Manual de usuario

SpeedFace-V5L [TI]

Fecha: julio de 2020

Versión Doc: 1.0

Inglés

Gracias por elegir nuestro producto. Lea atentamente las instrucciones antes de la operación. Siga estas instrucciones para asegurarse de que el producto funcione correctamente. Las imágenes que se muestran en este manual son solo para fines ilustrativos.

Para obtener más detalles, visite el sitio web de nuestra empresa.
www.zkteco.com .

Marca comercial

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

Descargo de responsabilidad

Este manual contiene información sobre el funcionamiento y mantenimiento del equipo ZKTeco. Los derechos de autor de todos los documentos, dibujos, etc. en relación con el equipo suministrado por ZKTeco pertenecen y son propiedad de ZKTeco. El receptor no debe usar ni compartir el contenido del presente con ningún tercero sin el permiso expreso por escrito de ZKTeco.

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

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

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

ZKTeco no ofrece garantía, garantía o representación con respecto a la integridad de cualquier información contenida en este manual o cualquiera de las enmiendas realizadas al 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 por ningún error u omisión en la información o los documentos a los que se hace referencia o están vinculados a este manual. El usuario asume todo el riesgo en cuanto a los resultados y el rendimiento obtenido del uso de la información.

ZKTeco en ningún caso será responsable ante el usuario o cualquier tercero por cualquier daño incidental, consecuente, indirecto, especial o ejemplar, incluyendo, sin limitación, pérdida de negocio, lucro cesante, interrupción del negocio, pérdida de información comercial o cualquier pérdida pecuniaria, que surja de, en conexión con, o

relacionados con el uso de la información contenida en este manual o a la que se hace referencia en él, incluso si ZKTeco ha sido advertido de la posibilidad de tales daños.

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

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

El producto se actualizará de vez en cuando sin previo aviso. Los últimos procedimientos operativos y documentos relevantes están disponibles en http: // www. zkteco .com

Si hay algún problema relacionado con el producto, comuníquese con nosotros.

Sede de ZKTeco

Habla a Parque industrial ZKTeco, No. 26, 188 Industrial Road, Tangxia Town, Dongguan, China.

Teléfono + 86 769 - 82109991

Fax + 86 755 - 89602394

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

Sobre la empresa

ZKTeco es uno de los fabricantes más grandes del mundo de lectores RFID y biométricos (huellas dactilares, faciales, venas dactilares). Las ofertas de productos incluyen lectores y paneles de control de acceso, cámaras de reconocimiento facial de rango cercano y lejano, controladores de acceso de ascensor / piso, torniquetes, controladores de puerta de reconocimiento de matrículas (LPR) y productos de consumo que incluyen cerraduras de puertas con lector de huellas dactilares y faciales a batería. Nuestras soluciones de seguridad son multilingües y están localizadas en más de 18 idiomas diferentes. En el estado de la técnica de ZKTeco

Planta de fabricación de 700,000 pies cuadrados con certificación ISO9001, controlamos la fabricación, el diseño de productos, el ensamblaje de componentes y la logística / envío, todo bajo un mismo techo.

Los fundadores de ZKTeco han sido determinados por la investigación y el desarrollo independientes de procedimientos de verificación biométrica y la producción de SDK de verificación biométrica, que inicialmente se aplicó ampliamente en los campos de autenticación de identidad y seguridad de PC. Con la mejora continua del desarrollo y una gran cantidad de aplicaciones de mercado, el equipo ha construido gradualmente un ecosistema de autenticación de identidad y un ecosistema de seguridad inteligente, que se basan en técnicas de verificación biométrica. Con años de experiencia en la industrialización de 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 la Empresa Nacional de Alta Tecnología durante 6 años consecutivos.

Acerca del manual

Este manual presenta las operaciones del producto SpeedFace-V5L [TI].

Todas las cifras que se muestran son solo para fines ilustrativos. Las cifras de este manual pueden no coincidir exactamente con los productos reales.

Características y parámetros con ★ no están disponibles en todos los dispositivos.

Convenciones de documentos

Las convenciones utilizadas en este manual se enumeran a continuación:

Convenciones GUI

Para software	
Convención	**Descripción**
Negrita	Se utiliza para identificar nombres de interfaz de software, p. Ej. **Aceptar, confirmar, cancelar**
>	Los menús de varios niveles están separados por estos corchetes. Por ejemplo, Archivo> Crear> Carpeta.
Para dispositivo	
Convención	**Descripción**
<>	Nombres de botones o teclas para dispositivos. Por ejemplo, presione <OK>
[]	Los nombres de las ventanas, los elementos del menú, la tabla de datos y los nombres de los campos están entre corchetes. Por ejemplo, abre la ventana [Usuario nuevo]
/	Los menús de varios niveles están separados por barras diagonales. Por ejemplo, [Archivo / Crear / Carpeta].

Simbolos

Convención	Descripción
	Esto implica sobre el aviso o presta atención, en el manual
	La información general que ayuda a realizar las operaciones más rápido.
	La información que es significativa
	Cuidado para evitar peligros o errores
	La declaración o el evento que advierte de algo o que sirve como ejemplo de advertencia.

Tabla de contenido

1 Medidas de seguridad

Las siguientes precauciones son para mantener la seguridad del usuario y evitar cualquier daño. Lea atentamente antes de la instalación.

1. **Lea, siga y conserve las instrucciones:** Todas las instrucciones de seguridad y funcionamiento deben estar correctamente leer y seguir antes de poner en servicio el dispositivo.
2. **No ignore las advertencias:** Siga todas las advertencias de la unidad y las instrucciones de funcionamiento.
3. **Accesorios -** Utilice solo accesorios recomendados por el fabricante o vendidos por el producto. No se deben utilizar accesorios no recomendados por el fabricante.
4. **Precauciones para la instalación** - No coloque este dispositivo sobre un soporte o marco inestable. Puede caerse y causar lesiones graves a personas y daños al dispositivo.
5. **Servicio -** No intente reparar esta unidad usted mismo. Abrir o quitar las cubiertas puede exponerlo a voltajes peligrosos u otros peligros.
6. **Daños que requieren servicio -** Desconecte el sistema de la fuente de alimentación principal de CA o CC y consulte 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 se cayó un artículo en el sistema.
   - Si se expone al agua y / o inclemencias del tiempo (lluvia, nieve y más). Si el sistema no funciona
   - normalmente según las instrucciones de funcionamiento.

Simplemente cambie los controles definidos en las instrucciones de funcionamiento. El ajuste inadecuado de otros controles puede resultar en daños e involucrar a un técnico calificado para regresar el dispositivo a la operación normal.

7. **Piezas de repuesto -** Cuando se necesitan piezas de repuesto, los técnicos de servicio solo deben utilizar repuestos proporcionados por el proveedor. Los sustitutos no autorizados pueden provocar quemaduras, descargas eléctricas u otros peligros.
8. **Verificación de seguridad -** Al finalizar el trabajo de servicio o reparación en la unidad, solicite al técnico de servicio que realice controles de seguridad para garantizar el funcionamiento correcto de la unidad.
9. **Fuentes de energía -** Utilice el sistema solo desde la fuente de alimentación de la etiqueta. Si no está claro el tipo de fuente de alimentación a utilizar, llame a su distribuidor.
10. **Rayo -** Se pueden instalar pararrayos externos para proteger contra tormentas eléctricas. Evita que los power-ups destruyan el sistema.

Los dispositivos deben instalarse en áreas con acceso limitado.

2 Visión general

SpeedFace-V5L [TI] utiliza **Reconocimiento facial de ingeniería inteligente de imágenes térmicas** algoritmos y lo último **Tecnología de visión por computadora.** Admite la verificación facial y de la palma de la mano con gran capacidad y reconocimiento rápido, además de mejorar el rendimiento de la seguridad en todos los aspectos.

Adopta tecnología de reconocimiento sin contacto y nuevas funciones, a saber **Detección de temperatura** y **Identificación individual enmascarada** que elimina las preocupaciones de higiene de manera efectiva. También está equipado con lo último **Spoofing de hormigas** algoritmo de reconocimiento facial contra casi todos los tipos de ataques de fotos y videos falsos. Tiene reconocimiento de palma 3 en 1 (forma de palma, impresión de palma y vena de palma) que se realiza en 0,35 segundos por mano; la palmdata adquirida se compara con un máximo de 3.000 plantillas de palma.

El terminal con detección de temperatura y mascarilla es un dispositivo perfecto para ayudar a reducir la propagación de gérmenes y ayudar a prevenir infecciones en cada punto de acceso de cualquier local y áreas públicas como hospitales, fábricas, escuelas, edificios comerciales, estaciones durante la reciente salud pública global. problema con su medición rápida y precisa de la temperatura corporal y funciones de identificación individual enmascaradas durante la verificación facial y de la palma de la mano.

Caracteristicas

- Reconocimiento facial de luz visible.
- Mejor higiene con autenticación biométrica sin contacto, detección de temperatura e identificación individual enmascarada.
- Detección de temperatura de imágenes térmicas, detección de alta velocidad de 0,1 s, distancia de medición de 30 a 120 cm.
- Algoritmo anti-spoofing contra ataque de impresión (láser, color y fotos en B / N), ataque de videos y ataque de máscara 3D.
- Múltiples métodos de verificación: **Rostro / Palma / Huella digital / Contraseña**

Funciones especiales

- Detección de máscara.
- Detección de temperatura corporal.
- Distancia de medición de temperatura: **30 cm ~ 120 cm (0,98 pies ~ 3,94 pies).**
- Precisión de la medición de temperatura: **± 0,3 ° C (± 0,54 ° F)**

  (Probado a una distancia de 80 cm (2,63 pies) a una temperatura de 25 ° C (77 ° F)) Rango de
- medición de temperatura: **20 ° C ~ 50 ° C (68 ° F ~ 122 ° F)**

3 Instrucciones de uso

Antes de entrar en las características del dispositivo y sus funciones, se recomienda estar familiarizado con los fundamentos siguientes.

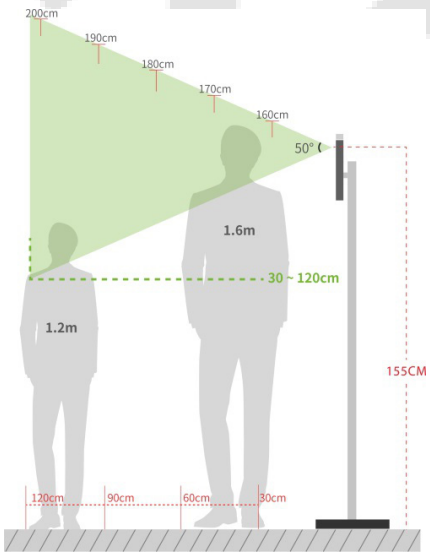
3.1 Posicionamiento de dedos

Dedos recomendados: Se recomienda usar el dedo índice, medio o anular para el registro y evitar usar el pulgar o el meñique, ya que son difíciles de presionar con precisión sobre el lector de huellas digitales.

NOTA : Utilice el método correcto cuando presione con los dedos el lector de huellas digitales para registrarse e identificarse. Nuestra empresa no asumirá ninguna responsabilidad por problemas de reconocimiento que puedan resultar del uso incorrecto del producto. Nos reservamos el derecho de interpretación final y modificación de este punto.

3.2 Posición de pie, postura y expresión facial

- **La distancia recomendada**



Se recomienda que la distancia entre el dispositivo y un usuario cuya altura esté en un rango de 1,55 m a 1,85 m sea de 0,3 a 2,5 m. Los usuarios pueden avanzar o retroceder ligeramente para mejorar la calidad de las imágenes faciales capturadas.

- **Postura de pie y expresión facial recomendadas**

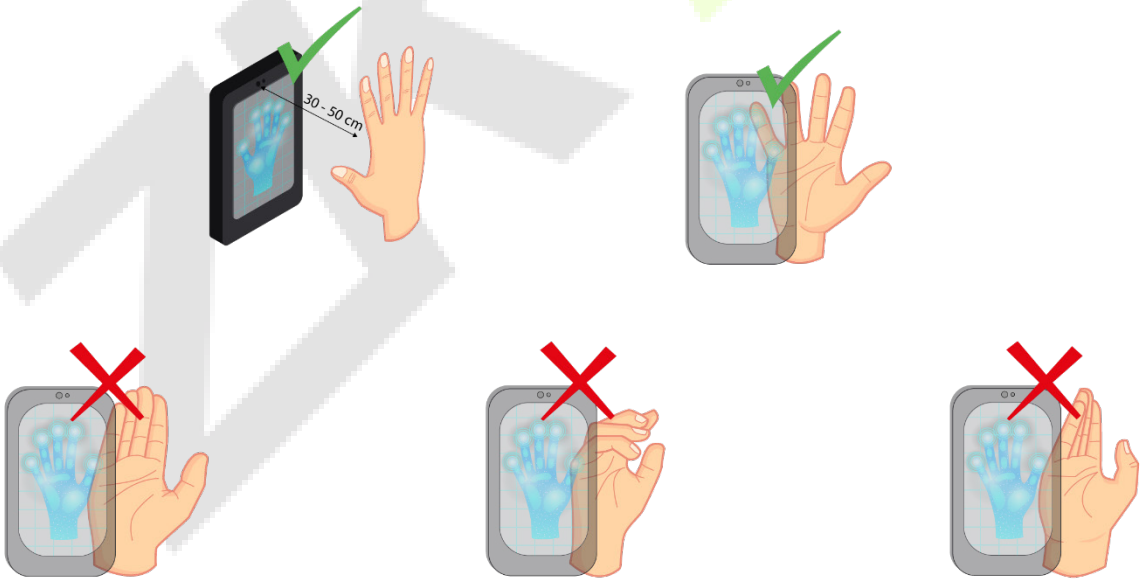
Postura de pie

Expresión facial

NOTA : Por favor, mantenga su expresión facial y postura de pie natural durante la inscripción o verificación.

3.3 PalmRegistration

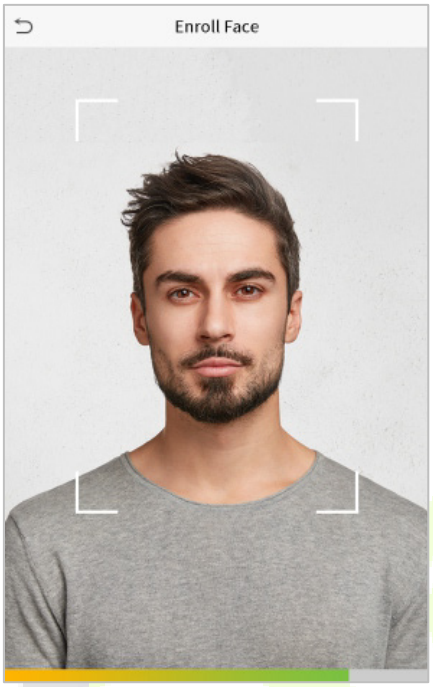
Coloque la palma de la mano en el área de recolección multimodo de la palma de la mano, de modo que la palma quede paralela al dispositivo. Asegúrese de dejar espacio entre los dedos.



NOTA : Coloque la palma de la mano entre 30 y 50 cm del dispositivo.

3.4 Registro facial

Intente mantener la cara en el centro de la pantalla durante el registro. Mire hacia la cámara y quédese quieto durante el registro facial. La pantalla debería verse así:



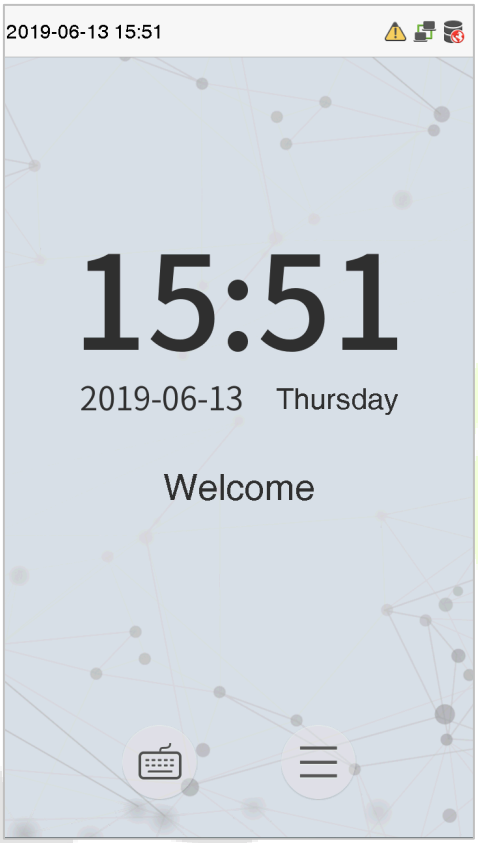
Método correcto de autenticación y registro facial

- **Recomendación para registrar un rostro**
  - Al registrar un rostro, mantenga una distancia de 40 cm a 80 cm entre el dispositivo y el rostro.
  - Tenga cuidado de no cambiar su expresión facial. (cara sonriente, cara dibujada, guiño, etc.)
  - Si no sigue las instrucciones que aparecen en pantalla, el registro facial puede tardar más o fallar.
  - Tenga cuidado de no cubrirse los ojos o las cejas.
  - No use sombreros, máscaras, gafas de sol o anteojos.
  - Tenga cuidado de no mostrar dos caras en la pantalla. Registre una persona a la vez.
  - Se recomienda que un usuario con gafas registre ambos rostros con y sin gafas.
- **Recomendación para autenticar un rostro**
  - Asegúrese de que la cara aparezca dentro de la línea guía que se muestra en la pantalla del dispositivo.
  - Si se han cambiado las gafas, la autenticación puede fallar. Si se ha registrado la cara sin gafas, autentique más la cara sin gafas. Si se ha registrado la cara con gafas, autentique la cara con las gafas usadas anteriormente.

- Si una parte de la cara está cubierta con un sombrero, una máscara, un parche en el ojo o gafas de sol, la autenticación puede fallar. No cubra la cara, permita que el dispositivo reconozca tanto las cejas como la cara.

3,5 Interfaz de espera

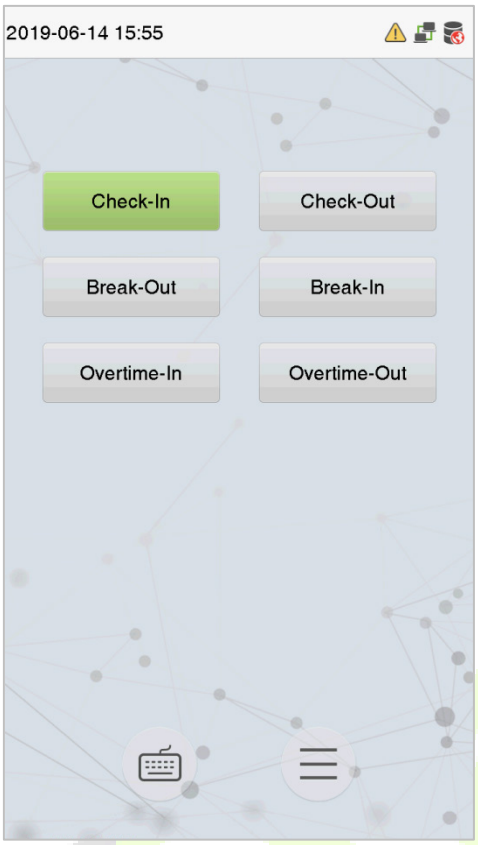
Después de conectar la fuente de alimentación, se muestra la siguiente interfaz de espera:



- Hacer clic para ingresar a la interfaz de entrada de ID de usuario.
- Cuando no haya un superadministrador configurado en el dispositivo, toque para ir al menú.
- Después de configurar el superadministrador en el dispositivo, se requiere la verificación del superadministrador antes de ingresar a las funciones del menú.

  NOTA : Para la seguridad del dispositivo, se recomienda registrar el superadministrador la primera vez que lo utilice.

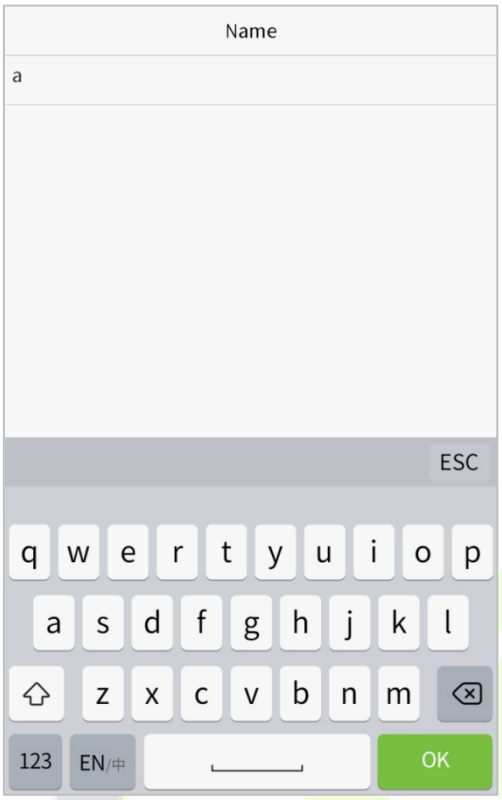
- Las opciones de estado de perforación también se pueden mostrar y utilizar directamente en la interfaz de espera. Haga clic en cualquier lugar de la pantalla, aparte de los iconos, y aparecerán seis teclas de acceso directo en la pantalla, como se muestra en la siguiente figura:



- Presione la tecla de estado de perforación correspondiente para seleccionar su estado de perforación actual, que se muestra en verde.

NOTA : Las opciones de estado de perforación están desactivadas de forma predeterminada y deben cambiarse a otra opción en el "9.4 Opciones de los estados de perforación " para obtener las opciones de estado de perforación en la pantalla de espera.

3.6 Teclado virtual



NOTA :

El dispositivo admite la entrada en chino, inglés, números y símbolos.

- Haga clic en [**En]** para cambiar al teclado en inglés. Prensa [**123]** para cambiar al
- teclado numérico y simbólico. haga clic en [**A B C]** para volver al teclado alfabético.
- Haga clic en el cuadro de entrada, aparece el teclado virtual. Haga clic en [**ESC]** para
- salir del teclado virtual.
-

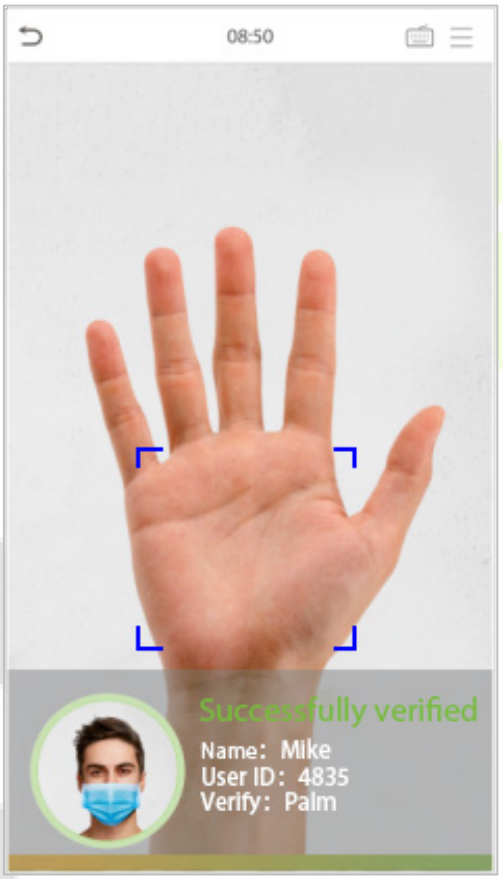
3,7 Modo de verificación

3.7.1 PalmVerification

- **1: N PalmVerificationmode**

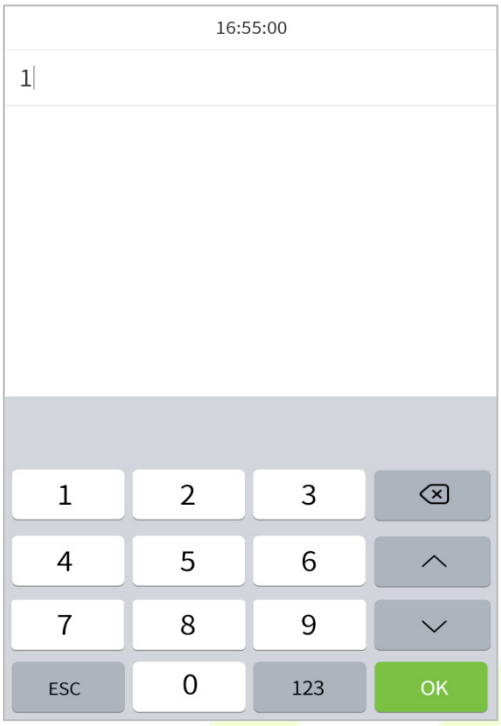
En este modo de verificación, el dispositivo compara la imagen de la palma recopilada por el colector de la palma con todos los datos de la palma en el dispositivo.

El dispositivo distingue automáticamente entre la palma y el modo de verificación facial cuando el usuario coloca su palma en el área de escaneo. Luego, el recolector de la palma recopila la imagen de la palma, y el dispositivo hace coincidir la imagen de la palma recopilada con toda la palma registrada y devuelve una salida.



