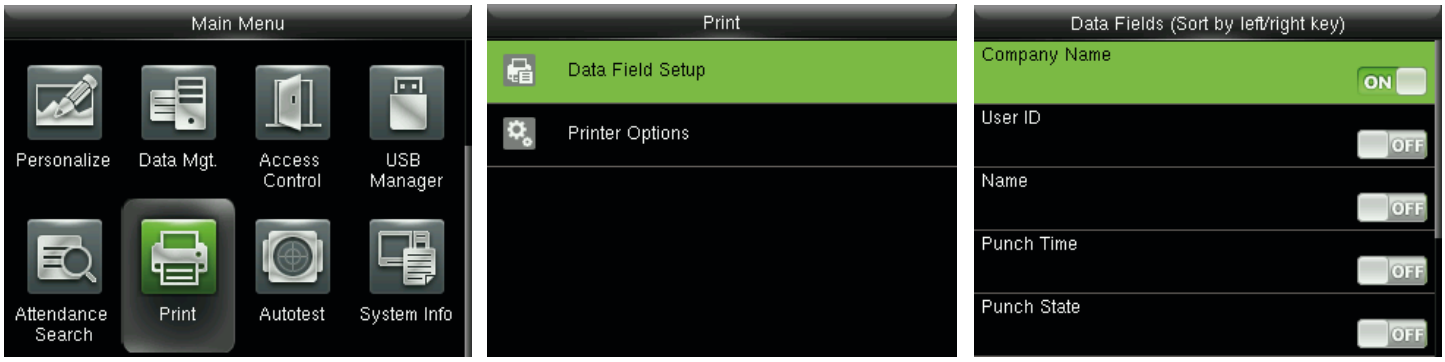
En la interfaz inicial, pulse [**M/OK] > Asistencia > Búsqueda Foto Lista Negra** > Seleccione el **Rango de Tiempo** > pulse **[M/OK]**, entonces las correspondientes fotografías se mostrarán en la lista negra.

Comentarios:
[Guardar falló en verificación] debe estar seleccionado en **[Modo Cámara]** (Pulse **[M/OK] > [System] > [asistencia] > [Modo Cámara]** > Seleccione **Guardar en falló la verificación**), así como para guardar fotos en la lista negra en el dispositivo.

13 Ajustes de Impresión★

Los dispositivos con la función de impresión puede imprimir registros de asistencia cuando se conecta una impresora (esta función es opcional y sólo estar equipado en algunos productos).

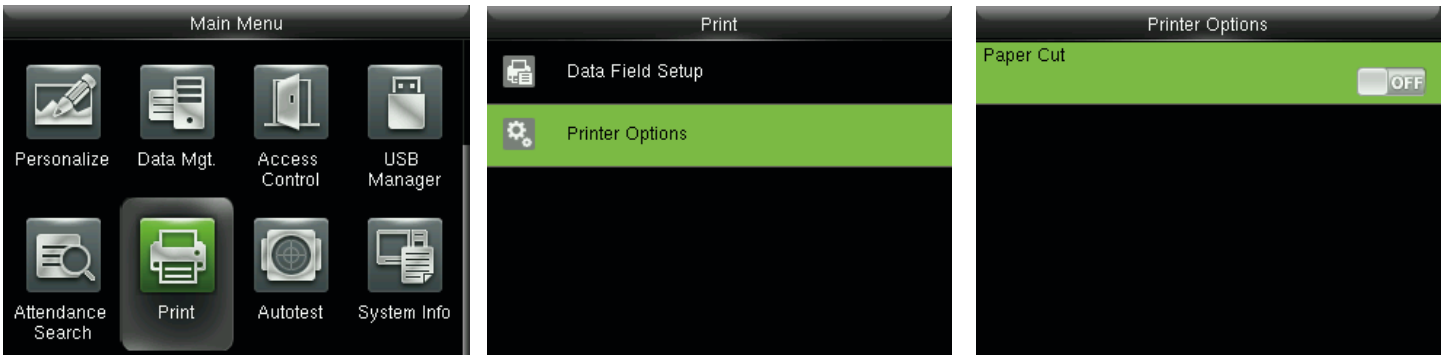
13.1 Ajustes de los Campos de Datos de Impresión



En la interfaz inicial, pulse **[M/OK] > Campo de datos > Imprimir > Configuración** > pulse **[M/OK]** para activar/desactivar los campos que necesitan ser impresos.

