

Manual de Usuario

Modelo aplicable(s): M2F PRO-UD

Fecha: Enero 2025
Versión: 1.0

Gracias por elegir nuestro producto. Por favor, lea atentamente las instrucciones antes de utilizarlo. Siga estas instrucciones para asegurarse de que el producto funciona correctamente. Las imágenes mostradas en este manual son sólo para fines ilustrativos. Para más información, visite el sitio www.zkteco.com

Copyright 2020 ZKTECO CO, LTD. Todos los derechos reservados.

Sin el consentimiento previo por escrito de ZKTeco, ninguna parte de este manual puede ser copiada o reenviada de ninguna manera o forma. Todas las partes de esta manual pertenecen a ZKTeco y sus filiales (en adelante, la «Empresa» o «ZKTeco").

Marca Registrada

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

Descargo de responsabilidad

Este manual contiene información sobre el funcionamiento y el mantenimiento del equipo ZKTeco. El copyright de todos los documentos, dibujos, etc. relacionados con el equipo suministrado por ZKTeco es propiedad de ZKTeco. Su contenido no debe ser utilizado ni compartido por el receptor con terceros sin la autorización expresa y por escrito de ZKTeco.

El contenido de este manual debe ser leído en su totalidad antes de iniciar la operación y mantenimiento del equipo suministrado. Si alguno de los contenidos del manual le parece poco claro o incompleto, póngase en contacto con ZKTeco antes de iniciar el funcionamiento y mantenimiento de dicho equipo.

Un requisito previo esencial para el funcionamiento y mantenimiento satisfactorios es que el personal de funcionamiento y mantenimiento esté totalmente familiarizado con el diseño y que dicho personal haya recibido una formación completa en el funcionamiento y mantenimiento de la máquina/unidad/equipo. Además, es esencial para el funcionamiento seguro de la máquina/unidad/equipo que el personal haya leído, comprendido y seguido las instrucciones de seguridad contenidas en el manual.

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

ZKTeco no ofrece ninguna garantía o representación con respecto a la integridad de cualquier información contenida en este manual o cualquiera de las modificaciones introducidas en el mismo, ZKTeco no extiende la garantía de ningún tipo, incluyendo, sin limitación, cualquier garantía de diseño, comerciabilidad o idoneidad para un propósito particular.

ZKTeco no asume responsabilidad alguna por errores u omisiones en la información o documentos a los que se hace referencia o que están vinculados a este manual. El usuario asume todo el riesgo en cuanto a los resultados y el rendimiento obtenidos de la utilización de la información.

ZKTeco no será responsable en ningún caso ante el usuario ni ante terceros de ningún daño incidental, consecuente, indirecto, especial o ejemplar, incluyendo, sin limitación, la pérdida de negocio, la pérdida de beneficios, la interrupción de negocio, la pérdida de información comercial o cualquier pérdida pecuniaria, que surja de, en conexión con, o en relación con el uso de la información contenida en o referenciada por este manual, incluso si ZKTeco ha sido advertido de la posibilidad de tales daños.

Este manual y la información contenida en el mismo pueden incluir imprecisiones técnicas, de otro tipo o errores tipográficos . ZKTeco modifica periódicamente la infformación aquí contenida, que se incorporará en nuevas adiciones/enmiendas al manual. ZKTeco se reserva el derecho de añadir, eliminar, enmendar o modifica r la información contenida en el manuala de vez en cuando en forma de circulares, vartas, notas, etc.

para un mejor funcionamiento y seguridad de la máquina/unidad/equipo. Dichas adiciones o modificaciones están destinadas a mejorar el funcionamiento de la máquina/unidad/equipo y dichas modificaciones no darán derecho a reclamar ninguna compensación o indemnización por daños y perjuicios en ninguna circunstancia.
ZKTeco no será responsable en ningún caso (i) en caso de mal funcionamiento de la máquina/unidad/equipo debido al incumplimiento de las instrucciones contenidas en este manual (II) en caso de funcionamiento de la máquina/unidad/equipo más allá de los límites de la tarifa (III) en caso de funcionamiento de la máquina y el equipo en condiciones diferentes a las prescritas en el manual.

El producto se actualizará de vez en cuando sin previo aviso. Los procedimientos de funcionamiento más recientes y los documentos pertinentes están disponibles en **https://www.zktecolatinoamerica.com**

Sede de ZKTeco

Dirección ZKTeco Industrial Park, No. 26, 188 Industrial Road, Tang Xia Town, Dong guan, China.

Teléfono +86 769 – 82109991

Fax +86 755 - 89602394

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

Acerca de la empresa

ZKTeco es uno de los mayores fabricantes del mundo de lectores RFID y biométricos (huella dactilar, facial y reconocimiento de vena). Su oferta de productos incluye lectores y paneles de control de acceso, cámaras de reconocimiento facial de corto alcance. Cámaras de reconocimiento facial de largo alcance, controladores de acceso de elevadores, torniquetes, controladores de puertas con reconocimiento de placas vehiculares (LPR) y productos de consumo, como cerraduras de puertas con lector facial y de huellas dactilares que funcionan con pilas. Nuestras soluciones de seguridad son multilingües y están localizadas en más de 18 idiomas. En las modernas instalaciones de fabricación de ZKTeco, de 700.000 pies cuadrados y con certificación 1509001, controlamos la fabricación, el diseño de productos, el montaje de componentes y la logística y el envío, todo bajo un mismo techo.

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

Acerca del Manual

Este manual presenta las operaciones del **M2F PRO-UD**.
Todas las figuras mostradas son sólo a título ilustrativo. Las figuras de este manual pueden no coincidir exactamente con los productos reales.
Las funciones y parámetros con* no están disponibles en todos los dispositivos.

Convenciones del Documento

A continuación, se enumeran las convenciones utilizadas en este manual:
Convenciones GUI

Para software	
Convención	**Descripción**
Negritas	Usado para identificar interfaz del software como: **OK, Confirmar, Cancelar**
>	Los menús de varios niveles están separados por estos corchetes. Por ejemplo, Archivo > Crear > Carpeta.
Para el dispositivo	
Convención	**Descripción**
<>	Nombres de botones o teclas para dispositivos. Por ejemplo, pulse <OK>.
[ ]	Los nombres de ventanas, opciones de menú, tablas de datos y campos aparecen entre corchetes. Por ejemplo, abra la ventana [Nuevo usuario].
/	Los menús de varios niveles se separan mediante barras inclinadas. Por ejemplo, [Archivo / Crear / Carpeta].

Símbolos

Convención	Descripción
	Esto implica sobre el aviso o presta atención en el manual.
	Información general que ayuda a realizar las operaciones más rápidamente.
	Información a considerar.
	Para evitar peligros o errores.
	Declaración o acontecimiento de advertencia de algo o que sirve de ejemplo.

Índice

DECLARACIÓN DE SEGURIDAD DE LOS DATOS 8

MEDIDAS DE SEGURIDAD 8

1 INSTRUCCIONES DE USO 10
- 1.1 POSICIÓN DE LOS DEDOS 10
- 1.2 POSICIÓN DE PIE, POSTURA Y EXPRESIÓN FACIAL 10
- 1.3 REGISTRO DE PLANTILLAS FACIALES 11
- 1.4 INTERFAZ DE ESPERA 12
- 1.5 MODO T9 13
- 1.6 MODO DE VERIFICACIÓN 14
  - 1.6.1 VERIFICACIÓN DE HUELLAS DACTILARES 14
  - 1.6.2 VERIFICACIÓN DE TARJETAS 15
  - 1.6.3 VERIFICACIÓN FACIAL 16
  - 1.6.4 VERIFICACIÓN DE CONTRASEÑA 17
  - 1.6.5 VERIFICACIÓN COMBINADA 18

2 VISIÓN GENERAL 20

- 2.1 APARIENCIA 20
- 2.2 DESCRIPCIÓN DE TERMINALES Y CABLEADO 21
  - 2.2.1 DESCRIPCIÓN DE TERMINALES 21
- 2.3 DESCRIPCIÓN DEL CABLEADO 21
  - 2.3.1 CONEXIÓN ELÉCTRICA 21
  - 2.3.2 CONEXIÓN DE SENSOR DE PUERTA Y PULSADOR DE SALIDA 22
  - 2.3.3 CONEXIÓN DEL RELÉ DE BLOQUEO 22
  - 2.3.4 CONEXIÓN ETHERNET 23

3 INSTALACIÓN 24
- 3.1 ENTORNO DE INSTALACIÓN 24
- 3.2 INSTALACIÓN DE DISPOSITIVOS 24

4 MENÚ PRINCIPAL 25

5 GESTIÓN DE USUARIOS 27

- 5.1 REGISTRO DE USUARIOS 27
  - 5.1.1 NOMBRE E ID DE USUARIO 27
  - 5.1.2 ROL DE USUARIO 27
  - 5.1.3 MODO DE VERIFICACIÓN 28
  - 5.1.4 REGISTRAR HUELLA DACTILAR 28
  - 5.1.5 PLANTILLA DE CARA AL REGISTRO 29
  - 5.1.6 TARJETA 29
  - 5.1.7 CONTRASEÑA 29
  - 5.1.8 FOTO DE PERFIL 30
  - 5.1.9 FUNCIÓN DE CONTROL DE ACCESO 30

5.2 BÚSQUEDA DE USUARIOS 31
5.3 EDITAR USUARIO 31
5.4 BORRAR USUARIO 31
5.5 ESTILO DE VISUALIZACIÓN....32

6 ROL DE USUARIO 33

7 AJUSTES DE COMUNICACIÓN 34
7.1 AJUSTES DE RED 34
7.2 CONEXIÓN PC 35
7.3 RED INALÁMBRICA* 35
7.4 CONFIGURACIÓN DEL SERVIDOR CLOUD....37
7.5 DIAGNÓSTICO DE LA RED....38

8 CONFIGURACIÓN DEL SISTEMA....39

8.1 FECHA Y HORA....39
8.2 CONFIGURACIÓN DE LOS REGISTROS DE ASISTENCIA/ACCESO 40
8.3 PARÁMETROS DE LA PLANTILLA FACIAL 42
8.4 PARÁMETROS DE HUELLAS DACTILARES 44
8.5 CONFIGURACIÓN DEL TIPO DE DISPOSITIVO 45
8.6 AJUSTE DE SEGURIDAD 45
8.7 USB UPGRADE 46
8.8 ACTUALIZAR EL FIRMWARE EN LÍNEA 47
8.9 RESTABLECIMIENTO DE FÁBRICA 49

9 PERSONALIZAR AJUSTES 50
9.1 CONFIGURACIÓN DE LA INTERFAZ DE USUARIO....50
9.2 AJUSTES DE VOZ 51
9.3 HORARIOS DE LAS CAMPANAS 51
9.4 ESTADOS DE PERFORACIÓN OPCIONES 52
.5 ASIGNACIÓN DE TECLAS DE ACCESO DIRECTO....53

10 GESTIÓN DE DATOS 55

11 CONTROL DE ACCESO 57
11.1 OPCIONES DE CONTROL DE ACCESO....57
11.2 AJUSTE DE LA REGLA TEMPORAL 59
11.3 VACACIONES 60
11.4 VERIFICACIÓN COMBINADA 61
11.5 OPCIONES DE COACCIÓN 62

12 GESTOR DE USB 63
12.1 USB DESCARGA 63
12.2 CARGA USB 64
12.3 OPCIONES DE DESCARGA 64

13 BÚSQUEDA DE ASISTENTES 65

14 AUTOTEST 66

15 INFORMACIÓN DEL SISTEMA 67

16 CONECTARSE AL SOFTWARE BIOTIME CLOUD 68
16.1 AÑADIR DISPOSITIVO EN EL SOFTWARE 68
16.2 AÑADIR PERSONAL AL PROGRAMA 69

17 CONECTAR CON EL SOFTWARE ZKBIO CVACCESS 70
17.1 ESTABLECER LA DIRECCIÓN DE COMUNICACIÓN 70
17.2 AÑADIR DISPOSITIVO EN EL SOFTWARE 70
17.3 AÑADIR PERSONAL AL PROGRAMA 72

ANEXO 1 73
REQUISITOS DE LA RECOGIDA EN VIVO Y EL REGISTRO DE PLANTILLAS DE ROSTROS DE LUZ VISIBLE 73
REQUISITOS DE LOS DATOS DE LAS PLANTILLAS DIGITALES DE ROSTROS CON LUZ VISIBLE 74

ANEXO 2 75
POLÍTICA DE PRIVACIDAD 75
FUNCIONAMIENTO ECOLÓGICO 77

Declaración de seguridad de datos

ZKTeco, como proveedor de productos inteligentes, también puede necesitar conocer y recopilar parte de su información personal para ayudarle mejor a utilizar los bienes y servicios de ZKTeco, y tratará su privacidad con cuidado mediante el desarrollo de una Política de Privacidad.

Por favor, lea y comprenda completamente todas las normas de la política de protección de la privacidad y los puntos clave que aparecen en el dispositivo antes de utilizar los productos ZKTeco.

Como usuario del producto, debe cumplir las leyes y normativas aplicables relacionadas con la protección de datos personales cuando recopile, almacene y utilice datos personales, lo que incluye, entre otras cosas, tomar medidas de protección de los datos personales, como realizar una gestión razonable de los derechos de los dispositivos, reforzar la seguridad física de los escenarios de aplicación de los dispositivos, etc.

Medidas de seguridad

Las siguientes precauciones están destinadas a garantizar la seguridad del usuario y prevenir cualquier daño. Por favor, léalas detenidamente antes de la instalación.

1. Leer, seguir y conservar las instrucciones: Todas las instrucciones de seguridad y operación deben ser leídas y seguidas correctamente antes de poner el dispositivo en funcionamiento.

2. No ignorar las advertencias: Cumpla con todas las advertencias indicadas en la unidad y en las instrucciones de operación.

Accesorios: Utilice únicamente accesorios recomendados por el fabricante o vendidos con el producto. No use componentes distintos a los sugeridos por el fabricante.

4. Precauciones para la instalación: No coloque este dispositivo en un soporte o marco inestable. Podría caerse, causar lesiones graves y dañar el dispositivo.

5. Servicio técnico: No intente reparar este dispositivo por su cuenta. Abrir o retirar las cubiertas puede exponerlo a voltajes peligrosos u otros riesgos.

6. Daños que requieren servicio técnico: Desconecte el sistema de la fuente principal de energía (CA o CC) y contacte al personal de servicio en las siguientes condiciones:

- Cuando se ve afectado el control del cable o de la conexión.
- Cuando se derramó el líquido o cayó un objeto en el sistema.
- Si el sistema está expuesto al agua y/o a las inclemencias del tiempo (lluvia, nieve, etc.).
- Si el sistema no funciona con normalidad según las instrucciones de funcionamiento.

Sólo modifique los controles definidos en las instrucciones de funcionamiento. El ajuste incorrecto de otros controles puede provocar daños y requerir la intervención de un técnico cualificado para devolver el aparato a su funcionamiento normal.

7. Repuestos: Cuando se necesiten piezas de repuesto, los técnicos de servicio deben utilizar únicamente piezas proporcionadas por el proveedor. Sustituciones no autorizadas pueden implicar riesgos de quemaduras, descargas eléctricas u otros peligros.

8. Revisión de seguridad: Una vez completado el servicio o la reparación del dispositivo, solicite al técnico que realice verificaciones de seguridad para garantizar el correcto funcionamiento del dispositivo.

9. Fuentes de alimentación: Operar el sistema solo con la fuente de energía indicada en la etiqueta del dispositivo. Si no está seguro del tipo de fuente de energía que debe usar, consulte a su distribuidor.

10. Protección contra rayos: Considere instalar conductores externos contra rayos para proteger el sistema de tormentas eléctricas, evitando daños al equipo.

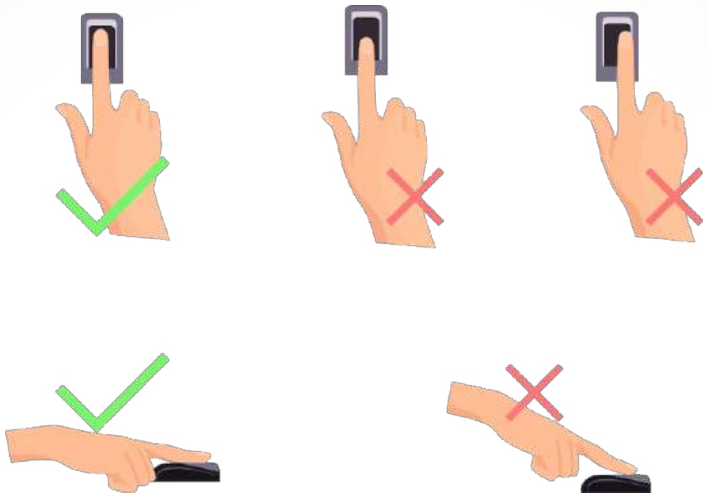
11. Instalación en áreas restringidas: Los dispositivos deben instalarse en áreas de acceso limitado.

1 Instrucciones de uso

Antes de explorar las características y funciones del dispositivo, se recomienda familiarizarse con los conceptos fundamentales que se describen a continuación.

1.1 Posición de los dedos

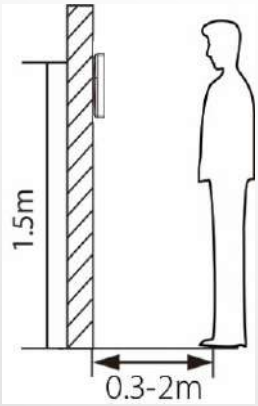
1.Dedos recomendados: Se recomienda utilizar los dedos índice, corazón o anular, y evitar el pulgar o el meñique, ya que son difíciles de colocar correctamente en el lector de huellas dactilares.



Nota: Utilice el método correcto al presionar los dedos sobre el lector de huellas dactilares para el registro y la identificación.
Nuestra empresa no asumirá ninguna responsabilidad por los problemas de reconocimiento que puedan derivarse de un uso incorrecto del producto. Nos reservamos el derecho de interpretación y modificación final en relación con este punto.

1.2 Posición de pie, postura y expresión facial

- La distancia recomendada



Se recomienda que la distancia entre el dispositivo y un usuario cuya estatura esté comprendida entre 1,55 m y 1,85 m sea de 0,3 m a 2 m.
Los usuarios pueden moverse ligeramente hacia delante o hacia atrás para mejorar la calidad de las imágenes faciales captadas.interpretación y modificación final en relación con este punto.

• Postura de pie y expresión facial recomendadas:



Nota: Durante la inscripción y la verificación, mantenga una expresión facial natural y una postura erguida.

1.3 Registro de plantillas faciales

Asegúrese de que la plantilla facial está en el centro de la pantalla durante el registro. Mire hacia la cámara y permanezca quieto durante el registro de la plantilla facial. La pantalla debe parecerse a la imagen siguiente:



• Método de registro y autenticación de rostro correcta

- **Recomendación para registrar una plantilla facial**
  - Al registrar una plantilla facial, mantenga una distancia de 40 cm a 80 cm de espacio entre el dispositivo y la plantilla facial.
  - Tenga cuidado de no cambiar su expresión facial. (Plantilla de cara sonriente, plantilla de cara dibujada, guiño, etc.)
  - Si no sigue las instrucciones de la , el registro de la plantilla facial puede tardar más o fallar.
  - Procure no tapar los ojos ni las cejas.
  - No lleve sombreros, máscaras, gafas de sol ni gafas de vista.
  - Tenga cuidado de no mostrar dos plantillas de caras en la pantalla. Registre a una persona cada vez.
  - Se recomienda que un usuario con gafas registre ambas plantillas faciales con y sin gafas.

- **Recomendación para autenticar una plantilla facial**
  - Asegúrese de que la plantilla facial aparece dentro de la directriz que aparece en la pantalla del dispositivo.
  - Si se han cambiado las gafas, la autenticación puede fallar. Si se ha registrado la plantilla facial sin gafas, siga autenticando la plantilla facial sin gafas. Si se ha registrado plantilla facial con gafas, autentique la plantilla facial con las gafas usadas anteriormente.
  - Si una parte de la plantilla facial está cubierta con un sombrero, una máscara, un parche en el ojo o unas gafas de sol, la autenticación puede fallar. No cubra la plantilla facial, permita que el dispositivo reconozca tanto las cejas como la plantilla facial.

1.4 Interfaz de espera

El dispositivo utiliza una pantalla en color de 2,4 pulgadas, y todas las operaciones se realizan a través del teclado. Tras conectar la fuente de alimentación, se muestra la siguiente interfaz de espera:



- Introduzca cualquier número para acceder a la interfaz de entrada de ID de usuario.





- Si no hay ningún superadministrador configurado en el dispositivo, pulse **M**/**OK** para ir al menú.





• Después de añadir un superadministrador en el dispositivo, se requiere la verificación del superadministrador antes de abrir las funciones del menú.



Nota: Nota: Por la seguridad del dispositivo, se recomienda registrarse como superadministrador la primera vez utilice el dispositivo.

• En la interfaz de espera, las opciones de estado de perforación también pueden mostrarse y utilizarse directamente. Las asignaciones de teclas de acceso directo se mostrarán en la pantalla si pulsa la tecla de acceso directo correspondiente en el teclado, como se muestra en la imagen siguiente. Para conocer el método de funcionamiento específico, consulte "Asignaciones de teclas de acceso directo."

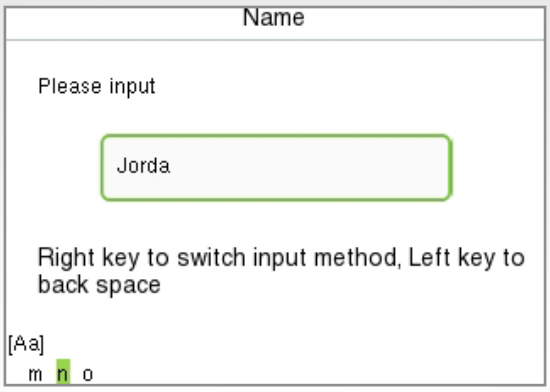


1.5 Modo T9

El modo T9 le permite introducir mayúsculas, minúsculas y caracteres especiales en los campos de entrada de texto.

Puede introducir los caracteres alfabéticos y especiales pulsando una tecla por letra. Pulse la tecla < ▶> en el cuadro de texto para activar el modo T9.

1. Desplácese hasta el campo de texto deseado y pulse <**M**/**OK**>.



2. Cada tecla del teclado tiene unas letras impresas encima. Por ejemplo, pulsando 3 puedes introducir D, E y F. Para introducir **"F"**, pulsa 3 tres veces. Esto se consigue comparando el número de pulsaciones con el diccionario sintáctico interno para determinar la letra.
3. Pulse < ▶>para cambiar entre mayúsculas, minúsculas y caracteres especiales.
4. Para añadir el carácter especial, pulse una vez la tecla correspondiente. Por ejemplo, para introducir "@" pulse 2 una vez.
5. Una vez finalizada la introducción, pulse dos veces la tecla **M**/**OK**<> para guardar.

1.6 Modo de verificación

1.6.1 Verificación de huellas dactilares

- **Modo de verificación de huellas dactilares**

El dispositivo compara la huella dactilar actual con los datos de huellas dactilares disponibles almacenados en su base de datos.
El modo de autenticación por huella dactilar se activa cuando el usuario coloca el dedo sobre el escáner de huellas dactilares.
Siga las recomendaciones para colocar el dedo en el sensor. Para más detalles, consulte la sección Colocación del dedo.

La verificación se ha realizado correctamente: Verificación fallida:



- **Modo de verificación de huellas dactilares**

El dispositivo compara la huella dactilar actual con las huellas dactilares vinculadas a la ID de usuario introducida a través del teclado.
En caso de que los usuarios no puedan acceder utilizando el método de autenticación 1:N, pueden intentar verificar su identidad utilizando el modo de verificación 1:1.

Introduzca el ID de usuario y pulse **M**/**OK** para entrar en el modo de verificación de huellas dactilares 1:1.
Si el usuario ha registrado la tarjeta, la cara y la contraseña además de la huella dactilar, y el método de verificación está configurado como Contraseña/Huella dactilar/Tarjeta/Cara, aparecerá la siguiente pantalla. Seleccione Huella dactilar para acceder al modo de verificación por huella dactilar.





Pulse la huella para verificar.

La verificación se ha realizado correctamente: Verificación fallida:

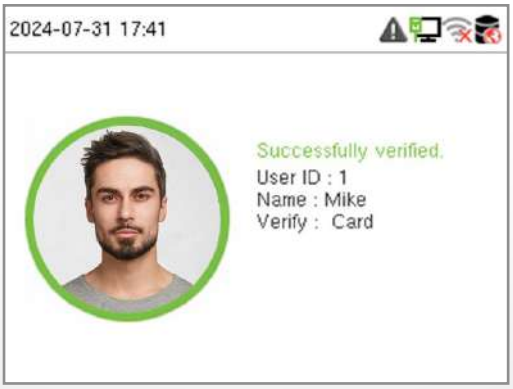




1.6.2 Verificación de huellas dactilares

- **Verificación de tarjetas 1:N**

El modo de verificación de tarjeta 1:N compara el número de tarjeta en el área de inducción de tarjeta con todos los datos de número de tarjeta registrados en el dispositivo; La siguiente pantalla se muestra en la verificación de tarjeta:



- **Verificación de tarjetas 1:1**

El modo de verificación de tarjetas 1:1 compara el número de tarjeta en el área de inducción de tarjetas con el número asociado al ID de usuario del empleado registrado en el dispositivo.
Introduzca el ID de usuario y pulse **M**/**OK** para entrar en el modo de verificación de tarjeta 1:1.