- **Modo de verificación de palma 1: 1**

Haga clic en el en la pantalla principal para ingresar al modo de verificación de palma 1: 1 e ingresar el ID de usuario y presione [OK], como se muestra en la imagen siguiente.



Si el usuario ha registrado la huella digital, el rostro y la contraseña además de la palma de su mano, y el método de verificación está configurado como verificación de palma / huella digital / rostro / contraseña, aparecerá la siguiente pantalla. Seleccione el icono de la palma  para ingresar al modo de verificación de palma. Luego coloque su palma para verificación.

3.7.2 Verificación de huellas dactilares

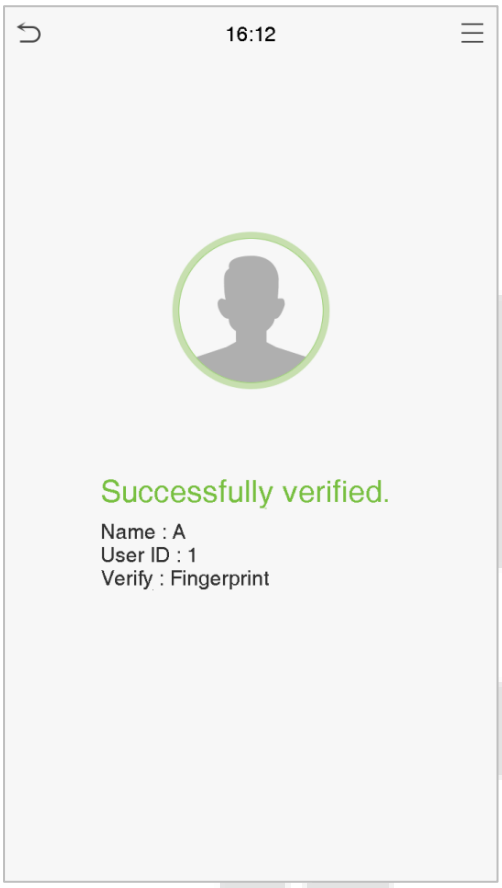
- **Modo de verificación de huellas dactilares 1: N**

En este modo de verificación, el dispositivo compara la huella dactilar que se está presionando en el lector de huellas dactilares con todos los datos de huellas dactilares que están almacenados en el dispositivo y devuelve una salida.

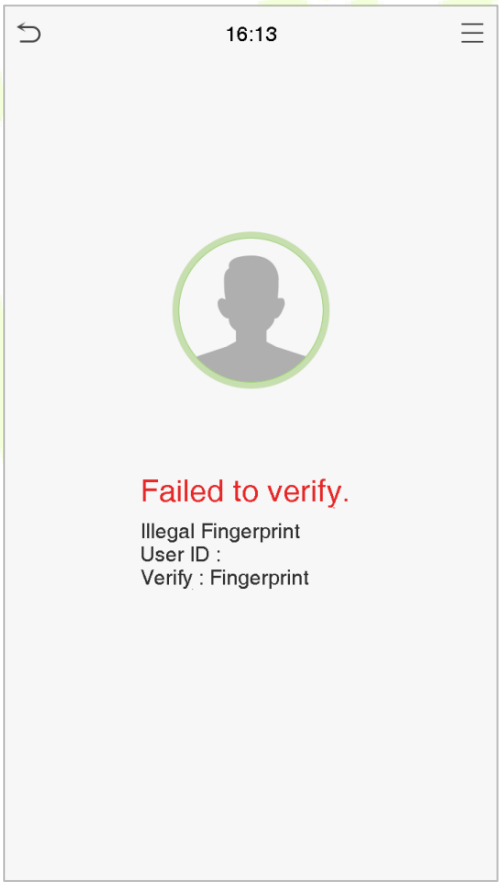
El dispositivo ingresa al modo de autenticación de huellas digitales cuando un usuario presiona su dedo sobre el escáner de huellas digitales.

NOTA : Siga la forma correcta de colocar el dedo en el sensor. Para obtener más información, consulte Posicionamiento de dedos

La verificación es exitosa.



Error de verificación.



- **Modo de verificación de huellas dactilares 1: 1**

En este modo, el dispositivo compara la huella dactilar que se está presionando en el lector de huellas dactilares con las huellas dactilares que están vinculadas a la entrada de ID de usuario a través del teclado virtual.

Los usuarios pueden intentar verificar sus identidades con el modo de verificación 1: 1 cuando no pueden obtener acceso con el método de autenticación 1: N.

Haga clic en el en la pantalla principal para ingresar al modo de verificación de huellas dactilares 1: 1 e ingresar el ID de usuario y presione [**OKAY].**

Si el usuario ha registrado palma, rostro y contraseña además de sus huellas dactilares, y el método de verificación está configurado como verificación de palma / huella dactilar / rostro / contraseña, aparecerá la siguiente pantalla. Seleccione el icono de huella digital

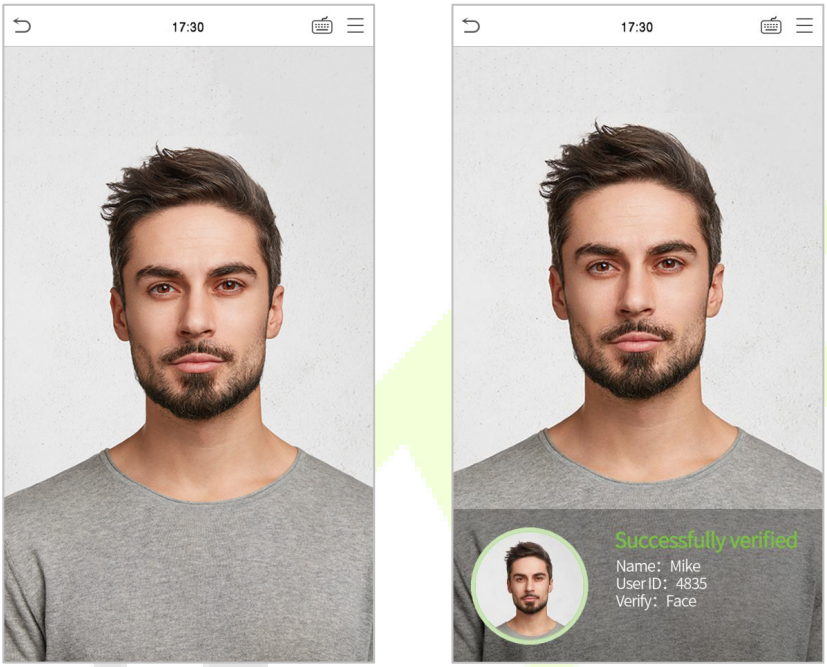
 para ingresar al modo de verificación de huellas digitales. Luego tome la huella digital presionando sobre el Lector de huellas dactilares para verificación.

3.7.3 Verificación facial

- **Verificación facial 1: N**

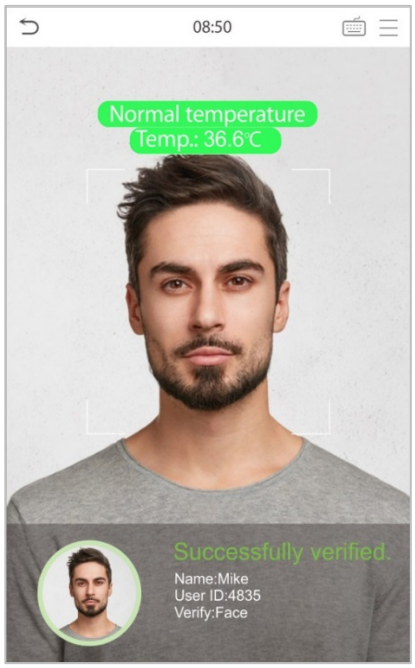
1. Verificación convencional

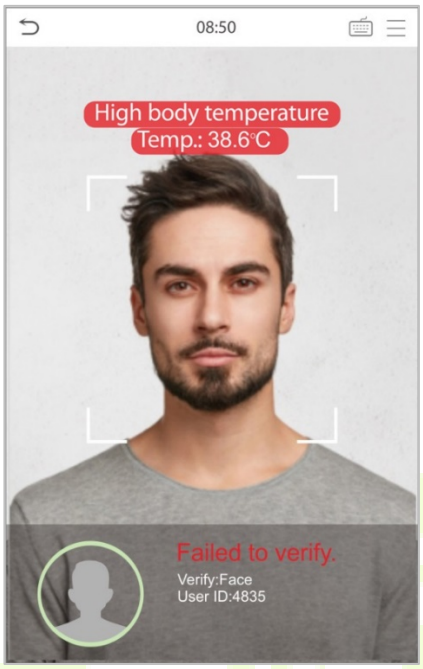
En este modo de verificación, el dispositivo compara las imágenes faciales recopiladas con todos los datos faciales registrados en el dispositivo. A continuación, se muestra el mensaje emergente de un resultado de comparación exitoso.



2. Habilitar la detección de temperatura con infrarrojos

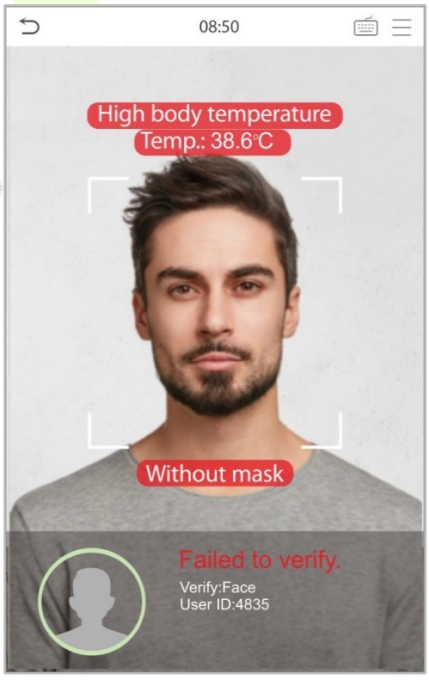
Cuando el usuario habilita **Habilite la detección de temperatura con infrarrojos** función, durante la verificación del usuario, además del método de verificación convencional, la cara del usuario debe estar alineada con el área de medición de temperatura para medir la temperatura corporal antes de que se pueda realizar la verificación. Las siguientes son las ventanas emergentes de la interfaz de solicitud de resultados de comparación. (Nota: esta función solo es aplicable a productos con módulo de medición de temperatura).





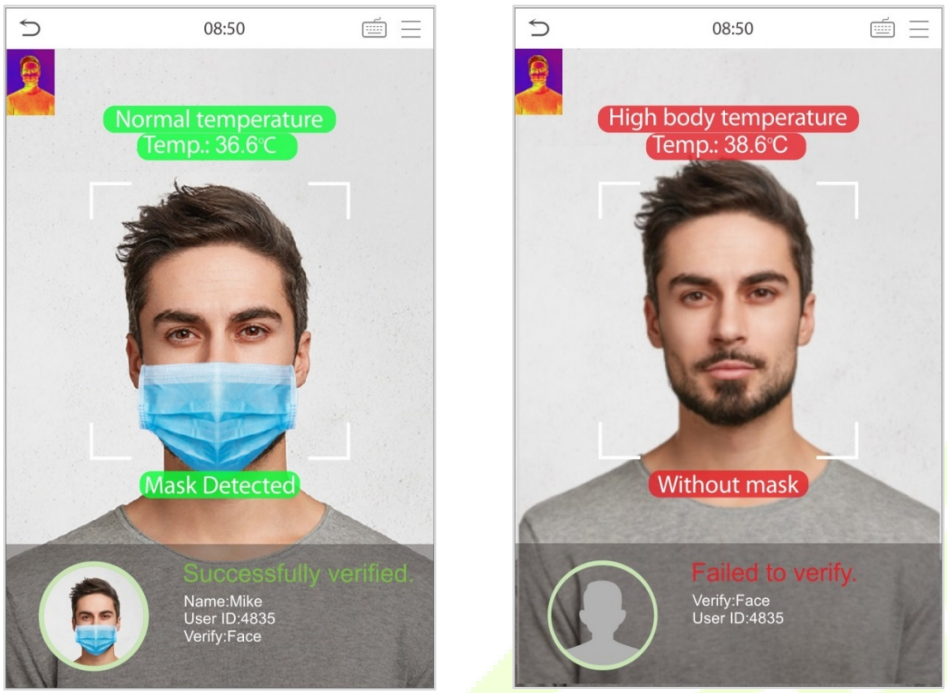
3. **Habilitar detección de máscara**

Cuando el usuario habilita **Habilitar la detección de máscara** función, el dispositivo identificará si el usuario está usando una máscara o no durante la verificación. Las siguientes son las ventanas emergentes de la interfaz de solicitud de resultados de comparación. (Nota: esta función solo es aplicable a productos con módulo de medición de temperatura).



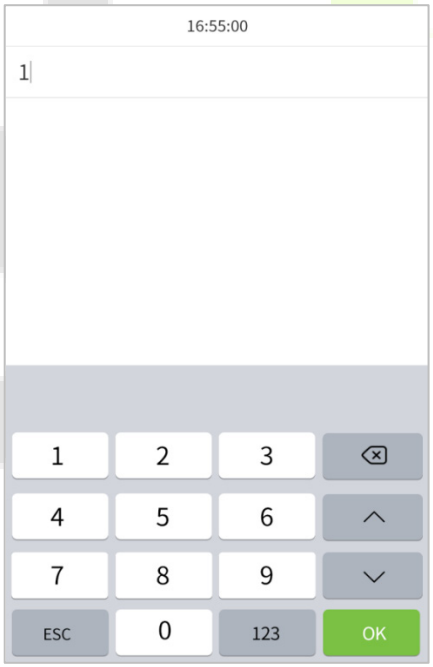
4. **Mostrar la figura de termodinámica**

Cuando el usuario habilita **Mostrar la figura de termodinámica** función, la imagen térmica de la persona se muestra en la esquina superior izquierda del dispositivo, durante la verificación. Como se muestra en las imágenes a continuación:



- **Verificación facial 1: 1**

En este modo de verificación, el dispositivo compara el rostro capturado por la cámara con la plantilla facial relacionada con el ID de usuario ingresado. prensa  en la interfaz principal e ingrese al modo de verificación facial 1: 1 e ingrese el ID de usuario y haga clic en [**OKAY].**



Si el usuario ha registrado la palma de la mano, la huella digital y la contraseña además de la cara, y el método de verificación está configurado como verificación de la palma de la mano / huella digital / cara / contraseña, aparecerá la siguiente pantalla. Seleccione el icono  para ingresar al modo de verificación facial.

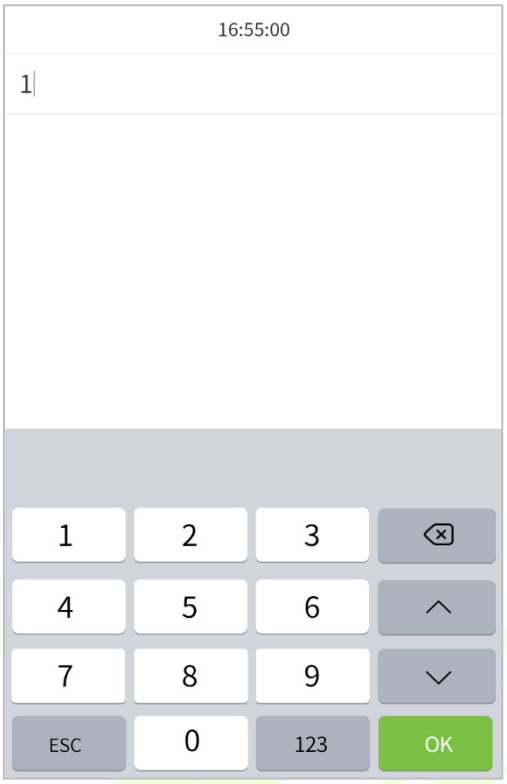
Después de una verificación exitosa, el cuadro de aviso muestra "Verificado exitosamente", como se muestra a continuación:

Si la verificación falla, aparecerá el mensaje "¡Por favor, ajuste su posición!".

3.7.4 Verificación de contraseña

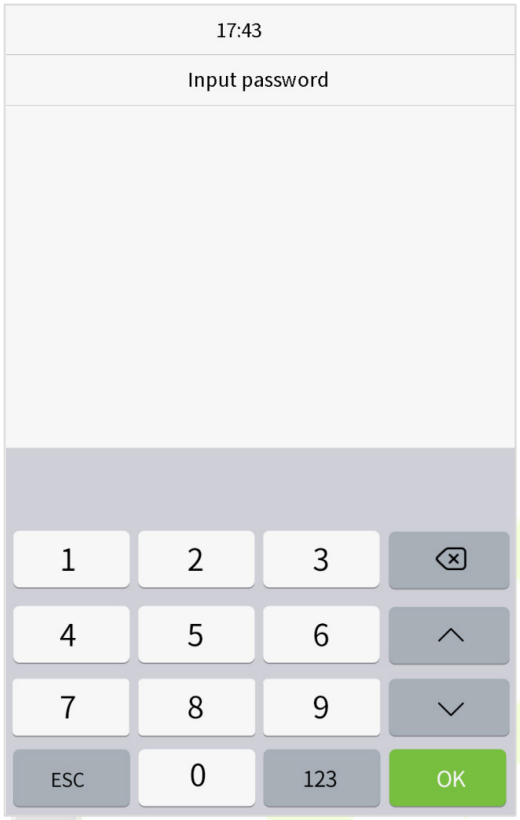
El dispositivo compara la contraseña ingresada con la contraseña registrada por el ID de usuario dado.

Haga clic en el en la pantalla principal para ingresar al modo de verificación de contraseña 1: 1. Luego, ingrese el usuario ID y presione [**OKAY].**



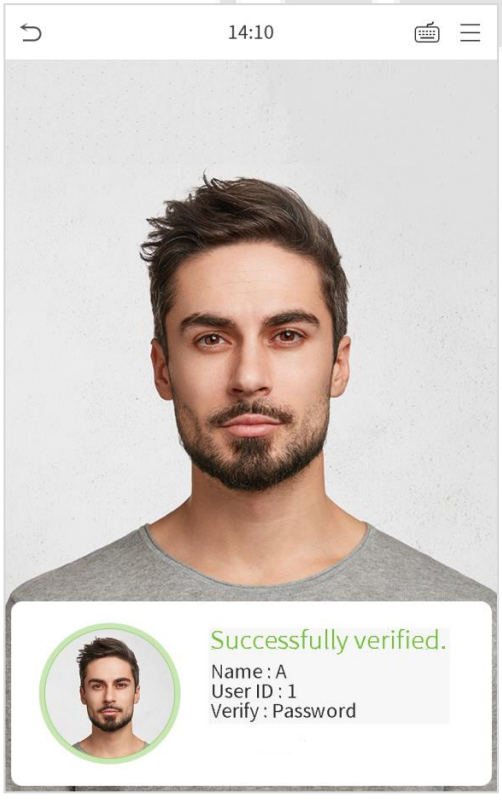
Si el usuario ha registrado la palma, la huella dactilar y el rostro además de la contraseña, y el método de verificación está configurado como verificación de palma / huella dactilar / rostro / contraseña, aparecerá la siguiente pantalla. Selecciona el icono para ingresar al modo de verificación de contraseña.

Ingrese la contraseña y presione [**OKAY].**

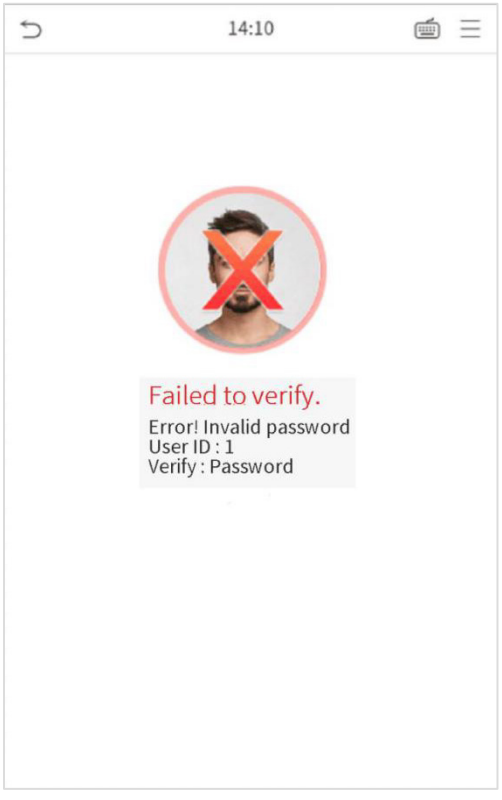


A continuación se muestra la pantalla de visualización después de ingresar una contraseña correcta y una contraseña incorrecta, respectivamente.

La verificación es exitosa:



Error de verificación:

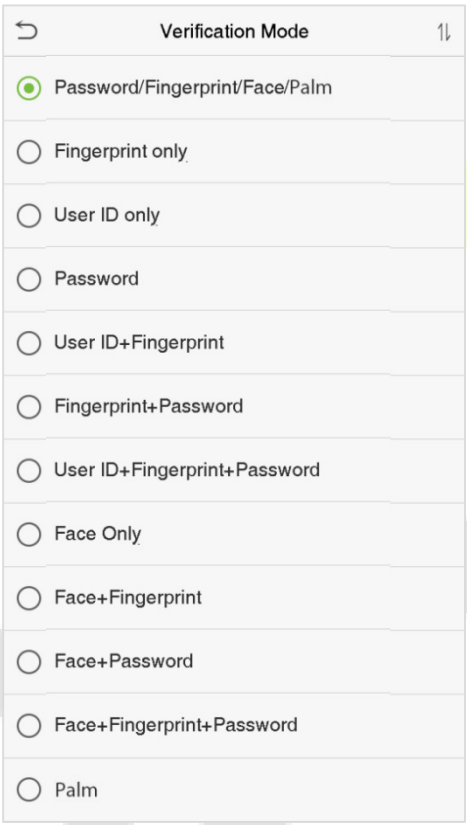


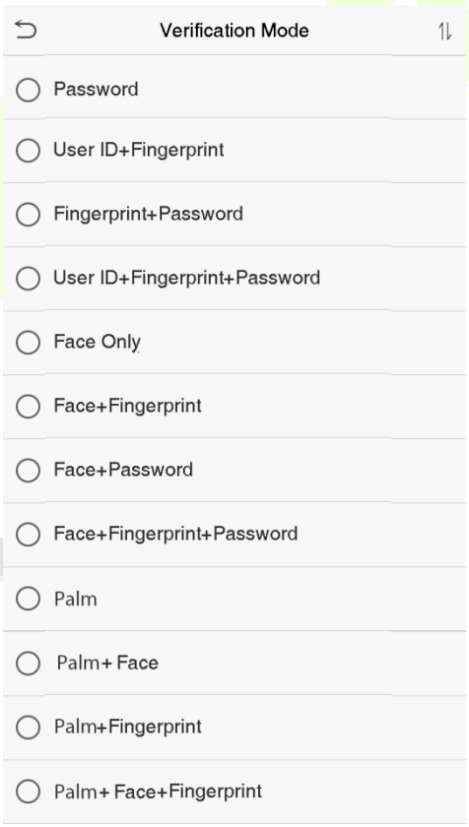
3.7.5 Verificación combinada

Para aumentar la seguridad, este dispositivo ofrece la opción de utilizar múltiples formas de métodos de verificación. Se pueden utilizar un total de 15 combinaciones de verificación diferentes, como se muestra a continuación:

Definición de símbolo de verificación combinada

Definición de símbolo		Explicación
/	o	Este método compara la verificación ingresada de una persona con la plantilla de verificación relacionada almacenada previamente con esa identificación de personal en el dispositivo.
+	y	Este método compara la verificación ingresada de una persona con toda la plantilla de verificación almacenada previamente con esa identificación de personal en el dispositivo.





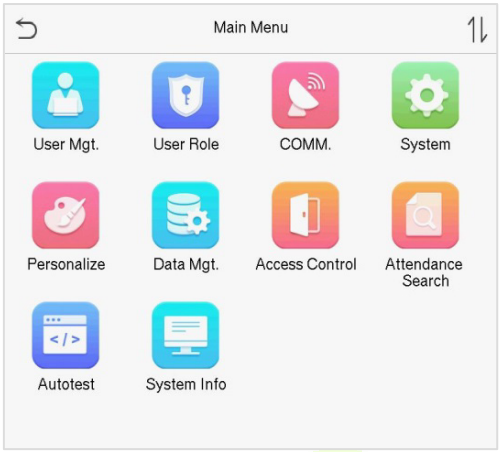
Procedimiento para configurar el modo de verificación combinado

- La verificación combinada requiere que el personal registre todos los diferentes métodos de verificación. De lo contrario, los empleados no podrán verificar con éxito el proceso de verificación combinado.
- Por ejemplo, cuando un empleado ha registrado solo los datos de la huella digital, pero el modo de verificación del dispositivo está configurado como "Huella digital + contraseña", el empleado no podrá completar el proceso de verificación con éxito.
- Esto se debe a que el Dispositivo compara la plantilla de huella digital escaneada de la persona con la plantilla de verificación registrada (tanto la Huella digital como la Contraseña) almacenada previamente con esa ID de personal en el Dispositivo.

- Pero como el empleado ha registrado solo la huella digital, pero no la contraseña, la verificación no se completará y el dispositivo muestra "Verificación fallida".