Comentarios:
En la impresión, la posición de los campos de la información puede ser ajustada mediante la tecla derecha/izquierda: pulse la tecla izquierda para moverse hasta el elemento anterior, y presiona la tecla derecha para pasar al siguiente elemento.

13.2 Ajustes de las Opciones de Impresión



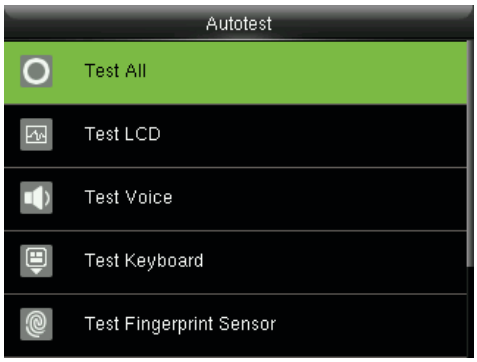
En la interfaz inicial, pulse **[M/OK] > Impresión > Imprimir > Opciones** > pulse **[M/OK]** para activar/desactivar la función de corte de papel.

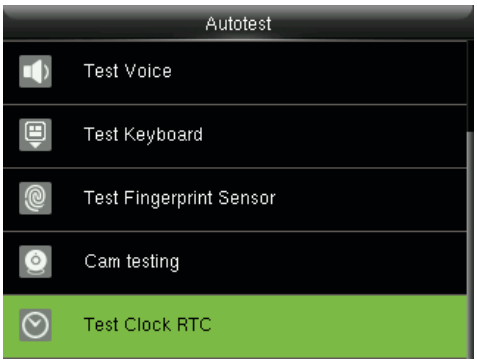
Comentarios:

Para activar la función de Corte de Papel, es necesario conectar el dispositivo con una impresora con función de corte de papel, de manera que la impresora corte papeles según la información de impresión seleccionado en el momento de la impresión.

14 Auto-prueba

Para comprobar automáticamente si todos los módulos en el dispositivo funcione correctamente, las cuales incluyen el LCD, voz, teclado, lector del sensor de huellas digitales, cámara y RTC (reloj de tiempo real).





En la interfaz inicial, pulse **[M/OK] > Auto-prueba** para entrar en la interfaz.

Probar todo: La prueba de LCD, voz, teclado, lector de huella dactilar, cámara y RTC. Durante la prueba, pulse **[M/OK]** para continuar con la siguiente prueba, mientras que presione la tecla [ESC] para salir de la prueba.

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

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

Teclado: para probar todas las llaves de cada tecla para ver si funciona correctamente. Pulse cualquier tecla en el teclado interfaz de prueba; si la tecla pulsada es coherente con el signo clave se muestra en la pantalla, y a continuación la tecla funciona correctamente. Pulse [M/OK] o [ESC] para salir de la prueba.

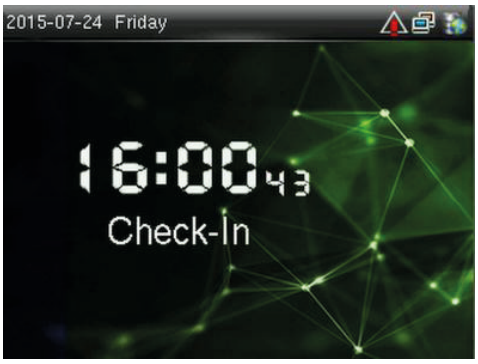
Sensor de huella: Para probar el sensor de huella dactilar pulsando la huella digital para comprobar si la imagen de la huella es clara. Al pulsar sobre el sensor de huellas dactilares, la imagen se visualiza en la pantalla. Pulse [M/OK] o [ESC] para salir de la prueba.