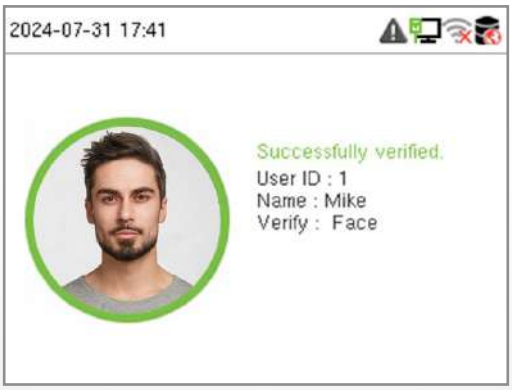
Si el usuario ha registrado la huella dactilar, la cara y la contraseña además de la tarjeta, y el método de verificación está configurado como Contraseña/Huella dactilar/Tarjeta/Cara, aparecerá la siguiente pantalla. Seleccione **Tarjeta** para acceder al modo de verificación con tarjeta.
Una vez realizada la verificación, aparecerá el mensaje **"Verificado correctamente"**, como se muestra a continuación:



1.6.3 **Verificación facial**

- **Verificación facial 1:N**

El dispositivo compara las imágenes faciales adquiridas actualmente con todos los datos de plantillas faciales registrados almacenados en su base de datos. A continuación se muestra el cuadro de diálogo emergente con el resultado de la comparación.



- **Verificación facial 1:1**

En este de verificación, el dispositivo compara la cara captada por la cámara con la plantilla facial relacionada con el ID de usuario introducido. Introduzca el ID de usuario y pulse **M/OK** para acceder al modo de verificación 1:1.



Si el usuario ha registrado la huella dactilar, la tarjeta y la contraseña además de la cara, y el método de verificación configurado como Contraseña/Huella dactilar/Tarjeta/Rostro, aparecerá la siguiente pantalla. Seleccione **Rostro** para acceder al modo de verificación facial.



Una vez realizada la verificación, aparecerá el mensaje **"Verificado correctamente"**, como se muestra a continuación:



Si falla la verificación, aparece el mensaje **"Persona no registrada"**.

1.6.4 Verificación de contraseñas

El dispositivo compara la contraseña introducida con la contraseña registrada y el ID de usuario.
Introduzca el ID de usuario y pulse **M**/**OK** para entrar en el modo de verificación de contraseña 1:1. A continuación, introduzca el ID de usuario y pulse **M**/**OK**.

Si el usuario ha registrado la huella dactilar, la tarjeta y la cara además de la contraseña, y el método de verificación está configurado como Contraseña/Huella dactilar/Tarjeta/Cara, aparecerá la siguiente pantalla. Seleccione Contraseña para acceder al modo de verificación de contraseña.





Después de introducir una contraseña correcta y una contraseña incorrecta, respectivamente, aparece la siguiente pantalla.

La verificación se ha realizado correctamente:



Verificación fallida:



1.6.5 Verificación combinada

Para aumentar la seguridad, este dispositivo ofrece la opción de utilizar múltiples formas de métodos de verificación. Se pueden utilizar un total de 21 combinaciones de verificación diferentes, como se muestra a continuación:

Símbolo de verificación combinada Definición:

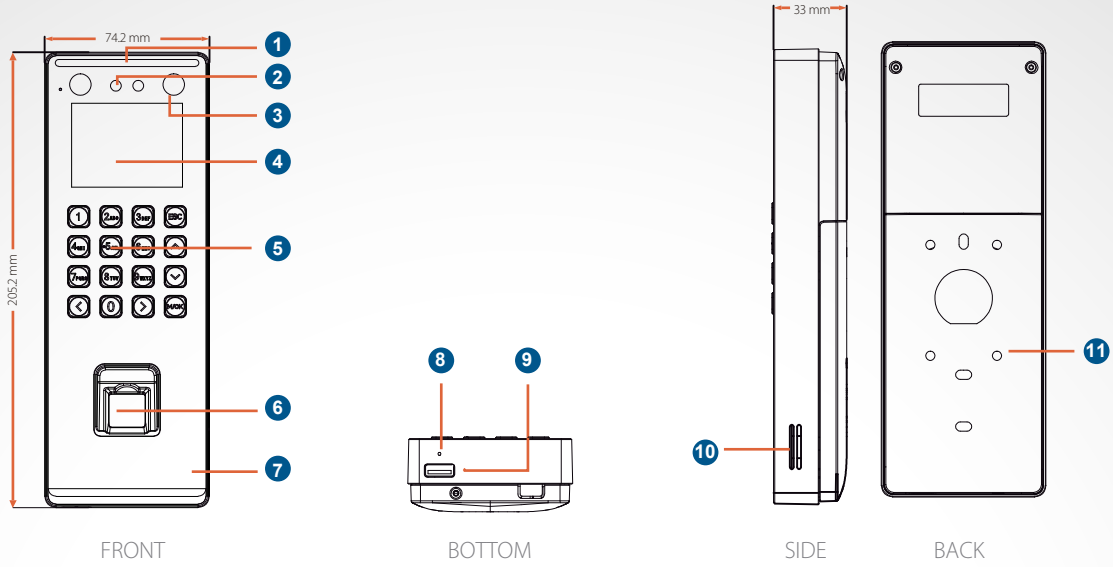
Símbolo	Definición	Explicación
/	o	Este método compara la verificación introducida de una persona con la plantilla de verificación relacionada almacenada previamente para ese ID de personal en el dispositivo.
+	y	Este método compara la verificación introducida de una persona con todas las plantillas de verificación almacenadas previamente para ese ID de personal en el dispositivo.



- **Procedimiento para configurar el modo de verificación combinada:**
  - La verificación combinada requiere que el personal registre todos los diferentes métodos de verificación. De lo contrario, los empleados no podrán verificar correctamente el proceso de verificación combinada.
  - Por ejemplo, cuando un empleado ha registrado sólo los datos, pero el modo de verificación del dispositivo está configurado como "Rostro + Contraseña", el empleado no podrá completar el proceso de verificación con éxito.
  - Esto se debe a que el Dispositivo compara la plantilla facial escaneada de la persona con plantilla de verificación registrada (tanto la plantilla facial como la contraseña) almacenada previamente para ese ID de personal en el dispositivo.
  - Pero como el empleado sólo ha registrado la plantilla facial pero no la contraseña, la verificación no se completará y el dispositivo mostrará "Verificación fallida".

2 Visión General

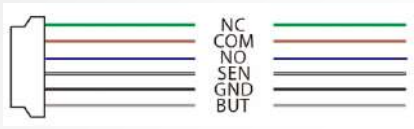
2.1 Apariencia



No.	Descripción
1	Flash
2	Cámara
3	Flash infrarrojo cercano
4	Pantalla en color de 2,4 pulgadas
5	Teclado
6	Sensor de huellas dactilares
7	Zona de lectura de tarjetas
8	Restablecer
9	USB
10	Altavoz
11	Interruptor de manipulación

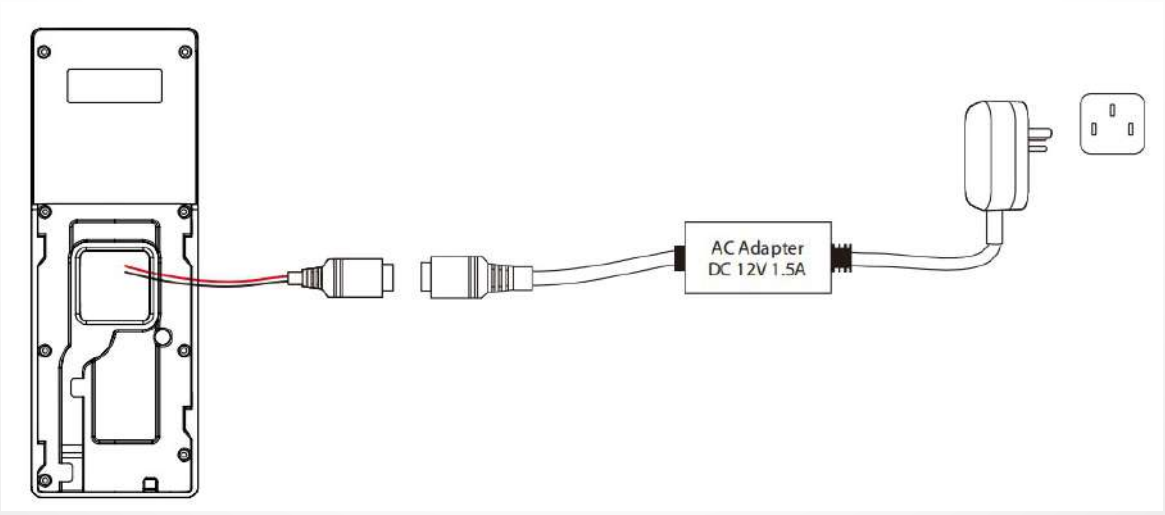
2.2 Descripción de terminales y cableado

2.2.1 Descripción del Dispositivo

Interfaz	Descripción	
	NC	Cerradura
	COM	
	NO	
	SEN	Sensor de puerta y pulsador de salida
	GND	
	PERO	
	12V Alimentación	
	Interfaz de red	

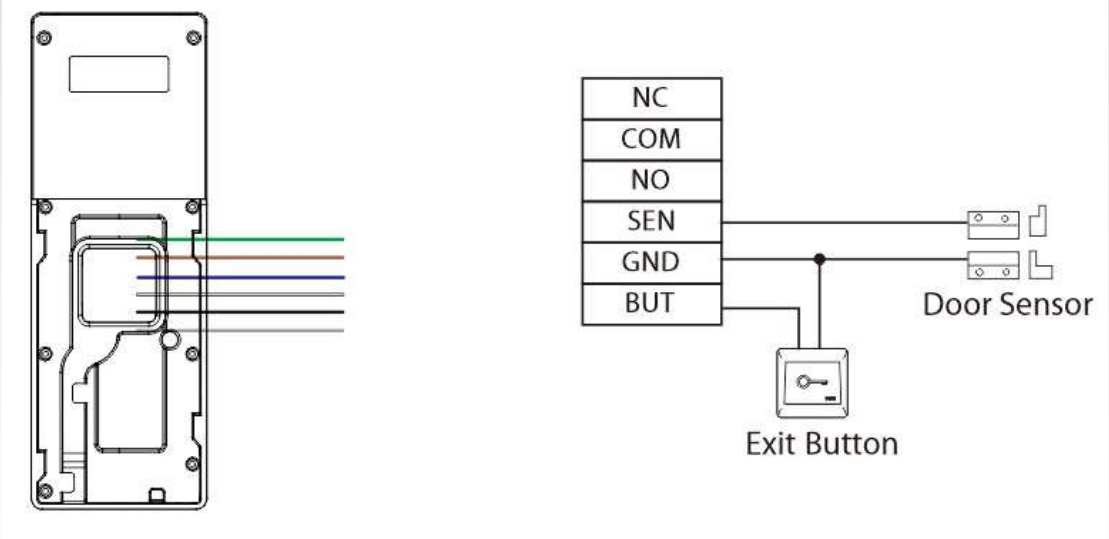
2.3 Descripción del cableado

2.3.1 Conexión eléctrica



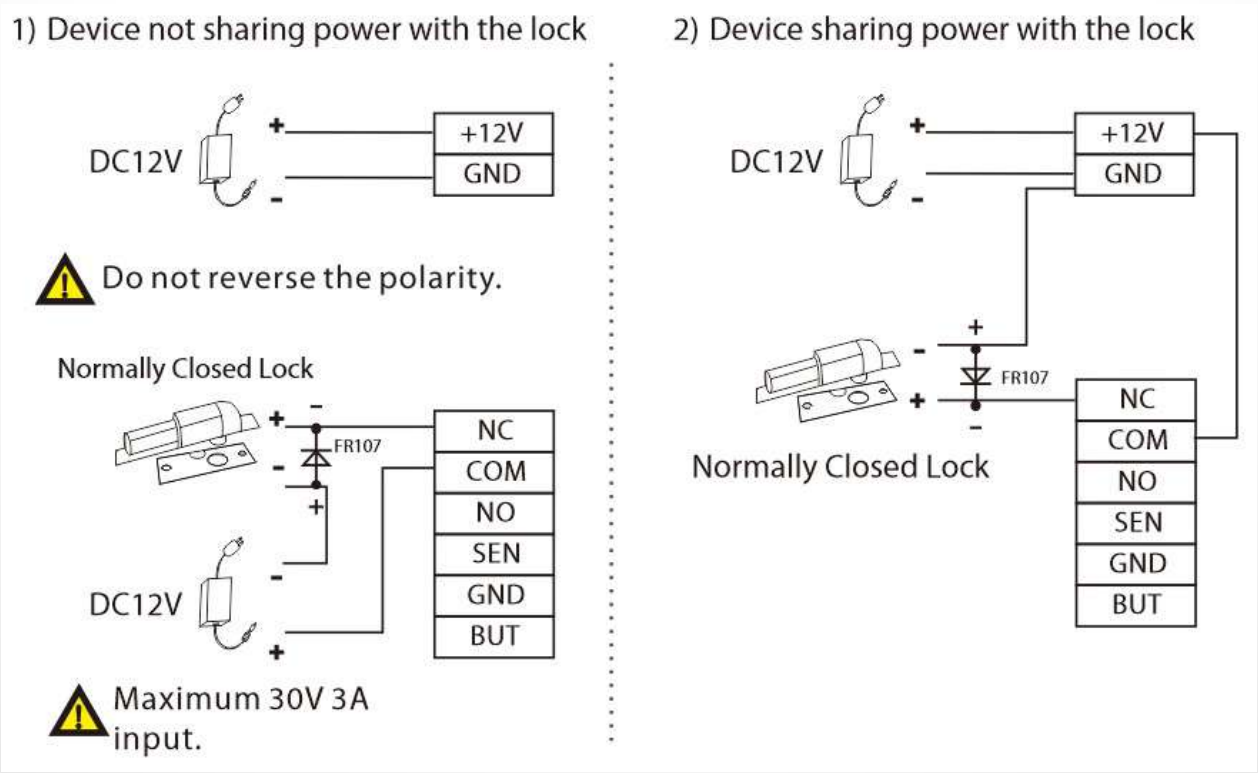
- **Fuente de alimentación recomendada**
  - Potencia nominal de 12 V y 1,5 A.
  - Para compartir la alimentación del dispositivo con otros aparatos, utilice una fuente de alimentación con mayor corriente nominal.

2.3.2 Conexión de sensor de puerta y pulsador de salida



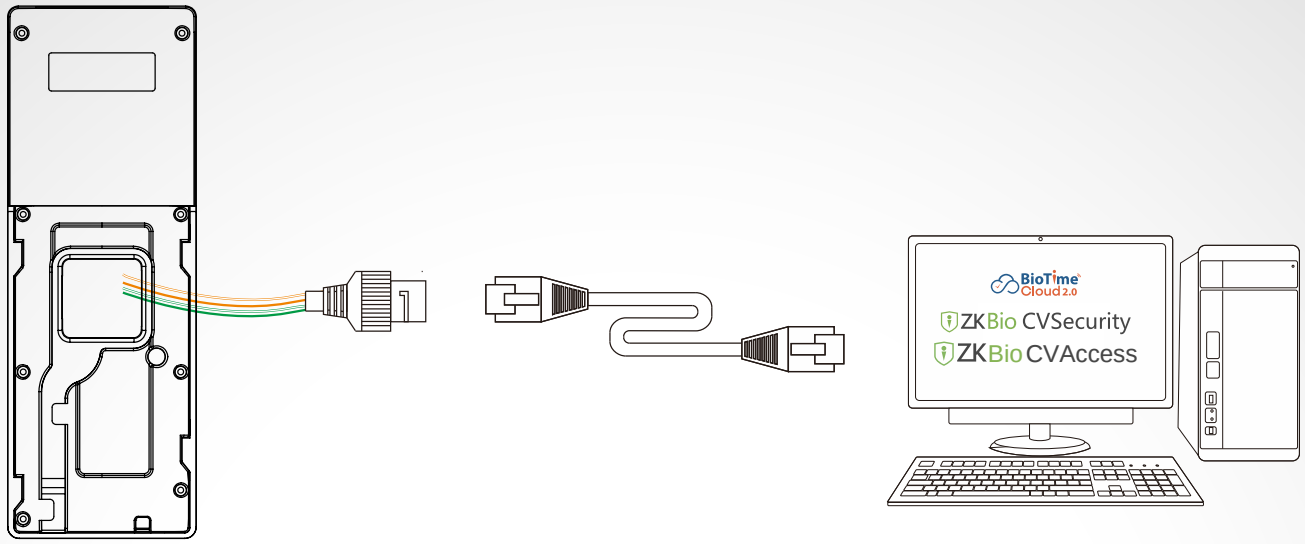
2.3.3 Conexión de sensor de puerta y pulsador de salida

El sistema admite tanto el bloqueo normalmente abierto como el bloqueo normalmente cerrado. La cerradura NO (normalmente abierta cuando está alimentada) se conecta con los terminales 'NO1' y 'COM1', y la cerradura NC (normalmente cerrada cuando está alimentada) se conecta con los terminales 'NC1' y 'COM1'. La alimentación puede ser compartida con cerradura o puede ser utilizada separadamente para la cerradura, como se muestra en el ejemplo con Cerradura NC abajo:



2.3.4 Conexión de sensor de puerta y pulsador de salida

Conecte el dispositivo al software del ordenador mediante un cable Ethernet. A continuación se muestra un ejemplo:



Default IP address: 192.168.1.201
Subnet mask: 255.255.255.0

IP address: 192.168.1.130
Subnet mask: 255.255.255.0

Nota: En una LAN, las direcciones IP del servidor (PC) y del dispositivo deben estar en el mismo segmento de red cuando se conecte al software.

3 Instalación

3.1 Entorno de instalación

Consulte las siguientes recomendaciones para la instalación.



KEEP DISTANCE


AVOID GLASS REFRACTION

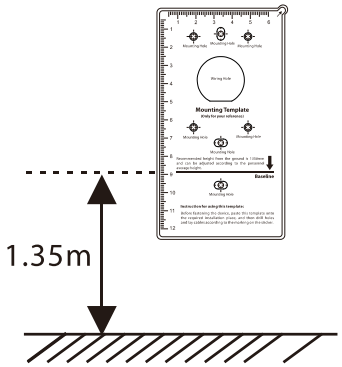

AVOID DIRECT SUNLIGHT AND EXPOSURE


AVOID USE OF ANY HEAT SOURCE NEAR THE DEVICE

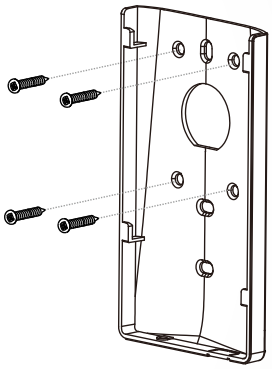
3.2 Instalación del dispositivo

1. Pega la plantilla de montaje en la pared y taladra los agujeros de acuerdo con la plantilla.
2. Fije la placa posterior en la pared con tornillos murales.
3. Fije el dispositivo a la placa posterior.
4. Fije el dispositivo a la placa posterior con un tornillo de seguridad.

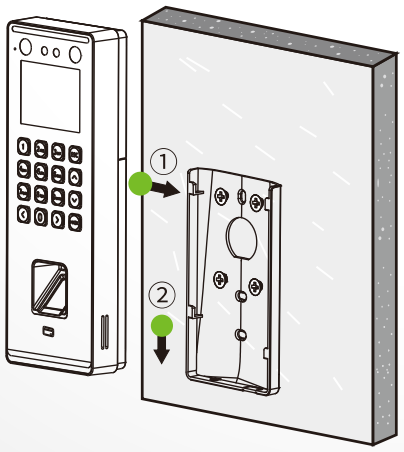
1



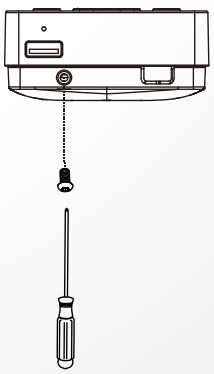
2



3



4



4 Instalación

Pulse ☰ en la interfaz de espera para entrar en el menú principal, se mostrará la siguiente pantalla:



Menú	Descripciones
Gestión de usuarios	Para añadir, editar, ver y eliminar información básica de un Usuario.
Función del usuario	Para establecer el ámbito de permiso del rol personalizado y el enrolador para los usuarios, es decir, los derechos para operar el sistema.
COM.	Para configurar los parámetros relevantes de red, conexión a pc, red inalámbrica* , servidor en la nube y diagnóstico de red.
Sistema	Para configurar los parámetros relacionados con el sistema, incluida la fecha y la hora, la configuración de los registros de asistencia/acceso, los parámetros de la plantilla facial y la huella dactilar, la configuración del tipo de dispositivo, la configuración de seguridad, la actualización del firmware en línea, la actualización USB y el restablecimiento de los valores de fábrica.
Personalice	Esto incluye la configuración de la interfaz de usuario, la voz, los horarios de timbre, las opciones de estado de perforación y las asignaciones de teclas de acceso directo.
Gestión de datos	Para borrar todos los datos relevantes del dispositivo.
Control de acceso	Para configurar los parámetros de la cerradura y el dispositivo de control de acceso correspondiente, incluidas opciones como la configuración de reglas horarias, la configuración de vacaciones, la verificación de combinación y la configuración de opciones de coacción.
Gestor USB	Para cargar o descargar los datos específicos mediante una unidad USB.
Búsqueda de asistentes	Para consultar los registros de eventos especificados, comprobar las fotos de asistencia y bloquear las fotos de asistencia.
Autotest	Para comprobar automáticamente si cada módulo funciona correctamente, incluidos la pantalla LCD, el audio, el teclado, la cámara, el sensor de huellas dactilares y el reloj en tiempo real.
Información del sistema	Para ver la capacidad de datos, la información sobre el dispositivo y el firmware y la política de privacidad del dispositivo.

Nota: Cuando los usuarios utilicen el producto por primera vez, deberán hacerlo después de configurar los privilegios de administrador. Pulse Gestión de usuarios para añadir un administrador o editar los permisos de usuario como superadministrador. Si el producto no tiene una configuración de administrador, el sistema mostrará una solicitud de comando de configuración de administrador cada vez que acceda al menú del dispositivo.


2024-07-31 14:34
14:34
2024-07-31 Wednesday
To ensure system security, please create an admin a
ccount.
OK

5 Instalación

5.1 Entorno de instalación

Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y entre en **User Mgt.**> **New User**.

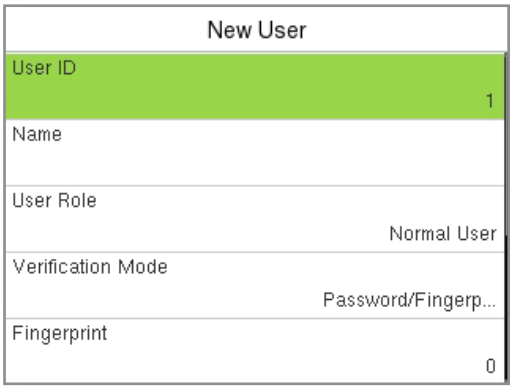




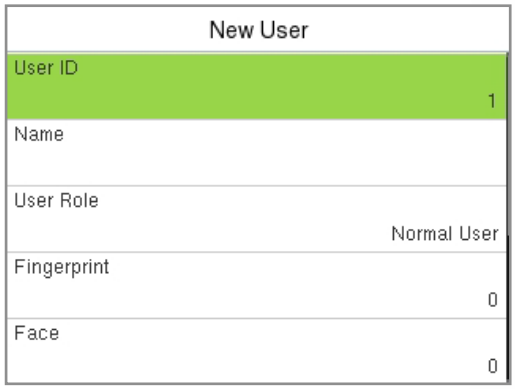
5.1.1 ID y nombre de usuario

Introduzca el **ID de usuario** y el **nombre**.

Dispositivo de gestión de asistencia:



Dispositivo de control de acceso:



Nota:

• Un nombre de usuario puede contener un máximo de 34 caracteres.

• El ID de usuario puede contener de 1 a 14 dígitos por defecto, admitiendo tanto números como caracteres alfabéticos.

• Durante el registro inicial, puede modificar su ID, que no podrá modificarse después del registro.

• Si el mensaje "¡Duplicado!", debe elegir otro ID, ya que el ID de usuario introducido ya existe.

5.1.1 Función del usuario

En la interfaz Nuevo usuario, seleccione **Rol de usuario** para establecer el rol del usuario como **Usuario normal** o **Superadministrador.**

• **Super Administrador**: El Super Administrador posee todos los privilegios de gestión en el Dispositivo.