4 Menú principal

prensa en la interfaz Standby para ingresar al **Menú principal,** Se mostrará la siguiente pantalla:



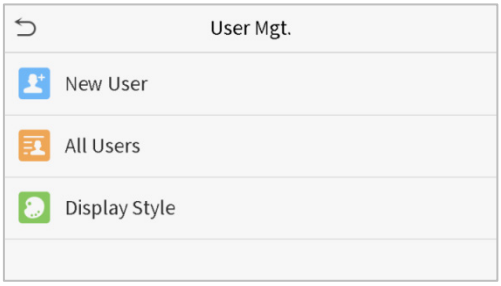
Función descriptiva

Menú	Descripciones
Administrador de usuarios	Para agregar, editar, ver y eliminar información básica de un usuario.
Rol del usuario	Para establecer el alcance de permisos del rol personalizado y el registrador para los usuarios, es decir, los derechos para operar el sistema.
COMM.	Para configurar los parámetros relevantes de Red, Comunicación en Serie, Conexión de PC, Red Inalámbrica, Servidor en la Nube y Wiegand.
Sistema	Para configurar los parámetros relacionados con el sistema, incluida la fecha y la hora, la configuración de registros de acceso, los parámetros de rostro, huella digital y palma, restablecimiento de la configuración de fábrica y administración de detección.
Personalizar	Esto incluye la interfaz de usuario, voz, horarios de timbre, opciones de estado de perforación y configuraciones de asignaciones de teclas de acceso directo.
DataMgt.	Para eliminar todos los datos relevantes en el dispositivo.
Control de acceso	Para configurar los parámetros de la cerradura y el dispositivo de control de acceso relevante, incluidas opciones como Programación de tiempo, Configuración de vacaciones, Verificación combinada, Configuración de anti-passback y Configuración de opciones de coacción.
Asistencia Buscar	Para consultar el registro de asistencia especificado, marque Fotos de asistencia y Fotos de asistencia de la lista de bloqueo.
Auto prueba	Para probar automáticamente si cada módulo funciona correctamente, incluida la pantalla LCD, el audio, la cámara, el sensor de huellas dactilares y el reloj en tiempo real.
Información del sistema	Para ver la capacidad de datos y la información del dispositivo y firmware del dispositivo actual.

5 Gestión de usuarios

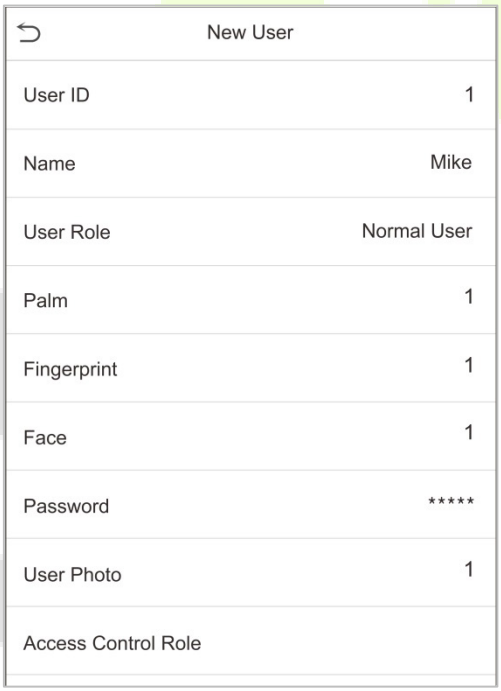
5.1 registro de usuario

Hacer clic **Administrador de usuarios** en el menú principal.



5.1.1 ID de usuario y nombre

Grifo **Nuevo Usuario.** Introducir el **ID de usuario** y **Nombre.**



Notas:

1) Un nombre puede tener hasta 17 caracteres.

2) El ID de usuario puede contener de 1 a 9 dígitos de forma predeterminada.

3) Durante el registro inicial, puede modificar su ID, que no se puede modificar después del registro.

4) Si un mensaje " **¡Duplicado! "** aparece, debe elegir otro ID ya que el ID de usuario ingresado ya existe.

5.1.2 Rol del usuario

En la interfaz de nuevo usuario, toque **Rol del usuario** para establecer el rol del usuario como **Usuario normal** o **súper Administración.**

- **Superadministrador:** El superadministrador posee todos los privilegios de administración en el dispositivo.
- **Usuario normal:** Si el superadministrador ya está registrado en el dispositivo, los usuarios normales no tendrán los privilegios para administrar el sistema y solo podrán acceder a las verificaciones de autenticación.
- **Roles definidos por el usuario:** El usuario normal también se puede configurar con **Rol definido por el usuario** que son los roles personalizados que se pueden configurar para el usuario normal.

Nota: Si el rol de usuario seleccionado es el superadministrador, el usuario debe pasar la autenticación de identidad para acceder al menú principal. La autenticación se basa en los métodos de autenticación que ha registrado el superadministrador. Por favor refiérase a 3.7 Método de verificación.

5.1.3 Palma

Grifo **Palma** en el **Nuevo Usuario** interfaz para ingresar a la página de registro de la palma de la mano.

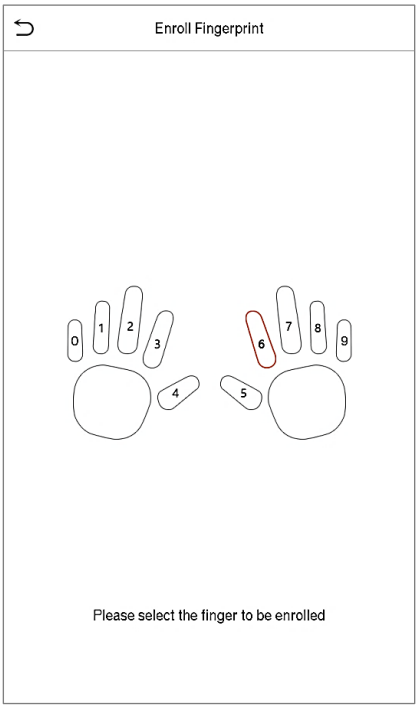
- Seleccione la palma que desea inscribir.
- Coloque la palma de la mano dentro de la caja guía y manténgala quieta mientras se registra. Aparece una barra de progreso al registrar la
- palma y un **"Inscrito correctamente"** se muestra cuando la barra de progreso se completa.

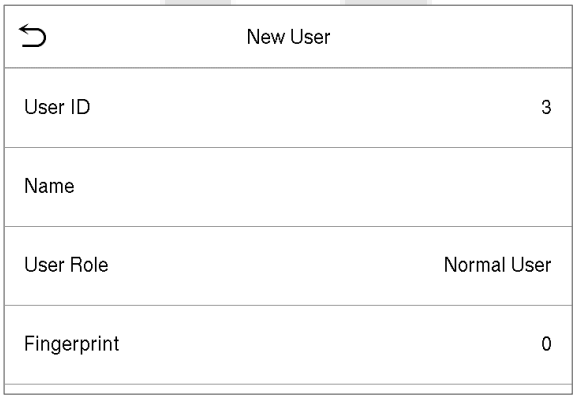
- Si la palma ya está registrada, la **"Palma duplicada"** aparece el mensaje. La interfaz de registro es la siguiente:

5.1.4 Huella dactilar

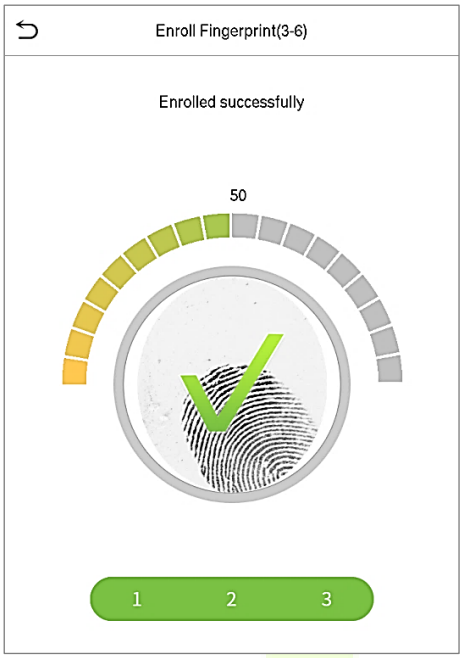
Sobre el **Nuevo Usuario** interfaz, toque en **Huella dactilar** para ir a la página de registro de huellas digitales.

- Sobre el **Inscribir huella digital** interfaz, seleccione el dedo a registrar.





- Después de seleccionar el dedo requerido, presione el mismo dedo en el lector de huellas dactilares tres veces.
- El verde indica que la huella digital se registró correctamente.



5.1.5 Cara

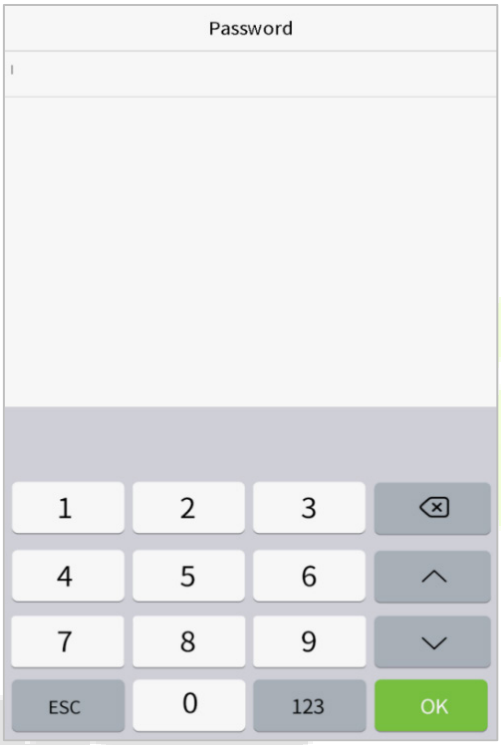
Grifo **Cara** en el **Nuevo Usuario** interfaz para ingresar a la página de registro facial.

- Mire hacia la cámara y coloque su rostro dentro de la caja guía blanca y permanezca quieto durante el registro facial.
- Aparece una barra de progreso al registrar la cara y un **"Inscrito correctamente"** se muestra cuando la barra de progreso se completa.
- Si el rostro ya está registrado, **"Cara duplicada"** aparece el mensaje. La interfaz de registro es la siguiente:

5.1.6 Contraseña

Grifo **Contraseña** en el **Nuevo Usuario** interfaz para ingresar a la página de registro de contraseña.

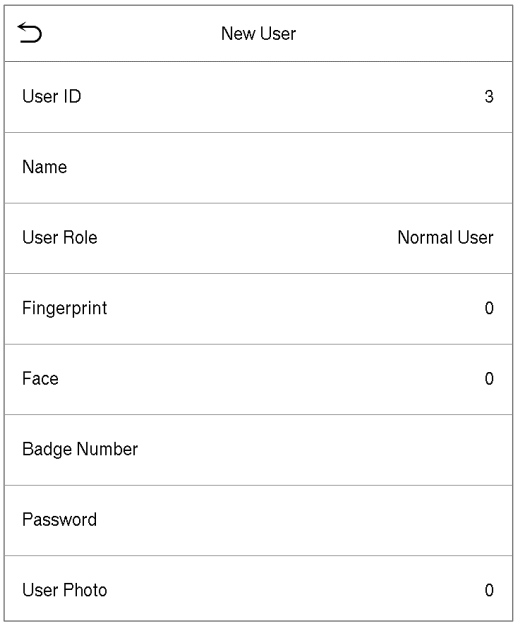
- En la interfaz de Contraseña, ingrese la contraseña requerida y vuelva a ingresar para confirmarla y toque **OKAY.**
- Si la contraseña reingresada es diferente de la contraseña ingresada inicialmente, entonces el dispositivo muestra el mensaje como " **¡La contraseña no coincide!",** donde el usuario necesita volver a confirmar la contraseña nuevamente.



Nota: La contraseña puede contener de 1 a 8 dígitos por defecto.

5.1.7 Foto de usuario

Toque en **Foto de usuario** en el **Nuevo Usuario** interfaz para ir a la página de registro de fotos de usuario.



- Cuando un usuario registrado con una foto pasa la autenticación, se mostrará la foto registrada.

- Grifo **Foto de usuario,** la cámara del dispositivo se abrirá, luego toque el ícono de la cámara para tomar una foto. La foto capturada se muestra en la esquina superior izquierda de la pantalla y la cámara se abre nuevamente para tomar una nueva foto, después de tomar la foto inicial.

Nota: Al registrar un rostro, el sistema captura automáticamente una imagen como foto de usuario. Si no registra una foto de usuario, el sistema configura automáticamente la imagen capturada durante el registro como la foto predeterminada.

5.1.8 Rol de control de acceso

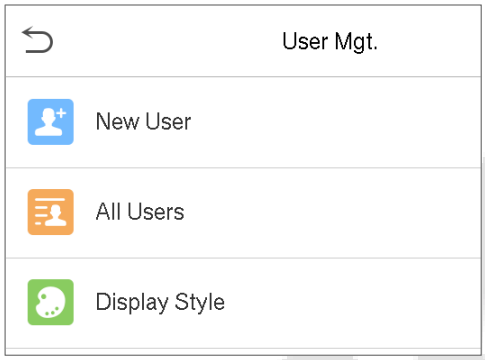
los **Rol de control de acceso** establece el privilegio de acceso a la puerta para cada usuario. Esto incluye el grupo de acceso, el modo de verificación, el privilegio de huellas digitales y también facilita la configuración del período de tiempo de acceso del grupo.

- Grifo **Función de control de acceso> Grupo de acceso,** asignar a los usuarios registrados a diferentes grupos para una mejor gestión. Los nuevos usuarios pertenecen al Grupo 1 de forma predeterminada y se pueden reasignar a otros grupos. El dispositivo admite hasta 99 grupos de control de acceso.
- Grifo **Periodo de tiempo,** para seleccionar el período de tiempo a utilizar.

5.2 Buscar usuarios

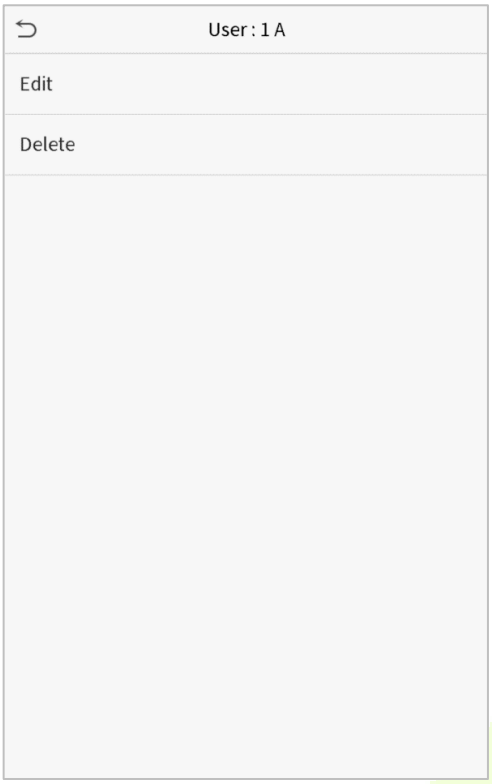
Sobre el **Menú principal,** grifo **Gestión de usuarios,** y luego toque **Todos los usuarios** para buscar un usuario.

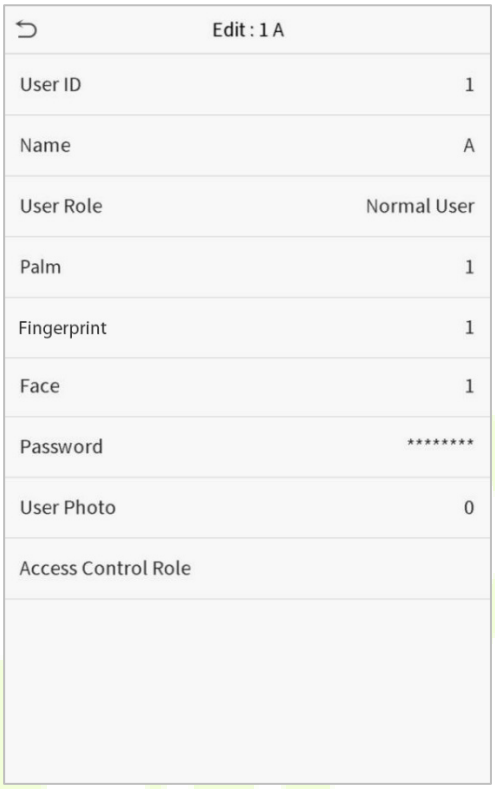
- Sobre el **Todos los usuarios** interfaz, toque en la barra de búsqueda en la lista del usuario para ingresar la palabra clave de recuperación requerida (donde la palabra clave puede ser el ID de usuario, apellido o nombre completo) y el sistema buscará la información de usuario relacionada.



5.3 editar usuario

En **Todos los usuarios** interfaz, toque el usuario requerido de la lista y toque **Editar** para editar la información del usuario.





NOTA : El proceso de editar la información del usuario es el mismo que el de agregar un nuevo usuario, excepto que el ID de usuario no se puede modificar al editar un usuario. El proceso en detalle se refiere a " 5.1 Gestión de usuarios ".

5.4 Borrar usuario

En **Todos los usuarios** interfaz, toque el usuario requerido de la lista y toque **Eliminar** para eliminar el usuario o la información de un usuario específico del dispositivo. Sobre el **Eliminar** interfaz, toque la operación requerida y luego toque OK para confirmar la eliminación.

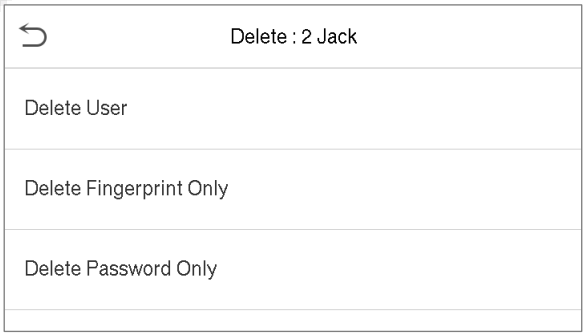
Eliminar operaciones

Borrar usuario: Elimina toda la información del usuario (elimina el usuario seleccionado como un todo) del dispositivo.

Eliminar solo huella digital: Elimina la información de la huella digital del usuario seleccionado.

Eliminar contraseña solamente: Elimina la información de la contraseña del usuario seleccionado.

Eliminar solo rostro: Elimina la información de la cara del usuario seleccionado.

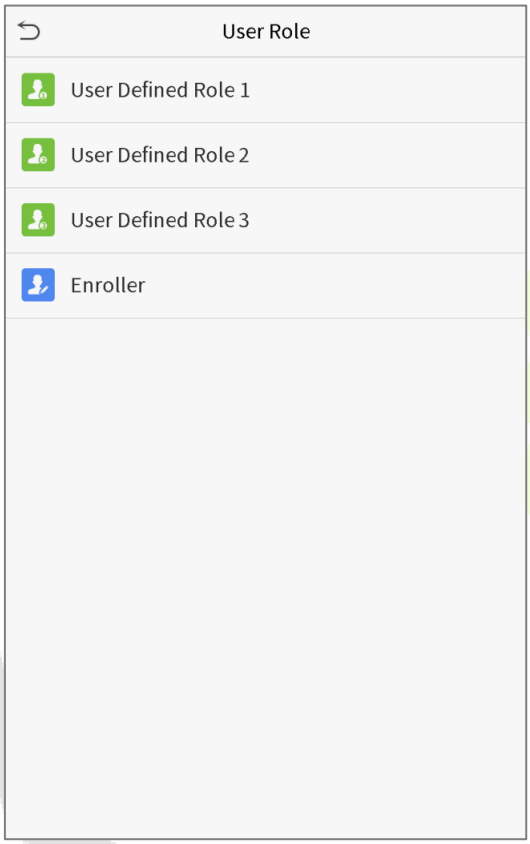


6 Rol del usuario

Rol del usuario facilita la asignación de algunos permisos específicos a determinados usuarios, según el requisito.

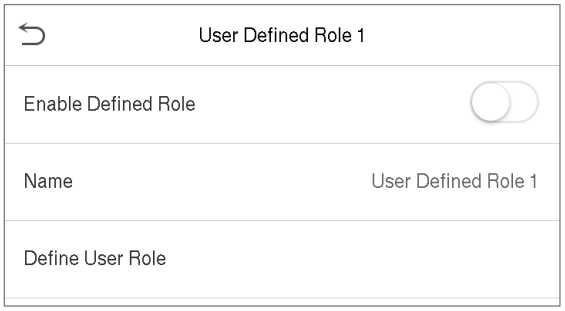
- Sobre el **Principal** menú, toque **Rol del usuario,** y luego toque en el **Rol definido por el usuario** para establecer los permisos definidos por el usuario.

- El alcance del permiso del rol personalizado se puede configurar hasta en 3 roles, es decir, el alcance operativo personalizado de las funciones del menú del usuario.



- Sobre el **Rol definido por el usuario** interfaz, alternar **Habilitar rol definido** para habilitar o deshabilitar el rol definido por el usuario.

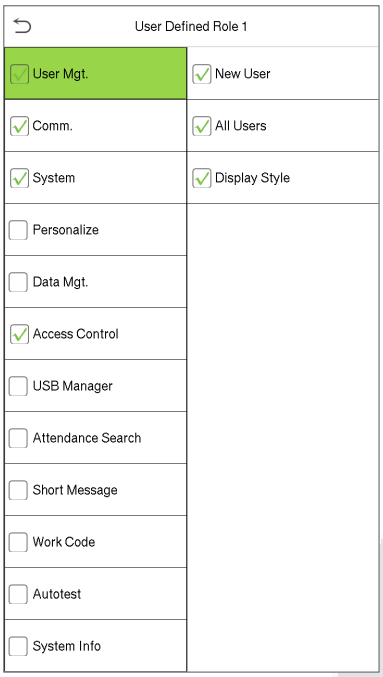
- Toque en **Nombre** e ingrese el nombre personalizado del rol.

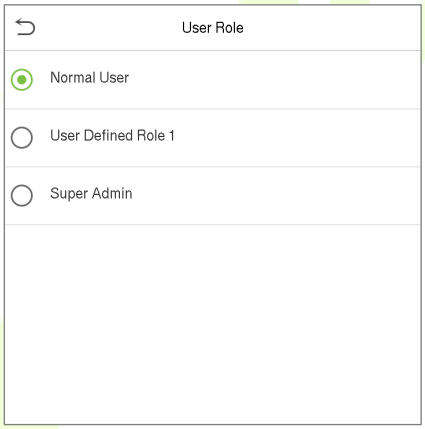


- Luego, toca **Definir rol de usuario** y seleccione los privilegios necesarios para asignar a la nueva función, y luego toque el **Regreso** botón.

- Durante la asignación de privilegios, los nombres de las funciones del menú principal se mostrarán a la izquierda y sus submenús se enumerarán a la derecha.

- Primero toque en el requerido **Menú principal** nombre de la función y, a continuación, seleccione los submenús necesarios de la lista.

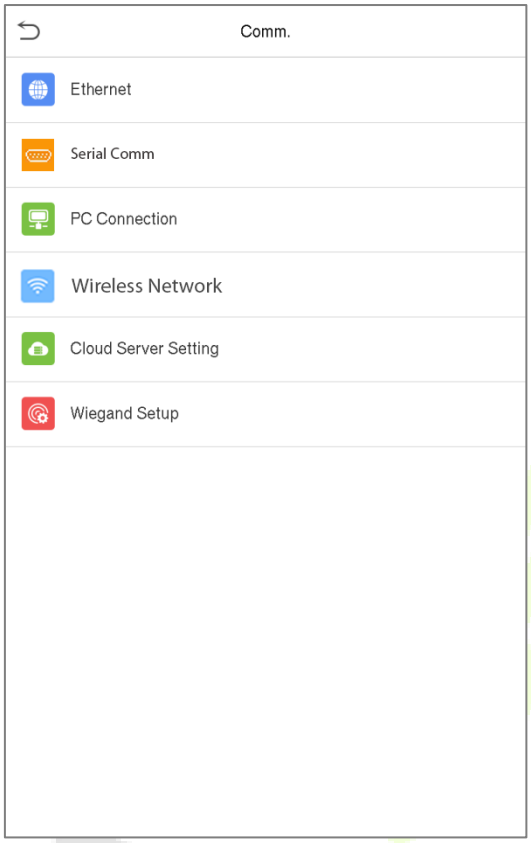




Nota: Si el rol de usuario está habilitado para el dispositivo, toque en **Administrador de usuarios > NewUser> Rol de usuario** para asignar los roles creados a los usuarios requeridos. Pero si no hay un superadministrador registrado en el dispositivo, el dispositivo le preguntará "¡Primero inscriba al superadministrador!" al habilitar la función de rol de usuario.