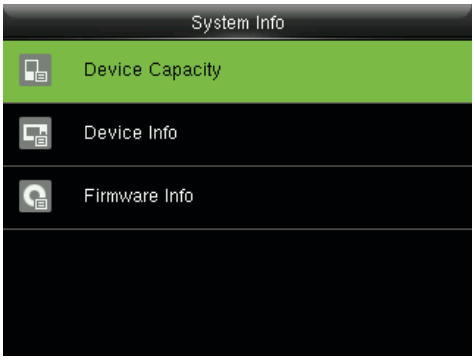
Cámara: para comprobar si la cámara funciona correctamente comprobando las fotos tomadas son claras para su uso. Pulse [M/OK] o [ESC] para salir de la prueba.

Reloj: Reloj de prueba para probar el reloj en tiempo real. El dispositivo comprueba si el reloj funciona correctamente y con precisión mediante el control del cronómetro. Pulse [M/OK] para empezar a contar el tiempo, y púlselo de nuevo para dejar de contar, para ver si el cronómetro cuenta el tiempo con precisión. Presione la tecla [ESC] para salir de la prueba.

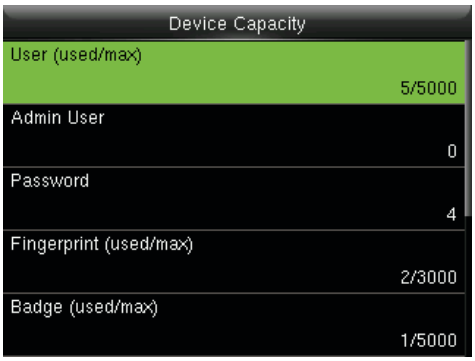
15 Información del Sistema

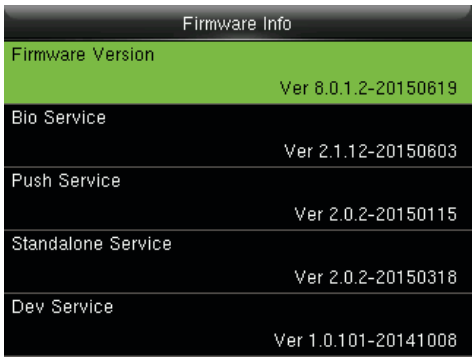
Compruebe la información del sistema, la capacidad de datos e información sobre el firmware del dispositivo.





En el interfaz inicial, pulse **[M/OK] > Info. Sistema** para entrar en la interfaz de Información del Sistema.





Capacidad del Dispositivo | Información del Dispositivo | Información de Firmware

Capacidad del dispositivo: Para mostrar el número de usuarios registrados, los administradores, las contraseñas, las huellas dactilares, las insignias, los registros de asistencia y fotos de asistencia ★, también para controlar el almacenamiento total de usuarios, huellas dactilares, insignias, registro de asistencia y fotos de asistencia.★

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

Info. Firmware: Para mostrar la versión de firmware, servicio Bio, servicio push, servicio independiente y servicio de dispositivo.

Comentarios:

La visualización de la capacidad del dispositivo, la información de dispositivo y de Info Firmware en el sistema de información de los diferentes productos de interfaz puede variar; el producto real prevalecerá.

16 Solución de problemas

Wel sensor de huella dactilar no es capaz de leer y comprobar la huella dactilar efectivamente

- Comprobar si el dedo está húmedo, o el sensor de huella dactilar está húmedo o polvoriento.
- Limpiar el dedo y el sensor de huella dactilar y vuelva a intentarlo.
- Si el dedo está demasiado seco, soplar aire en ella y vuelva a intentarlo.

- "Zona horaria no válida" se muestra después de la verificación.
  - Póngase en contacto con el administrador para comprobar si el usuario tiene privilegios para acceder dentro de ese horario.

- Verificación correcta pero el usuario no puede acceder.
  - Compruebe si el privilegio de usuario está configurado correctamente.
  - Compruebe si el bloqueo que el cableado está correcto.