• **Usuario Norma**l: Si el Super Admin ya está registrado en el Dispositivo, los Usuarios Normales no tendrán privilegios para gestionar el sistema y sólo podrán acceder a las verificaciones de autenticación.

• **Roles Definidos por el Usuario:** El Usuario Normal también puede ser configurado con **Roles Definidos** por el Usuario que son los roles personalizados que pueden ser configurados para el Usuario Normal.



Nota: Si el rol de usuario seleccionado es el de Superadministrador, el usuario debe pasar la autenticación de identidad para acceder al menú principal. La autenticación se basa en el método o métodos de autenticación que el superadministrador haya registrado. Consulte Modo de verificación.

5.1.3 Función del usuario

Seleccione el modo de verificación para el usuario, se pueden utilizar un total de 21 combinaciones de verificación diferentes. Consulte 1.6.5 verificación combinada para obtener más detalles.

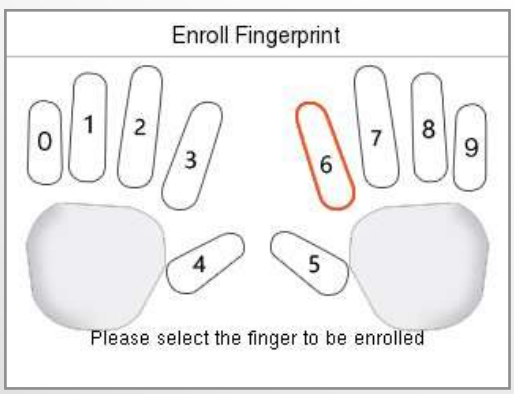
Nota: Esta función sólo es válida para el Terminal de Control Horario.



5.1.4 Registrar huella dactilar

Seleccione **Huella dactilar** en la interfaz **Nuevo usuario** para acceder a la página de registro de huellas dactilares.

- Seleccione el dedo que desea inscribir.
- Presiona el mismo dedo en el lector de huellas tres veces.
- El color verde indica que la huella digital se ha registrado correctamente.





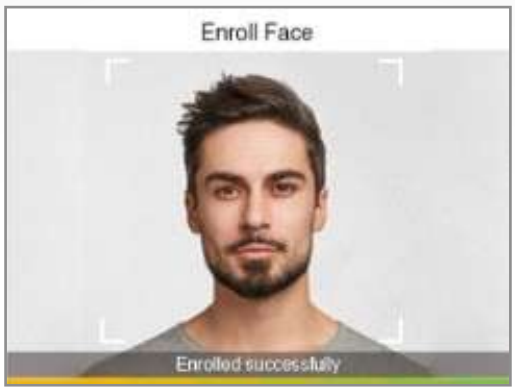
5.1.5 Plantilla de cara al registro

Seleccione **rostro** en la interfaz de **nuevo usuario** para acceder a la página de registro de caras.

• Mire hacia la cámara, coloque la plantilla facial dentro del recuadro blanco de guía y permanezca quieto durante el registro de la plantilla facial.

• Aparecerá una barra de progreso mientras se registra la plantilla facial y se mostrará el mensaje "Registrado correctamente"a medida que se completa la barra de progreso.

• Si la plantilla de cara ya está registrada, aparecerá el mensaje "Cara duplicada". La interfaz de registro es la siguiente:

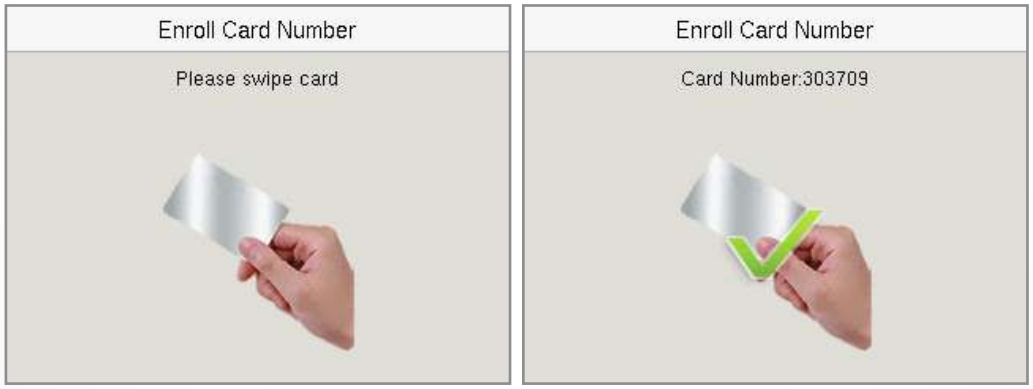


5.1.6 Tarjeta

Seleccione **Tarjeta** en la interfaz **Nuevo usuario** para acceder a la página de registro de tarjetas.

• En la interfaz de tarjetas, pase la tarjeta por debajo de la zona de lectura de tarjetas. El registro de la tarjeta realizará correctamente.

• Si la tarjeta ya está registrada, aparecerá el mensaje **"Tarjeta duplicada"**. La interfaz de registro es la siguiente:



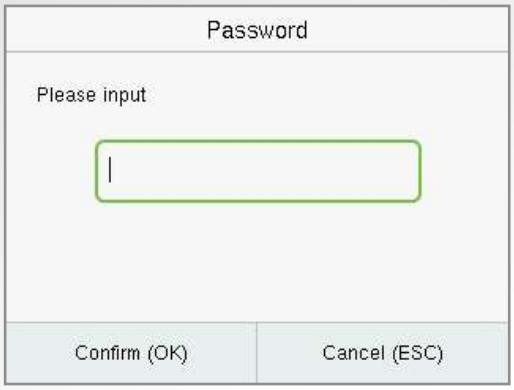
5.1.7 Contraseña

Seleccione **Contraseña** en la interfaz **Nuevo usuario** para acceder a la página de registro de la contraseña.

• En la interfaz Contraseña, introduzca la contraseña deseada, vuelva a introducirla para confirmarla y pulse **M**/**OK**.

• Si la reintroducida es diferente de la introducida inicialmente, el dispositivo mostrará el mensaje **"La contraseña no coincide"**, en el que el usuario deberá volver a confirmar la contraseña.

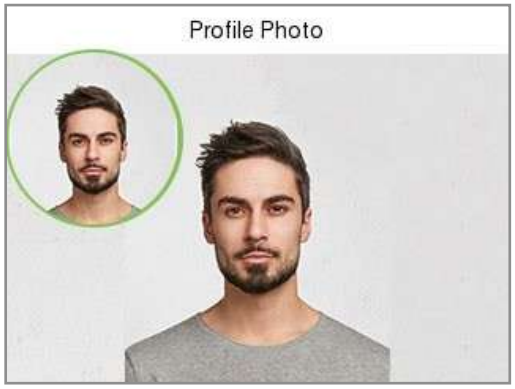
contraseña de nuevo.
• La contraseña puede contener de 6 a 8 dígitos por defecto.





5.1.8 Foto de perfil

Seleccione **Foto de perfil** en la interfaz de **nuevo usuario** para ir a la página de registro de Foto de perfil.



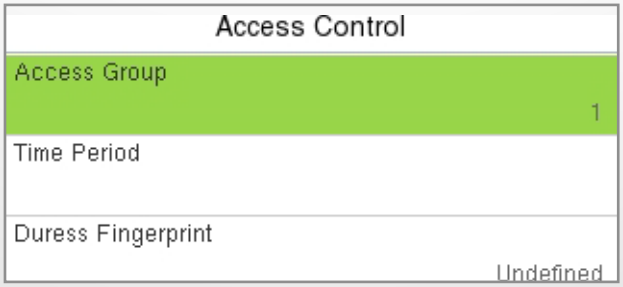
• Cuando un usuario registrado con una foto supere la autenticación, se mostrará la foto registrada.
• Pulse Foto de perfil, se abrirá la cámara del dispositivo y, a continuación, pulse M/OK para hacer una foto. La foto capturada se muestra en la esquina superior izquierda de la pantalla y la cámara se abre de nuevo para tomar una nueva foto, después de tomar la foto inicial.

Nota: Al registrar una plantilla facial, el sistema captura automáticamente una foto como foto de perfil del usuario. Si no
registra una foto de perfil, el sistema establece automáticamente la foto capturada durante el registro foto predeterminada.

5.1.9 Función de control de acceso

La función de control de acceso establece los privilegios de acceso a la puerta para cada usuario. Incluye el grupo de acceso, la huella dactilar de coacción y permite establecer el periodo de acceso del grupo.

Nota: Esta función sólo está disponible para el terminal de control de acceso.

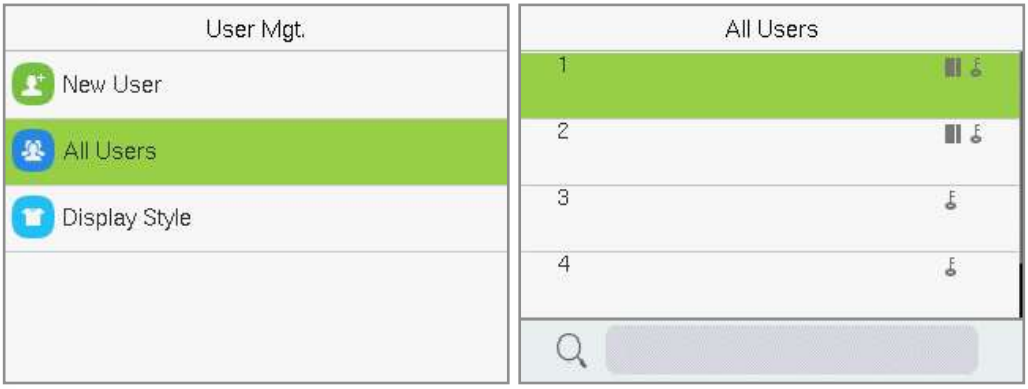


• Pulse **Access Control Role**> **Access Group**, para asignar los usuarios registrados a diferentes grupos para una mejor gestión. Los nuevos usuarios pertenecen al Grupo 1 por defecto y pueden ser reasignados a otros grupos. El dispositivo admite hasta 99 grupos de Control de Acceso.
• Pulse **Periodo de tiempo**, para seleccionar el periodo de tiempo a utilizar.
• El usuario puede especificar una o varias huellas dactilares registradas como huellas de coacción. Al pulsar el dedo correspondiente a la huella de coacción en el sensor y pasar la verificación, el sistema generará inmediatamente una alarma de coacción.

5.2 Entorno de instalación

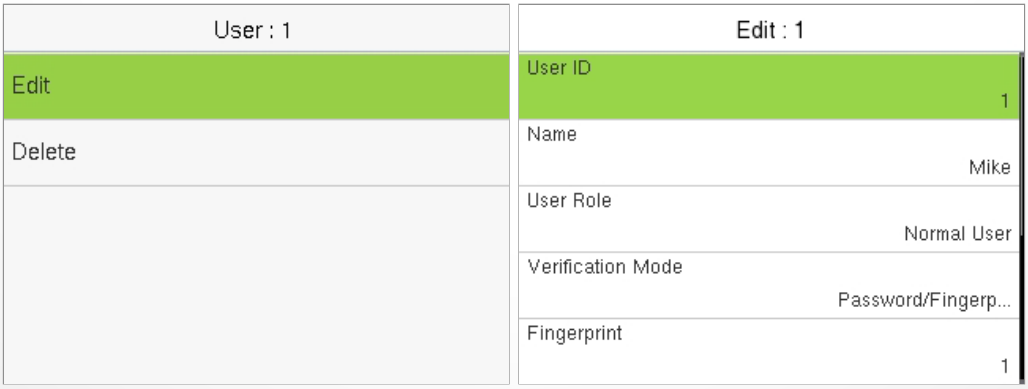
Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y entre en **User Mgt.**> **All Users**.

• En la interfaz **Todos los usuarios**, seleccione la barra de búsqueda de la lista de usuarios para introducir la palabra clave de recuperación necesaria (donde la palabra clave puede ser el ID de usuario, los apellidos o el nombre completo) y el sistema buscar la información del usuario relacionada.



5.3 Entorno de instalación

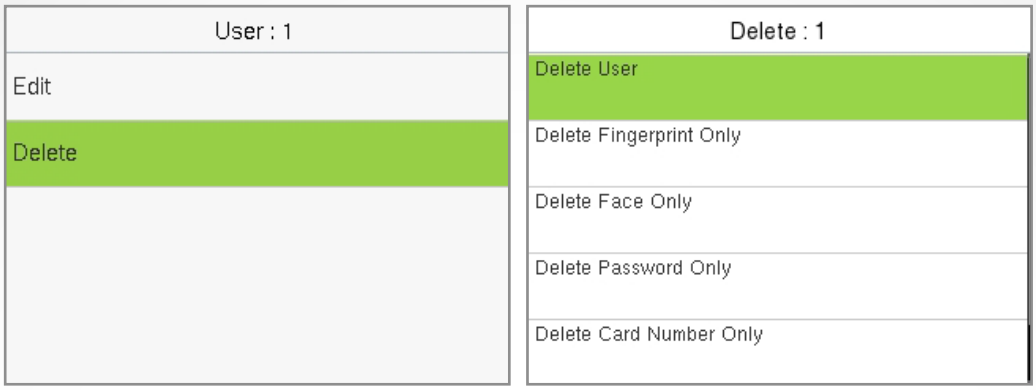
En la interfaz **Todos los usuarios**, seleccione el usuario deseado de la lista, pulse **M/OK** y seleccione **Editar** para editar la información del usuario.



5.4 Eliminar Usuario

En la interfaz **Todos los usuarios**, seleccione el usuario deseado de la lista, pulse **M/OK** y seleccione **Eliminar** para borrar el usuario o la información de un usuario específico del dispositivo. En la interfaz **Eliminar** , seleccione la operación deseada y pulse **M/OK** para confirmar la eliminación.

• Operaciones de supresión:
Borrar Usuario: Se borrará toda la información del usuario (borra el Usuario seleccionado en su totalidad) del Dispositivo.
Borrar sólo huella dactilar: Elimina la información de la huella dactilar del usuario seleccionado.
Borrar sólo Rostro: Borra la información de la plantilla facial del usuario seleccionado.
Borrar sólo contraseña: Borra la información de la contraseña del usuario seleccionado.
Borrar sólo número de tarjeta: Elimina la información de la tarjeta del usuario seleccionado.
Borrar sólo foto perfil: Elimina la foto de perfil del usuario seleccionado.

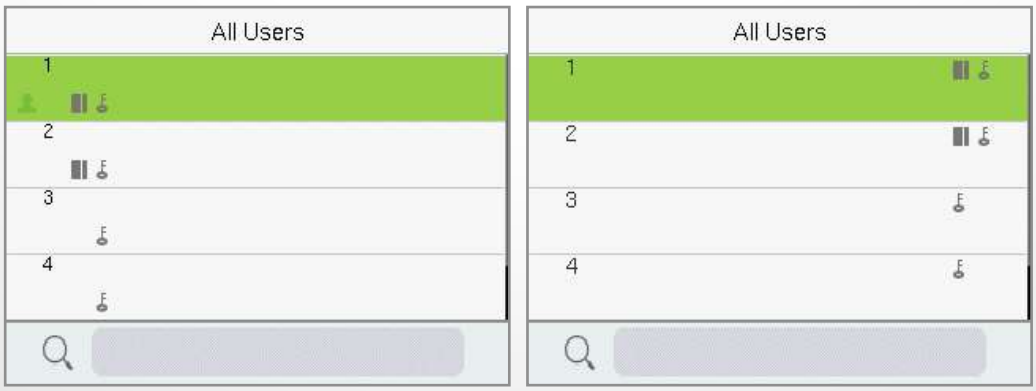


5.4 Estilo de visualización

Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y entre en **User Mgt.**> **Display Style**.



A continuación se muestran diferentes estilos de visualización:



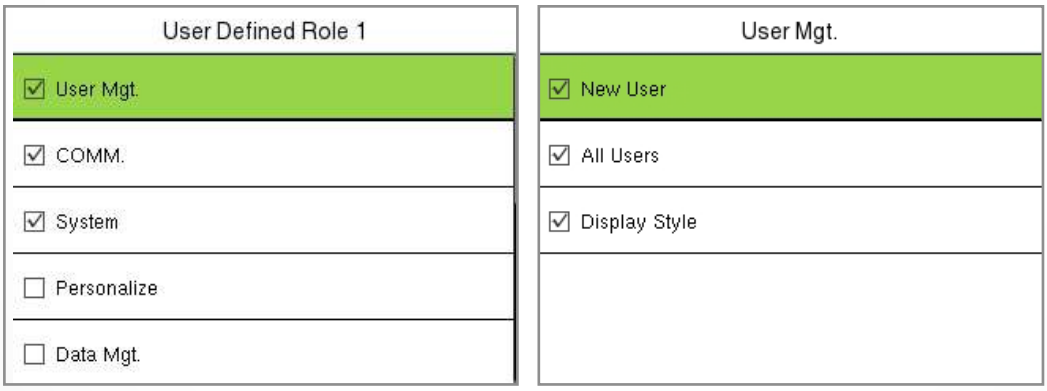
6 Función del usuario

El rol de usuario facilita la asignación de permisos específicos a usuarios concretos, en función de las necesidades.

- Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** e introduzca **User Role**> **User Defined Role** para establecer los permisos definidos por el usuario.
- El ámbito de permisos del rol personalizado se puede configurar en 3 roles, es decir, el rol personalizado ámbito operativo de las funciones de menú del usuario.



- A continuación, seleccionando en Definir rol de usuario, seleccione los privilegios necesarios para el nuevo rol y pulse la tecla **M/OK**.
- En primer lugar, seleccione el nombre de la función del menú principal que desee y, a continuación, pulse **M/OK** y seleccione los submenús que desee de la lista.

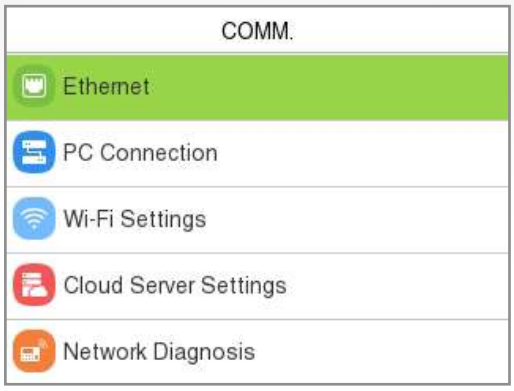


Nota: Si el rol de usuario está habilitado para el dispositivo, pulse **Gestión de usuarios** > **Nuevo usuario** > **Rol de usuario** para asignar los roles creados a los usuarios necesarios. Pero si no hay ningún superadministrador registrado en el equipo, éste le preguntará «Por favor, inscriba primero al superadministrador» cuando active la función Rol de usuario.

7 Ajustes de comunicación

Los Ajustes de Comunicación se utilizan para configurar los parámetros de la Red, Conexión a PC, Wi-Fi * , Servidor Cloud y Diagnóstico de Red.

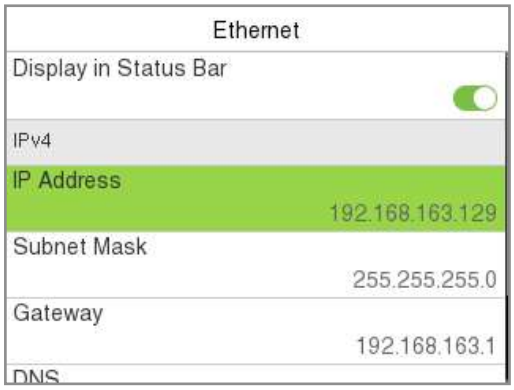
Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y seleccione COMM.



7.1 Ajustes de red

Cuando el dispositivo necesita comunicarse con un PC a través de Ethernet, es necesario configurar los ajustes de red y asegurarse de que el dispositivo y el PC se conectan al mismo segmento de red.

Seleccione **Ethernet** en la **interfaz COMM**. Settings para configurar los ajustes.



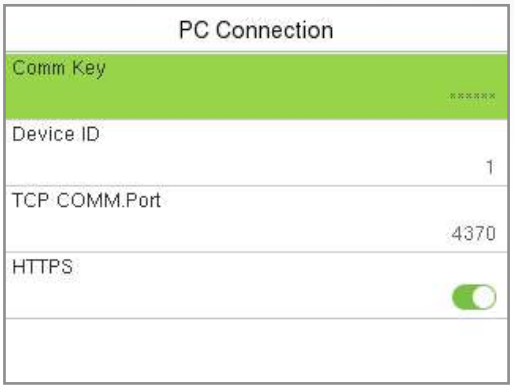
Nombre de la función	Descripciones
Visualización en la barra de estado	Seleccione si desea mostrar el icono de red en la barra de estado.
Dirección IP	La dirección IP por defecto es 192.168.1.201. Puede modificarse en función de la disponibilidad de la red.
Máscara de subred	La máscara de subred por defecto es 255.255.255.0. Puede modificarse en función de la disponibilidad de la red.
Pasarela	La dirección de puerta de enlace por defecto es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red.
DNS	La dirección DNS por defecto es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red.
DHCP	El protocolo de configuración dinámica de host sirve para asignar dinámicamente direcciones IP a los clientes a través del servidor.

7.2 Conexión a PC

Pulse **Conexión PC** en la interfaz **Config**. para configurar los ajustes de comunicación.

Comm Key facilita mejorar seguridad de los datos estableciendo la comunicación entre el dispositivo y el PC. Una vez configurada la Comm Key, se requiere una contraseña para conectar el dispositivo al software del PC.

Seleccione **Conexión PC** en la interfaz **COMM**. Ajustes para configurar los ajustes de comunicación.



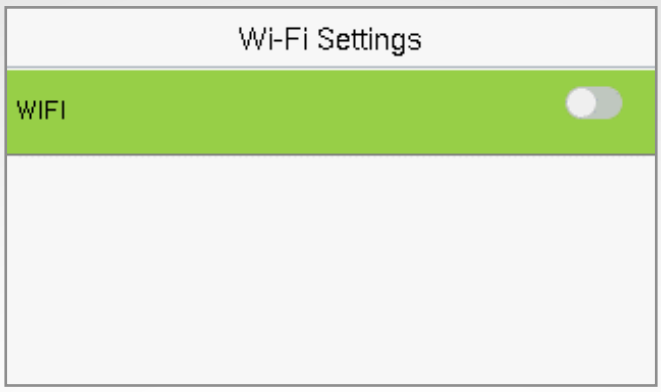
Nombre de la función	Descripciones
Clave de comunicación	La contraseña por defecto es 0 y puede cambiarse. La clave de comunicación puede contener de 1 a 6 dígitos.
ID del dispositivo	Número de identidad del , que oscila entre 1 y 254. Si el método de comunicación es RS232/RS485, deberá introducir este ID de dispositivo en la interfaz de comunicación del software.
TCP COMM. Puerto	El valor por defecto del puerto TCP COMM es 4370. Puede modificarse en función de la disponibilidad de la red.
HTTPS	Para aumentar la seguridad del acceso al software, los usuarios pueden activar el protocolo HTTPS para crear una transmisión de red segura y cifrada y garantizar la seguridad de los datos enviados mediante la autenticación de identidades y la comunicación cifrada. Esta función está activada por defecto. Esta función se puede activar o desactivar a través de la interfaz de menú, y al cambiar el estado HTTPS el dispositivo mostrará un mensaje de seguridad y se reiniciará después de la confirmación.

7.3 Conexión a PC ★

El dispositivo incluye un módulo Wi-Fi, que puede estar integrado en el molde del dispositivo o puede conectarse externamente.

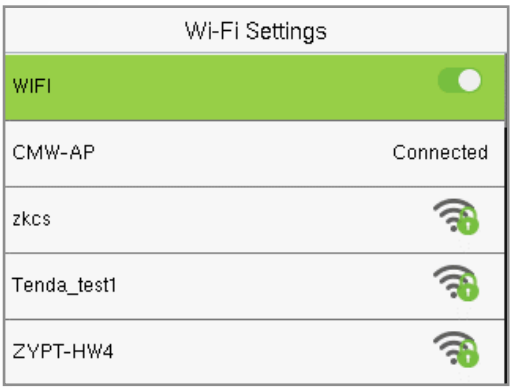
El módulo Wi-Fi permite la transmisión de datos a través de Wi-Fi (fidelidad inalámbrica) y establece un entorno de red inalámbrica. El Wi-Fi está activado por defecto en el dispositivo. Si no necesita utilizar la red Wi-Fi, puede desactivar el botón Wi-Fi.

Seleccione **Wi-Fi Settings** (Configuración Wi-Fi) en la interfaz **COMM**. Ajustes para configurar los ajustes Wi-Fi.

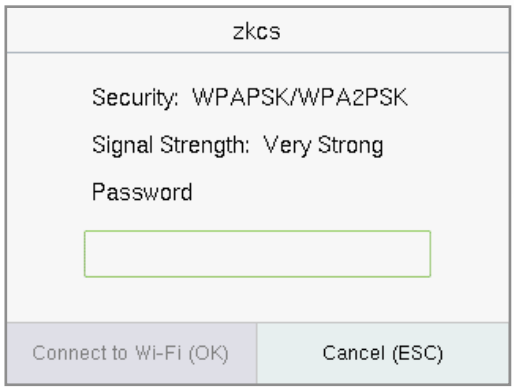


• Busque la red WIFI

• WIFI está activado en el dispositivo por defecto. Pulse el botón para activar o desactivar la WIFI.
• Una vez activada la WIFI, el dispositivo buscará las WIFI disponibles dentro del alcance de la red.
• Elija el nombre de la red Wi-Fi adecuada de la lista disponible, introduzca la contraseña correcta en la interfaz de contraseña y pulse M/OK.