7 Configuración de comunicación

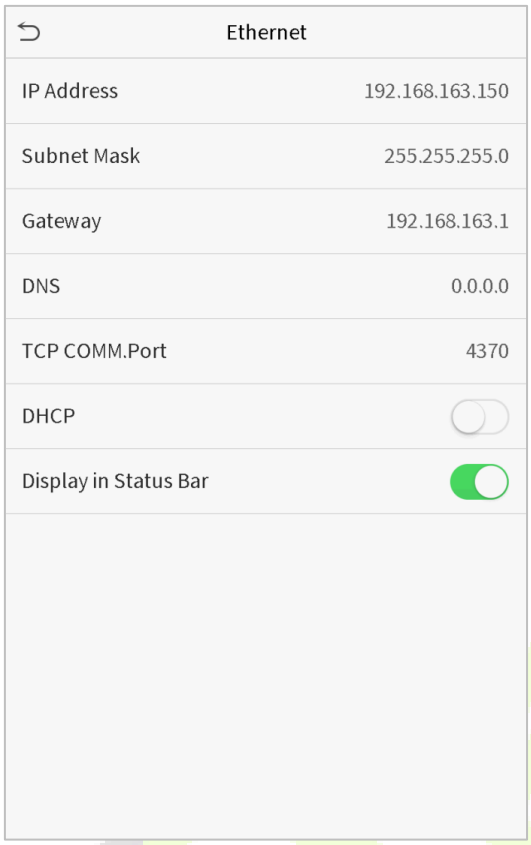
Grifo **COMM.** sobre el **Menú principal** para configurar la conexión Ethernet de la PC, la configuración de CloudServer y Wiegand.



7.1 Configuración de la red

Cuando el dispositivo necesita comunicarse con una PC a través de Ethernet, debe configurar los ajustes de red y asegurarse de que el dispositivo y la PC se conecten al mismo segmento de red.

Grifo **Ethernet** sobre el **Comm.** Interfaz de configuración para configurar los ajustes.



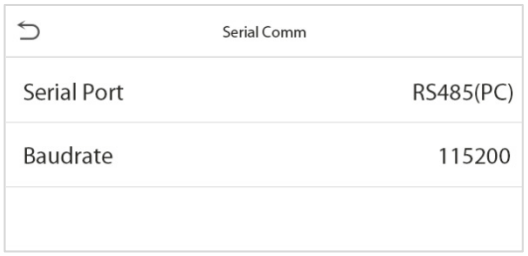
Función descriptiva

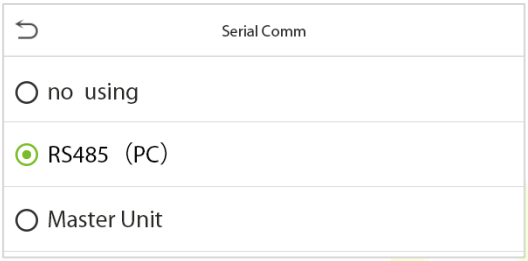
Nombre de la función	Descripciones
Dirección IP	La dirección IP predeterminada es 192.168.1.201. Puede modificarse según la disponibilidad de la red.
Máscara de subred	La máscara de subred predeterminada es 255.255.255.0. Puede modificarse según la disponibilidad de la red.
Puerta	La dirección de puerta de enlace predeterminada es 0.0.0.0. Puede modificarse según la disponibilidad de la red.
DNS	La dirección DNS predeterminada es 0.0.0.0. Puede modificarse según la disponibilidad de la red.
TCP COMM. Puerto	El valor predeterminado del puerto TCP COMM es 4370. Se puede modificar según la disponibilidad de la red.
DHCP	El Protocolo de configuración dinámica de host consiste en asignar direcciones IP de forma dinámica a los clientes a través del servidor.
Mostrar en la barra de estado	Alternar para establecer si se muestra el icono de red en la barra de estado.

7.2 Comunicaciones en serie

La función Serial Comm facilita el establecimiento de comunicación con el dispositivo a través de un puerto serie (/ RS485 / Master Unit).

Grifo **Comunicaciones en serie** sobre el **Comm.** Interfaz de configuración.





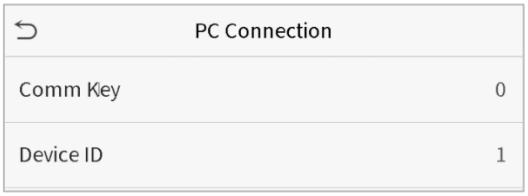
Función descriptiva

Nombre de la función	Descripciones
Puerto serial	**Inhabilitar:** No se comunique con el dispositivo a través del puerto serie. **RS485 (PC):** Se comunica con el dispositivo a través del puerto serie RS485. **Unidad maestra:** Cuando RS485 se utiliza como función de " **Unidad maestra** ", El dispositivo actuará como una unidad maestra y se puede conectar al lector de tarjetas y huellas dactilares RS485.
Tasa de baudios	La velocidad a la que se comunican los datos con la PC, hay 4 opciones de velocidad en baudios: 115200 (predeterminado), 57600, 38400 y 19200. Cuanto mayor es la velocidad en baudios, más rápida es la velocidad de comunicación, pero también menos confiable. Por tanto, se puede utilizar una velocidad en baudios más alta cuando la distancia de comunicación es corta; cuando la distancia de comunicación es larga, elegir una velocidad de transmisión más baja sería más confiable.

7.3 Conexión a PC

Comm Key facilita mejorar la seguridad de los datos configurando la comunicación entre el dispositivo y la PC. Una vez configurada la clave de comunicación, se debe proporcionar su contraseña de conexión antes de que el dispositivo se conecte al software de la PC.

Grifo **Conexión a PC** sobre el **Comm.** Interfaz de configuración para configurar los ajustes de comunicación.



Función descriptiva

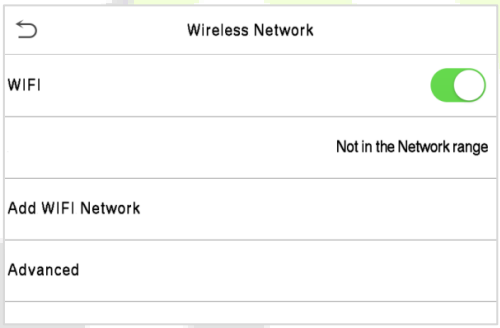
Nombre de la función	Descripciones
CommKey	La contraseña predeterminada es 0, que se puede cambiar. La clave de comunicación puede contener de 1 a 6 dígitos.
Identificación del dispositivo	Número de identidad del dispositivo, que oscila entre 1 y 254. Si el método de comunicación es RS232 / RS485, debe ingresar este ID de dispositivo en la interfaz de comunicación del software.

7.4 Red inalámbrica

El dispositivo proporciona un módulo Wi-Fi, que puede integrarse en el molde del dispositivo o conectarse externamente.

El módulo Wi-Fi permite la transmisión de datos a través de Wi-Fi (Wireless Fidelity) y establece un entorno de red inalámbrica. El Wi-Fi está habilitado de forma predeterminada en el dispositivo. Si no necesita usar la red Wi-Fi, puede alternar el botón Wi-Fi para deshabilitar.

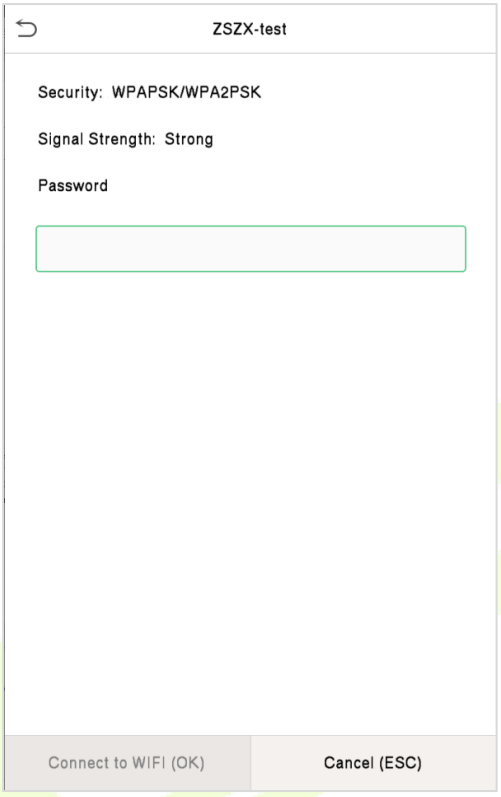
Grifo **Red inalámbrica** sobre el **Comm.** Interfaz de configuración para configurar los ajustes de WiFi.



Buscar en la red wifi

- WIFI está habilitado en el dispositivo de forma predeterminada. Activar  para habilitar o deshabilitar WIFI.
- Una vez que el Wi-Fi está encendido, el dispositivo buscará el WIFI disponible dentro del rango de la red.
- Toque el nombre de WiFi apropiado de la lista disponible, ingrese la contraseña correcta en la interfaz de contraseña y luego toque **Conéctese a WIFI (OK).**

Wi-Fi habilitado: Toque la red requerida de la lista de redes buscadas.

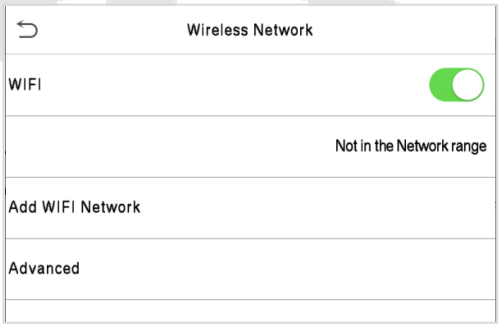


Toque en el campo de contraseña para ingresar la contraseña y luego toque en **Conectar a WIFI (OK).**

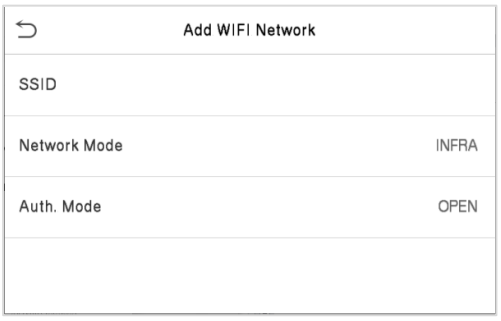
- Cuando el WIFI se conecta correctamente, la interfaz inicial mostrará el Wi-Fi logo.

Agregar red WIFI manualmente

El WIFI también se puede agregar manualmente si el WIFI requerido no se muestra en la lista.



Toque en **Agregar red WIFI** para agregar el WIFI manualmente.

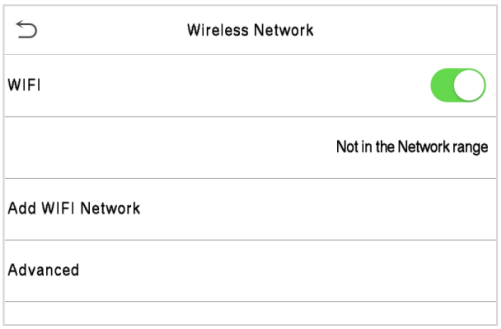


En esta interfaz, ingrese los parámetros de la red WIFI. (La red agregada debe

NOTA : Después de agregar con éxito el WIFI manualmente, siga el mismo proceso para buscar el nombre WIFI agregado. Hacer clic aquí para ver el proceso de búsqueda de la red WIFI.

Configuración avanzada

Sobre el **Red inalámbrica** interfaz, toque en **Avanzado** para configurar los parámetros relevantes según sea necesario.

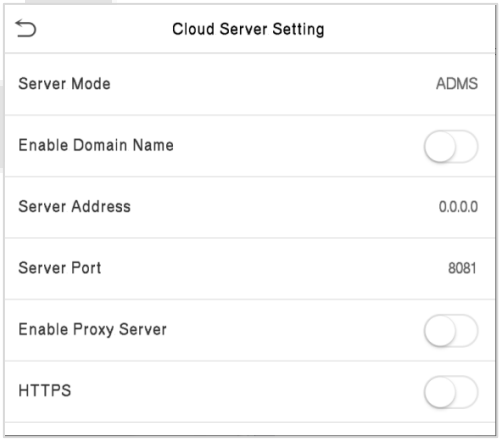


Función descriptiva

Nombre de la función	Descripción
DHCP	El Protocolo de configuración dinámica de host (DHCP) asigna de forma dinámica direcciones IP a los clientes de la red. Si el DHCP está habilitado, la IP no se puede configurar manualmente.
Dirección IP	Dirección IP para la red WIFI, la predeterminada es 0.0.0.0. Puede modificarse según la disponibilidad de la red.
Máscara de subred	La máscara de subred predeterminada de la red WIFI es 255.255.255.0. Puede modificarse según la disponibilidad de la red.
Puerta	La dirección de puerta de enlace predeterminada es 0.0.0.0. Puede modificarse según la disponibilidad de la red.

7.5 Configuración del servidor en la nube

Grifo **Configuración del servidor en la nube** sobre el **Comm.** Interfaz de configuración para conectarse con el servidor ADMS.

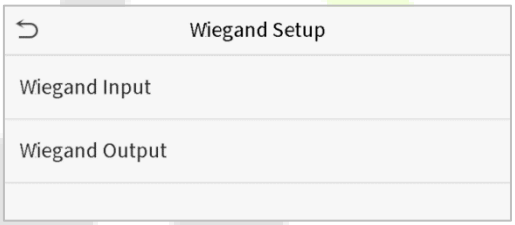


Función descriptiva

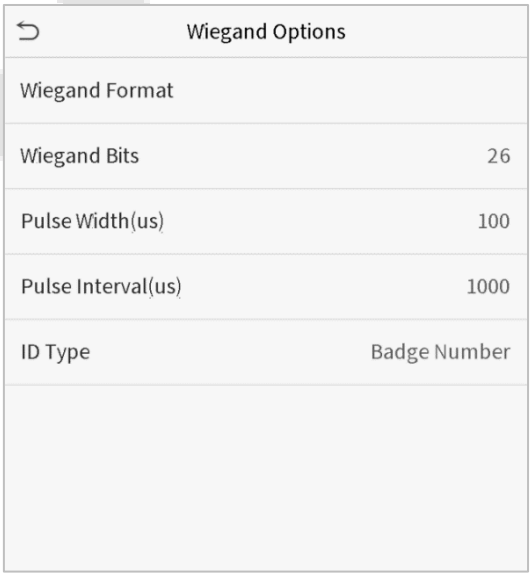
Nombre de la función		Descripción
Habilitar Dominio Nombre	**Dirección del servidor**	Una vez que esta función está habilitada, se utilizará el modo de nombre de dominio "http: // ...", como http://www.XYZ.com, mientras que "XYZ" denota el nombre de dominio (cuando se activa este modo **EN).**
Inhabilitar Dominio Nombre	**Dirección del servidor**	Dirección IP del servidor ADMS. Puerto
	Puerto de servicio	utilizado por el servidor ADMS.
Habilitar servidor proxy		Cuando elige habilitar el proxy, debe configurar la dirección IP y el número de puerto del servidor proxy.
HTTPS		Basado en HTTP, el cifrado de transmisión y la autenticación de identidad garantizan la seguridad del proceso de transmisión.

7,6 Configuración de Wiegand

Para configurar los parámetros de entrada y salida de Wiegand. Grifo **Configuración de Wiegand** sobre el **Comm.** Interfaz de configuración para configurar los parámetros de entrada y salida Wiegand.



7.6.1 Entrada Wiegand



Función descriptiva

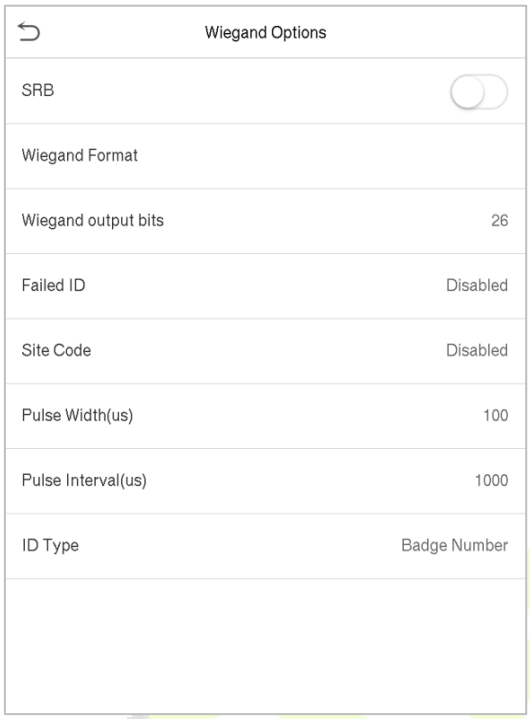
Nombre de la función	Descripciones
Formato Wiegand	Los valores oscilan entre 26 bits, 34 bits, 36 bits, 37 bits y 50 bits. Número de bits de
Bits de Wiegand	datos Wiegand.
PulseWidth (nosotros)	El valor del ancho de pulso enviado por Wiegand es 100 microsegundos por defecto, que se puede ajustar dentro del rango de 20 a 100 microsegundos.
Legumbres Intervalo (nosotros)	El valor predeterminado es 1000 microsegundos, que se puede ajustar dentro del rango de 200 a 20000 microsegundos.
tipo de identificación	Seleccione entre ID de usuario y número de tarjeta.

Varias descripciones del formato CommonWiegand:

Formato Wiegand	Descripción
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El 1 S t bit es el bit de paridad par del 2 Dakota del Norte a 13 th bits, mientras que los 26 th bit es el bit de paridad impar del 14 th hasta 25 th bits. El 2 Dakota del Norte hasta 25 th los bits son los números de las tarjetas.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El 1 S t bit es el bit de paridad par del 2 Dakota del Norte a 13 th bits, mientras que los 26 th bit es el bit de paridad impar del 14 th hasta 25 th bits. El 2 Dakota del Norte al 9 th bits son los códigos de sitio, mientras que los 10 th hasta 25 th los bits son los números de las tarjetas.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El 1 S t bit es el bit de paridad par del 2 Dakota del Norte hasta 17 th bits, mientras que el 34 th bit es el bit de paridad impar del 18 th hasta 33 rd bits. El 2 Dakota del Norte hasta 25 th los bits son los números de las tarjetas.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El 1 S t bit es el bit de paridad par del 2 Dakota del Norte hasta 17 th bits, mientras que el 34 th bit es el bit de paridad impar del 18 th hasta 33 rd bits. El 2 Dakota del Norte al 9 th bits son los códigos de sitio, mientras que los 10 th hasta 25 th los bits son los números de las tarjetas.
Wiegand36	APAGADOFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El 1 S t bit es el bit de paridad impar del 2 Dakota del Norte hasta 18 th bits, mientras que los 36 th bit es el bit de paridad par del 19 th hasta 35 th bits. El 2 Dakota del Norte hasta 17 th los bits son los códigos de dispositivo. El 18 th hasta 33 rd los bits son los números de la tarjeta, y los 34 th hasta 35 th los bits son los códigos del fabricante.

Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consta de 36 bits de código binario. El 1 S t bit es el bit de paridad par del 2 Dakota del Norte hasta 18 th bits, mientras que los 36 th bit es el bit de paridad impar del 19 th hasta 35 th bits. El 2 Dakota del Norte al 19 th bits son los códigos de dispositivo y los 20 th hasta 35 th los bits son los números de las tarjetas.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCE Consta de 37 bits de código binario. El 1 S t bit es el bit de paridad impar del 2 Dakota del Norte hasta 18 th bits, mientras que el 37 th bit es el bit de paridad par del 19 th hasta 36 th bits. El 2 Dakota del Norte para 4 th los bits son los códigos del fabricante. El 5 th hasta 16 th bits son los códigos de sitio, y los 21 S t hasta 36 th los bits son los números de las tarjetas.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consta de 37 bits de código binario. El 1 S t bit es el bit de paridad par del 2 Dakota del Norte hasta 18 th bits, mientras que el 37 th bit es el bit de paridad impar del 19 th hasta 36 th bits. El 2 Dakota del Norte para 4 th los bits son los códigos del fabricante. El 5 th hasta 14 th los bits son los códigos de dispositivo, y 15 th hasta 20 th bits son los códigos de sitio, y los 21 S t hasta 36 th los bits son los números de las tarjetas.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 50 bits de código binario. El 1 S t bit es el bit de paridad par del 2 Dakota del Norte hasta 25 th bits, mientras que los 50 th bit es el bit de paridad impar del 26 th hasta 49 th bits. El 2 Dakota del Norte hasta 17 th bits son los códigos de sitio, y los 18 th hasta 49 th los bits son los números de las tarjetas.
"C" denota el número de tarjeta; **"MI"** denota el bit de paridad par; **"O"** denota el bit de paridad impar; **"F"** denota el código de la instalación; **"METRO"** denota el código del fabricante; **"PAG"** denota el bit de paridad; y **"S"** denota el código del sitio.	

7.6.2 Salida Wiegand



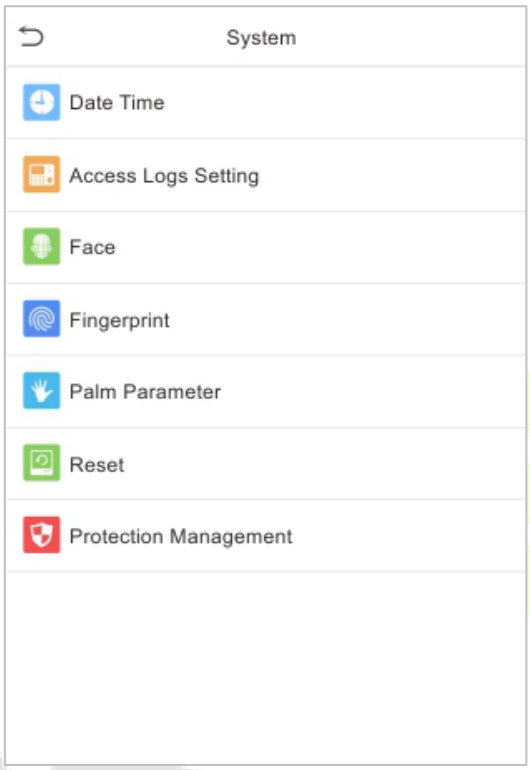
Función descriptiva

Nombre de la función	Descripciones
SRB	Cuando SRB está habilitado, el bloqueo es controlado por el SRB para evitar que se abra debido a la extracción del dispositivo.
Formato Wiegand	Los valores oscilan entre 26 bits, 34 bits, 36 bits, 37 bits y 50 bits.
Bits de salida Wiegand	Después de seleccionar el formato Wiegand requerido, seleccione los dígitos de bits de salida correspondientes del formato Wiegand.
Identificación fallida	Si la verificación falla, el sistema enviará el ID fallido al dispositivo y reemplazará el número de tarjeta o el ID de personal con el nuevo.
Código del sitio	Es similar al ID del dispositivo. La diferencia es que un código de sitio se puede configurar manualmente y es repetible en un dispositivo diferente. El valor válido varía de 0 a 256 de forma predeterminada.
PulseWidth (nosotros)	El ancho de tiempo representa los cambios de la cantidad de carga eléctrica con capacitancia regular de alta frecuencia dentro de un tiempo especificado.
Intervalo de pulso (nosotros)	El intervalo de tiempo entre pulsos.
tipo de identificación	Seleccione los tipos de ID como ID de usuario o número de tarjeta.

8 Ajustes del sistema

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

Grifo **Sistema** sobre el **Menú principal** interfaz para configurar los parámetros del sistema relacionados con el fin de optimizar el rendimiento del dispositivo.

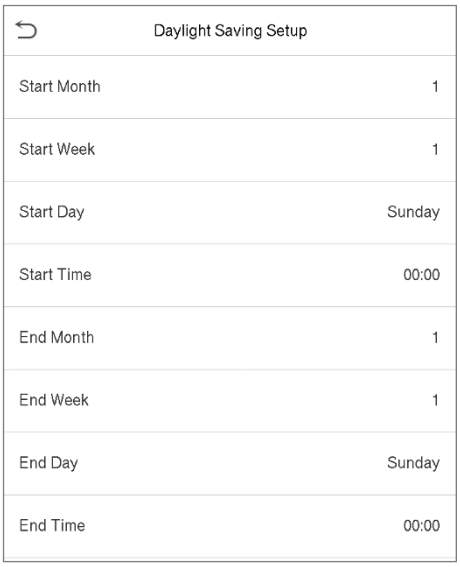


8.1 Fecha y hora

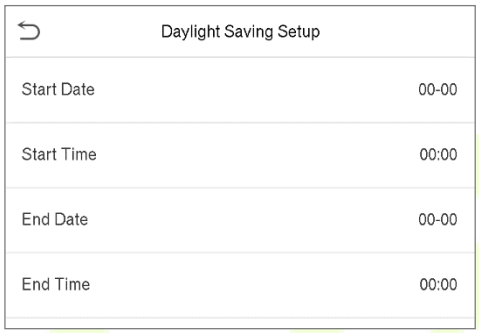
Grifo **Fecha y hora** sobre el **Sistema** interfaz para configurar la fecha y la hora.

- Grifo **Ajuste manual de la hora** para configurar manualmente la fecha y la hora y toque **Confirmar** ahorrar.
- Grifo **24 horas** para habilitar o deshabilitar este formato. Si está habilitado, seleccione el **Formato de fecha** para configurar el formato de fecha.
- ★ Grifo **Horario de verano** para habilitar o deshabilitar la función. Si está habilitado, toque **Modo de ahorro de luz diurna** para seleccionar un modo de horario de verano y luego toque **Configuración de horario de verano** para configurar el interruptor

hora.