- Suena la alarma de sabotaje.
  - Compruebe si el dispositivo y la placa trasera está fijado juntos; si no, el interruptor anti sabo taje en la parte posterior del dispositivo se activa y genera una alarma, se mostrará en la es quina superior derecha de la interfaz. Sólo cuando [Altavoz de Alarma] > Control de Acceso > Opciones > Altavoz de alarma está activada [ON] será el altavoz emitir una alarma.

17 Apéndices

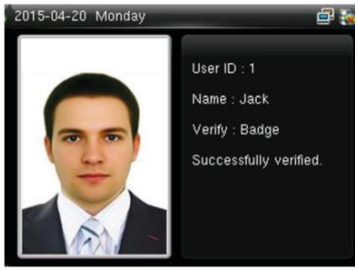
17.1 Especificaciones

Capacidad de Huellas	3000
Capacidad de Tarjetas	5000
Capacidad de Eventos	100,000
Capacidad de Fotos	6500
Pantalla	2.4"TFT LCD
Indicador LED	Rojo/Verde
Tipo de comunicación	Ethernet (10/100M), RS232, RS485, USB-Host
Comunicación Wiegand	Entrada / Salida
Velocidad de Reconocimiento	≤ 2 segundos
FAR	≤ 0.0001%
FRR	≤ 1%
Temperatura	0~45°C
Alimentación	12V / 3 A
Voltaje	12V
Corriente	3 A
Puestos de Control de Acceso	Alarma, Botón de Salida, Alarma de puerta, lector y Sensor de Puerta.

Comentarios

Algunos modelos admiten la función de identificación con foto.

Cuando la función ID está activada y el usuario pasa la verificación, no sólo la información de ID de usuario y nombre se mostrará, sino también la fotografía registrada por el usuario o guardada en eldisco USB será mostrado.



Procedimiento Operativo]

Si la foto de usuario tomada por el dispositivo es utilizado, la foto se mostrará a la derecha después de la verificación del usuario.

Si el usuario foto en un disco USB, se utiliza el procedimiento operativo es el siguiente:

(1) crear un archivo denominado **"photo"** en el disco USB y guardar la foto del usuario en el archivo.

(2) La foto debe ser formato JPG y el nombre del archivo debe ser como el ID de usuario. Por ejemplo: la fotografía correspondiente al usuario con el ID de 154 debería ser nombrada como 154.jpg.

(3) Inserte el disco USB en el puerto USB del dispositivo e ingrese a Gestion de USB > Cargar > Foto de usuario para cargar fotos de los usuarios. La foto se mostrará después de la verificación del usuario.

Nota:

(1) El nombre de la foto debe estar dentro de 9 dígitos.

(2) El tamaño de la foto debe ser inferior a 15k.

(3) La foto recientemente cargado reemplazará la foto original del usuario.

(4) Cuando descargue fotos de usuario, introducir Gestión de USB > Descargar > Foto de Usuario, un archivo denominado como "photo" se creará en el disco USB automáticamente, en el cual todas las fotos de los usuarios se guardarán.

17.3 Introducción Wiegand

Protocolo Wiegand 26 es un estándar de protocolo de control de acceso Control de Acceso desarrollado por el Subcomité estándar, afiliado a la asociación de la industria de seguridad (SIA). Es un protocolo utilizado para el lector de tarjetas IC sin contacto y puerto de salida.

El protocolo define el puerto entre el lector de tarjetas y el controlador, que son ampliamente utilizados en el control de acceso, seguridad y otras industrias relacionadas. Esto ha estandarizado la labor de lector de tarjeta controladora de diseñadores y fabricantes. Los dispositivos de control de acceso fabricados por nuestra empresa también aplicar este protocolo.