WIFI Activado: Pulse en la red deseada de la lista de redes buscadas.



Pulse en el campo de la contraseña para introducirla y, a continuación, pulse **M/OK**.

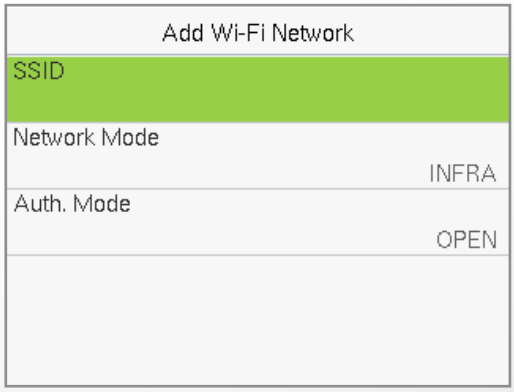
• Cuando la WIFI se haya conectado correctamente, la interfaz inicial mostrará el logotipo de Wi-Fi.

• Añadir red WIFI manualmente

La Wi-Fi también puede añadirse manualmente si la Wi-Fi requerida no aparece en la lista.



Pulse en **Añadir Red WIFI** para añadir la WIFI manualmente.

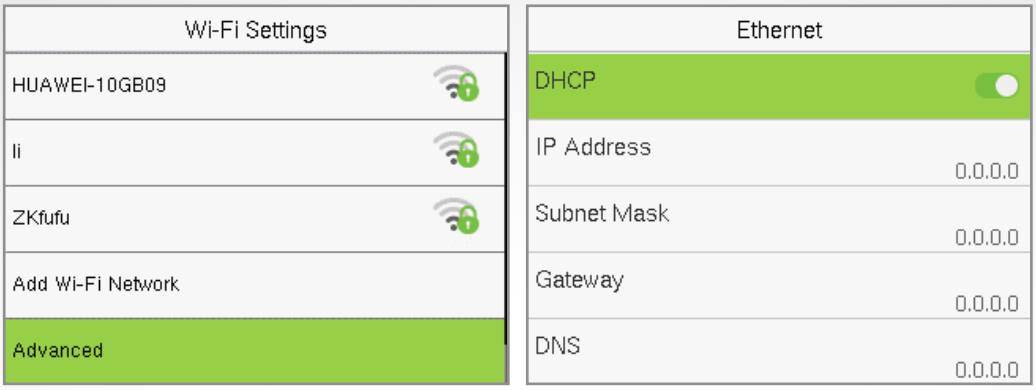


En esta plantilla de interfaz, introduzca los parámetros de la redWIFI. (La red añadida debe existir).

Note: After successfully adding the WIFI manually, follow the same process to search for the added WIFI name.

• Configuración avanzada

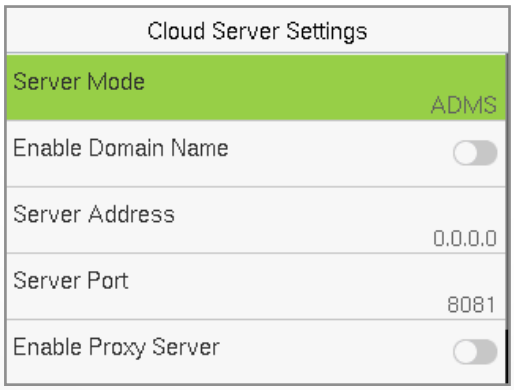
En la interfaz de red inalámbrica, pulse en Avanzado para configurar los parámetros pertinentes según sea necesario.



Nombre de la función	Descripciones
DHCP	El Protocolo de Configuración Dinámica de Host (DHCP) asigna dinámicamente direcciones IP a los clientes de la red. Si el DHCP está activado, la IP no se puede configurar manualmente.
Dirección IP	Dirección IP para la red WIFI, por defecto es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red.
Máscara de subred	La máscara de subred por defecto es 255.255.255.0. Puede modificarse en función de la disponibilidad de la red.
Pasarela	La dirección de puerta de enlace por defecto es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red.
DNS	La dirección DNS por defecto es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red.

7.4 Configuración del servidor en nube

Pulse **Cloud Server Setting** en la interfaz **Comm**. Settings para conectar con el servidor ADMS.

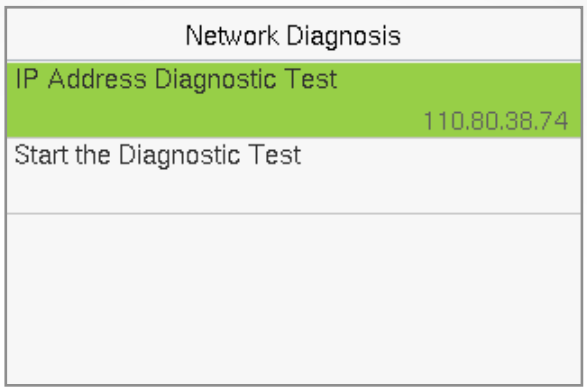


Nombre de la función		Descripciones
Habilitar nombre de dominio	**Dirección del servidor**	Una vez activada esta función, se utilizará el modo de nombre de dominio «http://... "como http://www.XYZ.com, mientras que "XYZ» denota el nombre de dominio (cuando este modo está activado).
Dirección IP	**Dirección del servidor**	Dirección IP del servidor ADMS.
	Puerto del Servidor	Puerto utilizado por el servidor ADMS.
Activar Servidor Proxy		Cuando elijas activar el proxy, deberás establecer la dirección IP y el número de puerto del servidor proxy.

7.4 Diagnóstico de la red

Ayuda a configurar los parámetros de diagnóstico de red.

Seleccione Diagnóstico de red en la interfaz COMM. Configuración. Introduzca la dirección IP que debe diagnosticarse y pulse Iniciar la prueba de diagnóstico para comprobar si la red puede conectarse al dispositivo.

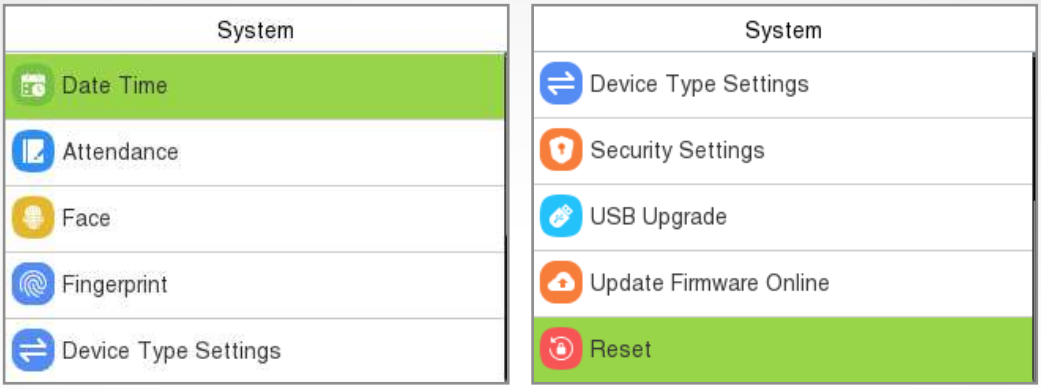


8 Configuración del Sistema

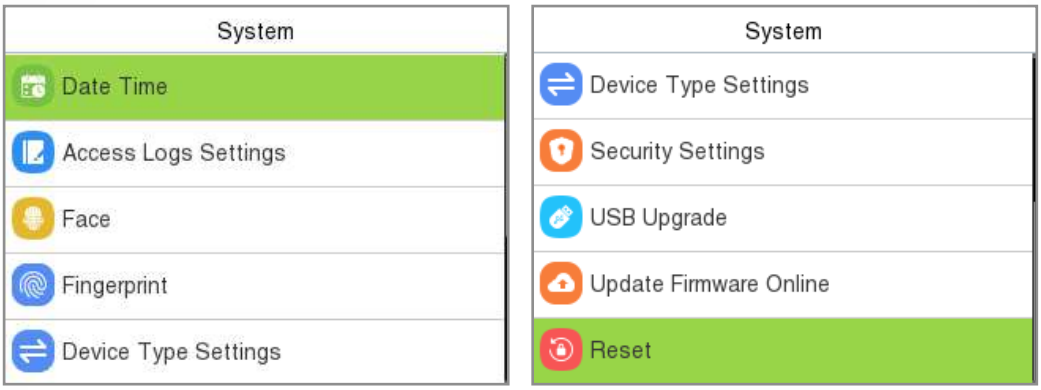
Configure los parámetros del sistema relacionados para optimizar el rendimiento del dispositivo.

Cuando el dispositivo se encuentre en la interfaz inicial, pulse **M/OK** y seleccione Sistema.

Dispositivo de gestion de asistencia:

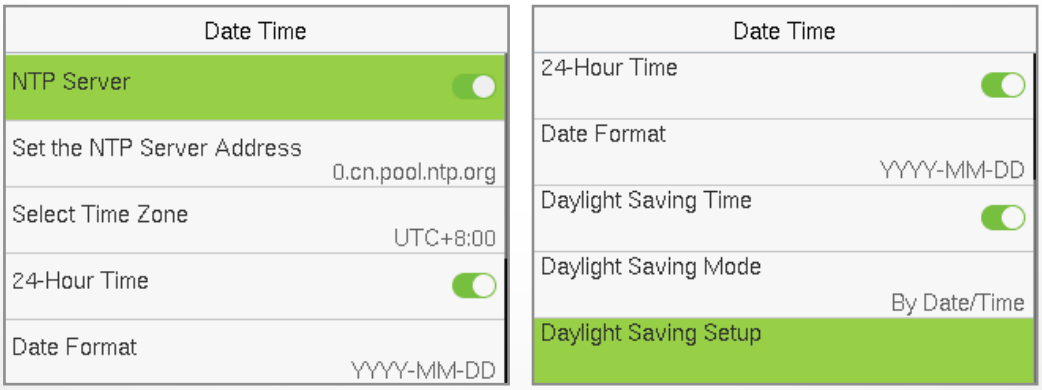


Dispositivo de Control de Accesol:



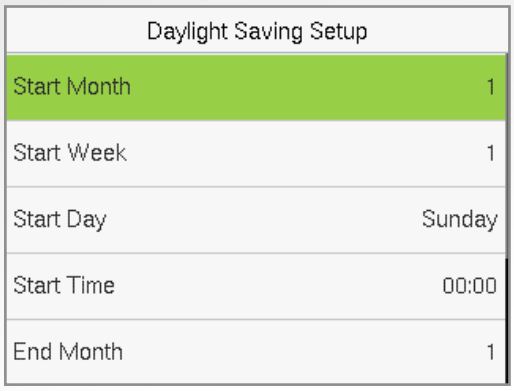
8.1 Fecha y hora

Seleccione Fecha Hora en la interfaz Sistema para ajustar la fecha y la hora.

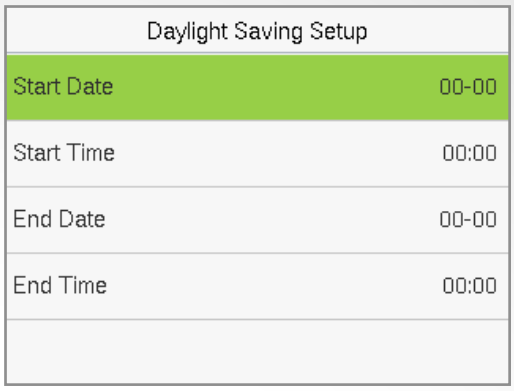


- Pulse **Servidor NTP** para activar la sincronización horaria automática basada en la dirección de servicio introducida.
- Pulse **Fecha y hora manual** para ajustar manualmente la fecha y la hora y, a continuación, pulse **M/OK** y Guardar.
- Pulse **Seleccionar zona horaria** para seleccionar manualmente la zona horaria en la que se encuentra el dispositivo.
- Active o desactive este formato seleccionando Hora 24 horas. Si está activado, pulse **Formato de fecha** para ajustar la fecha.

• Pulse **Horario de verano** para activar o desactivar la función. Si está activada, pulse **Modo de ahorro de luz diurna** para seleccionar un modo de ahorro de luz diurna y, a continuación, pulse Configurar **ahorro de luz diurna** para ajustar la hora del cambio.



Week Mode



Date Mode

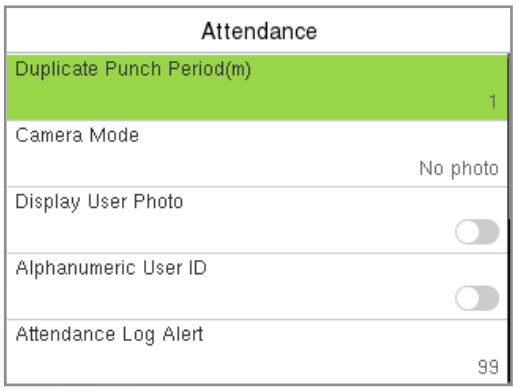
• Al restaurar los ajustes de fábrica, se puede restaurar la hora (24 horas) y el formato de fecha (AAAA-MM-DD), pero no se puede restaurar la fecha y la hora del dispositivo.

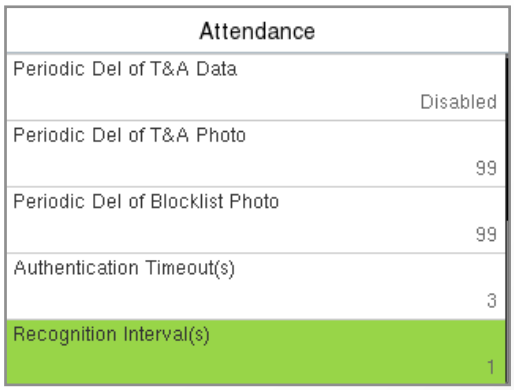
Nota: Por ejemplo, el usuario ajusta la hora del equipo (18:35 del 15 de marzo de 2019) a las 18:30 del 1 de enero de 2020.Tras restablecer los ajustes de fábrica, la hora del equipo seguirá siendo las 18:30 del 1 de enero de 2020.

8.2 Configuración de los registros de acceso

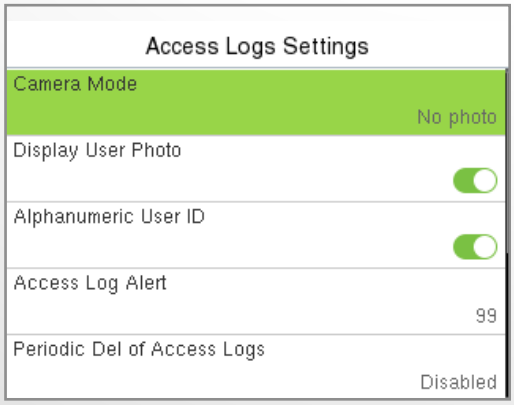
Seleccione Configuración de Asistencia/Registros de Acceso en la interfaz del Sistema.

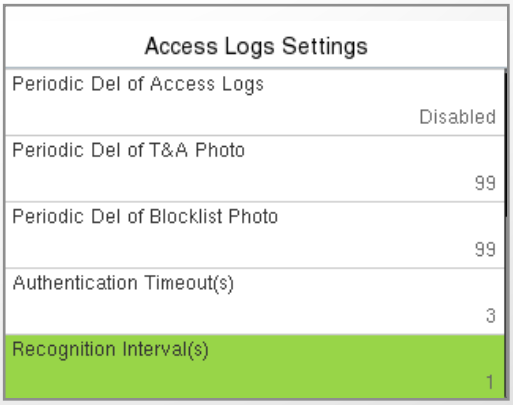
Dispositivo de Gestión de asistencia:





Dispositivo de Control de Accesol:





Nombre de la función	Descripciones
Umbral 1:N	En el modo de verificación 1:N, la verificación solo será exitosa cuando la similitud entre la imagen facial adquirida y todos los templates faciales registrados sea mayor que el valor establecido. El valor válido varía de 0 a 100. Cuanto más alto sea el umbral, menor será la tasa de error, pero mayor será la tasa de rechazo, y viceversa. Se recomienda establecer el valor predeterminado en 40.
Umbral 1:1	En el modo de verificación 1:1, la verificación solo será exitosa cuando la similitud entre la imagen facial adquirida y el template facial del usuario registrado en el dispositivo sea mayor que el valor establecido. El valor válido varía de 0 a 100. Cuanto más alto sea el umbral, menor será la tasa de error, pero mayor será la tasa de rechazo, y viceversa. Se recomienda establecer el valor predeterminado en 30.
Umbral de registro facial	Durante el registro del template facial, se utiliza la comparación 1:N para determinar si el usuario ya se ha registrado previamente. Cuando la similitud entre la imagen facial adquirida y todos los templates faciales registrados es mayor que este umbral, indica que el template facial ya ha sido registrado.
Calidad de imagen	Calidad de imagen para el registro y la comparación facial. Cuanto mayor sea el valor, más clara deberá ser la imagen.
Distancia de Reconicmiento facial	Cuanto más lejos esté la persona, más pequeña será la cara y menor será el número de píxeles de la cara obtenida por el algoritmo. Por lo tanto, ajustar este parámetro puede modificar la distancia máxima de comparación de las caras.
Valor de activación de la luz LED	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, la luz LED se encenderá o apagará con mayor frecuencia.
Detección de vida	Detecta el intento de suplantación utilizando imágenes con luz visible para determinar si la muestra biométrica proporcionada corresponde a una persona real (un ser humano en vivo) o una representación falsa.
Umbral de detección de vida	Facilita la evaluación de si la imagen visible capturada corresponde a una persona real (un ser humano en vivo). Cuanto mayor sea el valor, mejor será el rendimiento anti-suplantación utilizando luz visible.
Anti-suplantación utilizando NIR (Infrarrojo cercano)	Utilizando imágenes con espectros de infrarrojo cercano (NIR) para identificar y prevenir ataques de fotos y videos falsos.
Umbral de detección de vida binocular	Facilita la evaluación de si la imagen con espectro de infrarrojo cercano es una foto o video falso. Cuanto mayor sea el valor, mejor será el rendimiento anti-suplantación de la imagen con espectro de infrarrojo cercano.
AE de Rostro (Ajuste de exposición facial)	Cuando el rostro está frente a la cámara en el modo AE de rostro, el brillo del área del rostro aumenta, mientras que las otras áreas se vuelven más oscuras.
WDR	El Rango Dinámico Amplio (WDR) equilibra la luz y amplía la visibilidad de la imagen en videos de vigilancia en escenas con iluminación de alto contraste, mejorando la identificación de objetos en entornos con luces brillantes y oscuras. Mejorar el plan, Mayor acceso a los mejores modelos.
Modo anti-parpadeo	Se utiliza cuando el WDR está desactivado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea a la misma frecuencia que la luz. Mayor acceso a los mejores modelos.
Algoritmo facial	Información relacionada con el algoritmo facial y pausa en la actualización del template facial.

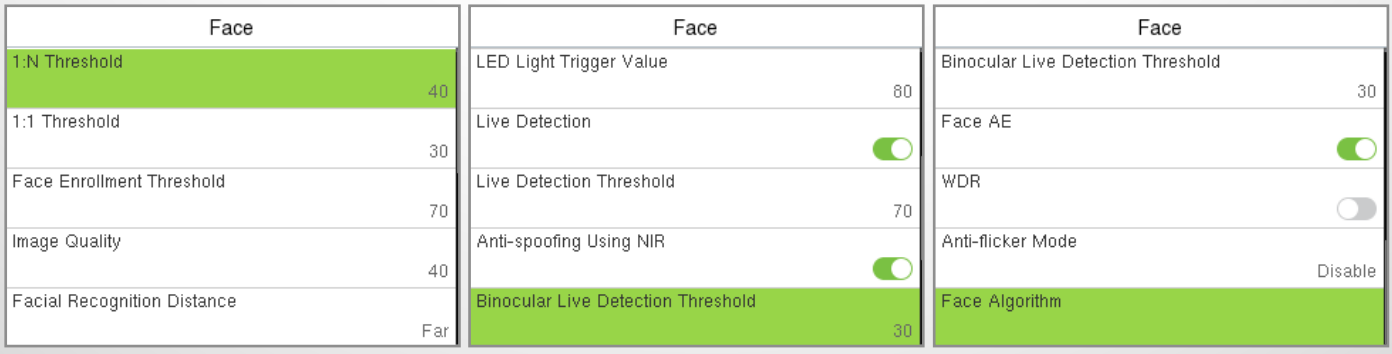
Nota: Un ajuste incorrecto de los parámetros de exposición y calidad puede afectar gravemente el rendimiento del dispositivo. Por favor, ajuste el parámetro de exposición solo bajo la supervisión del personal de servicio postventa de nuestra empresa.

Descripción de la función del Dispositivo de control de acceso:

Nombre de la función	Descripciones
Modos de Cámara	Esta función está desactivada por defecto. Si está activada, aparecerá un aviso de seguridad y el sonido del obturador de la cámara se activará obligatoriamente.Hay 5 modos: **Sin foto**: No se toma ninguna foto durante la verificación del usuario. **Tomar foto, no guardar:** Se toma una foto pero no se guarda durante la verificación. **Tomar foto y guardar**: Se guardan todas las fotos tomadas durante la verificación. **Guardar cuando la verificación se realiza correctamente**: Se toma una foto y se guarda cada vez que se realiza una verificación. Guardar en verificación fallida: La foto se toma y se guarda sólo para cada verificación fallida.
Mostrar foto de usuario	Esta función está deshabilitada por defecto. Cuando se habilita, aparecerá un aviso de seguridad.
ID de usuario alfanumérico	Habilitar/Deshabilitar el alfanumérico como ID de usuario.
Alerta de registros de acceso	Cuando el espacio de registro de acceso de asistencia alcanza el valor máximo del umbral, el dispositivo mostrará automáticamente una advertencia de espacio de memoria. Los usuarios pueden deshabilitar la función o establecer un valor válido entre 1 y 9999.
Eliminación periódica de registros de acceso	Cuando los registros de acceso alcancen su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de registros antiguos. Los usuarios pueden deshabilitar la función o establecer un valor válido entre 1 y 999.
Eliminación periódica de fotos de T&A (Asistencia y Registro)	Cuando las fotos de asistencia alcancen su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos antiguas. Los usuarios pueden deshabilitar la función o establecer un valor válido entre 1 y 99.
Eliminación periódica de fotos de lista de bloqueos	Cuando las fotos en la lista de bloqueos alcancen su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos antiguas de la lista de bloqueos. Los usuarios pueden deshabilitar la función o establecer un valor válido entre 1 y 99.
Authentication Timeout(s)	La duración del mensaje de verificación exitosa. Valor válido: de 1 a 9 segundos.
Intervalo de reconocimiento(s)	To set the facial template matching time interval as required. Valid value: 0~9 seconds.

8.3 Parámetros del template facial

Selecciona **Face** en la interfaz del **sistema** para acceder a la configuración de los parámetros del template facial.



Nombre de la función	Descripciones
1:N Umbral	En el modo de verificación 1:N, la verificación sólo tendrá éxito cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas sea superior al valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será el porcentaje de fallos y mayor el de rechazos, y viceversa. Se recomienda fijar el valor por defecto en 40.
1:1 Umbral	En el modo de verificación 1:1, la verificación sólo tendrá éxito cuando la similitud entre la imagen facial adquirida y las plantillas faciales del usuario registradas en el dispositivo sea superior al valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será el porcentaje de fallos y mayor el de rechazos, y viceversa. Se recomienda fijar el valor por defecto de 30
Umbral de inscripción de Rostros	Durante el registro de la plantilla facial, se utiliza la comparación 1:N para determinar si el usuario ya se ha registrado anteriormente. Cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas es superior a este umbral, indica que la plantilla facial ya ha sido registrada.
Calidad de imagen	Calidad de imagen para el registro y la comparación facial. Cuanto mayor sea el valor, más clara será la imagen requerida.
Distancia de reconocimiento facial	Cuanto más lejos esté el individuo, más pequeño será el rostro y menor será el número de píxeles del rostro obtenidos por el algoritmo. Por lo tanto, el ajuste de este parámetro puede ajustar la distancia de comparación más lejana de las caras.
Valor de activación de la luz LED	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, la luz LED se encenderá o apagará con más frecuencia.
Detección en directo	Detecta el intento de suplantación utilizando imágenes de luz visible para determinar si la muestra de origen biométrico proporcionada es de una persona real (un ser humano vivo) o una representación falsa.
Umbral de detección en vivo	Facilita juzgar si la imagen visible capturada es una persona real (un ser humano vivo). Cuanto mayor sea el valor, mejores serán las prestaciones anti-spoofing mediante luz visible.
Anti-spoofing mediante NIR	Utilización de imágenes espectrales en el infrarrojo cercano para identificar y prevenir ataques con fotos y vídeos falsos.
Umbral de detección binocular en vivo	Es conveniente juzgar si las imágenes espectrales en infrarrojo cercano son fotos y vídeos falsos. Cuanto mayor sea el valor, mejor será la eficacia antifalsificación de las imágenes espectrales en el infrarrojo cercano.
Rostro AE	Cuando el Rostro está delante de la cámara en el modo Face AE, el brillo de la zona de la cara aumenta, mientras que las otras zonas se oscurecen.
WDR	El amplio rango dinámico (WDR) equilibra la luz y amplía la visibilidad de la imagen para vídeos de vigilancia en escenas con iluminación de alto contraste y mejora la identificación de objetos en entornos claros y oscuros.
Modo antiparpadeo	Se utiliza cuando el WDR está desactivado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea con la misma frecuencia que la luz.
Algoritmo facial	Información relacionada con el algoritmo facial y actualización de la plantilla facial en pausa.