Weekmode



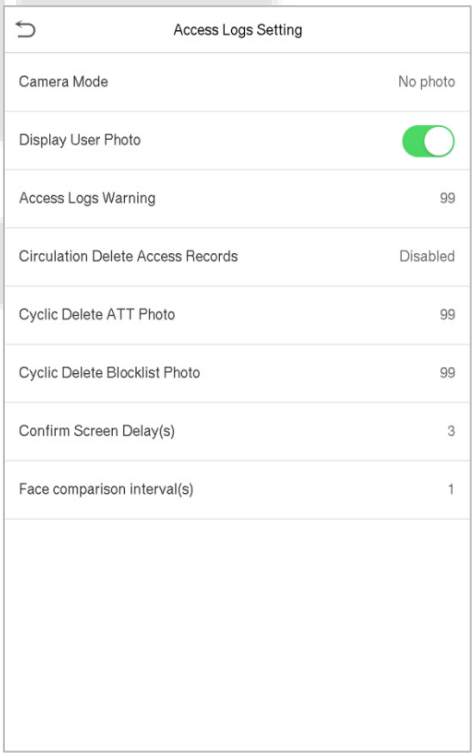
Modo de fecha

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

NOTA : Por ejemplo, el usuario establece la hora del dispositivo (18:35 del 15 de marzo de 2019) a las 18:30 del 1 de enero, 2020. Tras restaurar la configuración de fábrica, la hora del equipo seguirá siendo las 18:30 del 1 de enero de 2020.

8.2 Configuración de registros de acceso

Hacer clic **Configuración de registros de acceso** en la interfaz del sistema.

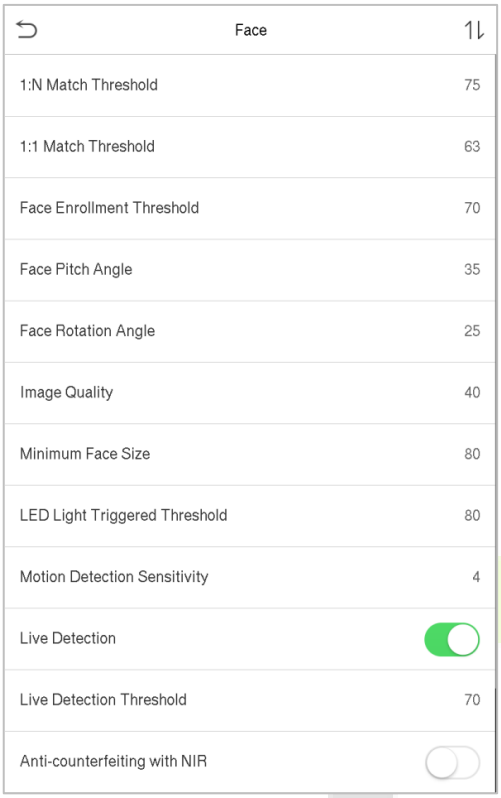


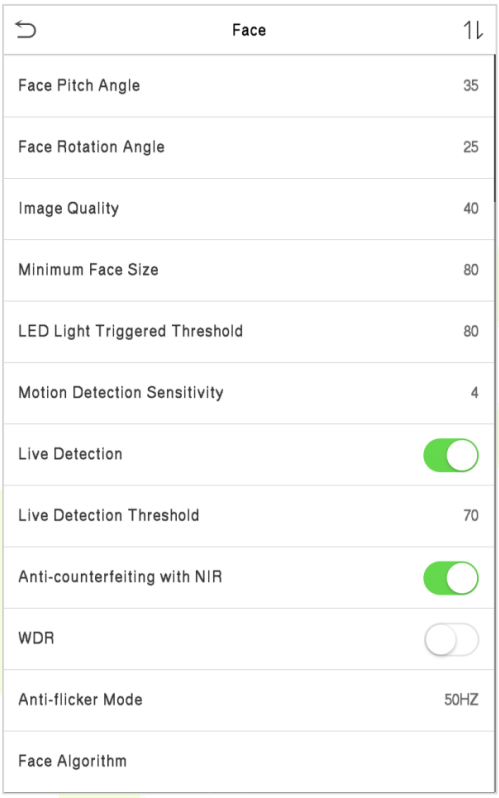
Función descriptiva

Nombre de la función	Descripción
Modo cámara	Ya sea para capturar y guardar la imagen instantánea actual durante la verificación. Hay 5 modos: **Sin fotografía:** No se toma ninguna foto durante la verificación del usuario. **Tomar una foto, no guardar:** Se toma una foto, pero no se guarda durante la verificación. **Tomar una foto y guardar:** La foto se toma y se guarda durante la verificación. **Ahorre en la verificación exitosa:** Se toma una foto y se guarda para cada verificación exitosa. **Guardar en verificación fallida:** La foto se tomará y guardará solo por cada verificación fallida.
Mostrar foto de usuario	Si mostrar la foto del usuario cuando el usuario pasa la verificación.
Registros de acceso	Cuando el espacio de registro del acceso de asistencia alcanza el valor de umbral máximo, el dispositivo mostrará automáticamente la advertencia de espacio de memoria. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999.
Eliminación de circulación Registros de acceso	Cuando los registros de acceso hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de registros de acceso antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 999.
Eliminación cíclica ATT Foto	Cuando las fotos de asistencia hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos de asistencia antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Lista de bloqueo de eliminación cíclica Foto	Cuando las fotos de la lista de bloques hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos antiguas de la lista de bloques. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Confirmar Pantalla Retraso (s)	Se muestra la duración del mensaje de verificación exitosa. Valor válido: 1 ~ 9 segundos.
Comparación de caras Intervalo (s)	Para configurar el intervalo de tiempo de coincidencia de la plantilla facial según sea necesario. Valor válido: 0 ~ 9 segundos.

8.3 Parámetros faciales

Grifo **Cara** sobre el **Sistema** interfaz para ir a la configuración de los parámetros faciales.





FRR	LEJOS	Umbrales coincidentes recomendados	
		1: N	1: 1
Alto	Bajo	85	80
Medio	Medio	82	75
Bajo	Alto	80	70

Función descriptiva

Nombre de la función	Descripción
1: Umbral de captura	En el modo de verificación 1: N, la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas sea mayor que el valor establecido. El valor válido varía de 65 a 120. Cuanto más altos sean los umbrales, menor será la tasa de errores de juicio, mayor será la tasa de rechazo y viceversa. Se recomienda establecer el valor predeterminado de 75.
Umbral de coincidencia 1: 1	En el modo de verificación 1: 1, la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y las plantillas faciales del usuario registradas en el dispositivo sea mayor que el valor establecido. El valor válido varía de 55 a 120. Cuanto más altos sean los umbrales, menor será la tasa de errores de juicio, mayor será la tasa de rechazo y viceversa. Se recomienda establecer el valor predeterminado de 63.
Cara **Umbral de inscripción**	Durante el registro facial, se utiliza la comparación 1: N para determinar si el usuario ya se ha registrado antes. Cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas es mayor que este umbral, indica que la cara ya ha sido registrada.
Ángulo de inclinación de la cara	La tolerancia del ángulo de inclinación de una cara para el registro facial y la comparación. Si el ángulo de inclinación de una cara excede este valor establecido, el algoritmo lo filtrará, es decir, ignorado por el terminal, por lo que no se activará ninguna interfaz de registro y comparación.
Ángulo de rotación de la cara	La tolerancia del ángulo de rotación de una cara para el registro y la comparación de plantillas faciales. Si el ángulo de rotación de una cara excede este valor establecido, será filtrado por el algoritmo, es decir, ignorado por el terminal, por lo que no se activará ninguna interfaz de registro y comparación.
La calidad de imagen	Calidad de imagen para registro facial y comparación. Cuanto mayor sea el valor, más clara será la imagen requerida.
Tamaño mínimo de la cara	Requerido para el registro facial y la comparación. Si el tamaño mínimo de la figura capturada es menor que este valor establecido, entonces se filtrará y no se reconocerá como una cara. Este valor puede entenderse como la distancia de comparación de caras. Cuanto más lejos esté la persona, más pequeña será la cara y el algoritmo obtendrá el píxel de la cara más pequeño. Por lo tanto, ajustar este parámetro puede ajustar la distancia de comparación más lejana de caras. Cuando el valor es 0, la distancia de comparación de caras no está limitada.

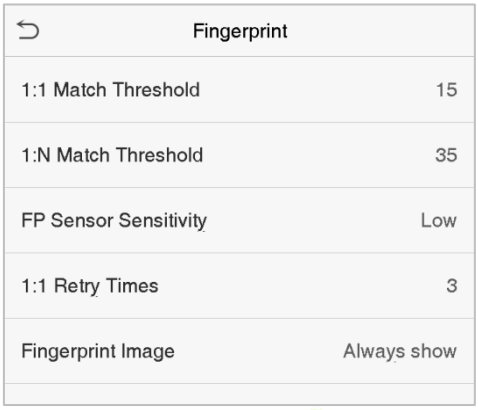
Luz LED activada Límite	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, con más frecuencia se encenderá la luz LED.
Detección de movimiento Sensibilidad	Sirve para establecer el valor de la cantidad de cambio en el campo de visión de una cámara, lo que se conoce como detección de movimiento potencial que activa el terminal desde el modo de espera a la interfaz de comparación. Cuanto mayor sea el valor, más sensible será el sistema, es decir, si se establece un valor mayor, la interfaz de comparación es mucho más fácil y la detección de movimiento se activa con frecuencia.
Detección en vivo	Detectar el intento de falsificación utilizando imágenes de luz visible para determinar si la muestra de fuente biométrica proporcionada es realmente una persona (un ser humano vivo) o una representación falsa.
Detección en vivo Límite	Facilita juzgar si la imagen visible capturada es realmente una persona (un ser humano vivo). Cuanto mayor sea el valor, mejor será el rendimiento anti-spoofing con luz visible.
Lucha contra la falsificación con NIR	Uso de imágenes de espectros de infrarrojo cercano para identificar y prevenir ataques de fotos y videos falsos.
WDR	Amplio rango dinámico (WDR), que equilibra la luz y extiende la visibilidad de la imagen para videos de vigilancia en escenas de iluminación de alto contraste y mejora la identificación de objetos en ambientes brillantes y oscuros.
Modo anti-parpadeo	Se utiliza cuando WDR está desactivado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea a la misma frecuencia que la luz.
Algoritmo facial	Información relacionada con el algoritmo facial y actualización de la plantilla facial de pausa.
Notas	Un ajuste inadecuado de los parámetros de exposición y calidad puede afectar gravemente el rendimiento del dispositivo. Ajuste el parámetro de exposición solo bajo la guía del personal de servicio postventa de nuestra empresa.

Proceso para modificar la precisión del reconocimiento facial

- Sobre el **Sistema** interfaz, toque en **Cara** y luego alternar para habilitar Anti-Spoofing usando NIR para configurar el Anti-Spoofing.
- Entonces, en el **Menú principal,** grifo **Prueba automática> Cara de prueba** y realice la prueba facial.
- Toque tres veces para ver las puntuaciones en la esquina superior derecha de la pantalla y aparecerá el cuadro rectangular rojo para comenzar a ajustar el modo.
- Mantenga la distancia de un brazo entre el dispositivo y la cara, y se recomienda no mover la cara en un rango amplio.

8.4 Parámetros de huellas dactilares

Grifo **Huella dactilar** sobre el **Sistema** interfaz para configurar los ajustes de huellas dactilares.



FRR	LEJOS	Umbrales coincidentes recomendados	
		1: N	1: 1
Alto	Bajo	45	25
Medio	Medio	35	15
Bajo	Alto	25	10

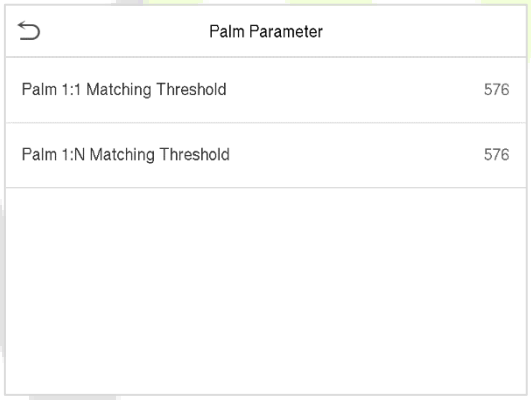
Función descriptiva

Nombre de la función	Descripciones
Umbral de coincidencia 1: 1	En el método de verificación 1: 1, la verificación solo tendrá éxito cuando la similitud entre los datos de huellas dactilares adquiridos y la plantilla de huellas dactilares asociada con la ID de usuario ingresada que está inscrita en el dispositivo es mayor que el valor establecido.
1: Umbral de captura	En el método de verificación 1: N, la verificación solo será exitosa cuando la similitud entre los datos de huellas digitales adquiridos y las plantillas de huellas digitales registradas en el dispositivo sea mayor que el valor establecido.
Sensibilidad del sensor FP	Para establecer la sensibilidad de la adquisición de huellas dactilares. Se recomienda utilizar el nivel predeterminado " **Medio".** Cuando el ambiente está seco, lo que resulta en una detección lenta de huellas dactilares, puede establecer el nivel en " **Alto"** elevar la sensibilidad; cuando el ambiente es húmedo, lo que dificulta la identificación de la huella digital, puede establecer el nivel en " **Bajo** ".
Tiempos de reintento 1: 1	Los usuarios pueden olvidar la huella digital registrada o presionar el dedo de manera incorrecta. La verificación 1: 1 permite configurar los intentos de reintento de autenticación para los usuarios

Nombre de la función	Descripciones
	para reducir el proceso de volver a ingresar la identificación de usuario y aumentar la seguridad.
Imagen de huella digital	Para configurar si se muestra la imagen de la huella digital en la pantalla durante el registro o la verificación de la huella digital. Hay cuatro opciones disponibles: • **Mostrar para inscribirse:** para mostrar la imagen de la huella digital en la pantalla solo durante el registro. • **Mostrar para el partido:** para mostrar la imagen de la huella digital en la pantalla solo durante la verificación. • **Siempre muestra:** para mostrar la imagen de la huella digital en la pantalla durante el registro y la verificación. • **Ninguna:** no mostrar la imagen de la huella digital.

8.5 Parámetros de la palma

Grifo **Palma** sobre el **Sistema** interfaz para configurar los ajustes de la palma.



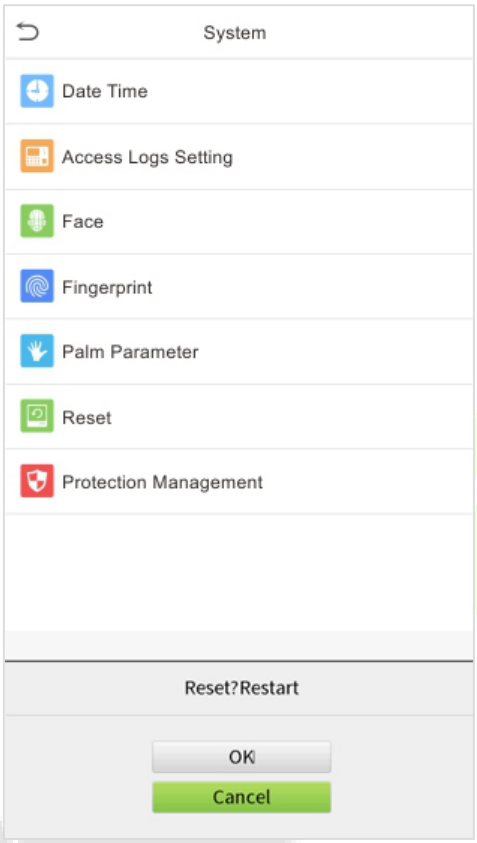
Función descriptiva

Nombre de la función	Descripción
Palm1: 1 Umbral coincidente	Solo cuando la similitud entre la palma de verificación y la palma registrada del usuario es mayor que este valor, la verificación puede tener éxito.
Palm1: Umbral de captura la palma verificadora y toda la palma registrada es mayor que este valor	Bajo el método de verificación 1: N, solo cuando la similitud entre ¿Puede la verificación tener éxito?

8,6 Restablecimiento de fábrica

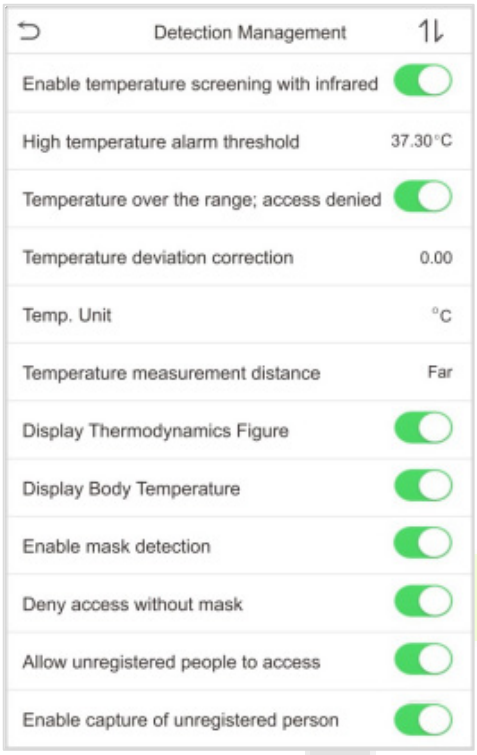
La función Factory Reset restaura la configuración del dispositivo, como la configuración de comunicación y la configuración del sistema, a la configuración predeterminada de fábrica (esta función no borra los datos de usuario registrados).

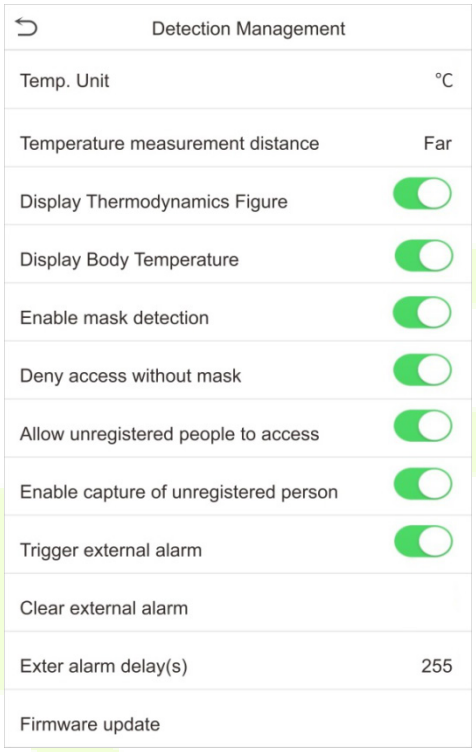
Grifo **Reiniciar** sobre el **Sistema** interfaz y luego toque **Okay** para restaurar la configuración predeterminada de fábrica.



8.7 Gestión de detección

Hacer clic **Gestión de detección** sobre el **Sistema** interfaz para configurar los ajustes de Gestión de detección.





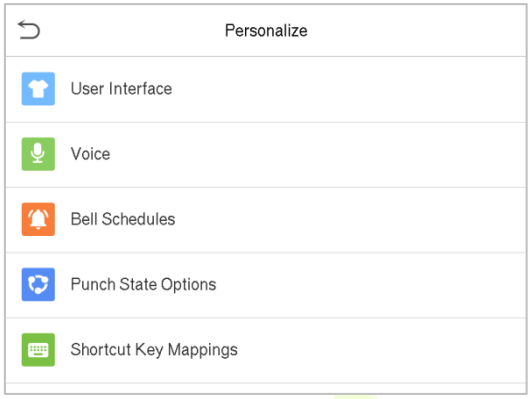
Función descriptiva

Nombre de la función	Descripción
Habilitar temperatura proyección con infrarrojo	Para habilitar o deshabilitar la medición de temperatura por infrarrojos. Cuando esta función está habilitada, los usuarios deben pasar el control de temperatura además de la verificación de identidad antes de que se otorgue el acceso. Para medir la temperatura corporal, las caras del usuario deben estar alineadas con el área de medición de temperatura.
Alta temperatura umbral de alarma	Para establecer el valor del umbral de alarma para temperatura corporal alta. Cuando la temperatura medida durante la verificación es más alta que el valor establecido, el dispositivo emitirá un aviso y una alarma sonora. El umbral de alarma predeterminado es 37,30 ° C.
Temperatura sobre el rango; acceso negado	Cuando está habilitado, si la temperatura corporal del usuario medida está por encima (o por debajo) del umbral de alarma, no se le concederá acceso al usuario incluso si se verifica su identidad. Cuando está deshabilitado, se otorga acceso al usuario si se verifica su identidad, independientemente de su temperatura corporal.

Temperatura corrección de desviación	A medida que el módulo de medición de temperatura lee un pequeño rango de variación de un valor observado en entornos inusuales (humedad, ambiente extremo temperatura y tal), los usuarios pueden establecer el valor de desviación aquí para reflejar la verdadera temperatura de la persona.
Temperatura. Unidad	La unidad de temperatura corporal se puede alternar entre Celsius (° C) y Fahrenheit (° F).
Temperatura medición distancia	Hay tres modos al medir la temperatura durante el proceso de verificación, son: **Cerca, Cerca** y **Lejos.**
Monitor Termodinámica Figura	Activar o desactivar la visualización de la imagen térmica de una persona. Cuando está habilitado, la imagen térmica de la persona se muestra en la esquina superior izquierda del dispositivo durante el proceso de detección.
Cuerpo de la pantalla Temperatura	Para habilitar o deshabilitar la visualización de la temperatura corporal. Cuando está habilitado, el dispositivo mostrará el valor de temperatura corporal del usuario durante el proceso de verificación.
Enablemask detección	Para habilitar o deshabilitar la función de detección de máscara. Cuando está habilitado, el dispositivo identificará si el usuario está usando una máscara o no durante la verificación.
Denegar el acceso sin máscara	Para habilitar o deshabilitar el acceso de una persona sin máscara. Cuando está habilitado, el dispositivo denegará el acceso de una persona, si no usa una máscara.
Permitir no registrados personas para acceder	Para habilitar o deshabilitar el acceso de una persona no registrada. Cuando está habilitado, el dispositivo permite que la persona ingrese sin registrarse, siempre que la persona que pase la detección.
Habilitar captura de persona no registrada	Para habilitar o deshabilitar la captura de fotografía de una persona no registrada. Cuando está habilitado, el dispositivo capturará automáticamente la foto de la persona no registrada, habilitar esta función requiere habilitar **Permitir personas no registradas para acceder.**
Disparador externo alarma	Cuando está habilitado, si la temperatura del usuario es más alta que el valor del umbral establecido o la detección de la máscara está habilitada, pero la persona no usa la máscara, se activará una alarma.
Borrar alarma externa	Borra los registros de alarma activada del dispositivo.
Alarma externa retraso (s)	El tiempo de retardo para activar una alarma externa. Se puede configurar en segundos. Los usuarios pueden desactivar la función o establecer un valor entre 1 y 255.
Actualización de firmware	Elija si desea actualizar la versión del software del módulo de detección de temperatura de imagen térmica.

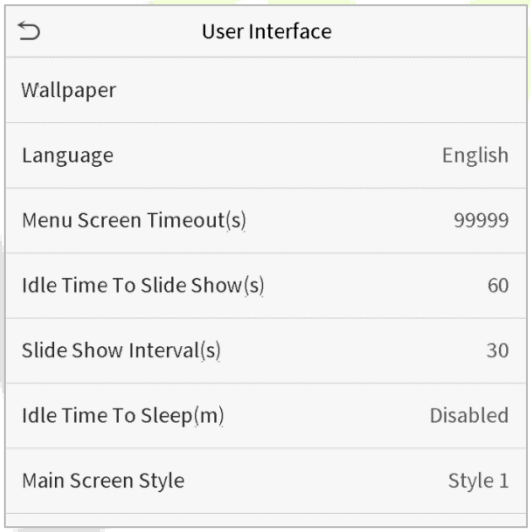
9 Personalizar la configuración

Grifo **Personalizar** sobre el **Menú principal** interfaz para personalizar la configuración de la interfaz, voz, timbre, opciones de estado de marcado y asignaciones de teclas de acceso directo.



9.1 Configuración de la interfaz

Grifo **Interfaz de usuario** sobre el **Personalizar** interfaz para personalizar el estilo de visualización de la interfaz principal.



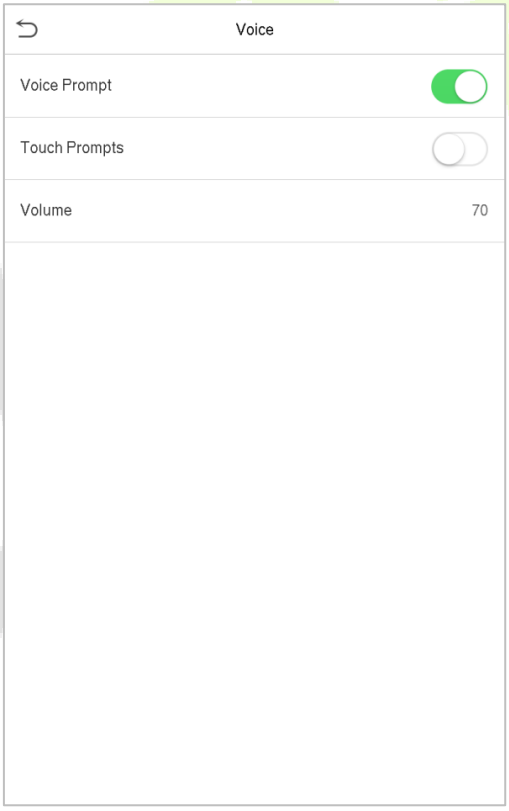
Función descriptiva

Nombre de la función	Descripción
Fondo de pantalla	El fondo de pantalla de la pantalla principal se puede seleccionar de acuerdo con las preferencias del usuario.
Idioma	Seleccione el idioma del dispositivo.
Pantalla de menú **Tiempo de espera (s)**	Cuando no hay operación y el tiempo excede el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. La función puede desactivarse o configurarse el valor requerido entre 60 y 99999 segundos.