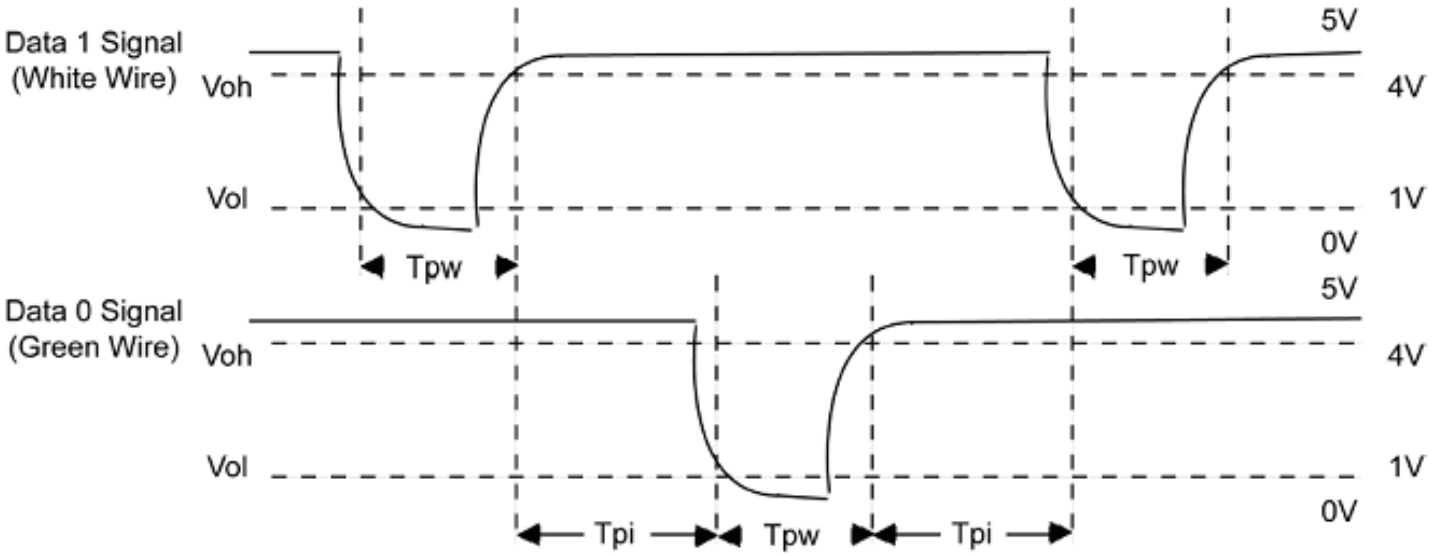
Señal digital

La figura1 muestra el diagrama de secuencia del lector de tarjeta del envío de señal digital en bits al controlador de acceso. El Wiegand en este diagrama sigue el protocolo estándar de control de acceso de SIA, que apunta a Wiegand de 26 bits lector (con un tiempo de pulso dentro de 20us a 100us y pulso hopping plazo 200us y 20ms). Data1 y Data0 son señales de nivel alto (mayor que Voh) hasta que el lector está listo para enviar un flujo de datos. El lector de tarjetas envía un pulso asíncrono de nivel bajo (menos de vol), transmisión de flujo de datos a través de datos1 o datos0 cable para acceder a la caja de control (como la onda de diente de sierra en la figura 1). Data1 y Data0 impulsos no se superponen o sincronizar. La figura 1 muestra el máximo y el mínimo de ancho de pulso (pulsos suficientes) y sucesivos saltos de pulso (tiempo entre dos pulsos) que permite el control de acceso de huellas digitales de la serie F de terminales.

Tabla 1: Tiempo de Pulso

Señal	Definición	Valor Típico del Lector de Tarjeta
Tpw	Ancho de pulso	100 µs
Tpi	Intervalo de pulso	1 ms

Figura 1: Diagrama de Secuencia



17.4 Regla para Subir Imagen

1. **Foto del usuario★:** Es necesario crear un fichero llamado **"photo"** en el archivo de disco USB y poner fotos de usuario en el archivo. La capacidad es de 8.000 imágenes (teniendo en cuenta la capacidad real del dispositivo, se sugiere para cargar imágenes de 5000 en la mayoría), con cada uno de ellos no exceda de 15k. El nombre de la imagen es x.jpg (x es el ID de usuario real, máx. 9 dígitos). La foto debe ser formato JPG.

2. Publicidad de imagen: es necesario crear un fichero llamado **"advertise"** en el archivo de disco USB y poner publicidad de imágenes en el archivo. La capacidad es de 20 imágenes con cada uno de ellos no exceda de 30k. El nombre de la imagen y el formato no están restringidos.