• Proceso para modificar la precisión del reconocimiento facial

• En la interfaz del sistema, presione en "Face" y luego active la opción "Anti-Spoofing using NIR" para configurar la protección contra suplantación.

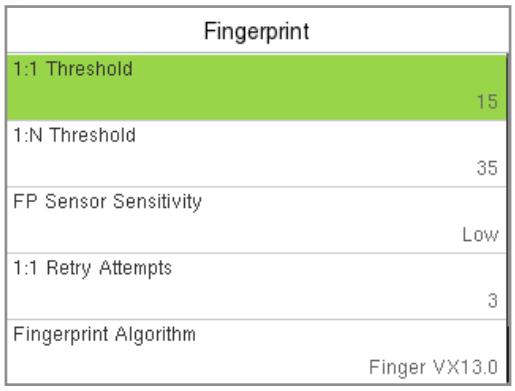
• Luego, en el menú principal, presione "Autotest" > "Test Face" y realice la prueba facial.

• Presione tres veces sobre la puntuación en la esquina superior derecha de la pantalla, y aparecerá un cuadro rectangular rojo para comenzar a ajustar el modo.

• Mantenga una distancia de un brazo entre el dispositivo y el rostro. Se recomienda no mover el rostro en un rango amplio.

8.4 Parámetros de huella dactilar

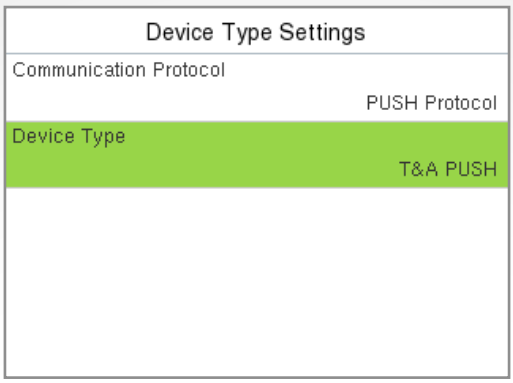
Seleccione **Fingerprint** en la interfaz del **sistema** para acceder a la configuración de los parámetros de huella dactilar.



Nombre de la función	Descripciones
Umbral 1:1	En el método de verificación 1:1, la verificación solo será exitosa cuando la similitud entre los datos de huella dactilar adquiridos y el template de huella dactilar asociado con el ID de usuario ingresado en el dispositivo sea mayor que el valor establecido.
Umbral 1:N	En el método de verificación 1:N, la verificación solo será exitosa cuando la similitud entre los datos de huella dactilar adquiridos y los templates de huella dactilar registrados en el dispositivo sea mayor que el valor establecido.
Sensibilidad del sensor de huella dactilar (FP)	Ajuste de la sensibilidad para la adquisición de huellas dactilares. Se recomienda usar el nivel predeterminado "**Medio**". Cuando el ambiente esté seco, lo que resulta en una detección lenta de huellas, puede establecer el nivel en "**Alto**" para aumentar la sensibilidad; cuando el ambiente esté húmedo, dificultando la identificación de la huella, puede establecer el nivel en "**Bajo**".
Intentos de reintento 1:1	En la verificación 1:1, los usuarios pueden olvidar la huella registrada o colocar el dedo de manera incorrecta. Para reducir el proceso de reingreso del ID de usuario, se permite el reintento.
Algoritmo de huella dactilar	Versión del algoritmo de huella dactilar. El valor predeterminado es ZKFinger VX13.0, pero se puede cambiar a ZKFinger VX10.0.
Algoritmo de huella dactilar	Esta función está deshabilitada por defecto. Después de desactivarla, la imagen de la huella dactilar no se mostrará durante el registro y la verificación de huellas. La interfaz del menú permite habilitar o deshabilitar esta función, y aparecen avisos de seguridad al cambiarla. Hay cuatro opciones disponibles: **Mostrar para Registro**: para mostrar la imagen de la huella solo durante el registro. **Mostrar para Coincidencia**: para mostrar la imagen de la huella solo durante la verificación. **Mostrar Siempre**: para mostrar la imagen de la huella en la pantalla durante el registro y la verificación. **Ninguno**: para no mostrar la imagen de la huella.

8.5 Configuración del tipo de dispositivo

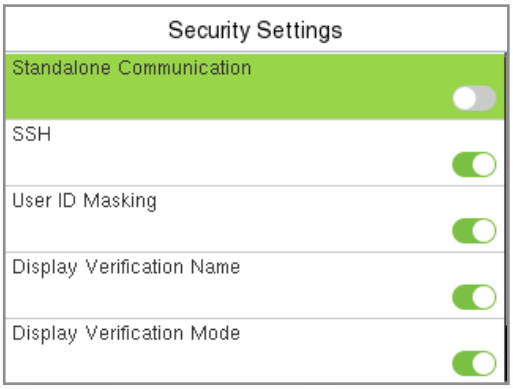
Seleccione **Configuración del tipo de dispositivo** en la interfaz del **sistema** para acceder a la configuración del tipo de dispositivo.



Nombre de la función	Descripciones
Protocolo de comunicación	Configurar el protocolo de comunicación del dispositivo.
Tipo de dispositivo	Configurar el dispositivo como terminal de control de asistencia (T&A PUSH) o como terminal de control de acceso (A&C PUSH).

8.6 Configuración de seguridad

Seleccione **Configuración de seguridad** en la interfaz del **sistema** para acceder a las opciones de seguridad.



Nombre de la función	Descripciones
Comunicación autónoma	Por defecto, esta función está deshabilitada. Se puede habilitar o deshabilitar a través de la interfaz del menú. Al activarla, aparecerá un aviso de seguridad y el dispositivo se reiniciará después de la confirmación.
SSH	El dispositivo no admite la función Telnet, por lo que normalmente se utiliza SSH para la depuración remota. Por defecto, SSH está habilitado. La interfaz del menú permite habilitar y deshabilitar SSH. Cuando se habilita, aparecerá un aviso de seguridad, pero el dispositivo no necesitará reiniciarse después de la confirmación.
Enmascarado del ID de usuario	Una vez habilitado, el ID de usuario se mostrará parcialmente después del resultado de la verificación del personal (solo los IDs de usuario con más de 2 dígitos admiten la visualización enmascarada), y está habilitado por defecto.
Mostrar nombre de verificación	Una vez habilitada, el nombre del usuario se mostrará después del resultado de la verificación del personal. Si se deshabilita, el resultado de la verificación no mostrará el nombre.
Mostrar nombre de verificación	Una vez habilitada, el resultado de la verificación del personal mostrará el modo de verificación del usuario. Si se deshabilita, el resultado de la verificación no mostrará el modo de verificación.
Guardar foto como plantilla	Después de deshabilitar esta función, será necesario volver a registrar la plantilla facial tras una actualización del algoritmo.

8.7 Actualización por USB

Seleccione **Actualización por USB** en la interfaz del **sistema**.

El firmware del dispositivo se puede actualizar utilizando un archivo de actualización almacenado en una unidad USB. Antes de realizar esta operación, asegúrese de que la unidad USB contenga el archivo de actualización correcto y esté correctamente insertada en el dispositivo.

Si no se detecta una unidad USB insertada , el sistema mostrará un mensaje de advertencia después de presionar "Actualización por USB" en la interfaz del sistema.

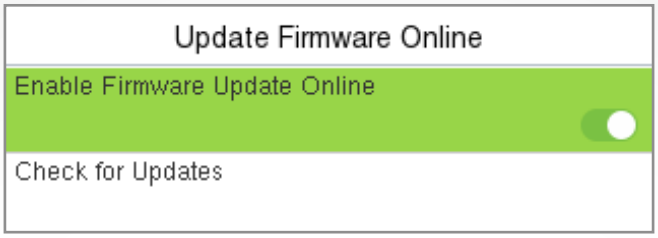


Nota: Si se requiere un archivo de actualización, comuníquese con nuestro soporte técnico. La actualización del firmware no se recomienda bajo circunstancias normales.

8.8 Actualizar Firmware en Línea

Presione "Actualizar Firmware en Línea" en la interfaz del sistema.

Presione **Habilitar actualización de firmware en línea**. El dispositivo mostrará una advertencia indicando que la actualización puede implicar riesgos de seguridad de datos, lo que requerirá una confirmación manual por parte del usuario. (Si la función de configuración de seguridad está desactivada, la advertencia de riesgo no se mostrará al habilitar la actualización en línea).

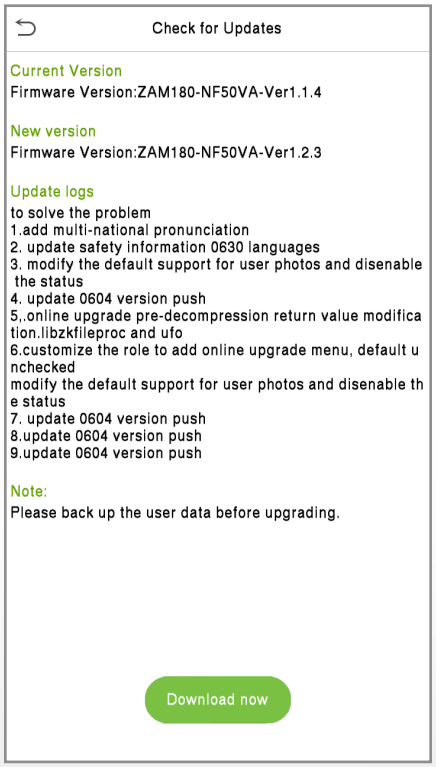


Presione **Verificar actualizaciones**, lo que puede dar lugar a los siguientes 3 escenarios:

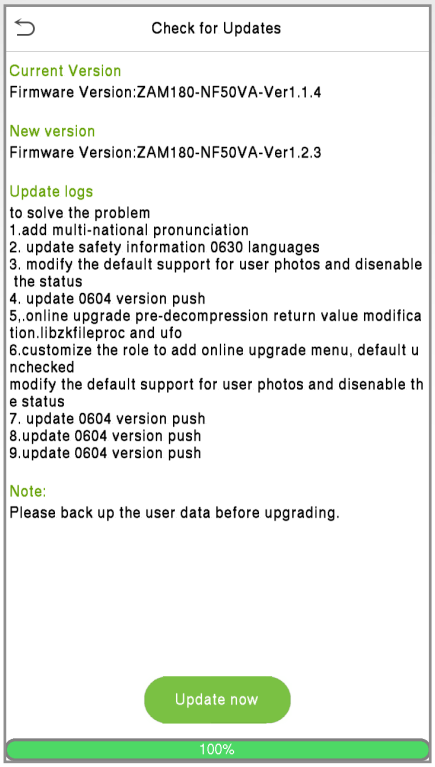
- Si la consulta falla, la interfaz mostrará "Consulta fallida".
- Si la versión del firmware del dispositivo es la más reciente, se mostrará un mensaje indicando que la versión actual del firmware ya está actualizada.
- Si la versión del firmware del dispositivo no es la más reciente, se mostrará el número de versión y el registro de cambios de la versión más reciente. Los usuarios pueden elegir si desean actualizar a la última versión del firmware.

Actualizar firmware

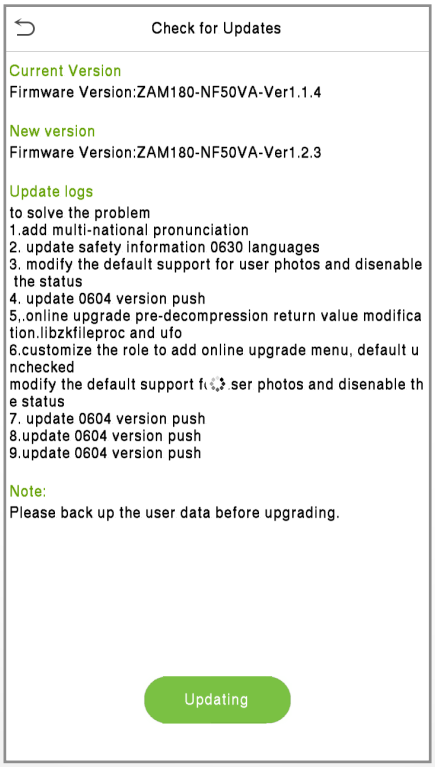
1. Presione **Descargar ahora** para comenzar la descarga. Una vez que la descarga esté completa, podrá elegir si actualizar inmediatamente.



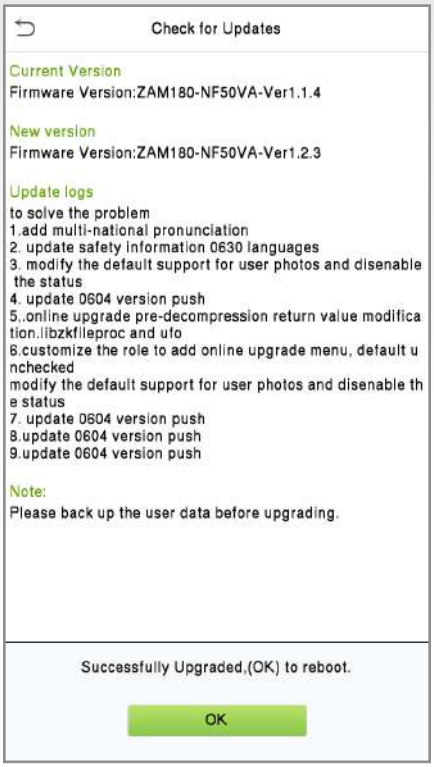
2. Durante el proceso de descarga, puede presionar la tecla **ESC** para ir a otros menús, y luego regresar a este menú para realizar la actualización una vez que la descarga esté completa.



3. La velocidad de descarga está relacionada con el entorno de red del usuario, y puede tardar aproximadamente 10 minutos en completar la descarga. La actualización puede tardar alrededor de 3 minutos.



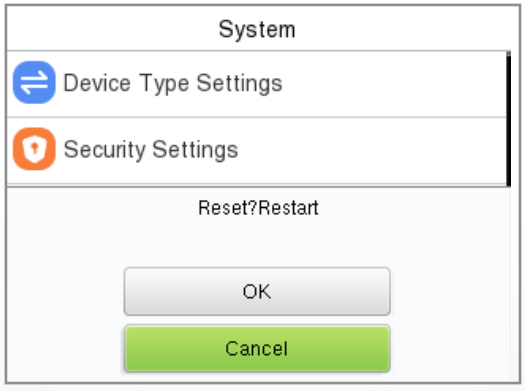
3. Después de que la actualización esté completa, el dispositivo solicitará reiniciarse. Después del reinicio, podrá ingresar a la información del sistema para ver la versión más reciente del firmware tras la actualización.



8.9 Restablecimiento de fábrica

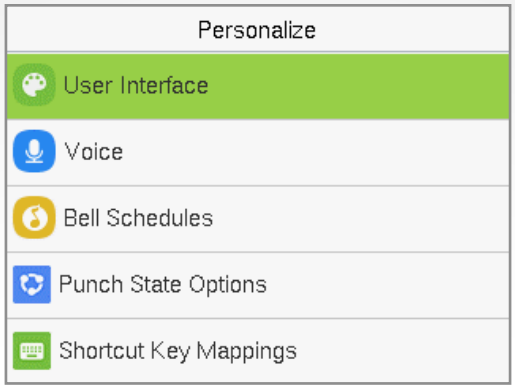
La función de restablecimiento de fábrica restaura la configuración del dispositivo, como la configuración de comunicación y los ajustes del sistema, a los valores predeterminados de fábrica (esta función no borra los datos de usuario registrados).

Seleccione **Restablecer** en la interfaz del **sistema** y luego presione **M/OK** para restaurar los ajustes predeterminados de fábrica.



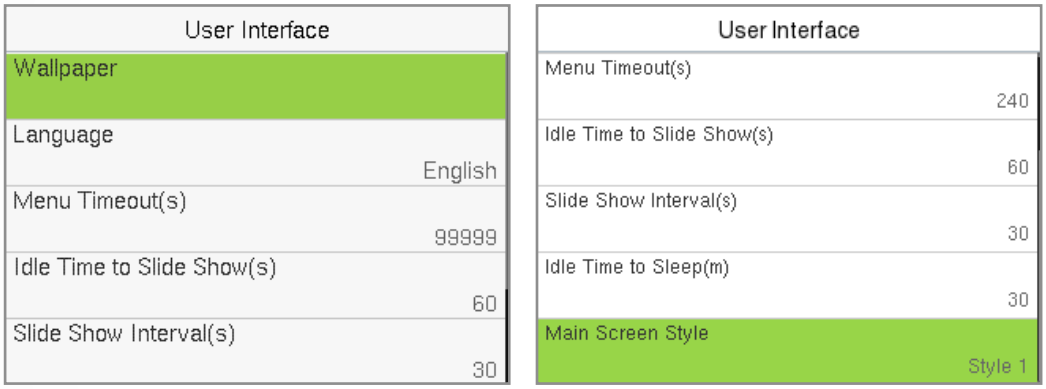
9 Configuraciones personalizadas

Cuando el dispositivo esté en la interfaz inicial, presione **M/OK** y seleccione **Personalizar** para ajustar la configuración de la interfaz, voz, campanillas, opciones de estado de registro y asignación de teclas de acceso rápido.



9.1 Configuración de la interfaz de usuario

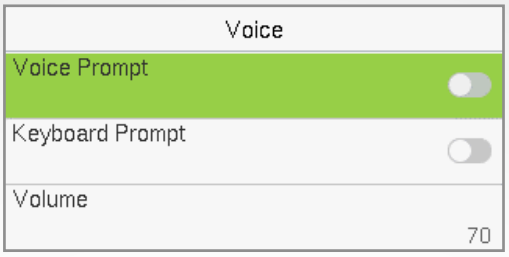
Seleccione **Interfaz** de usuario en la interfaz de **personalización** para personalizar el estilo de visualización de la interfaz principal.



Nombre de la función	Descripciones
Fondo de pantalla	El fondo de pantalla de la pantalla principal se puede seleccionar según la preferencia del usuario.
Idioma	Seleccione el idioma del dispositivo.
Tiempo de espera del menú (segundos)	Cuando no hay ninguna operación y el tiempo supera el valor establecido, el dispositivo regresará automáticamente a la interfaz inicial. Esta función puede ser deshabilitada o configurada con un valor entre 60 y 99999 segundos.
Tiempo de inactividad para la presentación (segundos)	Cuando no haya ninguna operación y el tiempo supere el valor establecido, se iniciará una presentación de diapositivas. Esta función puede ser deshabilitada o configurada con un valor entre 3 y 999 segundos.
Intervalo de presentación de diapositivas (segundos)	Es el intervalo de tiempo para cambiar entre las diferentes fotos de la presentación de diapositivas. La función puede ser deshabilitada o puede configurarse con un intervalo entre 3 y 999 segundos.
Tiempo de inactividad para entrar en modo de suspensión (minutos)	Si se activa el modo de suspensión, y no hay operaciones en el dispositivo, este entrará en modo de espera. Presione el teclado para reanudar el modo de trabajo normal. Esta función puede ser deshabilitada o configurada con un valor entre 1 y 999 minutos.
Estilo de pantalla principal	El estilo de la pantalla principal se puede seleccionar según la preferencia del usuario.

9.2 Configuración de voz

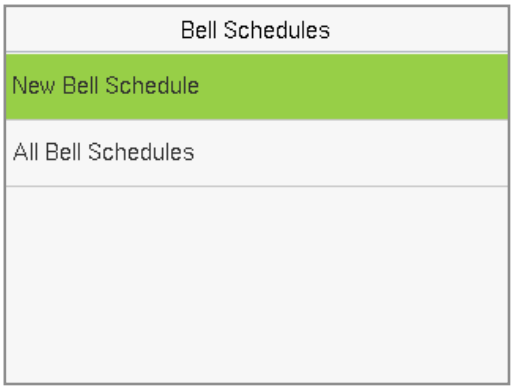
Seleccione **Voz** en la interfaz de personalización para configurar los ajustes de voz.



Nombre de la función	Descripciones
Indicación de voz	Alternar para habilitar o deshabilitar las indicaciones de voz durante las operaciones del dispositivo.
Indicación táctil	Alternar para habilitar o deshabilitar los sonidos del teclado.
Volumen	Ajustar el volumen del dispositivo, que puede configurarse entre 0 y 100.

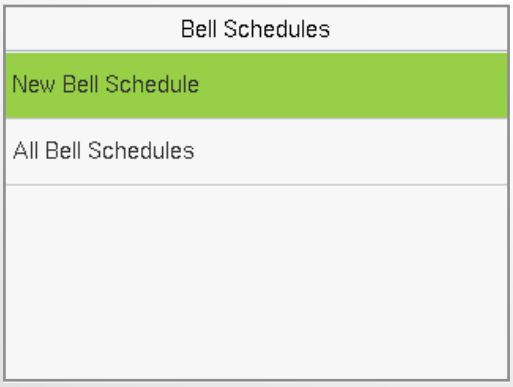
9.3 Horarios de timbre

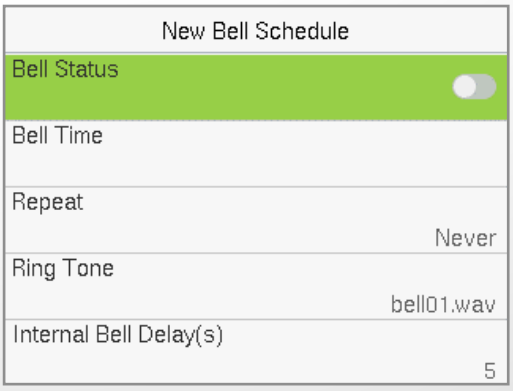
Seleccione **Horarios de timbre** en la interfaz de personalización para configurar los ajustes del timbre.



9.4 Nuevo horario de timbre

Seleccione **Nuevo horario de timbre** en la interfaz de **horarios de timbre** para agregar un nuevo horario de timbre.





Nombre de la función	Descripciones
Estado del timbre	Alternar para habilitar o deshabilitar el estado del timbre.
Hora del Timbre	Una vez que se establezca la hora requerida, el dispositivo activará automáticamente el timbre a esa hora.
Repetir	Una vez que se establezca la hora requerida, el dispositivo activará automáticamente el timbre a esa hora.
Tono de Timbre	Seleccionar el tono de Timbre
Retraso del timbre interno (segundos)	Establezca el tiempo de repetición del timbre interno. Los valores válidos van de 1 a 999 segundos.

• Todos los horarios de timbre:

Una vez que se haya programado el timbre, en la interfaz de **horarios de timbre**, presione **Todos los horarios de timbre** para ver el timbre recién programado.

• Editar el timbre programado:

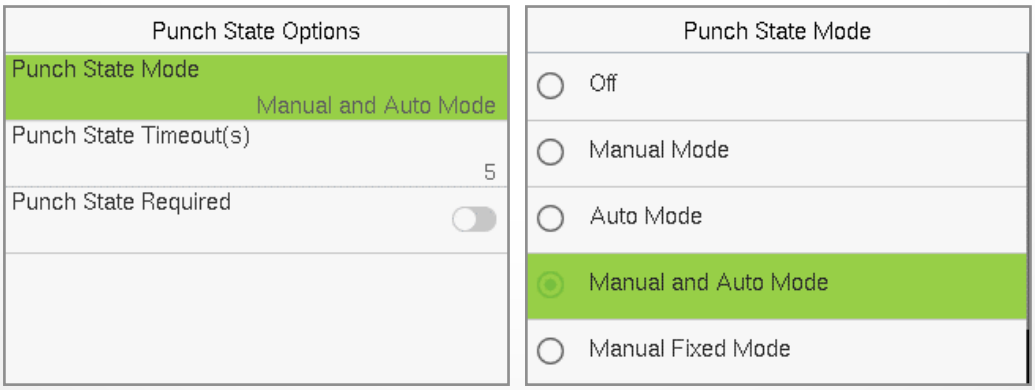
En la interfaz de **Todos los horarios de timbre**, seleccione el horario de timbre requerido y luego seleccione **Editar** para modificar el horario de timbre seleccionado. El método de edición es el mismo que el de agregar un nuevo horario de timbre.

• Eliminar un timbre:

En la interfaz de **Todos los horarios de timbre**, seleccione el horario de timbre requerido, luego seleccione **Eliminar** y presione **M/OK** para borrar el timbre seleccionado.

9.4 Estados de Perforación Opciones

Seleccione **Opciones de estado de perforación** en la interfaz **Personalizar** para configurar los ajustes de estado de perforación.