Tiempo de inactividad para la presentación de diapositivas	Cuando no hay ninguna operación y el tiempo excede el valor establecido, se reproducirá una presentación de diapositivas. La función puede desactivarse o puede establecer el valor entre 3 y 999 segundos.
Intervalo de presentación de diapositivas (s)	Es el intervalo de tiempo para cambiar entre diferentes imágenes de presentación de diapositivas. La función puede desactivarse o puede establecer el intervalo entre 3 y 999 segundos.
Tiempo inactivo para dormir (m)	Si el modo de suspensión está activado y cuando no hay ninguna operación en el dispositivo, el dispositivo entrará en el modo de espera. Presione cualquier tecla o dedo para reanudar el modo de trabajo normal. Esta función se puede desactivar o establecer un valor dentro de 1-999 minutos.
Estilo de pantalla principal	El estilo de la pantalla principal se puede seleccionar según las preferencias del usuario.

9.2 Configuración de voz

Grifo **Voz** sobre el **Personalizar** interfaz para configurar los ajustes de voz.



Función descriptiva

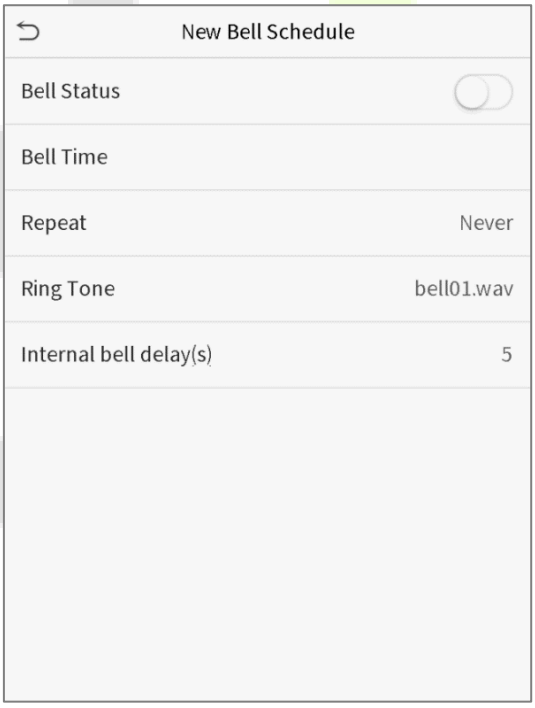
Nombre de la función	Descripción
Mensaje de voz	Cambie para habilitar o deshabilitar las indicaciones de voz durante las operaciones de la función. Cambie para
Toque Indicación	habilitar o deshabilitar los sonidos del teclado.
Volumen	Ajuste el volumen del dispositivo que se puede configurar entre: 0-100.

9.3 Horarios de campana

Grifo **Horarios de campana** sobre el **Personalizar** interfaz para configurar los ajustes de la campana.

Nuevo horario de timbre

Grifo **Horario NewBell** sobre el **Horario de campana** interfaz para agregar un nuevo horario de timbre.



Función descriptiva

Nombre de la función	Descripción
Estado de la campana	Cambie para habilitar o deshabilitar el estado de la campana.
Tiempo de campana	Una vez que se establece el tiempo requerido, el dispositivo se activará automáticamente para hacer sonar la campana durante ese tiempo.
Repetir	Configure el número requerido de conteos para repetir la campana programada. Seleccione un tono
Tono de llamada	de llamada.
Retardo de campana interna	Configure el tiempo de repetición de la campana interna. Los valores válidos oscilan entre 1 y 999 segundos.

Todos los horarios de campana

Una vez programada la campana, el **Horarios de campana** interfaz, toque **Todos los horarios de campana** para ver la campana recién programada.

Editar la campana programada

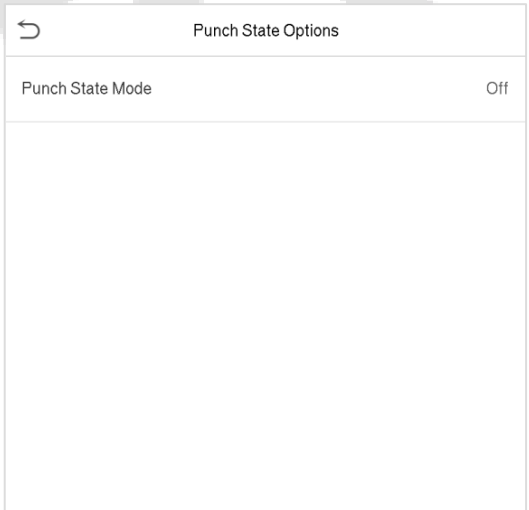
Sobre el **Todos los horarios de campana** interfaz, toque el horario de timbre requerido y toque **Editar** para editar el horario de timbre seleccionado. El método de edición es el mismo que el de agregar un nuevo horario de campana.

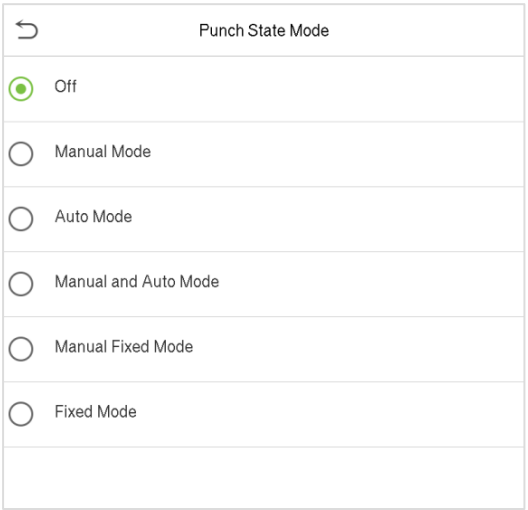
Eliminar una campana

Sobre el **Todos los horarios de campana** interfaz, toque el horario de timbre requerido y toque **Eliminar,** y luego toque **si** para eliminar la campana seleccionada.

9.4 Opciones de estados de perforación

Grifo **Opciones de estados de perforación** sobre el **Personalizar** interfaz para configurar los ajustes del estado de perforación.





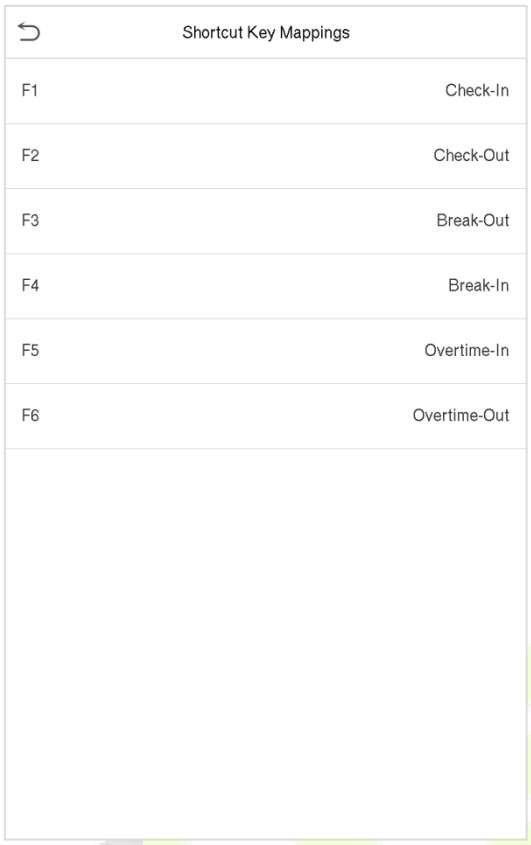
Función descriptiva

Nombre de la función	Descripción
Modo de estado de perforación	**Apagado:** Deshabilite la función de estado de perforación. Por lo tanto, la clave de estado de perforación establecida en **Asignaciones de teclas de método abreviado** el menú dejará de ser válido. **Modo manual:** Cambie la tecla de estado de perforación manualmente y la tecla de estado de perforación desaparecerá después **Tiempo de espera del estado de perforación.** **Modo automático:** La tecla de estado de perforación cambiará automáticamente a un estado de perforación específico de acuerdo con el horario predefinido que se puede configurar en las asignaciones de teclas de acceso directo. **Modo manual y automático:** La interfaz principal mostrará la tecla de estado de perforación de cambio automático. Sin embargo, los usuarios aún podrán seleccionar una alternativa que sea el estado de asistencia manual. Después del tiempo de espera, la tecla de estado de perforación de conmutación manual se convertirá en la tecla de estado de perforación de conmutación automática. **Modo fijo manual:** Después de que la tecla de estado de perforación se configure manualmente a un estado de perforación particular, la función permanecerá sin cambios hasta que se cambie manualmente nuevamente. **Modo fijo:** Solo se mostrará la clave de estado de perforación fijada manualmente. Los usuarios no pueden cambiar el estado presionando otras teclas.

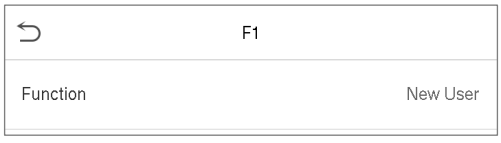
9.5 Asignaciones de teclas de método abreviado

Los usuarios pueden definir teclas de acceso directo para el estado de asistencia y para las teclas funcionales que se definirán en la interfaz principal. Por lo tanto, en la interfaz principal, cuando se presionan las teclas de acceso directo, el estado de asistencia correspondiente o la interfaz de función se mostrará directamente.

Grifo **Asignaciones de teclas de método abreviado** sobre el **Personalizar** interfaz para configurar las teclas de método abreviado necesarias.



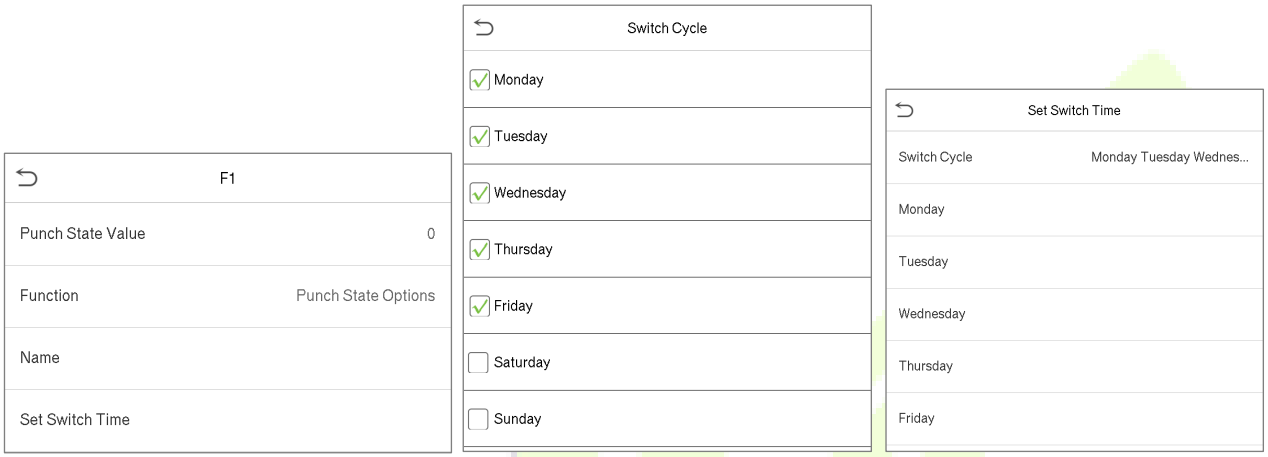
- Sobre el **Asignaciones de teclas de método abreviado** interfaz, toque la tecla de acceso directo requerida para configurar los ajustes de la tecla de acceso directo.
- Sobre el **Tecla de acceso directo (** que es "F1"), toque **función** para configurar el proceso funcional de la tecla de método abreviado como tecla de estado de perforación o tecla de función.
- Si la tecla de acceso directo se define como una tecla de función (como Nuevo usuario, Todos los usuarios, etc.), la configuración se completa como se muestra en la imagen siguiente.



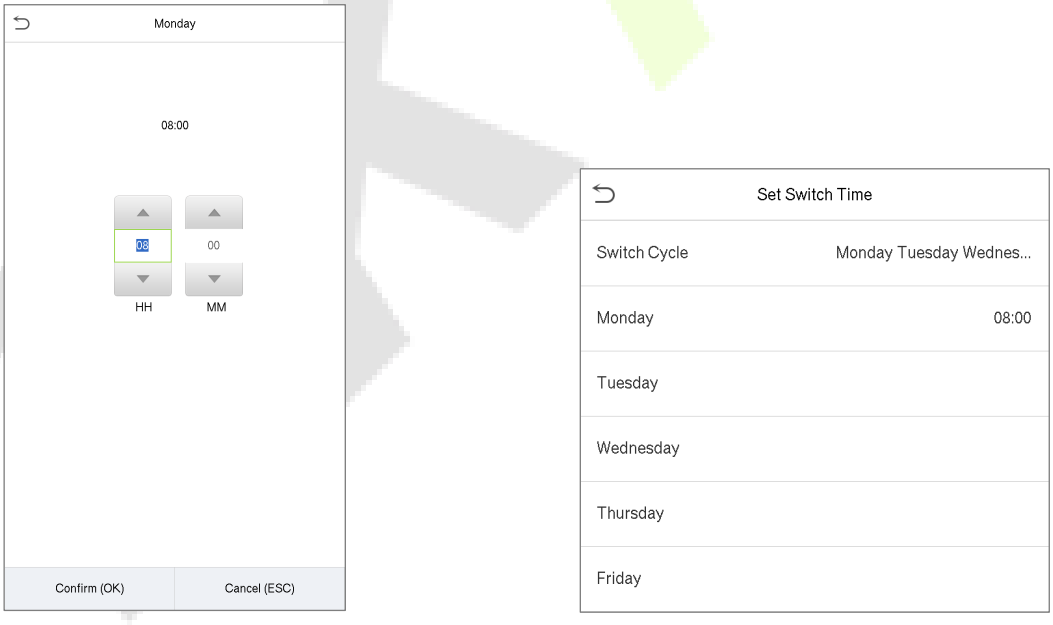
- Si la tecla de acceso directo está configurada como una tecla de estado de perforación (como registro de entrada, salida, etc.), entonces es necesario configurar el valor del estado de perforación (valor válido 0 ~ 250), el nombre y la hora de conmutación.

Establecer la hora del cambio

- El tiempo de conmutación se establece de acuerdo con las opciones de estado de perforación. Cuando el **punch statemode** se
- establece en **Modo automático,** debe establecerse el tiempo de conmutación. Sobre el **Tecla de acceso directo** interfaz,
- toque **Establecer hora de cambio** para configurar la hora del cambio.
- Sobre el **Ciclo de cambio** interfaz, seleccione el ciclo de cambio (lunes, martes, etc.) como se muestra en la imagen siguiente.



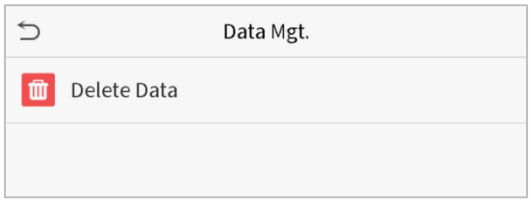
- Una vez que se selecciona el ciclo de cambio, configure el tiempo de cambio para cada día y toque **Okay** para confirmar, como se muestra en la imagen de abajo.



Nota: Cuando la función está configurada como Indefinida, el dispositivo no habilitará la tecla de estado de perforación.

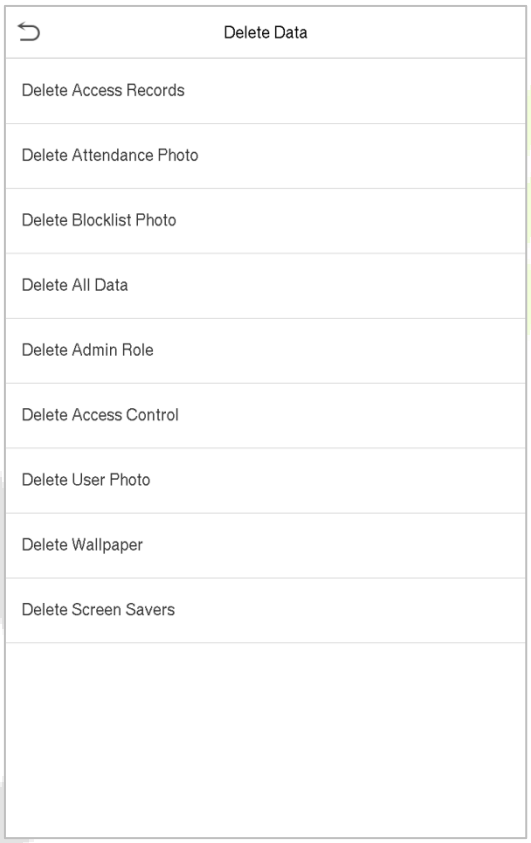
10 Gestión de datos

Sobre el **Menú principal,** grifo **Gestión de datos** para eliminar los datos relevantes en el dispositivo.



10.1 Borrar datos

Grifo **Borrar datos** sobre el **Gestión de datos** interfaz para eliminar los datos requeridos.

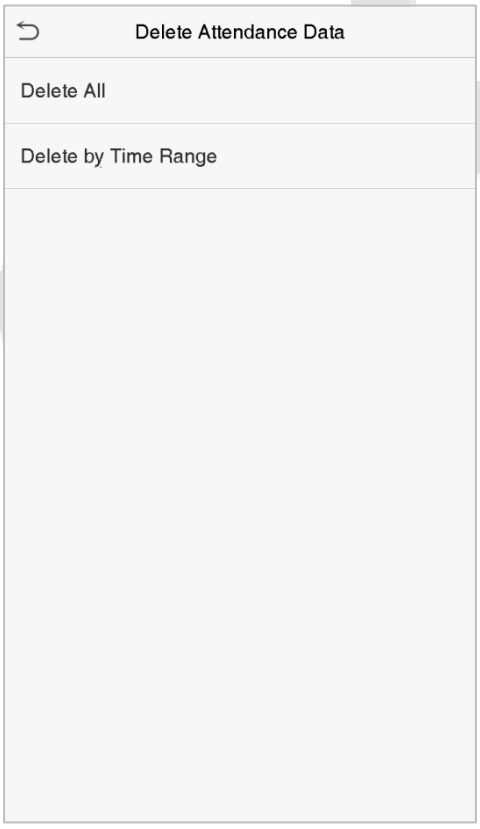


Función descriptiva

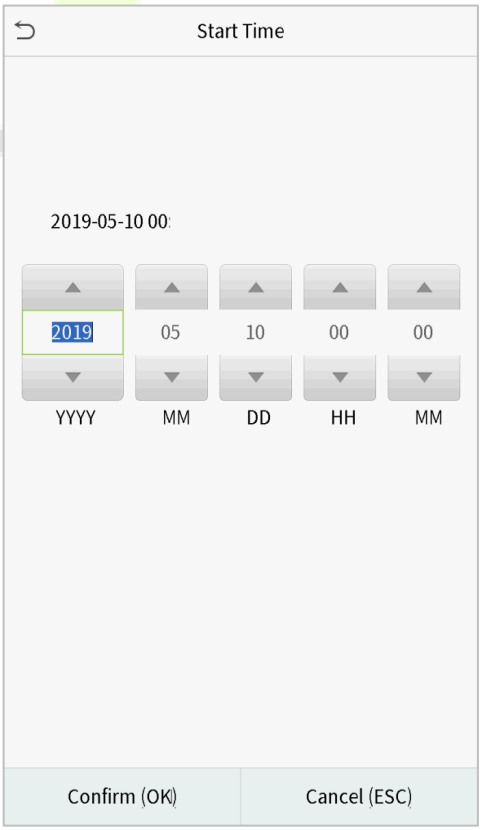
Nombre de la función	Descripción
Eliminar registros de acceso	Eliminar datos de asistencia / registros de acceso condicionalmente. Eliminar
Eliminar foto de asistencia	fotos de asistencia del personal designado. Para eliminar las fotos tomadas
Eliminar foto de la lista de bloqueo	durante verificaciones fallidas.
Eliminar todos los datos	Eliminar información y registros de asistencia / registros de acceso de todos los usuarios registrados.
Eliminar función de administrador	Para eliminar todos los privilegios de administrador. Para
Eliminar control de acceso	borrar todos los datos de acceso.
Eliminar foto de usuario	Para eliminar todas las fotos de usuario en el dispositivo.
Eliminar fondo de pantalla	Para eliminar todos los fondos de pantalla del dispositivo.
Eliminar protectores de pantalla	Para eliminar los protectores de pantalla del dispositivo.

El usuario puede seleccionar Eliminar todo o Eliminar por intervalo de tiempo al eliminar los registros de acceso, las fotos de asistencia o bloquear las fotos de la lista.

Al seleccionar Eliminar por rango de tiempo, debe establecer un rango de tiempo específico para eliminar todos los datos dentro de un período específico.



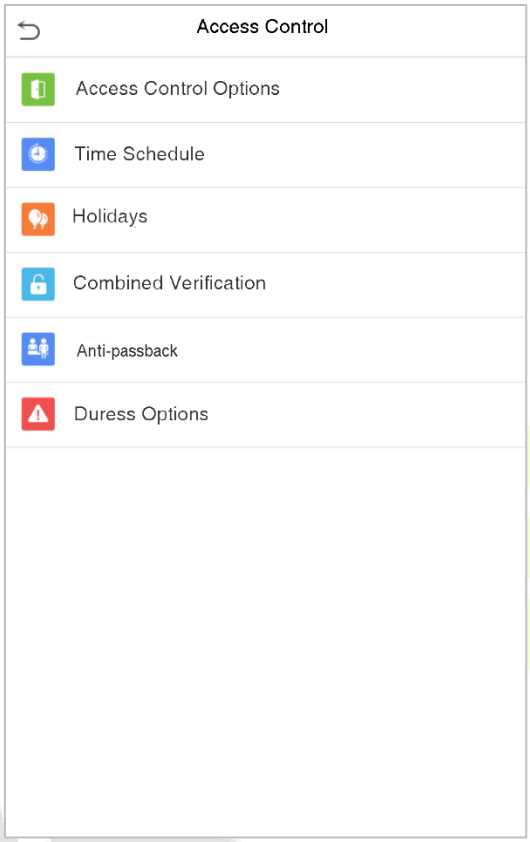
Seleccione Eliminar por rango de tiempo.



Establezca el rango de tiempo y haga clic en **OKAY.**

11 Control de acceso

Sobre el **Menú principal,** grifo **Control de acceso** para establecer el horario de apertura de puertas, control de cerraduras y configurar otros parámetros relacionados con el control de acceso.

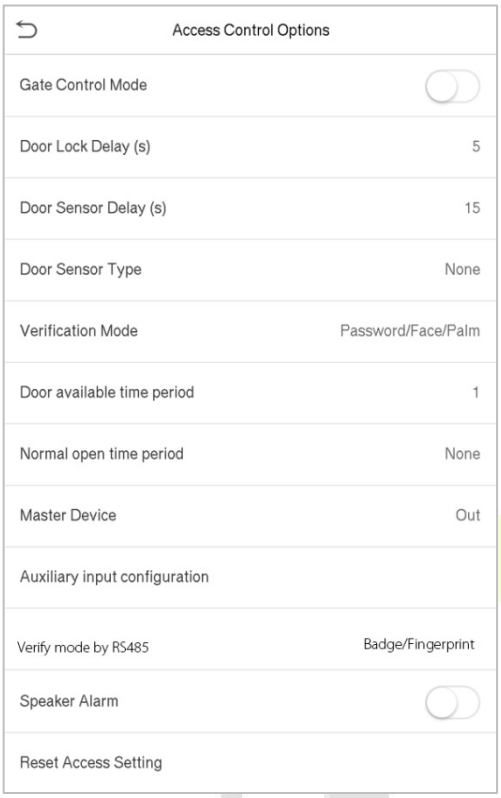


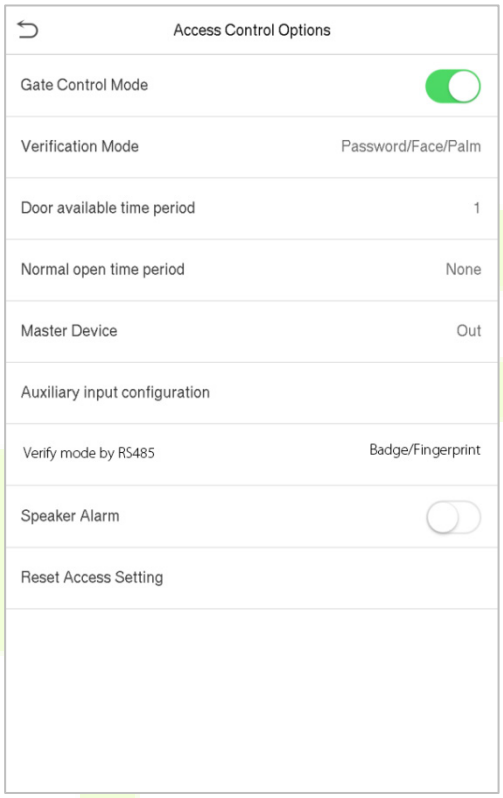
Para acceder, el usuario registrado debe cumplir las siguientes condiciones:

- El tiempo de desbloqueo actual de la puerta correspondiente debe estar dentro de cualquier zona horaria válida del período de tiempo del usuario.
- El grupo de usuario correspondiente ya debe estar configurado en la combinación de desbloqueo de puerta (y si hay otros grupos, que se configuran en el mismo combo de acceso, entonces también se requiere la verificación de los miembros de ese grupo para desbloquear la puerta).
- En la configuración predeterminada, los nuevos usuarios se asignan al primer grupo con la zona horaria predeterminada del grupo, donde el combo de acceso es "1" y está configurado en estado de desbloqueo de manera predeterminada.