3. **Fondo de Pantalla:** es necesario crear un fichero llamado **"wallpaper"** en el archivo de disco USB y poner wallpaper en el archivo. La capacidad es de 20 imágenes con cada uno de ellos no exceda de 30k. El nombre de la imagen y el formato no están restringidos.

Nota: Cuando cada usuario y asistencia foto no exceda de 10k, el dispositivo puede guardar un total de 10000 usuarios y asistencia fotos (teniendo en cuenta la capacidad real del dispositivo, se recomienda cargar 5000 usuario y asistencia en la mayoría de las fotos).

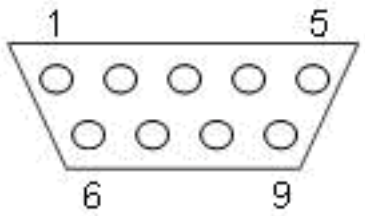
17.5 Función de Impresión★

Comentarios:

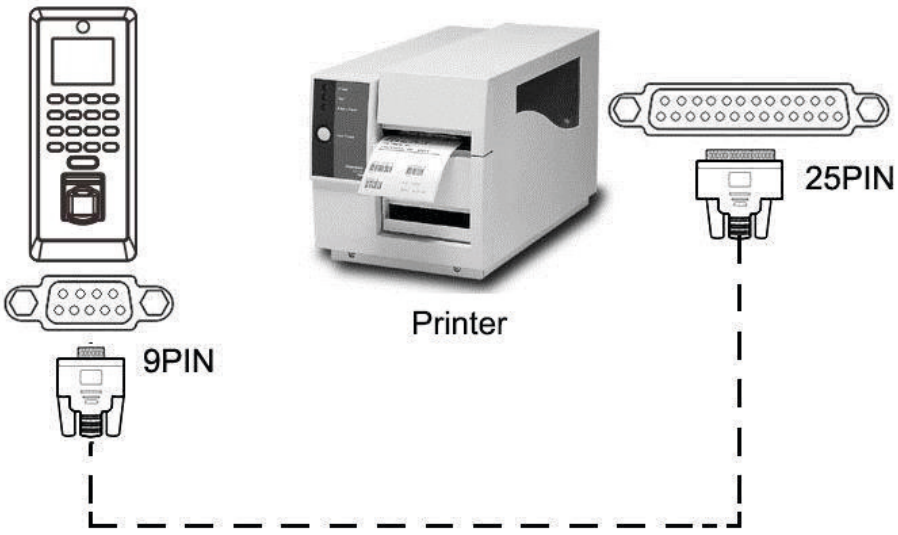
Sólo algunos modelos admiten la función de impresión.

Instrucción Función

Esta función sólo es compatible con el puerto serie, pero no la impresión de puerto paralelo. Imprimir contenido se emite a través de RS232 formato; información de verificación será siempre de salida al puerto serie. La impresión está disponible si se ha conectado una impresora o una híper terminal puede ser usada para leer el contenido de salida.

La conexión entre el dispositivo y la impresora	Dispositivo Impresora 2 TXD < ---------- > 3 RXD 3 RXD < ---------- > 2 TXD 5 GND < ---------- >7 FG
PIN para línea RS232	

[Diagrama de Conexión]



[Operación]

1. En el interfaz inicial, pulse **[M/OK] > Comm. > Serial Comm > Baudrate**, y elija 19200 la velocidad en baudios.
2. En el interfaz inicial, pulse **[M/OK] > Imprimir**. Para establecer el formato de impresión y los parámetros, consulte 13 Ajustes de impresión.

Nota:

1. La velocidad en baudios del dispositivo e impresora (Híper Terminal) deben ser coherentes.
2. Si el formato predeterminado de la impresión no es satisfactoria, puede ponerse en contacto con nuestra empresa para personalizar otros formatos.

17.6 Declaración de Derechos Humanos y Privacidad

Estimado cliente:

Gracias por elegir el híbrido productos biométricos diseñados y fabricados por nosotros. Como un proveedor de renombre mundial de tecnologías y servicios biométricos, prestamos mucha atención al cumplimiento de las leyes relativas a los derechos humanos y privacidad en cada país mientras que constantemente realiza actividades de investigación y desarrollo.