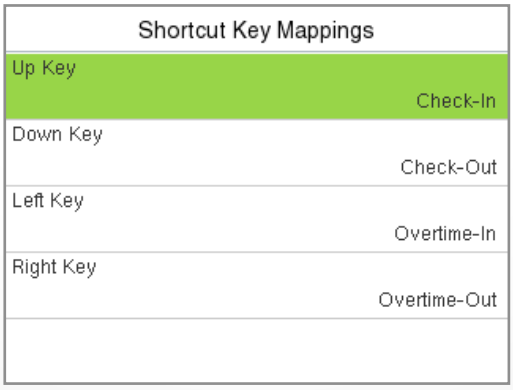


Nombre de la función	Descripciones
Modo de estado de marcado	**Apagado**: Deshabilita la función de estado de marcado. Por lo tanto, la tecla de estado de marcado configurada en el menú de Mapeo de teclas rápidas se volverá inválida. **Modo manual**: Cambia el estado de marcado manualmente, y la tecla de estado de marcado desaparecerá después del tiempo de espera del estado de marcado. **Modo automático**: La tecla de estado de marcado cambiará automáticamente a un estado de marcado específico según el horario predefinido, que se puede configurar en el Mapeo de teclas rápidas.
Modo de estado de marcado	**Modo manual y automático**: La interfaz principal mostrará la tecla de estado de marcado de cambio automático. Sin embargo, los usuarios aún podrán seleccionar una alternativa, que es el estado de marcado manual. Después del tiempo de espera, la tecla de estado de marcado manual se convertirá en la tecla de estado de marcado de cambio automático. **Modo manual fijo**: Después de que la tecla de estado de marcado se configure manualmente en un estado de marcado específico, la función permanecerá sin cambios hasta que se cambie manualmente nuevamente. **Modo fijo**: Solo se mostrará la tecla de estado de marcado fijo manual. Los usuarios no podrán cambiar el estado presionando ninguna otra tecla.
Tiempo de espera del estado de marcado (segundos)	Es el tiempo durante el cual se muestra el estado de marcado. El valor puede configurarse entre 5 y 999 segundos.
Estado de marcado requerido:	Seleccione si se requiere seleccionar un estado de asistencia después de la verificación. **ON**: Se debe seleccionar un estado de asistencia después de la verificación. **OFF**: No es necesario seleccionar un estado de asistencia después de la verificación.

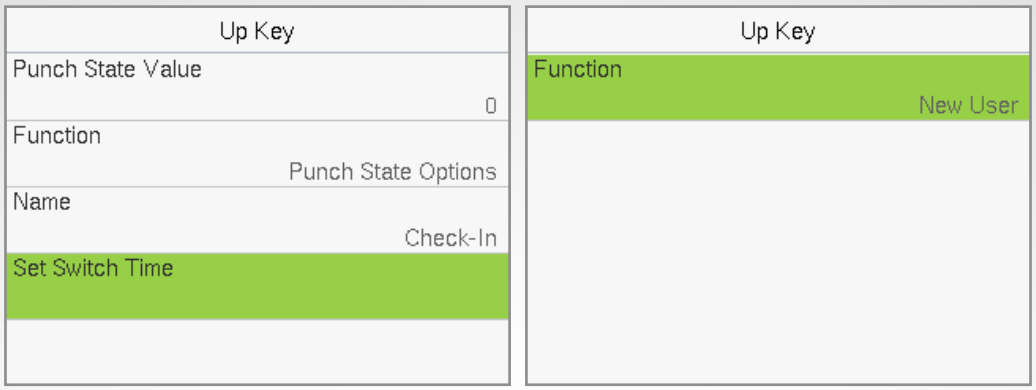
9.5 Asignación de teclas de acceso rápido:

Los usuarios pueden definir teclas de acceso rápido para los estados de asistencia y para las teclas funcionales que se definirán en la interfaz principal. De esta manera, al presionar las teclas de acceso rápido en la interfaz principal, se mostrará directamente el estado de asistencia correspondiente o la interfaz de la función seleccionada.

Selecciona Mapeo de **teclas de acceso rápido** en la interfaz de **Personalización** para configurar las teclas de acceso rápido requeridas.



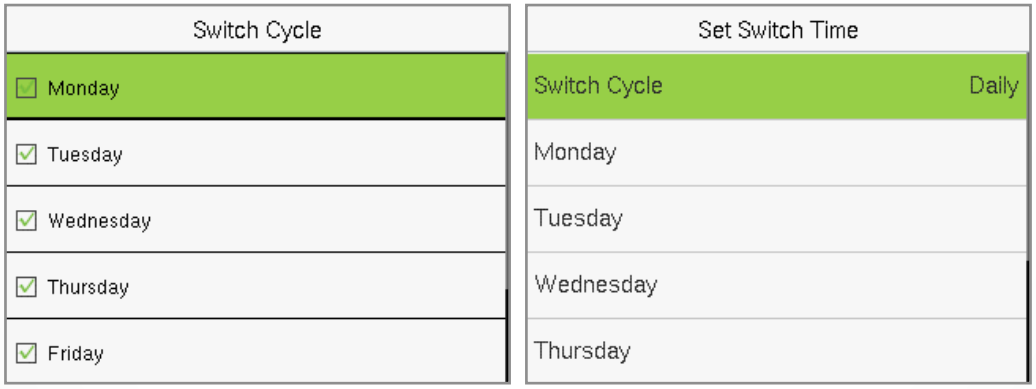
• En la interfaz de Mapeo de teclas de acceso rápido, selecciona la tecla de acceso rápido requerida para configurar los ajustes de la tecla de acceso rápido.
• En la interfaz de la tecla de acceso rápido (que es "F1"), presiona función para configurar el proceso funcional de la tecla de acceso rápido como tecla de estado de asistencia o tecla de función.
• Si la tecla de acceso rápido está definida como una tecla de función (como Nuevo usuario, Todos los usuarios, etc.), la configuración se completa como se muestra en la imagen a continuación.



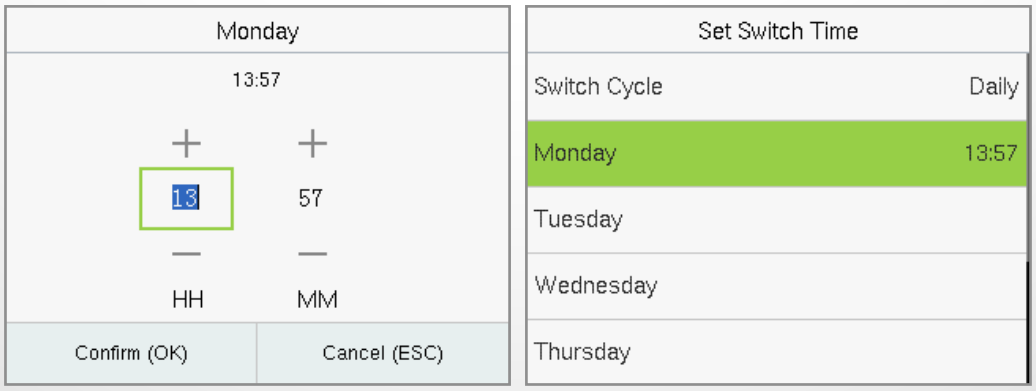
• Si la tecla de acceso rápido está configurada como una tecla de estado de asistencia (como entrada, salida, etc.), entonces es necesario establecer el valor del estado de asistencia (valor válido de 0 a 250) y el nombre.

• Establecer el tiempo de cambio

• El tiempo de cambio se establece de acuerdo con las opciones del estado de asistencia.
• Cuando el modo de **estado de asistencia** está configurado en **Modo automático**, se debe establecer el tiempo de cambio.
• En la interfaz de **Tecla de acceso rápido**, presiona **Establecer tiempo de cambio** para configurar el | tiempo de cambio.
• En la interfaz de **Ciclo de cambio**, selecciona el ciclo de cambio (lunes, martes, etc.) como se muestra en la imagen a continuación.



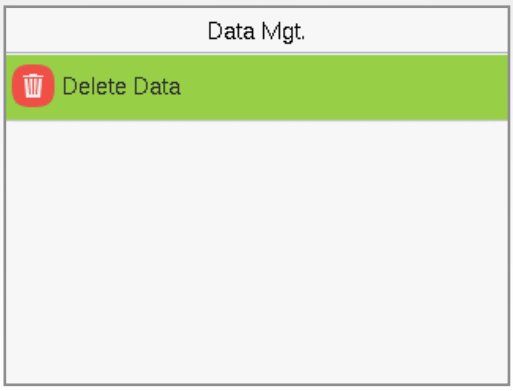
• Una vez que se seleccione el ciclo de cambio, configura el tiempo de cambio para cada día y presiona **M/OK** para confirmar, como se muestra en la imagen a continuación.



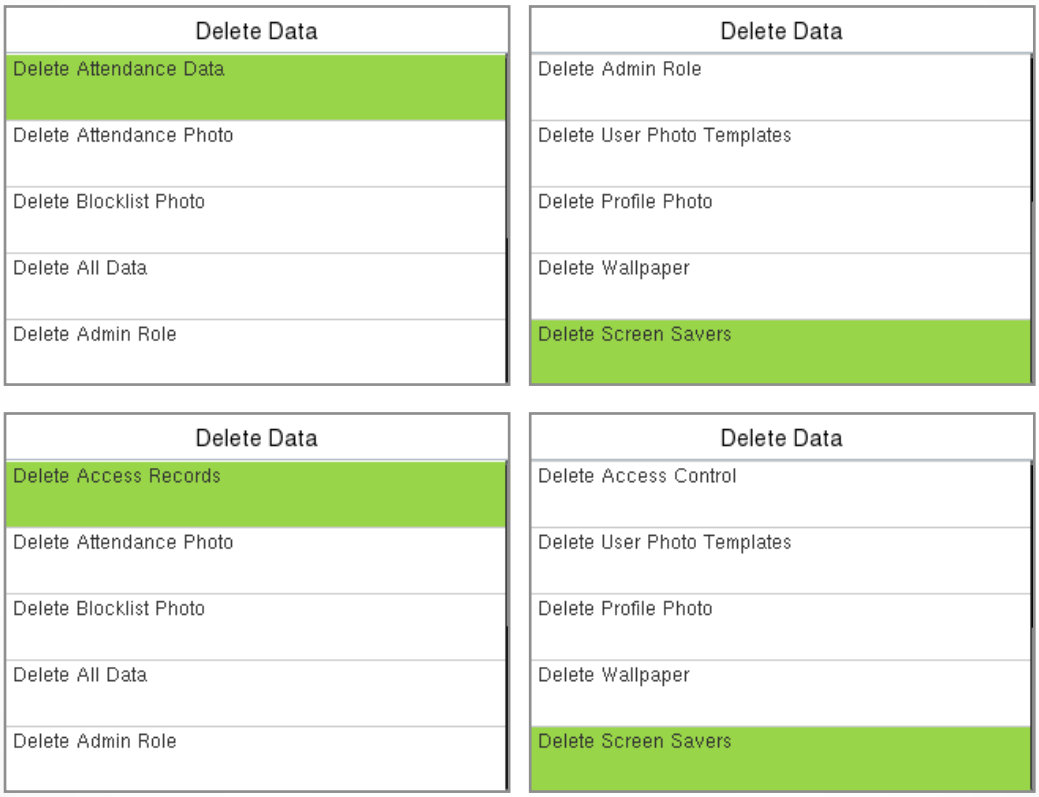
Nota: Cuando la función está configurada como No Definida, el dispositivo no habilitará la tecla de estado de asistencia.

10 Gestión de Datos

Cuando el dispositivo esté en la interfaz inicial, presiona **M/OK** y selecciona **Gestión de Datos** para gestionar los datos relevantes en el dispositivo.



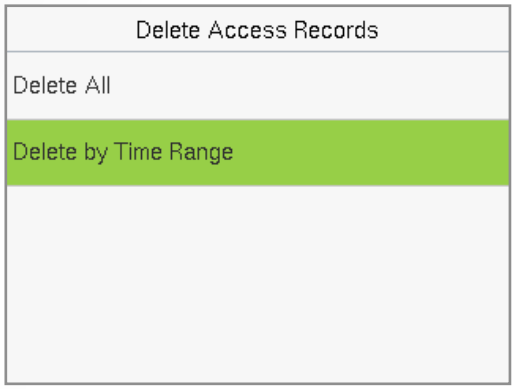
Selecciona **Eliminar Datos** en la interfaz de **Gestión de Datos** para eliminar los datos necesarios.



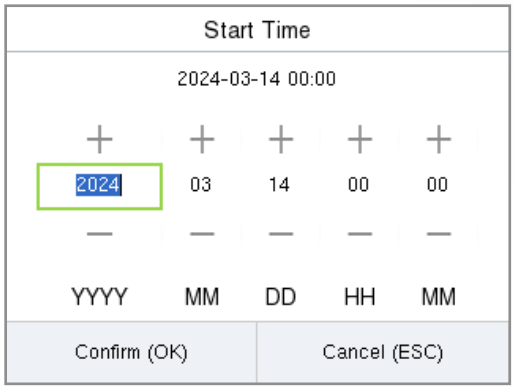
Nombre de la función	Descripciones
Eliminar Registros de Asistencia/Acceso	Para eliminar los datos de asistencia/registros de acceso de forma condicional.
Eliminar foto de asistencia	Eliminar las fotos de asistencia del personal designado.
Eliminar la foto de la lista bloqueada.	Eliminar las fotos tomadas durante las verificaciones fallidas.
Eliminar todos los datos.	Eliminar toda la información y los registros de asistencia de todos los usuarios registrados.
Eliminar el rol de administrador.	To remove all administrator privileges.

Eliminar las plantillas de fotos de los usuarios.	Para eliminar las plantillas de fotos de los usuarios en el dispositivo. Al eliminar las fotos de plantilla, aparecerá un recordatorio de riesgo: **"Se requiere la re-registro facial después de una actualización del algoritmo."**
Eliminar control de acceso	Para eliminar todos los datos de acceso. Nota: Esta función es solo para terminales de control de acceso.
Eliminar foto de perfil	Para eliminar todas las fotos de los usuarios en el dispositivo.
Eliminar fondo de pantalla	Para eliminar todos los fondos de pantalla en el dispositivo.
Eliminar salvapantallas	Para eliminar los salvapantallas en el dispositivo.

El usuario puede seleccionar **Eliminar todo** o **Eliminar por rango de tiempo** al eliminar los datos de asistencia/registros de acceso, fotos de asistencia o fotos de lista negra. Al seleccionar **Eliminar por rango de tiempo**, se debe establecer un rango de tiempo específico para eliminar todos los datos dentro de ese período.



Selecciona **Eliminar por Rango de Tiempo**.

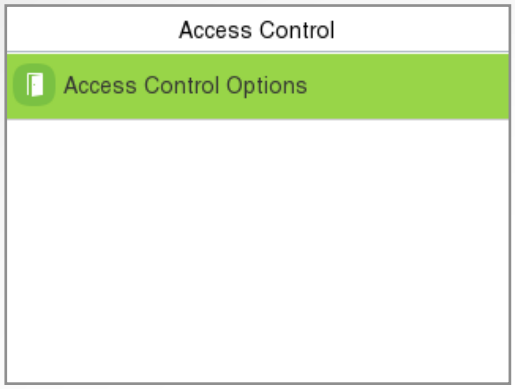


Establece el rango de tiempo y presiona **M/OK**.

11 Control de Acceso

Cuando el dispositivo esté en la interfaz inicial, presiona **M/OK** y selecciona **Control de Acceso** para configurar el horario de apertura de puertas, control de cerraduras y otros parámetros relacionados con el control de acceso.

Dispositivo de Asistencia de Tiempo



Dispositivo de Control de Acceso:

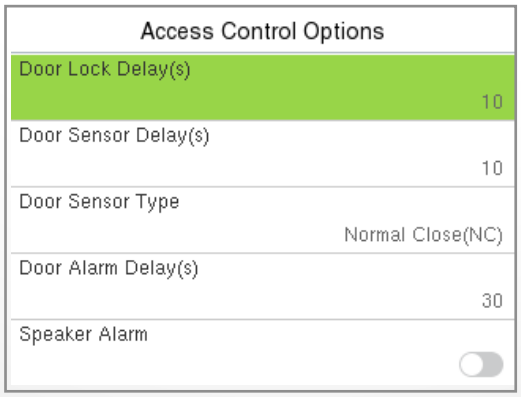


- **Para obtener acceso, el usuario registrado debe cumplir con las siguientes condiciones:**
  - El tiempo actual de desbloqueo de la puerta debe estar dentro de cualquier zona horaria válida del período de tiempo del usuario.
  - El grupo correspondiente del usuario debe estar ya configurado en la combinación de desbloqueo de la puerta (y si hay otros grupos, también deben estar configurados en la misma combinación de acceso, por lo que se debe verificar a los miembros de esos grupos para desbloquear la puerta).
  - En la configuración predeterminada, a los nuevos usuarios se les asigna el primer grupo con la zona horaria predeterminada, donde la combinación de acceso es "1" y está configurada en estado desbloqueado por defecto.

11.1 Opciones de Control de Acceso

Seleccione **Opciones de Control de Acceso** en la interfaz de **Control de Acceso** para configurar los parámetros del control de la cerradura del terminal y del equipo relacionado.

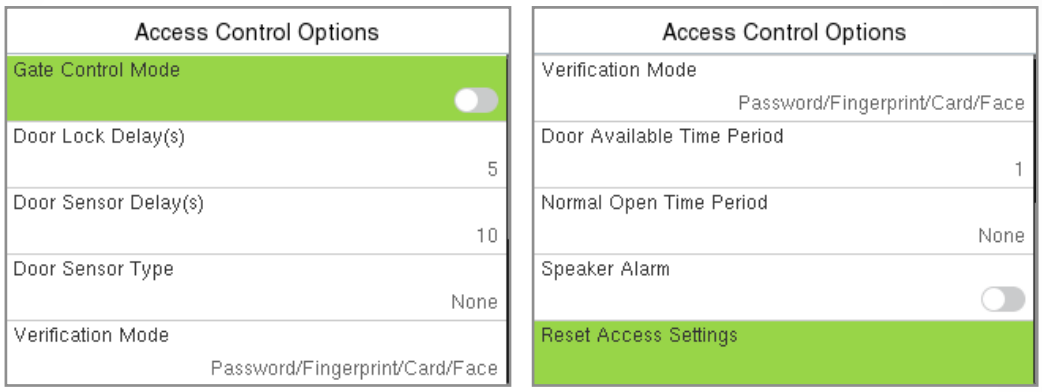
Terminal de Asistencia de Tiempo:



Nombre de la función	Descripciones
Retraso de Bloqueo de Puerta (s)	Define el tiempo durante el cual el dispositivo mantiene la cerradura eléctrica en estado desbloqueado. Valores válidos: 1~10 segundos; 0 segundos desactiva la función.

Retraso del Sensor de Puerta (s)	Si la puerta no se cierra y permanece abierta durante un tiempo determinado (Retraso del Sensor de Puerta), se activará una alarma. Valores válidos: 1~255 segundos.
Tipo de sensor de puerta	Existen tres tipos de sensores: Ninguno, Normal Abierto (NO) y Normal Cerrado (NC). Ninguno: Significa que el sensor de la puerta no está en uso. Normal Abierto (NO): La puerta permanece abierta cuando la alimentación eléctrica está activada. Normal Cerrado (NC): La puerta permanece cerrada cuando la alimentación eléctrica está activada.
Retraso de Alarma de Puerta (s)	Si el estado del sensor de la puerta no coincide con el tipo de sensor configurado, se activará una alarma después de un período de tiempo. Este período es el Retraso de Alarma de Puerta, cuyo valor puede configurarse entre 0 y 999 segundos.
Alarma del Altavoz	El altavoz emite una alarma sonora o una alarma de desensamblaje desde el dispositivo local. Cuando la puerta se cierra o la verificación es exitosa, el sistema cancela la alarma automáticamente.

Dispositivo de Control de Acceso:



Nombre de la función	Descripciones
Modo de Control de Puerta	Alterna entre el interruptor ON o OFF para activar o desactivar el modo de control de acceso. Cuando se configura en **ON**, en esta interfaz se eliminarán las opciones de relé de cerradura de puerta, relé de sensor de puerta y tipo de sensor de puerta.
Retraso en cerradura de puerta (segundos).	La duración del tiempo durante el cual el dispositivo controla la cerradura eléctrica para que esté en estado de desbloqueo. Valor válido: 1~99 segundos; 0 segundos representa desactivar la función.
Retraso del sensor de la puerta (segundos).	Si la puerta no está cerrada y se deja abierta durante un cierto tiempo (Retraso del Sensor de la Puerta), se activará una alarma. El valor válido del Retraso del Sensor de la Puerta varía entre 1 y 255 segundos.
Tipo de Sensor de la Puerta:	Existen tres tipos de sensores: **Ninguno**: Significa que el sensor de puerta no está en uso. **Normalmente Abierto**: Significa que la puerta siempre se deja abierta cuando la energía eléctrica está encendida. **Normalmente Cerrado**: Significa que la puerta siempre se deja cerrada cuando la energía eléctrica está encendida.

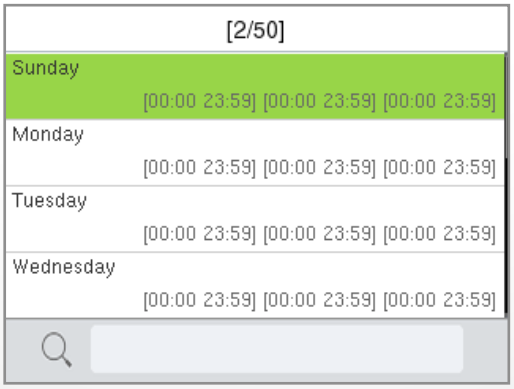
Modo de verificación	Selecciona el modo de verificación para el usuario, se pueden usar un total de 21 combinaciones de verificación diferentes. Consulta el apartado 1.6.5 verificación combinada para más detalles.
Período de tiempo disponible para la puerta.	Para establecer el período de tiempo en el que la puerta estará disponible, de modo que la puerta solo se pueda abrir durante ese período.
Período de tiempo de apertura normal	Período de tiempo programado para el modo "Abierto Normal" (Normal Open), de modo que la puerta permanezca siempre abierta durante este período.
Altavoz de Alarma	Transmite una alarma sonora o de desmantelamiento desde el local. Cuando la puerta se cierra o la verificación es exitosa, el sistema cancelará la alarma local.
Restablecer la configuración de acceso.	Los parámetros de restablecimiento de control de acceso incluyen el retraso de la cerradura de la puerta, el retraso del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el período de tiempo disponible para la puerta, el período de tiempo de apertura normal, el dispositivo principal y la alarma. Sin embargo, los datos de control de acceso borrados en la gestión de datos no se incluyen.

11.2 Configuración de la Regla de Tiempo

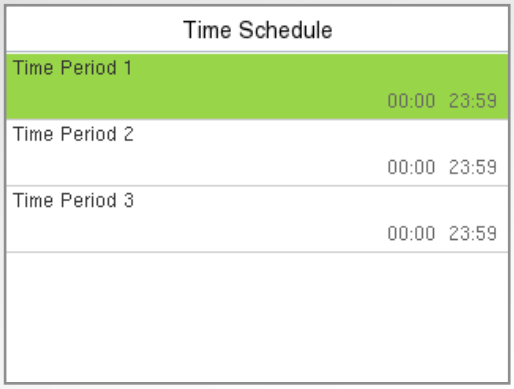
Presiona Configuración de Reglas de Tiempo en la interfaz de Control de Acceso para configurar los ajustes de tiempo.
Nota: Esta función solo está disponible para el Terminal de Control de Acceso.

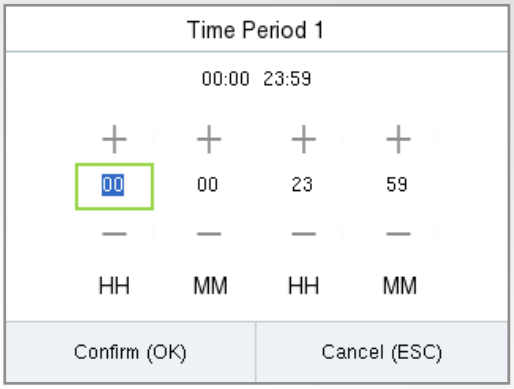
- El sistema puede definir hasta 50 Períodos de Tiempo.
- Cada Período de Tiempo representa 10 Zonas Horarias, es decir, 1 semana y 3 días festivos, y cada zona horaria es un periodo estándar de 24 horas por día. El usuario solo puede verificar dentro del periodo de tiempo válido.
- Se puede configurar un máximo de 3 períodos de tiempo para cada zona horaria. La relación entre estos períodos es "O". Así que, cuando el tiempo de verificación caiga en cualquiera de estos períodos de tiempo, la verificación será válida.
- El formato de la Zona Horaria para cada Período de Tiempo es: HH MM-HH MM, lo cual es preciso hasta los minutos según el reloj de 24 horas.

Presiona el cuadro gris para buscar la zona horaria requerida y especifica el número de la zona horaria requerida (máximo: hasta 50 zonas).