11,1 Opciones de control de acceso

Grifo **Opciones de control de acceso** sobre el **Control de acceso** Interfaz para configurar los parámetros de la cerradura de control del terminal y equipos relacionados.





Función descriptiva

Nombre de la función	Descripción
Modo de control de puerta	Cambie entre el interruptor de ENCENDIDO o APAGADO para entrar en el modo de control de puerta o no. Cuando se establece en **EN,** en esta interfaz eliminará las opciones de tipo de sensor de puerta, relé de bloqueo de puerta y sensor de puerta.
Retraso de bloqueo de puerta (s)	El tiempo que el dispositivo controla que la cerradura eléctrica esté en estado de desbloqueo. Valor válido: 1 ~ 10 segundos; 0 segundos representa la desactivación de la función.
Retraso (s) del sensor de puerta	Si la puerta no está bloqueada y se deja abierta durante un tiempo determinado (Sensor de puerta Retraso), se activará una alarma. El valor válido del retardo del sensor de puerta varía de 1 a 255 segundos.

Tipo de sensor de puerta	Hay tres tipos de sensores: **Ninguno, normalmente abierto** y **Normal Cerrado. Ninguna:** Significa que el sensor de la puerta no está en uso. **Abierto normal:** Significa que la puerta siempre se deja abierta cuando la energía eléctrica está encendida. **Normal Cerrado:** Significa que la puerta siempre se deja cerrada cuando la energía eléctrica está encendida.
VerificationMode	El modo de verificación admitido incluye contraseña / rostro, solo ID de usuario, contraseña, solo rostro y rostro + contraseña.
Puerta disponible tiempo período	Para establecer un período de tiempo para la puerta, de modo que la puerta esté disponible solo durante ese período.
Tiempo abierto normal Período	Período de tiempo programado para el modo de “apertura normal”, de modo que la puerta siempre se deje abierta durante este período.
Dispositivo maestro	Al configurar el maestro y el esclavo, el estado del maestro se puede configurar para salir al entrar. **Salida:** El registro verificado en el host es el registro de salida. **Entrar:** El registro verificado en el host es el registro de entrada.
Entrada auxiliar configuración	Establece el período de tiempo de desbloqueo de la puerta y el tipo de salida auxiliar del dispositivo terminal auxiliar. Los tipos de salidas auxiliares incluyen Ninguno, Puerta del gatillo abierta, Alarma del gatillo, Puerta del gatillo abierta y Alarma.
Verificar modo por RS485	El modo de verificación se usa cuando el dispositivo se usa como host o esclavo. El modo de verificación admitido incluye Tarjeta / Huella digital, Solo huella digital, Solo tarjeta, Huella digital + Contraseña, Tarjeta + Contraseña, Tarjeta + Huella digital y Tarjeta + Huella digital + Contraseña.
Alarma de altavoz	Transmite una alarma sonora o una alarma de desmontaje desde el local. Cuando la puerta esté cerrada o la verificación sea exitosa, el sistema cancelará la alarma del local.
Restablecer configuración de acceso	Los parámetros de restablecimiento del control de acceso incluyen el retardo de la cerradura de la puerta, el retardo del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el período de tiempo disponible de la puerta, el período de tiempo de apertura normal, el dispositivo maestro y la alarma. Sin embargo, los datos de control de acceso borrados en Data Mgt. está excluido.

11,2 Horario

Grifo **Configuración de la regla de tiempo** en la interfaz de control de acceso para configurar los ajustes de tiempo.

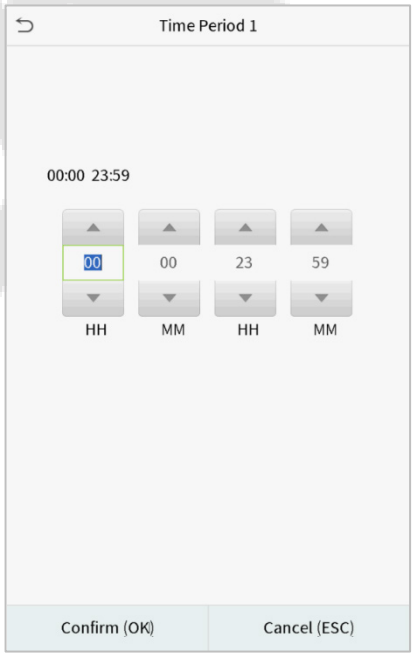
- Todo el sistema puede definir hasta 50 períodos de tiempo.
- Cada período de tiempo representa **10** Zonas horarias, es decir **1** semana y **3** días festivos, y cada zona horaria es un período estándar de 24 horas por día y el usuario solo puede verificar dentro del período de tiempo válido.

- Se puede establecer un máximo de 3 períodos de tiempo para cada zona horaria. La relación entre estos períodos de tiempo es " **O".** Por lo tanto, cuando el tiempo de verificación cae en cualquiera de estos períodos de tiempo, la verificación es válida.

- El formato de zona horaria de cada período de tiempo: HH MM-HH MM, que tiene una precisión de minutos según el reloj de 24 horas.

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

En la interfaz de número de zona horaria seleccionada, toque el día requerido (es decir, lunes, martes, etc.) para establecer la hora.



Especifique la hora de inicio y finalización y luego toque **OKAY.**

NOTA :

1) Cuando la hora de finalización es anterior a la hora de inicio (por ejemplo, 23: 57 ~ 23: 56), indica que el acceso es Prohibido todo el día.

2) Cuando la hora de finalización es posterior a la hora de inicio (por ejemplo, 00: 00 ~ 23: 59), indica que el intervalo es válida.

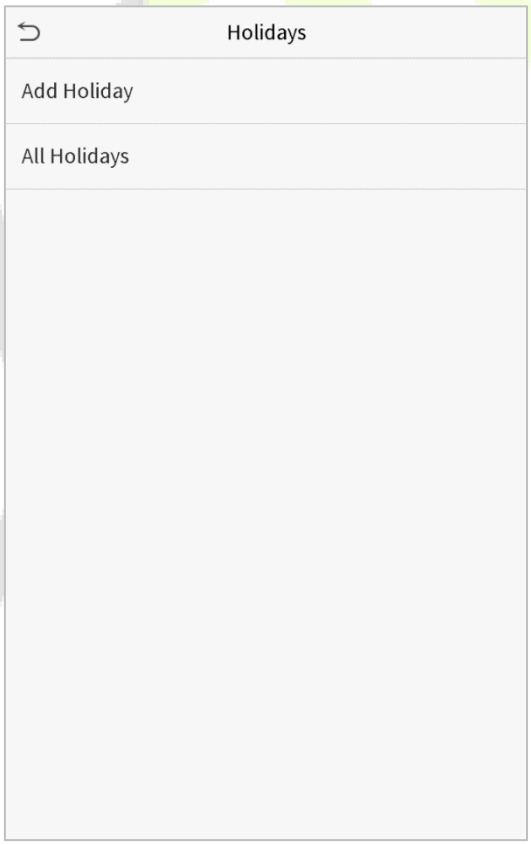
3) El período de tiempo efectivo para mantener la puerta abierta o desbloqueada todo el día es (00: 00 ~ 23: 59) o también cuando la hora de finalización es posterior a la hora de inicio (como 08: 00 ~ 23: 59).

4) La zona horaria predeterminada 1 indica que la puerta está abierta todo el día.

11,3 Días festivos

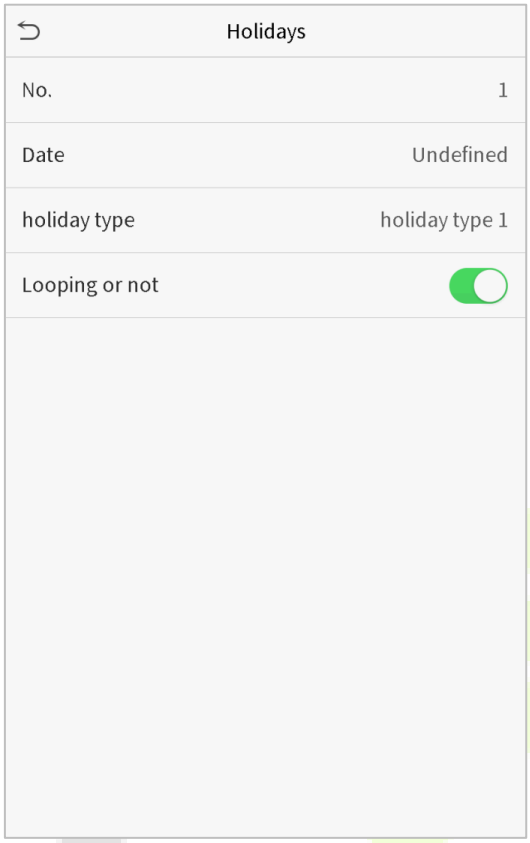
Siempre que haya un día festivo, es posible que necesite un horario de acceso especial; pero cambiar el tiempo de acceso de todos uno por uno es extremadamente engorroso, por lo que puede establecer un tiempo de acceso de vacaciones que sea aplicable a todos los empleados, y el usuario podrá abrir la puerta durante las vacaciones.

Grifo **Días festivos** sobre el **Control de acceso** interfaz para configurar el acceso de vacaciones.



- **Agregar un nuevo feriado**

Grifo **Agregar feriado** sobre el **Días festivos** interfaz y configure los parámetros de vacaciones.



- **Editar un feriado**

  Sobre el **Días festivos** interfaz, seleccione un elemento de vacaciones para modificarlo. Grifo **Editar** para modificar los parámetros de vacaciones.

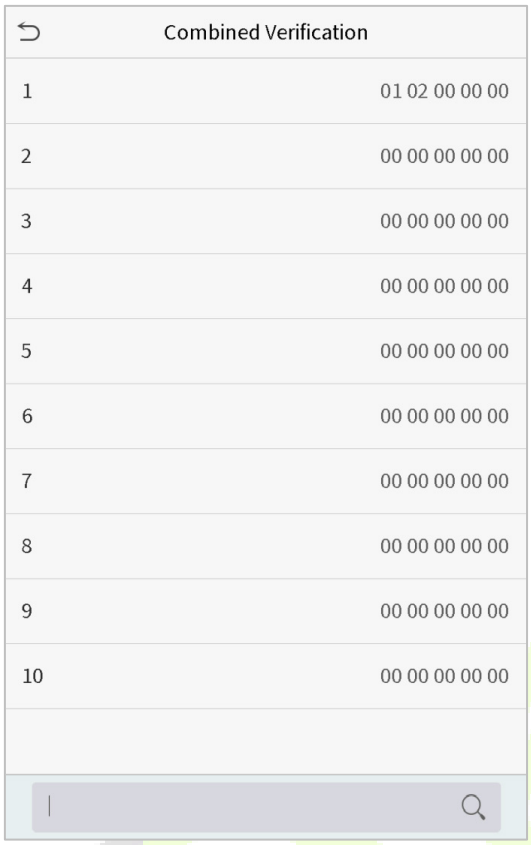
- **Eliminar un feriado**

  Sobre el **Días festivos** interfaz, seleccione un elemento de vacaciones para eliminar y toque **Eliminar.** prensa **Okay** para confirmar la eliminación. Después de la eliminación, este día festivo ya no se muestra en **Todos los días festivos** interfaz.

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 pueden pertenecer todos a un grupo de acceso o pueden pertenecer a cinco grupos de acceso diferentes.

Grifo **Verificación combinada en** los **Control de acceso** interfaz para configurar la configuración de verificación combinada.



En la interfaz de verificación combinada, toque la combinación de desbloqueo de puerta que desee configurar y toque el **arriba** y **abajo** flechas para ingresar el número de combinación, y luego presione **OKAY.**

Por ejemplo:

- los **Combinación de desbloqueo de puerta 1** se establece como (**01 03 05 06 08),** indicando que el desbloqueo
  La combinación 1 consta de 5 personas, y las 5 personas son de 5 grupos, es decir, **Grupo de control de acceso** 1 (grupo de CA 1), grupo de CA 3, grupo de CA 5, grupo de CA 6 y grupo de CA 8, respectivamente.
- los **Combinación de desbloqueo de puerta 2** se establece como (**02 02 04 04 07),** indicando que el desbloqueo
  la combinación 2 consta de 5 personas; los dos primeros son del grupo 2 de CA, los dos siguientes son del grupo 4 de CA y la última persona es del grupo 7 de CA.
- los **Combinación de desbloqueo de puerta 3** se establece como (**09 09 09 09 09),** indicando que hay 5 personas en esta combinación; todos los cuales son del grupo AC 9.
- los **Combinación de desbloqueo de puerta 4** se establece como (**03 05 08 00 00),** indicando que el desbloqueo
  La combinación 4 consta de solo tres personas. La primera persona es del grupo AC 3, la segunda persona es del grupo AC 5 y la tercera persona es del grupo AC 8.

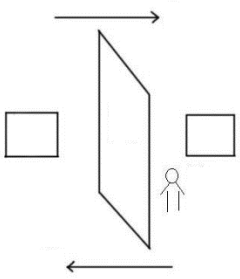
Eliminar una combinación de desbloqueo de puertas

Establezca todas las combinaciones de desbloqueo de puertas en 0 si desea eliminar las combinaciones de desbloqueo de puertas.

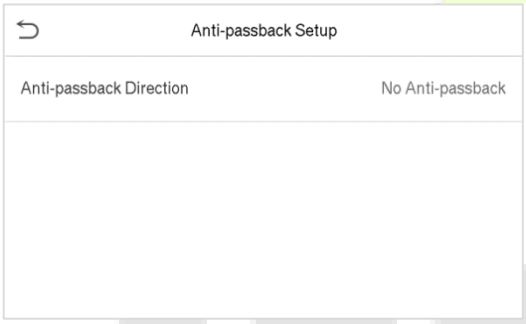
11,5 Configuración anti-passback

Es posible que algunas personas sigan a los usuarios para entrar por la puerta sin verificación, lo que resultará en una brecha de seguridad. Entonces, para evitar tal situación, se desarrolló la opción Anti-Passback. Una vez habilitado, el registro de entrada debe coincidir con el registro de salida para poder abrir la puerta.

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



Grifo **Configuración anti-passback** sobre el **Control de acceso** interfaz.



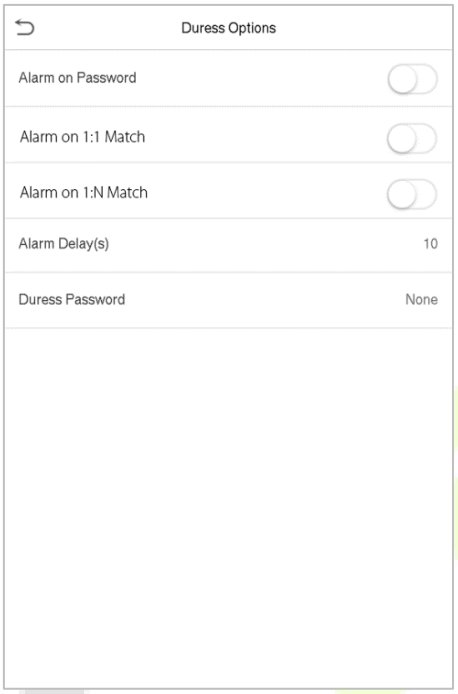
Función descriptiva

Nombre de la función	Descripción
Anti-passback dirección	**Sin Anti-passback:** La función anti-passback está deshabilitada, lo que significa que la verificación exitosa a través del dispositivo maestro o esclavo puede desbloquear la puerta. El estado de asistencia no se guarda en esta opción. **Fuera Anti-passback:** Después de que un usuario se retira, solo si el último registro es un registro de entrada, el usuario puede volver a retirar; de lo contrario, se activará la alarma. Sin embargo, el usuario puede registrarse libremente. **En Anti-passback:** Después de que un usuario se registra, solo si el último registro es un registro de salida, el usuario puede registrarse nuevamente; de lo contrario, se activará la alarma. Sin embargo, el usuario puede realizar el check-out libremente. **Anti-passback de entrada / salida:** Después de que un usuario ingresa / sale, solo si el último registro es un registro de salida, el usuario puede registrarse nuevamente; o si se trata de un registro de entrada, el usuario puede volver a realizar la salida; de lo contrario, se activará la alarma.

11,6 Opciones de coacción

Una vez que un usuario activa la función de verificación de coacción con métodos de autenticación específicos, y cuando está bajo coacción y se autentica mediante la verificación de coacción, el dispositivo desbloqueará la puerta como de costumbre, pero al mismo tiempo, se enviará una señal. para activar la alarma.

En **Control de acceso** interfaz, toque **Opciones de coacción** para configurar los ajustes de coacción.



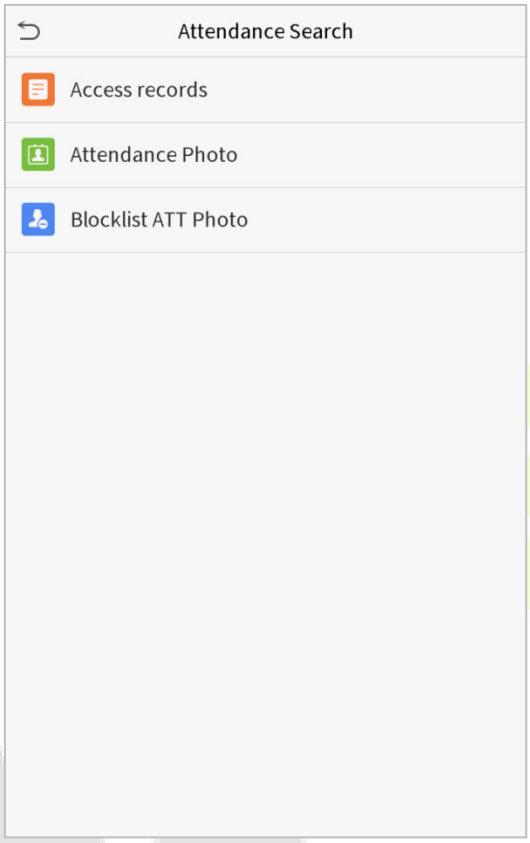
Función descriptiva

Nombre de la función	Descripción
Alarmon Password	Cuando un usuario usa el método de verificación de contraseña, se generará una señal de alarma solo cuando la verificación de contraseña sea exitosa; de lo contrario, no habrá señal de alarma.
Alarmon 1: 1 Partido	Cuando un usuario usa cualquier huella digital para realizar la verificación 1: 1, se generará una señal de alarma solo cuando la verificación 1: 1 sea exitosa; de lo contrario, no habrá señal de alarma.
Alarmon 1: NMatch	Cuando un usuario usa cualquier huella dactilar para realizar la verificación 1: N, se generará una señal de alarma solo cuando la identificación 1: N sea exitosa; de lo contrario, no habrá señal de alarma.
Retraso de alarma (s)	La señal de alarma no se transmitirá hasta que haya transcurrido el tiempo de retardo de la alarma. El valor varía de 1 a 999 segundos.
Contraseña de coacción	Configure la contraseña de coacción de 6 dígitos. Cuando el usuario ingresa esta contraseña de coacción para verificación, se genera una señal de alarma.

12 Búsqueda de asistencia

Una vez que se verifica la identidad de un usuario, el registro de acceso se guardará en el dispositivo. Esta función permite a los usuarios verificar sus registros de acceso.

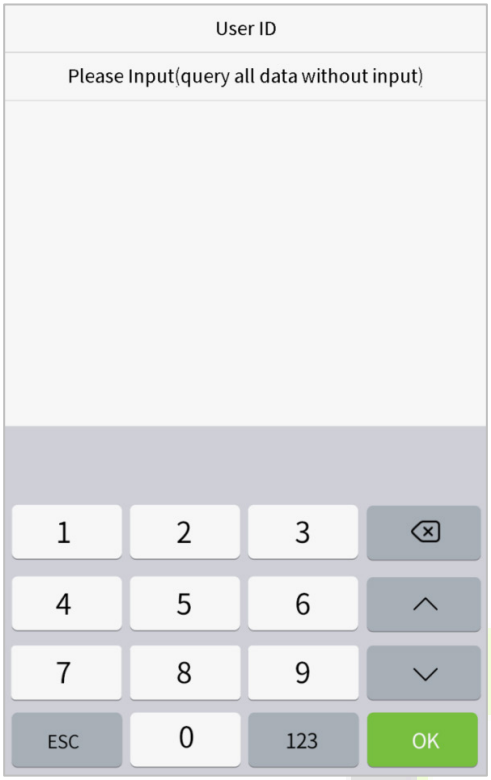
Hacer clic **Búsqueda de asistencia** sobre el **Menú principal** interfaz para buscar el registro de acceso / asistencia requerido.



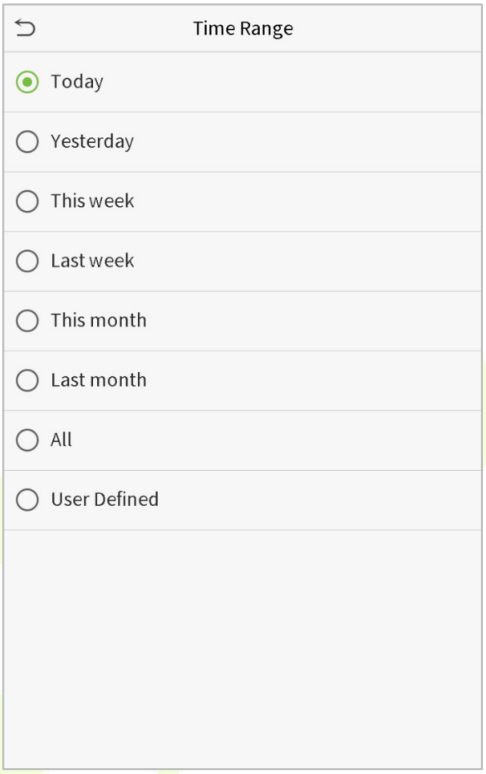
El proceso de búsqueda de fotos de asistencia y de lista de bloqueo es similar al de buscar registros de acceso. El siguiente es un ejemplo de búsqueda de registros de acceso.

Sobre el **Búsqueda de asistencia** interfaz, toque **Registro de acceso** para buscar el registro requerido.

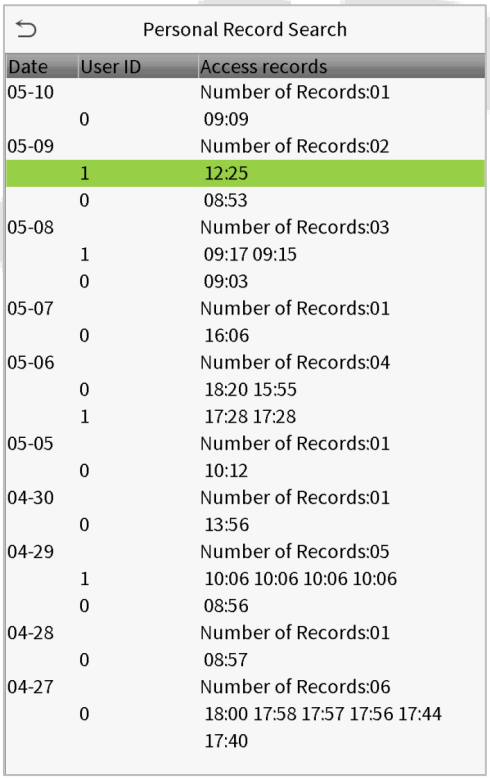
1. Introduzca la ID de usuario que se buscará y haga clic en Aceptar. Si desea buscar registros de todos los usuarios, haga clic en Aceptar sin ingresar ningún ID de usuario.