Nos queda hacer las siguientes afirmaciones:

1. Todos nuestros dispositivos de reconocimiento de huellas dactilares para uso civil solamente se recogen los puntos característicos de las huellas dactilares en lugar de las imágenes de la huella dactilar y, por lo tanto, no intervienen cuestiones de privacidad.
2. Los puntos característicos de las huellas dactilares recogidas por nuestros productos no se pueden utilizar para restaurar las imágenes de la huella original y, por lo tanto, no intervienen cuestiones de privacidad.
3. Nosotros, como el proveedor del equipo, no será jurídicamente responsables, directa o indirectamente, de las consecuencias que se derivan de la utilización de nuestros productos.
4. Para cualquier controversia relacionada con los derechos humanos o la privacidad al usar nuestros productos, póngase en contacto con su empleador directamente.

Nuestros productos de huellas dactilares para uso policial, o herramientas de desarrollo apoyar la recopilación de las imágenes de la huella original. En cuanto a si este tipo de recogida de huellas dactilares constituye una violación de su privacidad, por favor póngase en contacto con el gobierno o el proveedor de equipamiento final. Nosotros, como fabricante de equipos originales, no deberán ser considerados jurídicamente responsables de toda infracción resultante de la misma.

La ley de la República Popular de China tiene las siguientes normas relativas a la libertad personal:

1. La detención ilegal, la detención o la búsqueda de los ciudadanos de la República Popular de China está prohibida; la violación de la privacidad individual está prohibida.
2. La dignidad personal de los ciudadanos de la República Popular de China es inviolable.
3. La casa de los ciudadanos de la República Popular de China es inviolable.
4. La libertad y la privacidad de la correspondencia de los ciudadanos de la República Popular de China están protegidos por la ley.

Por último, recalcamos una vez más que la biometría, como una avanzada tecnología de reconocimiento, será aplicado en un montón de sectores como el comercio electrónico, la banca, los seguros y asuntos jurídicos. Cada año, personas de todo el mundo sufren grandes pérdidas debido a la inseguridad de las contraseñas. Los productos biométricos proporcionan una protección adecuada para su identidad en un entorno de alta seguridad.

17.7 Descripción de Uso Favorable para el Medio Ambiente

- El periodo de uso respetuoso con el medio ambiente (EFUP) marcado en este producto se refiere a la seguridad periodo de tiempo en el que el producto sea utilizado bajo las condiciones especificadas en las instrucciones del producto sin escapes de sustancias nocivas y sustancias nocivas.
- El EFUP de este producto no cubre las piezas consumibles que necesitan ser reemplazadas regularmente como baterías y así sucesivamente. El EFUP de las baterías es de 5 años.

Nombre y concentración de sustancias o elementos tóxicos y peligrosos

Nombre de la Pieza	Sustancias o Elementos Tóxicos y Peligrosos					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip Resistencia	x	o	o	o	o	o
Chip Capacitor	x	o	o	o	o	o
Chip de Inductor	x	o	o	o	o	o
Chip de Diodo	x	o	o	o	o	o
Componentes ESD	x	o	o	o	o	o
Altavoz	x	o				
Adaptador	x	o	o	o	o	o
Tornillos	x	o	o	o	o	o

o: indica que esta sustancia tóxica o peligrosa contenida en todos los materiales homogéneos utilizados para esta parte está por debajo de los LÃ mites establecidos en SJ/T11363-2006.

×: indica que esta sustancia tóxica o peligrosa incluida en al menos uno de los materiales homogéneos utilizados para esta parte está por encima de los LÃ mites establecidos en SJ/T11363-2006.

Nota: el 80% de las piezas de este producto son fabricados con los no peligrosos materiales respetuosos con el medio ambiente. Las sustancias peligrosas o elementos contenidos no se pueden reemplazar con materiales respetuosos con el medio ambiente en la actualidad debido a limitaciones técnicas o económicas.

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