En la interfaz del número de Zona Horaria seleccionado, presiona el día requerido (es decir, lunes, martes, etc.) para configurar la hora.





Especifica la hora de inicio y de finalización, luego presiona **M/OK**.

Notas:

• Cuando la hora de finalización es anterior a la hora de inicio (por ejemplo, 23:5723:56), indica que el acceso está prohibido todo el día.

• Cuando la hora de finalización es posterior a la hora de inicio (por ejemplo, 00:0023:59), indica que el intervalo es válido.

• El intervalo de tiempo efectivo para mantener la puerta desbloqueada o abierta todo el día es (00:0023:59) o también cuando la hora de finalización es posterior a la hora de inicio (por ejemplo, 08:0023:59).

• La zona horaria predeterminada 1 indica que la puerta está abierta todo el día.• Si la consulta falla, la interfaz mostrará "Consulta fallida".

11.3 Días festivos

Siempre que haya un día festivo, puede que necesite un horario de acceso especial; pero cambiar el horario de acceso de cada persona una por una es extremadamente tedioso. Por eso, puede configurar un horario de acceso para los días festivos que sea aplicable a todos los empleados, permitiendo que el usuario abra la puerta durante los días festivos.

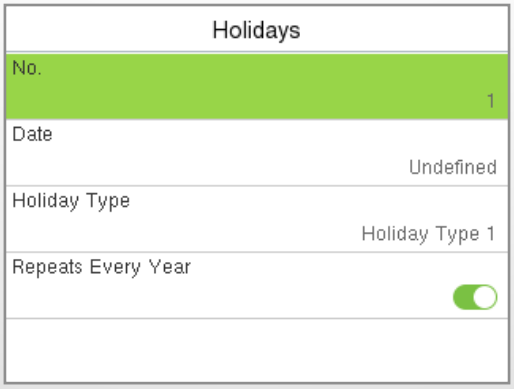
Nota: Esta función solo está disponible para el Dispositivo de Control de Acceso.

Presiona "Holidays" en la interfaz de Control de Acceso para configurar el acceso en días festivos.



• **Agregar un Nuevo Día Festivo**:

Presiona **Agregar Día Festivo** en la interfaz de **Días Festivos** y configura los parámetros del día festivo.



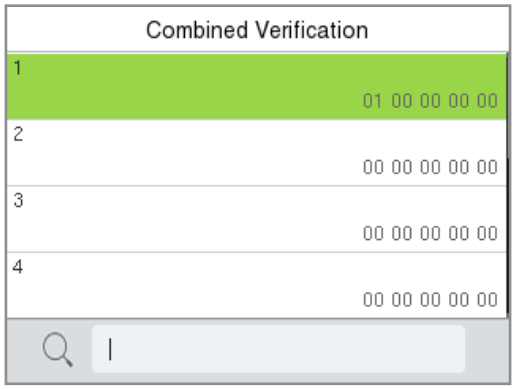
• **Editar un Día Festivo**:
En la interfaz de **Días Festivos**, selecciona el ítem del día festivo que deseas modificar. Presiona **Editar** para modificar los parámetros del día festivo.

• **Eliminar un Día Festivo**:
En la interfaz de **Días Festivos**, selecciona el ítem del día festivo que deseas eliminar y presiona **Eliminar**. Presiona **M/OK** para confirmar la eliminación. Después de la eliminación, este día festivo ya no aparecerá en la interfaz de **Todos los Días Festivos**.

11.4 Verificación Combinada

Los grupos de acceso se organizan en diferentes combinaciones de desbloqueo de puertas para lograr múltiples verificaciones y fortalecer la seguridad. En una combinación de desbloqueo de puerta, el rango del número combinado N es: 0 ≤ N ≤ 5, y el número de miembros N puede pertenecer todo a un grupo de acceso o a cinco grupos de acceso diferentes. **Nota**: Esta función solo está disponible para el Terminal de Control de Acceso.

Presiona **Verificación Combinada** en la interfaz de **Control de Acceso** para configurar la configuración de verificación combinada.



En la interfaz de verificación combinada, presiona la combinación de desbloqueo de puerta que deseas configurar, y luego usa las flechas hacia arriba y hacia abajo para ingresar el número de la combinación. Después, presiona **M/OK**.
Por ejemplo:

- La combinación de desbloqueo de puerta 1 se configura como (01 03 05 06 08), lo que indica que la combinación de desbloqueo 1 está compuesta por 5 personas, y las 5 personas provienen de 5 grupos, es decir, Grupo de Control de Acceso 1 (AC grupo 1), AC grupo 3, AC grupo 5, AC grupo 6 y AC grupo 8, respectivamente.
- La combinación de desbloqueo de puerta 2 se configura como (02 02 04 04 07), lo que indica que la combinación de desbloqueo 2 está compuesta por 5 personas; las primeras dos son del AC grupo 2, las siguientes dos son del AC grupo 4, y la última persona es del AC grupo 7.
- La combinación de desbloqueo de puerta 3 se configura como (09 09 09 09 09), lo que indica que hay 5 personas en esta combinación; todas son del AC grupo 9.
- La combinación de desbloqueo de puerta 4 se configura como (03 05 08 00 00), lo que indica que la combinación de desbloqueo 4 está compuesta por solo tres personas. La primera persona es del AC grupo 3, la segunda persona es del AC grupo 5 y la tercera persona es del AC grupo 8.

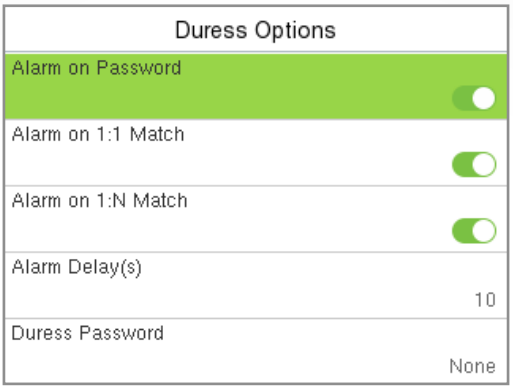
• **Eliminar una combinación de desbloqueo de puerta:**
Configura todas las combinaciones de desbloqueo de puerta a 0 si deseas eliminar las combinaciones de desbloqueo de puerta.

11.5 Opciones de Coacción

Una vez que un usuario active la función de verificación por coacción con el(los) método(s) de autenticación específicos, y cuando se encuentre bajo coacción y se autentique usando la verificación por coacción, el dispositivo desbloqueará la puerta como de costumbre, pero al mismo tiempo, se enviará una señal para activar la alarma.

Nota: Esta función es solo para el terminal de control de acceso.

En la interfaz de **Control de Acceso**, presiona **Opciones de Coacción** para configurar los ajustes de coacción.



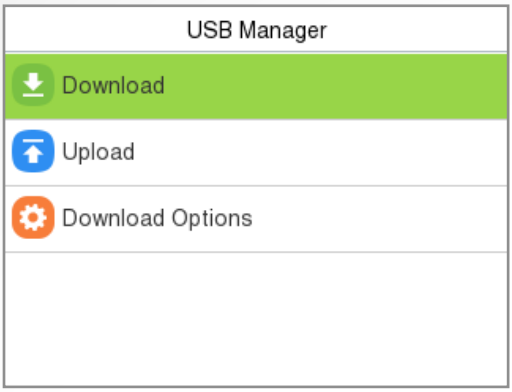
Nombre de la función	Descripciones
Alarma con Contraseña	El fondo de pantalla de la pantalla principal se puede seleccionar según la preferencia del usuario.
Alarma en el modo 1:1	Cuando un usuario utilice cualquier huella dactilar para realizar la verificación 1:1, se generará una señal de alarma, de lo contrario no habrá señal de alarma.
Alarma en el modo 1:N	Cuando un usuario utilice cualquier huella dactilar para realizar una verificación 1:N, se generará una señal de alarma, de lo contrario no habrá señal de alarma.
Retrsaso de alarma (segusndos)	La señal de alarma no se transmitirá hasta que transcurra el tiempo de retardo de la alarma. El valor oscila entre 1 y 999 segundos.
Contraseña de coacción	Establezca la contraseña de coacción de 6 dígitos. Cuando el usuario introduce esta contraseña de coacción para su verificación, se genera una señal de alarma.

12 Gestor USB

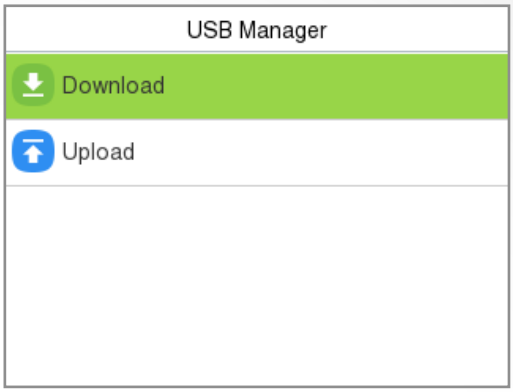
Puede importar la información del usuario y los datos de asistencia de la máquina al software de asistencia correspondiente para procesarlos mediante un disco USB, o importar la información del usuario a otros dispositivos para realizar copias de seguridad.

Seleccione USB Manager en la interfaz del menú principal.

Dispositivo de Asistencia de Tiempo



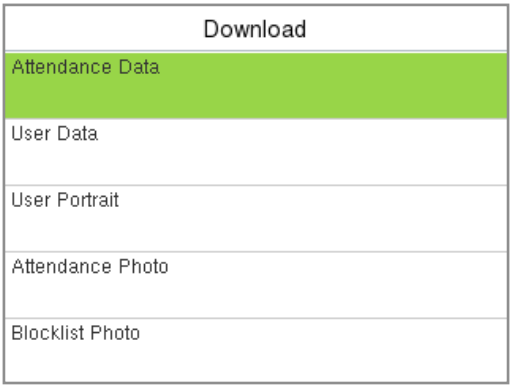
Dispositivo de Control de Acceso:



Nota: Sólo se admite el formato FAT32 cuando se descargan datos utilizando un disco USB.

12.1 Descarga USB

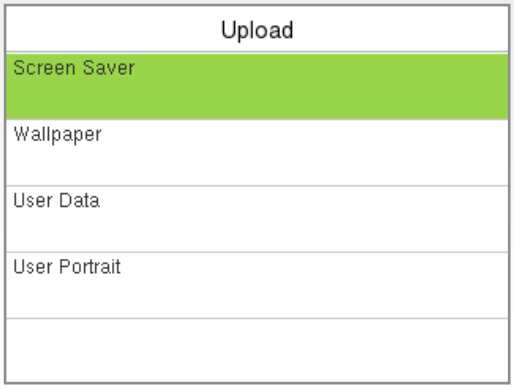
En la interfaz del **Administrador USB**, pulse **Descargar**.



Nombre de la función	Descripciones
AsistenciaDatos/ Registros de acceso	Para descargar todos los datos de asistencia/acceso en un periodo de tiempo especificado en un disco USB.
Datos del usuario	Para descargar toda la información del usuario del dispositivo en un disco USB.
Retrato de usuario	Para descargar todos los retratos de usuario del dispositivo en un disco USB.
Foto de asistencia	Para descargar todas las fotos de asistencia del dispositivo en un disco USB.
Lista de bloqueo de fotos	Para descargar todas las fotos bloqueadas (fotos tomadas después de verificaciones fallidas) del dispositivo al disco USB.

12.2 Carga USB

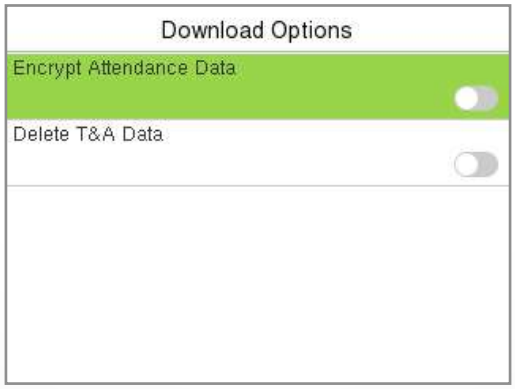
En la interfaz del **Administrador USB**, pulse **Descargar**.



Nombre de la función	Descripciones
Protector de pantalla	Para cargar todos los protectores de pantalla del disco USB en el dispositivo. Puede elegir Cargar la foto seleccionada o cargar todas las fotos. Las imágenes se mostrarán en la interfaz principal del dispositivo después de la carga.
Papel pintado	Para cargar todos los fondos de pantalla del disco USB en el dispositivo. Puede elegir Cargar la foto seleccionada o cargar todas las fotos. Las imágenes se mostrarán en la pantalla después de la carga.
Datos del usuario	Para cargar toda la información del usuario desde el disco USB al dispositivo.
Retrato de usuario	Para cargar todos los retratos de usuario desde el disco USB al dispositivo.

12.3 Descargar opciones

En la interfaz del **Administrador USB**, pulse **Opciones de descarga**.
Nota: Esta función sólo es válida para el Terminal de Control Horario.



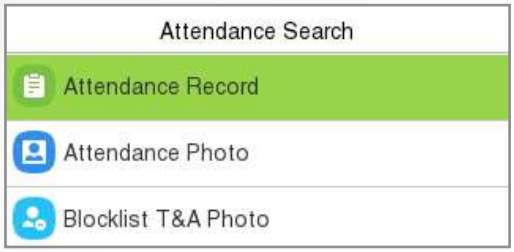
Nombre de la función	Descripciones
Cifrar fecha de asistencia	Los datos de asistencia se encriptan durante la carga y la descarga.
Borrar datos de T&A	Una vez realizada la descarga, se borrarán los datos de asistencia del dispositivo.

13 Búsqueda de asistentes

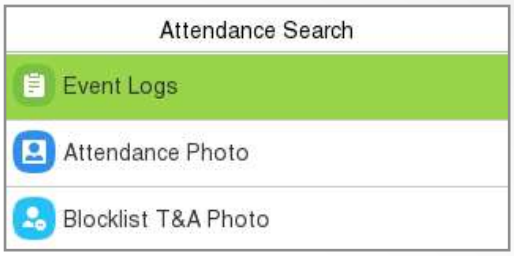
Una vez verificada la identidad de un usuario, los registros de eventos se guardarán en el dispositivo. Esta función permite a los usuarios comprobar sus registros de acceso.

Cuando el dispositivo se encuentre en la interfaz inicial, pulse **M/OK** y seleccione **Búsqueda de Asistencia** para buscar el registro de asistencia/acceso requerido.

Dispositivo de Tiempo & Asistencia

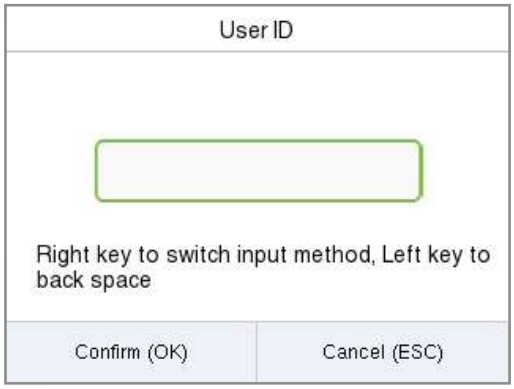


Dispositivo de Control de Acceso



El proceso de búsqueda de fotos de asistencia y listas de bloqueo es similar al de búsqueda de registros de eventos. A continuación se muestra un ejemplo de búsqueda de registro de asistencia.

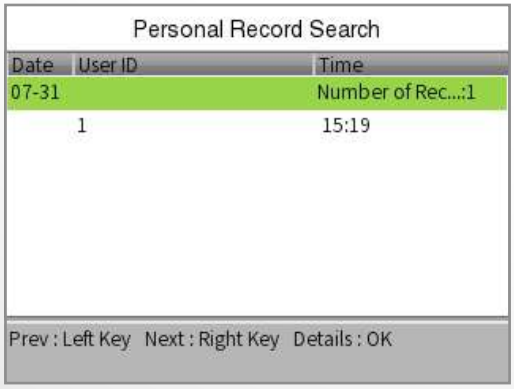
En la interfaz de **búsqueda de asistencia**, pulse **Registro de asistencia/Registros de eventos** para buscar el registro deseado.



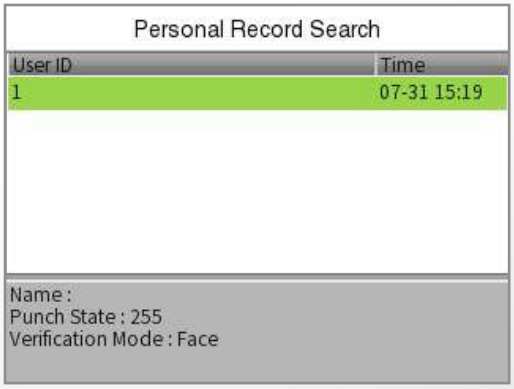
1. Introduzca el ID de usuario que desea buscar y pulse **M/OK**. desea buscar registros de todos los usuarios, **pulse M/OK** sin introducir ningún ID de usuario.



2. Seleccione el intervalo de tiempo en el que buscarse los registros.



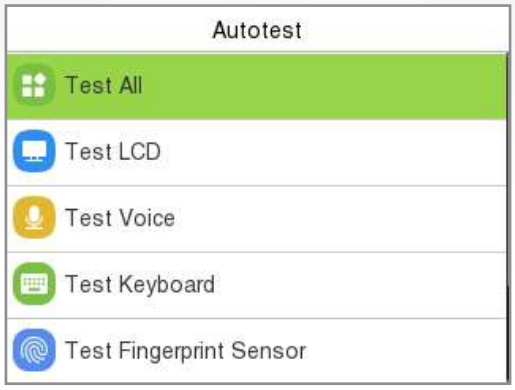
3. Una vez finalizada la búsqueda de registros. Pulse el registro resaltado en verde para ver sus detalles.



4. La figura muestra los detalles del registro seleccionado.

14 Autotest

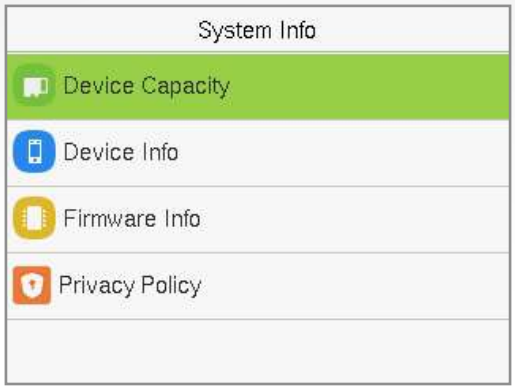
Cuando el dispositivo está en la interfaz inicial, pulse **M/OK** y seleccione **Autotest**, permite al sistema probar automáticamente si las funciones de varios módulos funcionan con normalidad, incluyendo el LCD, Voz, Teclado, Huella Dactilar, Cámara y Reloj en Tiempo Real (RTC).



Nombre de la función	Descripciones
Probar todo	Para comprobar automáticamente si la pantalla LCD, el audio, la cámara y el RTC son normales.
LCD de prueba	Para probar automáticamente el efecto de visualización de la pantalla LCD mediante la visualización a todo color, blanco puro y negro puro para comprobar si la pantalla muestra los colores con normalidad.
Voz de prueba	Para comprobar automáticamente si los archivos de audio almacenados en el dispositivo están completos y la calidad de la voz es buena.
Teclado de prueba	El terminal comprueba si todas las teclas teclado funcionan con normalidad. Pulse cualquier tecla de la interfaz **Teclado de prueba** para comprobar si la tecla pulsada coincide con la tecla mostrada en la pantalla. Las teclas se muestran en gris oscuro antes y se vuelven verdes después de pulsarlas. Pulse **ESC** para salir de la prueba.
Prueba de micrófono	Compruebe si el micrófono funciona hablando al micrófono y reproduciendo la grabación del mismo.
Prueba del sensor de huellas dactilares	Para probar el sensor de huellas dactilares, presione con el dedo sobre el escáner para comprobar si la imagen de la huella dactilar adquirida es nítida. Cuando presione con un dedo sobre el escáner, la imagen de la huella dactilar aparecerá en la pantalla.
Prueba de cámara	Para comprobar si la cámara funciona correctamente, compruebe si las fotos tomadas son lo suficientemente claras. (Igual que "Probar cara").
Reloj de prueba RTC	Para probar el RTC. El aparato comprueba si el reloj funciona con normalidad y precisión con un cronómetro. Pulse M/OK para iniciar el conteo y púlselo de nuevo para detenerlo.

15 Información del sistema

Cuando el dispositivo esté en la interfaz inicial, pulse **M/OK** y seleccione **Información del sistema** para ver el estado de almacenamiento, la información de la versión del dispositivo, la información del firmware y la política de privacidad.



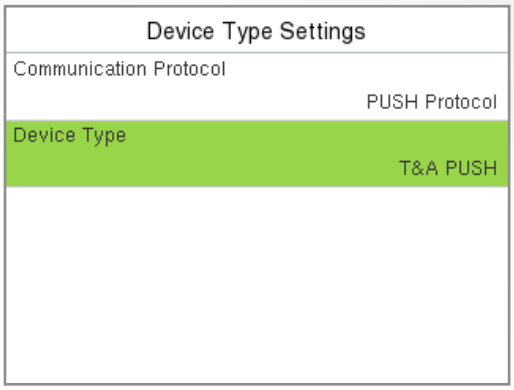
Nombre de la función	Descripciones
Capacidad del dispositivo	Muestra el almacenamiento del usuario del dispositivo actual, la contraseña, la plantilla facial, el almacenamiento de huellas dactilares y tarjetas, los registros de T&A, las fotos de asistencia y de la lista de bloqueo, y las fotos del perfil.
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la dirección MAC, el algoritmo de la huella dactilar, el algoritmo de la plantilla facial, la información de la plataforma, la versión de la MCU y la fecha de fabricación.
Información del firmware	Muestra la versión del firmware y otra información sobre la versión del dispositivo.
Política de privacidad	El control de la política de privacidad aparecerá cuando el se encienda por primera vez. Tras hacer clic en "La he leído", el cliente puede utilizar el producto con regularidad. Haga clic en Información del sistema > Política de privacidad para ver el contenido de la política de privacidad. El contenido de la política de privacidad no permite la exportación de discos U. **Nota**: El texto actual de la política de privacidad sólo está disponible en chino simplificado/inglés. Sin embargo, la traducción de otros contenidos multilingües está en marcha, con más iteraciones.

16 Conectar con el software BioTime Cloud

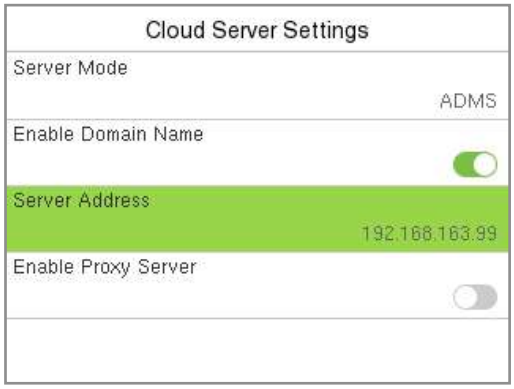
16.1 Añadir dispositivo en el software

1. Pulse **COMM.** > **Ethernet** en el menú principal para configurar la dirección IP y la puerta de enlace del dispositivo.
2. Pulse **Sistema** > **Configuración de tipo de dispositivo** > **Tipo de dispositivo** para ver y asegurarse de que el tipo de dispositivo está configurado como T&A PUSH.

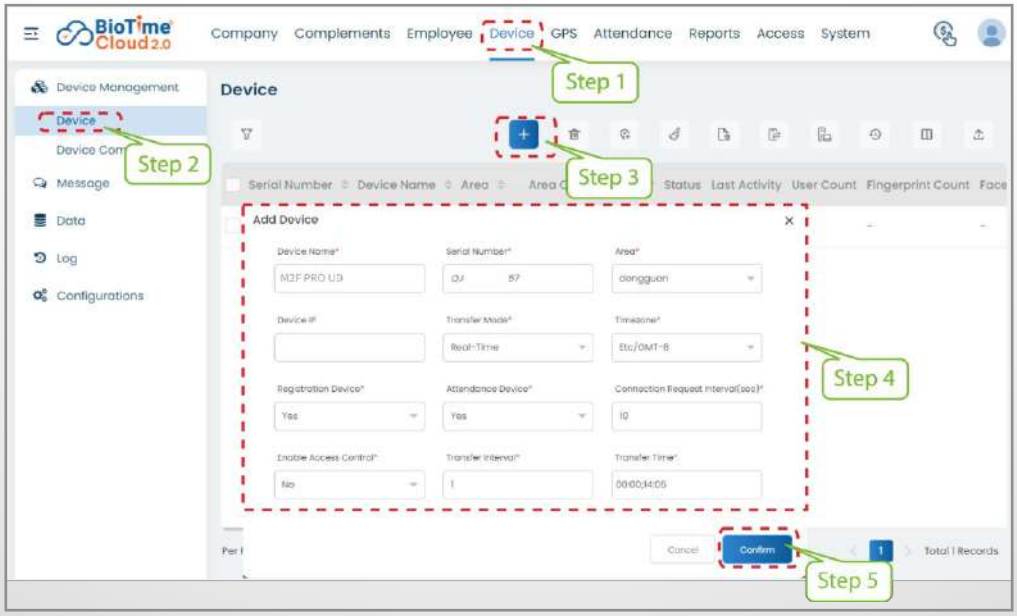




3. En el menú principal, pulse COMM. > Configuración del Servidor Cloud para activar Nombre de Dominio e introduzca el nombre de dominio correcto.