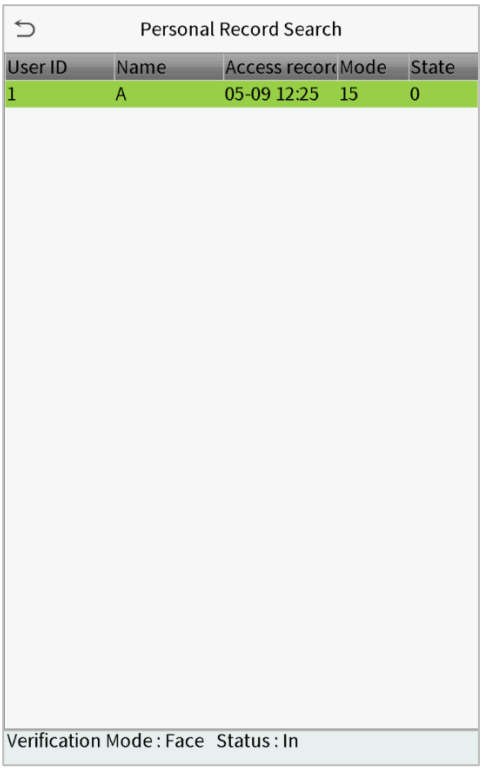
2. Seleccione el intervalo de tiempo en el que se deben buscar los registros.



3. Una vez que la búsqueda de registros sea exitosa. Toque el registro resaltado en verde para ver sus detalles.

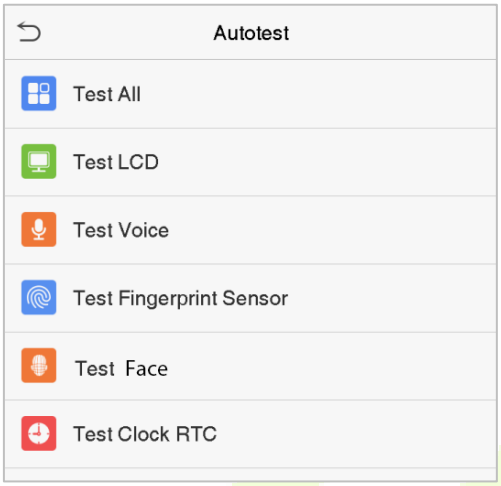


4. La siguiente figura muestra los detalles del registro seleccionado.



13 Auto prueba

Sobre el **Menú principal,** grifo **Auto prueba** para probar automáticamente si todos los módulos del dispositivo funcionan correctamente, que incluyen la pantalla LCD, la voz, el sensor de huellas dactilares, la cámara y el reloj en tiempo real (RTC).

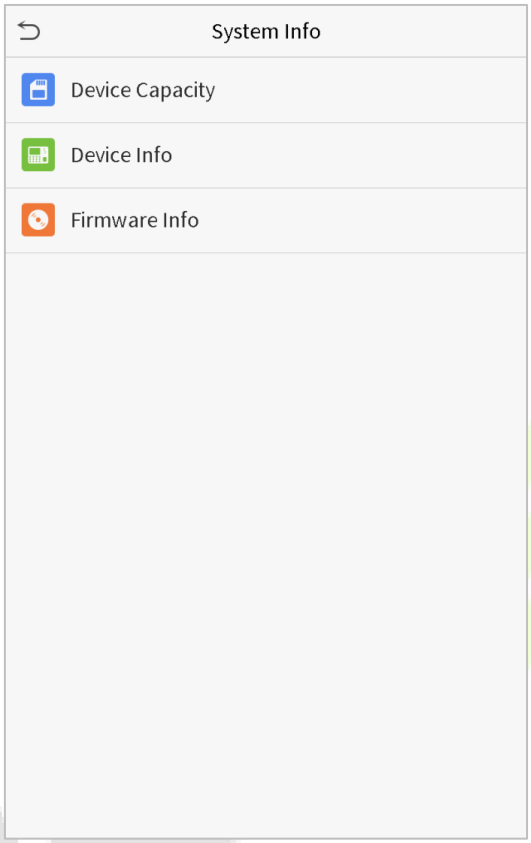


Función descriptiva

Nombre de la función	Descripción
Probar todo	Para probar automáticamente si la pantalla LCD, el audio, la cámara y el RTC son normales.
Prueba de LCD	Para probar automáticamente el efecto de visualización de la pantalla LCD mostrando a todo color, blanco puro y negro puro para comprobar si la pantalla muestra los colores normalmente.
Prueba de voz	Para probar automáticamente si los archivos de audio almacenados en el dispositivo están completos y la calidad de voz es buena.
Prueba del sensor de huellas dactilares	Para probar el sensor de huellas digitales presionando un dedo en el escáner para verificar si la imagen de la huella digital adquirida es clara. Cuando presiona un dedo en el escáner, la imagen de la huella digital se mostrará en la pantalla.
Cara de prueba	Para probar si la cámara funciona correctamente, verifique las imágenes tomadas para ver si son lo suficientemente claras.
Prueba de reloj RTC	Para probar el RTC. El dispositivo prueba si el reloj funciona con normalidad y precisión con un cronómetro. Toque la pantalla para comenzar a contar y presiónela nuevamente para dejar de contar.

14 Información del sistema

Sobre el **Menú principal,** grifo **Información del sistema** para ver el estado del almacenamiento, la información de la versión del dispositivo y la información del firmware.



Función descriptiva

Nombre de la función	Descripción
Capacidad del dispositivo	Muestra el almacenamiento de usuario del dispositivo actual, palma, huella digital, contraseña y almacenamiento facial, administradores, registros de acceso, fotos de lista de bloqueo y asistencia, y fotos de usuario.
Información del dispositivo	Muestra el nombre, el número de serie, la dirección MAC, la palma, el algoritmo de huellas dactilares y de rostro del dispositivo, la información de la versión, la información de la plataforma y el fabricante y la fecha de fabricación.
Información de firmware	Muestra la versión de firmware y otra información de versión del dispositivo.

15 Conéctese al software MTD ZKBioAccess

15,1 Establecer la dirección de comunicación

- **Lado del dispositivo**

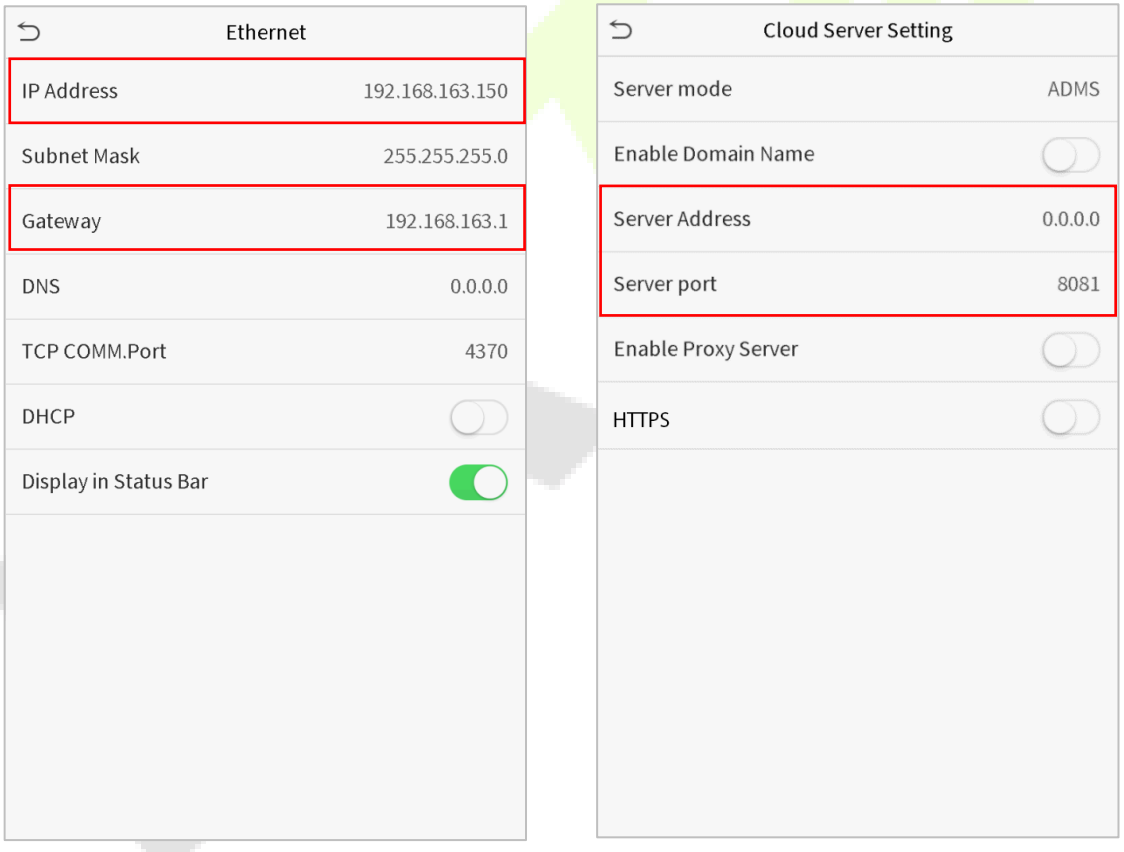
1. Grifo **COMM. > Ethernet** en el menú principal para configurar la dirección IP y la puerta de enlace del dispositivo.

   (**Nota:** La dirección IP debe poder comunicarse con el servidor MTD de ZKBioAccess, preferiblemente en el mismo segmento de red con la dirección del servidor)

2. En el menú principal, haga clic en **COMM. > Configuración del servidor en la nube** para configurar la dirección y el puerto del servidor.

   Dirección del servidor: Configure la dirección IP como del servidor MTD ZKBioAccess.

   Puerto de servicio: Configure el puerto del servidor como ZKBioAccess MTD (el predeterminado es 8088).



- **Lado del software**

Inicie sesión en el software ZKBioAccess MTD, haga clic en **Sistema> Comunicación> Monitor de comunicación** para configurar el puerto de servicio ADMS, como se muestra en la siguiente figura:

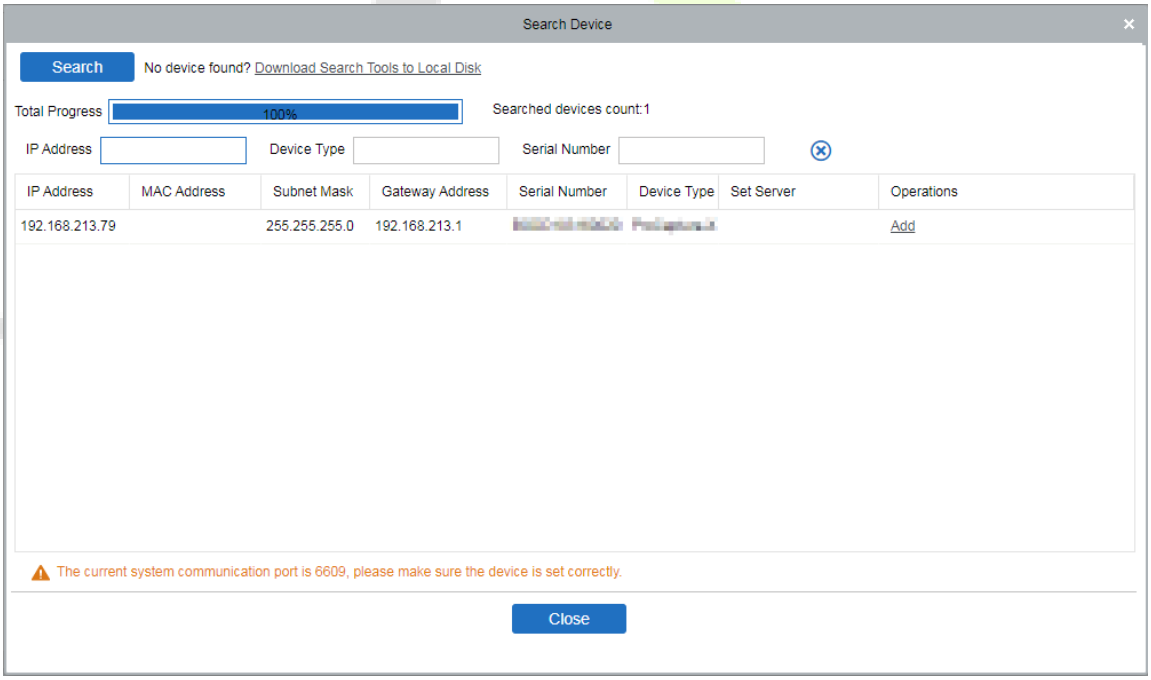
15,2 Agregar dispositivo en el software

Agregue el dispositivo buscando. El proceso es el siguiente:

1) Hacer clic **Control de acceso> Dispositivo> Dispositivo de búsqueda,** para abrir la interfaz de búsqueda en el software.

2) Hacer clic **Buscar,** y le indicará [**buscando** ……].

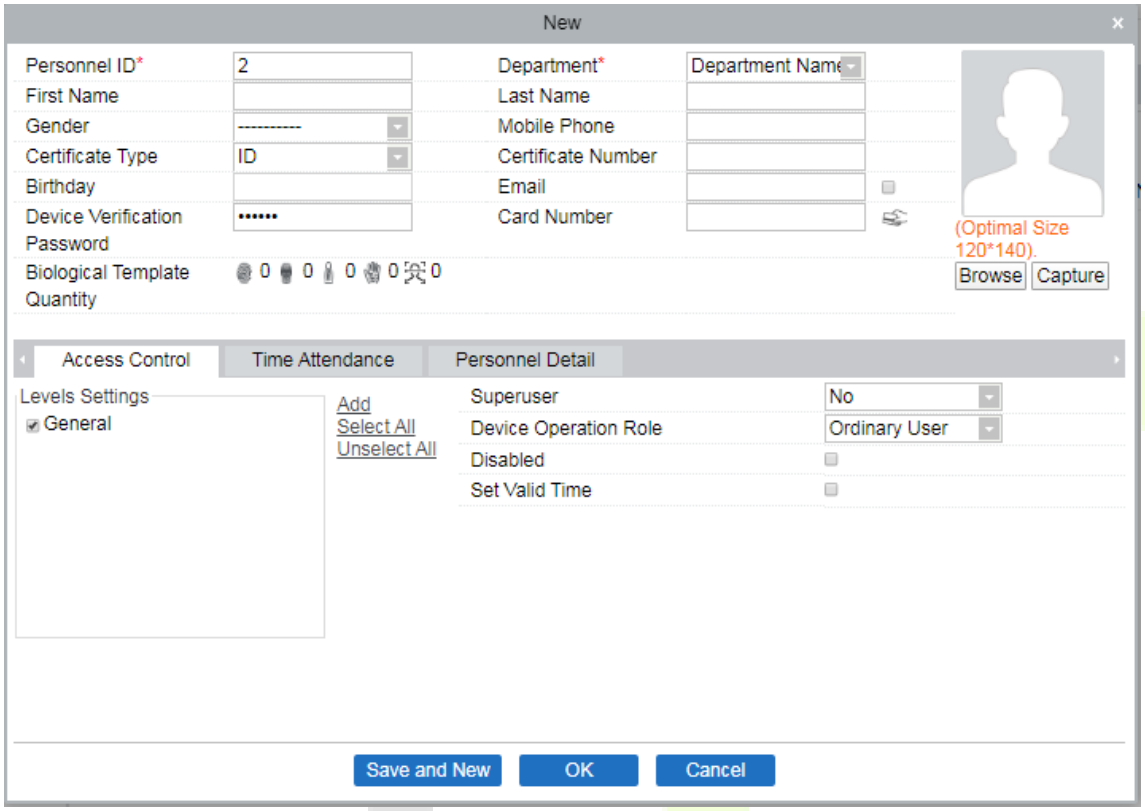
3) Después de la búsqueda, se mostrará la lista y el número total de controladores de acceso.



4) Haga clic en [**Añadir]** en la columna de operación, aparecerá una nueva ventana. Seleccione Tipo de icono, Área y Agregar a Nivele en cada menú desplegable y haga clic en [**OKAY]** para agregar el dispositivo.

15,3 Agregar personal al software

1. Hacer clic **Personal> Persona> Nuevo:**



2. Complete todos los campos obligatorios y haga clic en [**OKAY]** para registrar un nuevo usuario.

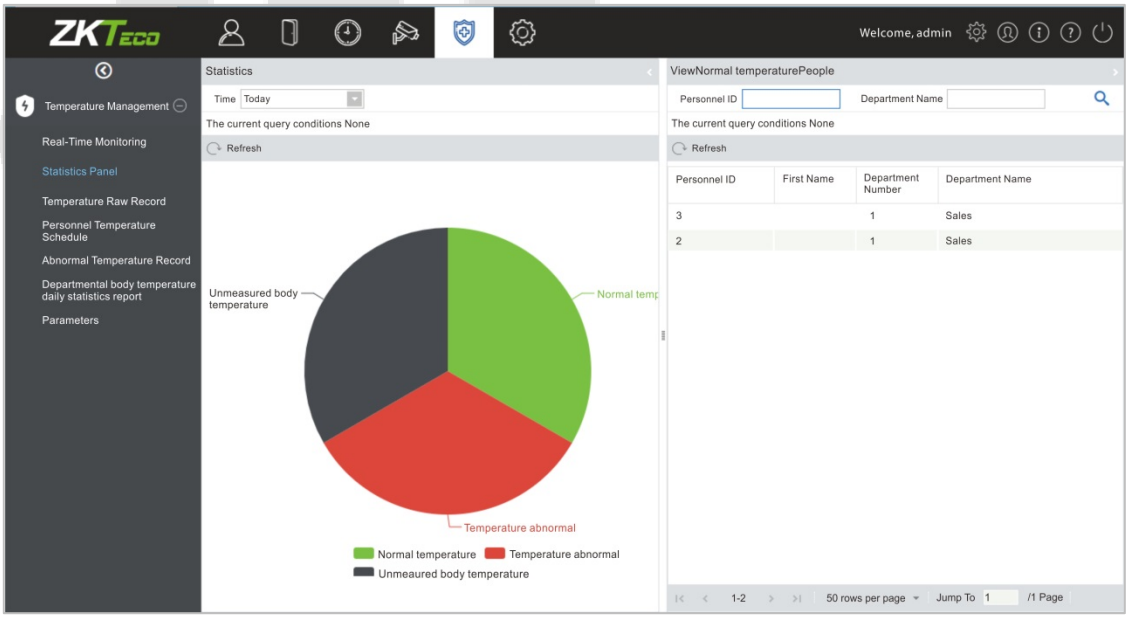
3. Hacer clic **Acceda> Dispositivo> Control de dispositivos> Sincronizar todos los datos con los dispositivos** para sincronizar todos los datos al dispositivo, incluidos los nuevos usuarios.

15,4 Monitoreo en tiempo real en el software ZKBioAccess MTD

1. Hacer clic **Prevención> Epidemia> Detección de temperatura> Monitoreo en tiempo real** para ver todos los eventos del personal presentes en los registros de temperatura anormal, sin máscaras y normal.

Los datos de usuario de temperatura corporal anormal se muestran en la barra de información de temperatura anormal automáticamente de acuerdo con la configuración del umbral de temperatura.

2. Hacer clic **Epidemia> Gestión de la temperatura> Panel de estadísticas** para ver el análisis de estadísticas datos en forma de gráfico circular y ver el personal con temperatura normal, temperatura anormal y temperatura corporal no medida. Además, la información detallada del personal se puede ver a la derecha haciendo clic en la categoría particular en el gráfico circular.



NOTA : Para otras operaciones específicas, consulte *Manual de usuario de ZKBioAccessMTD*.

Apéndice 1

Requisitos de la recopilación en vivo y el registro de imágenes de caras de luz visible

1) Se recomienda realizar el registro en un entorno interior con una luz adecuada fuente sin subexposición o sobreexposición.

2) No coloque el dispositivo hacia fuentes de luz exteriores como puertas o ventanas u otra luz fuerte fuentes.

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

4) Exponga la cara y la frente correctamente y no se cubra la cara y las cejas con su cabello.

5) Se recomienda mostrar una expresión facial sencilla. (Una sonrisa es aceptable, pero no cierre la ojos o inclinar la cabeza hacia cualquier orientación).

6) Se requieren dos imágenes para una persona con anteojos, una imagen con anteojos y la otra sin los anteojos.

7) No use accesorios como bufandas o mascarillas que puedan cubrir su boca o barbilla.

8) Mire a la derecha hacia el dispositivo de captura y ubique su rostro en el área de captura de imágenes como se muestra en la imagen de abajo.

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

10) Se recomienda una distancia de 50 cm a 80 cm para capturar la imagen. (la distancia es ajustable, sujeta a la altura del cuerpo).

Requisitos para datos de imagen facial digital con luz visible

La fotografía digital debe ser recta, coloreada, retratada a medias con una sola persona, y la persona debe ser inexplorada y casual. Las personas que usan anteojos deben quedarse para ponerse los anteojos para tomar fotografías.

- **Distancia del ojo**

Se recomiendan 200 píxeles o más con no menos de 115 píxeles de distancia.

- **Expresión facial**

Se recomienda rostro neutro o sonrisa con ojos naturalmente abiertos.

- **Gesto y Angel**

El ángulo de rotación horizontal no debe exceder ± 10 °, la elevación no debe exceder ± 10 ° y el ángulo de depresión no debe exceder ± 10 °.

- **Accesorios**

No se permiten máscaras ni anteojos de colores. El marco de los anteojos no debe cubrir los ojos y no debe reflejar la luz. Para personas con montura de anteojos gruesa, se recomienda capturar dos imágenes, una con anteojos y la otra sin anteojos.

- **Cara**

Rostro completo con contorno claro, escala real, luz distribuida uniformemente y sin sombras.

- **Formato de imagen**

Debe estar en BMP, JPG o JPEG.

- **Requisito de datos**

Debe cumplir con los siguientes requisitos:

1) Fondo blanco con ropa de color oscuro.

2) Modo de color verdadero de 24 bits.

3) Imagen comprimida en formato JPG con un tamaño máximo de 20 kb.

4) La resolución debe estar 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 la persona capturada deben estar abiertos y con un iris claramente visible.

8) Se prefiere una cara o sonrisa neutra, no se prefiere 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 cara o en el fondo. El nivel de contraste y luminosidad debe ser apropiado.

Apéndice 2

Declaración sobre el derecho a la privacidad

Queridos clientes:

Gracias por elegir este producto de reconocimiento biométrico híbrido, que fue diseñado y fabricado por ZKTeco. Como proveedor de renombre mundial de tecnologías básicas de reconocimiento biométrico, estamos constantemente desarrollando e investigando nuevos productos y nos esforzamos por seguir las leyes de privacidad de cada país en el que se venden nuestros productos.

Declaramos que:

1. Todos nuestros dispositivos de reconocimiento de huellas dactilares de usuarios capturan solo características, no imágenes de huellas dactilares, y no incluyen protección de privacidad.
2. Ninguna de las características de la huella dactilar que capturamos se puede utilizar para reconstruir una imagen de la huella dactilar original y no implica la protección de la privacidad.
3. Como proveedor de este dispositivo, no asumiremos ninguna responsabilidad directa o indirecta por las consecuencias que puedan resultar de su uso de este dispositivo.
4. Si desea disputar cuestiones de derechos humanos o privacidad relacionados con el uso de nuestro producto, comuníquese directamente con su distribuidor.

Nuestros otros dispositivos de huellas dactilares de aplicación de la ley o herramientas de desarrollo pueden capturar las imágenes originales de las huellas dactilares del usuario. En cuanto a si esto constituye o no una infracción de sus derechos, comuníquese con su gobierno o el proveedor final del dispositivo. Como fabricante del dispositivo, no asumiremos ninguna responsabilidad legal.

Nota:

La ley incluye las siguientes disposiciones sobre la libertad personal de sus ciudadanos:

1. No habrá arresto, detención, registro o infracción ilegal de personas;

2. La dignidad personal está relacionada con la libertad personal y no debe ser violada;

3. No se puede violar la casa de un ciudadano;

4. El derecho a la comunicación de un ciudadano y la confidencialidad de esa comunicación están protegidos por la ley.

Como último punto, nos gustaría enfatizar aún más que el reconocimiento biométrico es una tecnología avanzada que sin duda se utilizará en los sectores de comercio electrónico, banca, seguros, judicial y otros en el futuro. Cada año, el mundo sufre pérdidas importantes debido a la naturaleza insegura de las contraseñas. Los productos biométricos sirven para proteger su identidad en entornos de alta seguridad.

Operación ecológica

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

El período de funcionamiento ecológico especificado para este producto no incluye baterías u otros componentes que se desgastan fácilmente y deben reemplazarse periódicamente. El período de funcionamiento ecológico de la batería es de 5 años.

Sustancias peligrosas o tóxicas y sus cantidades

Componente Nombre	Sustancia / elemento peligroso / tóxico					
	Plomo (Pb)	Mercurio (Hg)	Cadmium (Cd)	Polibrominato cromo (Cr6 +)	hexavalente Polibromado d Bifenilos (PBB)	Éteres de difenilo (PBDE)
Resistencia de chip	×	○	○	○	○	○
Condensador de chip	×	○	○	○	○	○
Inductor de chip	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
ESD componente	×	○	○	○	○	○
Zumbador	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Empulgueras	○	○	○	×	○	○

○ indica que la cantidad total de contenido tóxico en todos los materiales homogéneos está por debajo del límite especificado en SJ / T 11363-2006.

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

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

Parque industrial ZKTeco, No. 26, 188 Industrial Road, Tangxia

Town, Dongguan, China.

Teléfono: +86769-82109991 Fax

: +86 755 - 89602394

www.zkteco.com