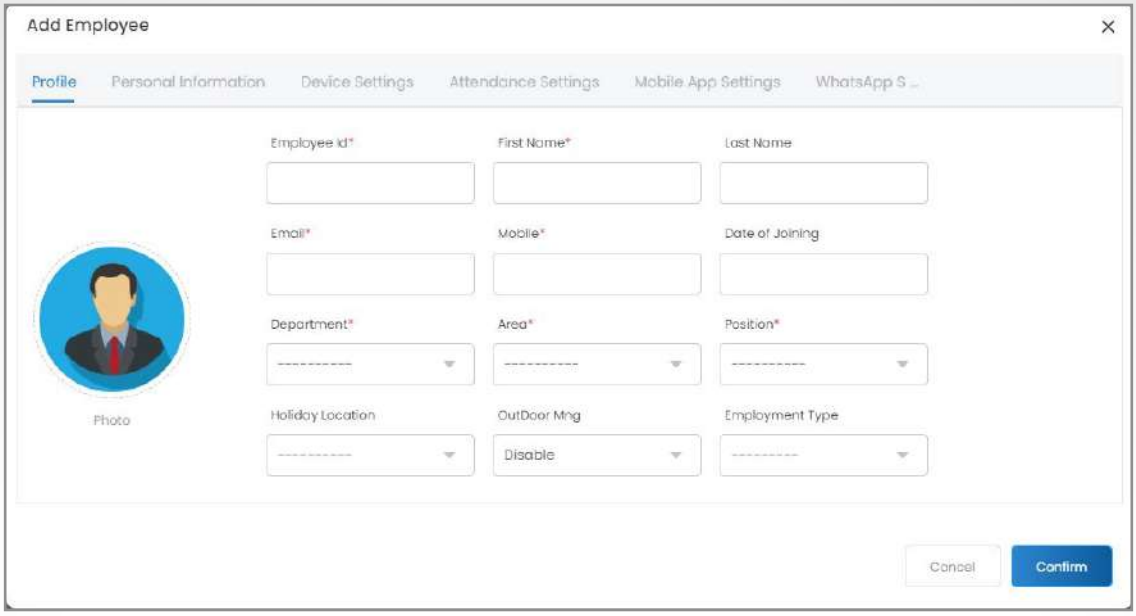


4. Abra BioTime Cloud y en la interfaz Dispositivo, haga clic en Añadir + para añadir el nuevo dispositivo montado al software.



16.2 Añadir personal al programa

1. Haga clic en **Empleado** > **Perfil** > **Empleado** > + y rellene todos los campos necesarios para registrar nuevos usuarios en el software.



2. Rellene todos los campos obligatorios y haga clic en Confirmar para registrar un nuevo usuario.

3. Haga clic en **Empleado** > **Perfil** > **Empleado** >> Resincronizar a dispositivos para sincronizar todos los datos en el dispositivo, incluidos los nuevos usuarios.

17 Conectarse al software ZKBio CVAccess

17.1 Establecer la dirección de comunicación

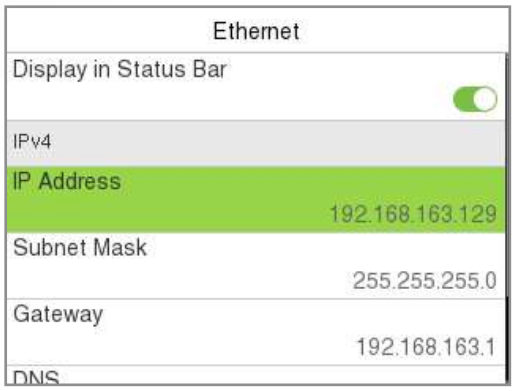
• Lado del dispositivo

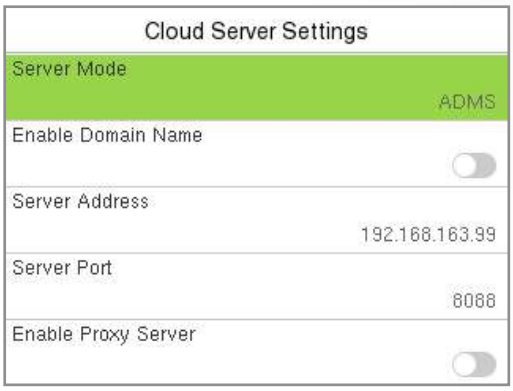
1. Pulse **System**> **Device Type Settings**> **Device Type** para cambiar el tipo de dispositivo a A&C PUSH.
2. Pulse **COMM.** > **Ethernet** en el menú principal para configurar la dirección IP y la puerta de enlace del dispositivo.

Nota: Asegúrese de que la dirección IP se encuentra en el mismo segmento de red que la dirección del servidor y puede comunicarse con el servidor ZKBio CVAccess.

3. En el menú principal, pulse **COMM.** > **Configuración Servidor Nube** para configurar la dirección del servidor y el puerto del servidor.

Dirección del servidor: Establezca la dirección IP del servidor ZKBio CVAccess.
Puerto del servidor: Establezca el puerto del servidor a partir de ZKBio CVAccess.





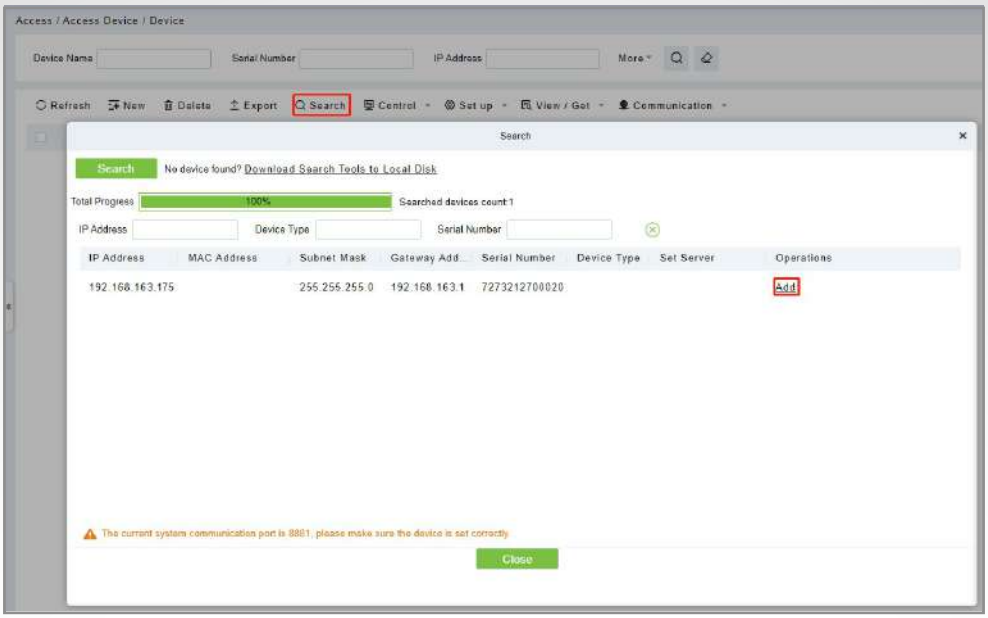
• Lado del Software

Inicie sesión en el software ZKBio CVAccess, haga clic en System> Communication> Communication Monitor para configurar el puerto de servicio ADMS, como se muestra en la figura siguiente:



17.2 Añadir dispositivo en el software

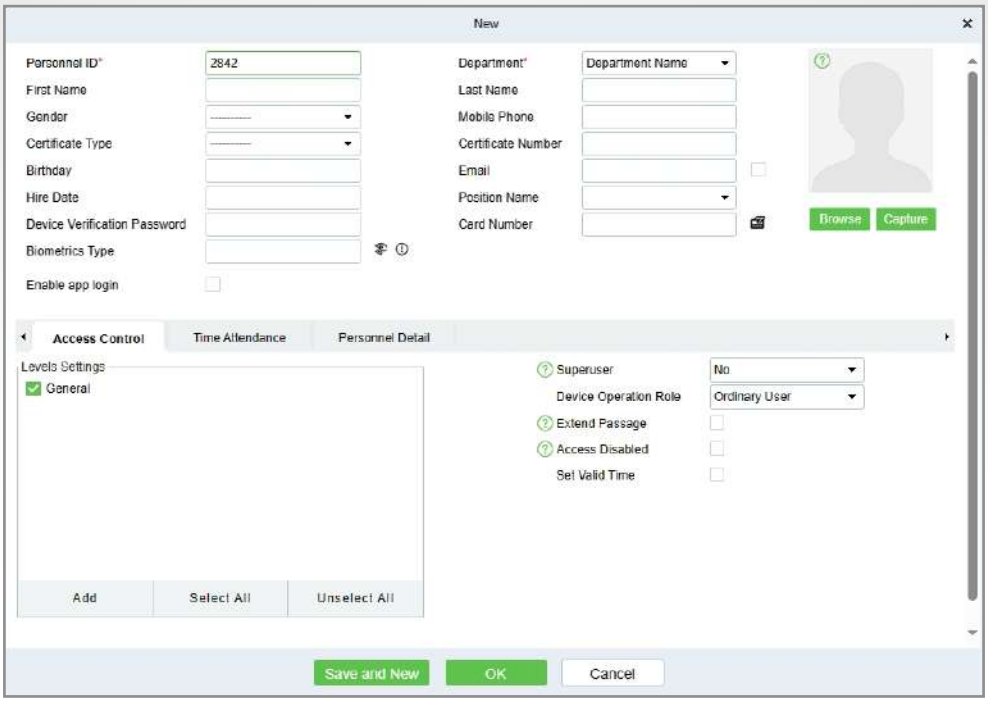
Añada el dispositivo mediante la búsqueda. El proceso es el siguiente:
1. Haga clic en **Access**> **Device**> **Search Device**, para abrir la interfaz de búsqueda en el software.
2. Haga clic en **Buscar**, y aparecerá Searching.....
3. Tras la búsqueda, se mostrará la lista y el número total de controladores de acceso.



4. Haga clic en **Añadir** en la columna de operación, aparecerá una nueva ventana. Seleccione Tipo de icono, Área y Añadir a nivel en cada desplegable y haga clic en **Aceptar** para añadir el dispositivo.

17.3 Añadir personal al programa

1. Haga clic en **Personal**> **Persona**> **Nuevo**:



2. Rellene todos los campos obligatorios y pulse **OK** para registrar un nuevo usuario.
3. Haga clic en **Acceso** > **Dispositivo** > **Control** > **Sincronizar todos los datos con los dispositivos** para sincronizar todos los datos con el dispositivo, incluidos los nuevos usuarios.

Anexo 1

Requisitos de la recogida en vivo y el registro de plantillas de rostros de luz visible

1. Se recomienda realizar el registro en un ambiente interior con una luz adecuada fuente sin subexposición ni sobreexposición.

2. No coloque el aparato hacia fuentes de luz exteriores como puertas o ventanas u otras fuentes de luz intensa.

3. Para el registro se recomienda ropa de color oscuro, diferente del color de fondo.

4. Por favor, exponga la plantilla de su cara y la frente correctamente y no cubra la plantilla de su cara y cejas con el pelo.

5. Se recomienda mostrar una expresión facial sencilla. (Una sonrisa es aceptable, pero no cierre los ojos ni incline la cabeza hacia ninguna orientación).

6. Se necesitan dos plantillas para una persona con gafas, una plantilla con gafas y otra sin las gafas.

7. No lleve accesorios como bufanda o mascarilla que puedan taparle la boca o la barbilla.

8. Por favor, dirija la plantilla facial hacia el dispositivo de captura, y localice su plantilla facial en el área de captura de plantillas como se muestra en la plantilla siguiente.

9. No incluya más de una plantilla de cara en el área de captura.

10. Se recomienda una distancia de 50 cm a 80 cm para capturar la plantilla. (La distancia es ajustable, en función de la altura del cuerpo).



Requisitos de los datos de las plantillas digitales de rostros con luz visible

La foto digital debe ser de bordes rectos, en color, medio retratada con una sola persona, y la persona debe estar desencajada y en ropa informal. Las personas que lleven gafas no deben para hacerse la foto.

• **Distancia ocular**
Se recomiendan 200 píxeles o más con no menos de 115 píxeles de distancia.

• **Expresión facial**
Se recomienda una plantilla facial neutra o una sonrisa con los ojos abiertos de forma natural.

• **Gesto y ángel**
El ángulo de rotación horizontal no debe exceder de ±10°, el de elevación no debe exceder de ±10° y el de depresión no debe exceder de ±10°.

• **Accesorios**
No se permiten máscaras ni gafas de colores. La montura de las gafas no debe cubrir los ojos ni reflejar la luz. Para las personas con monturas de gafas gruesas, se recomienda capturar dos plantillas, una con gafas y otra sin ellas.

• **Plantilla facial**
Plantilla facial completa con contorno claro, escala real, luz distribuida uniformemente y sin sombras.

• **Formato de plantilla**
Debe estar en BMP, JPG o JPEG.

• **Datos necesarios**
Debe cumplir los siguientes requisitos:

1. Fondo blanco con ropa de color oscuro.
2. Modo de color verdadero de 24 bits.
3. Plantilla comprimida en formato JPG con un tamaño no superior a 20kb.
4. La resolución debe estar comprendida entre 358 x 441 y 1080 x 1920.
5. La escala vertical de la cabeza y el cuerpo debe estar en una proporción de 2:1.
6. La foto debe incluir los hombros de la persona capturada al mismo nivel horizontal.
7. Los ojos de a persona capturada deben estar abiertos y con el iris claramente visible.
8. Se prefiere una plantilla facial neutra o una sonrisa, no es preferible mostrar los dientes.
9. La persona capturada debe ser claramente visible, de color natural, sin sombras duras o puntos de luz o reflejo en la plantilla de la cara o en el fondo. El nivel de contraste y luminosidad debe ser adecuado.

Anexo 2

Política de privacidad

Aviso:
Para ayudarle a utilizar mejor los productos y servicios de ZKTeco (en lo sucesivo, "nosotros", "nuestro" o "nos"), un proveedor de servicios inteligentes, recopilamos sistemáticamente su información personal. Puesto que entendemos la importancia de su información personal, tomamos su privacidad sinceramente y hemos formulado esta política de privacidad para proteger su información personal. Hemos enumerado las políticas de privacidad a continuación para entender con precisión las medidas de protección de datos y privacidad relacionadas con nuestros productos y servicios inteligentes.

Antes de utilizar nuestros productos y servicios, lea atentamente y comprenda todas las normas y disposiciones de la presente Política de Privacidad. Si no está de acuerdo con el acuerdo correspondiente o con alguna de sus cláusulasdeberá dejar de utilizar nuestros productos y servicios.

I. Información recogida

Para garantizar el funcionamiento normal del producto y contribuir a la mejora del serviciorecopilaremos la información que nos facilite voluntariamente o que nos autorice durante el registro y el uso o que se genere como resultado de su uso de los servicios.

1. **Información de registro del usuario:** En su primer registro, la plantilla de características (**plantilla de huella dactilar/plantilla de rostro/plantilla de palma**) se guardará en el dispositivo según el tipo de dispositivo que haya seleccionado para verificar la similitud única entre usted y el ID de usuario que ha registrado. Opcionalmente puede introducir su Nombre y Código. La información anterior es necesaria para que pueda utilizar nuestros productos. Si no facilita dicha información, no podrá utilizar regularmente algunas funciones del producto.

2. **Información sobre el producto:** De acuerdo con el modelo de producto y su permiso concedido instala y utiliza nuestros servicios, la información relacionada del producto en el que se utilizan nuestros servicios se recopilará cuando el producto se conecte al software, incluido el modelo de producto, el número de versión del firmware, el número de serie del producto y la información de capacidad del producto. **Cuando conecte su producto al software, lea atentamente la política de privacidad del software específico.**

II. Seguridad y gestión de productos

Para garantizar el funcionamiento normal del producto y contribuir a la mejora del serviciorecopilaremos la información que nos facilite voluntariamente o que nos autorice durante el registro y el uso o que se genere como resultado de su uso de los servicios.

1. Cuando utilice nuestros productos por primera vez, deberá establecer el privilegio de administrador antes de realizar operaciones específicas. De lo contrario, se le recordará con frecuencia que debe establecer el privilegio de administrador cuando acceda a la interfaz del menú principal. **Si sigue sin establecer el privilegio de administrador después de recibir el aviso del sistema, debe ser consciente del posible riesgo para la seguridad (por ejemplo, los datos pueden modificarse manualmente).**

2. Todas las funciones de visualización de la información biométrica están desactivadas por defecto en nuestros productos. Puede elegir Menú > Configuración del sistema para establecer si desea mostrar la información biométrica. Si habilita estas funciones, asumimos que es consciente de los riesgos para la seguridad de la privacidad personal especificados en la política de privacidad.

3. Por defecto, sólo se muestra su ID de usuario. Puede configurar si desea mostrar otra información de verificación del usuario (como Nombre, Departamento, Foto, etc.) bajo el privilegio de Administrador. **E liges mostrar dicha información, asumimos que eres consciente de los posibles riesgos de seguridad (por ejemplo, tu foto se mostrará en la interfaz del dispositivo).**

4. La función de cámara está desactivada por defecto en nuestros productos. Si desea habilitar esta función para tomar fotografías de usted mismo para el registro de asistencia o tomar fotografías de extraños para el control de acceso, el producto habilitará el tono de aviso de la cámara. **Una vez habilitada esta función, asumimos que es consciente de los posibles riesgos de seguridad.**

5. Todos los datos recopilados por nuestros productos se cifran mediante el algoritmo AES 256. Todos los datos cargados por el Administrador en nuestros productos se cifran automáticamente utilizando el algoritmo AES 256 y se almacenan de forma segura. Si el Administrador descarga datos de nuestros productos, asumimos que usted necesita procesar los datos y que conoce el riesgo potencial de seguridad. En tal , usted asumirá la responsabilidad de almacenar los datos. Debe saber que algunos datos no pueden descargarse por motivos de seguridad.

6. Toda la información personal de nuestros productos puede consultarse, modificarse o borrarse. Si ya no utiliza nuestros productos, borre sus datos personales.

III. Cómo tratamos la información personal de los menores

Nuestros productos, sitio web y servicios están diseñados principalmente para adultos. Sin el consentimiento de los padres o tutores, los menores no podrán crear su propia cuenta. Si es usted menor de edad, le recomendamos que pida a sus padres o tutores que lean atentamente esta Política, y que sólo utilice nuestros servicios o la información que le proporcionamos con el consentimiento de sus padres o tutores.

Sólo utilizaremos o divulgaremos la información personal de menores recopilada con el consentimiento de sus padres o tutores si y en la medida en que dicho uso o divulgación esté permitido por la ley o hayamos obtenido el consentimiento explícito de sus padres o tutores, y dicho uso o divulgación tenga por objeto proteger a los menores.

Cuando nos demos cuenta de que hemos recopilado información personal de menores sin el consentimiento previo de los padres verificable, eliminaremos dicha información lo antes posible.

IV. Otros

Puede visitar https://www.zkteco.com/cn/index/Index/privacy_protection.html para obtener más información sobre cómo recopilamos, utilizamos y almacenamos de forma segura su información personal. Para seguir el ritmo del rápido desarrollo de la tecnología, el ajuste de las operaciones comerciales y hacer frente a las necesidades de los clientes, deliberaremos y optimizaremos constantemente nuestras medidas y políticas de protección de la privacidad. Le invitamos a visitar nuestro sitio web oficial en cualquier momento para conocer nuestra política de privacidad más reciente.

Funcionamiento ecológico

El "período de funcionamiento ecológico" del producto se refiere al tiempo durante el cual este producto no descargará ninguna sustancia tóxica o peligrosa cuando se utilice de acuerdo con los requisitos previos de este manual.

El período de funcionamiento ecológico especificado para este producto no incluye las pilas ni otros componentes que se desgastan con facilidad y deben sustituirse periódicamente. El periodo de funcionamiento ecológico de la batería es de 5 años.

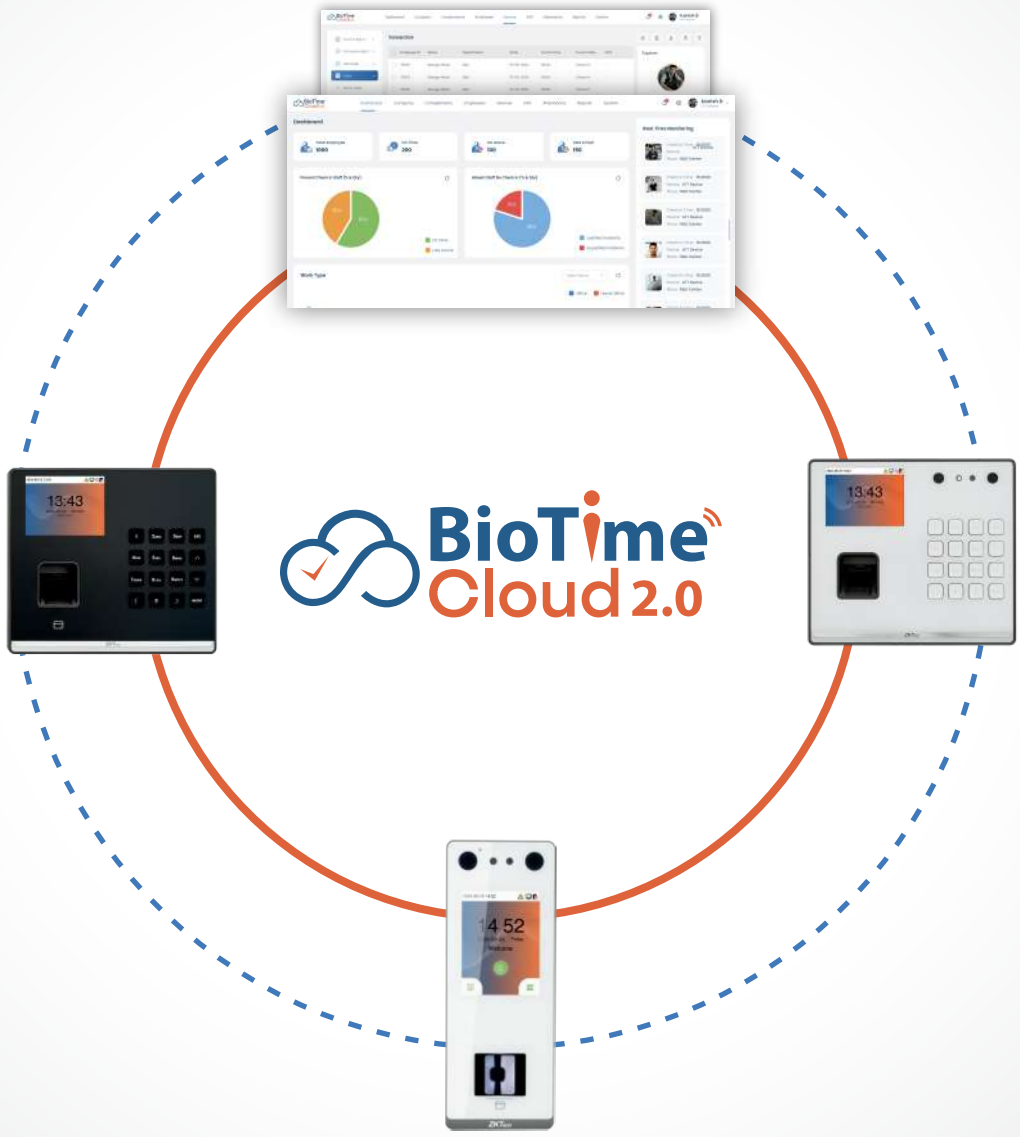
Sustancias peligrosas o tóxicas y sus cantidades

Nombre del componente	Sustancia/elemento peligroso/tóxico					
	Plomo (Pb)	Mercurio (Hg)	Cadmium (Cd)	Cromo hexavalente (Cr6+)	Polibromobifenilos (PBB)	Éteres difenílicos polibromados (PBDE)
Resistencia de chip	X	O	O	O	O	O
Condensador de chip	X	O	O	O	O	O
Inductor de chip	X	O	O	O	O	O
Diodo	X	O	O	O	O	O
ESD componente	X	O	O	O	O	O
Zumbador	X	O	O	O	O	O
Adaptador	X	O	O	O	O	O
Tornillos	O	O	O	X	O	O

O indica que la cantidad total de contenido tóxico en todos los materiales homogéneos está por debajo del como se especifica en SJ/T 11363-2006.

X indica que la cantidad total de contenido tóxico en todos los materiales homogéneos supera el límite especificado en SJ/T 11363-2006.

Nota: El 80% de los componentes de este producto están fabricados con materiales no tóxicos y ecológicos. Los componentes que contienen toxinas o elementos nocivos se incluyen debido a las limitaciones económicas o técnicas actuales que impiden su sustitución por materiales o elementos no tóxicos.



Your AI Workforce Cloud Attendance Management Platform

www.zkteco.com

www.zkteco.mx

Copyright © 2024 ZKTECO CO., LTD. All rights reserved.