

# Manual de usuario

## Serie SpeedFace-V5L

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](http://www.zkteco.com) .

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

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

### 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 prerrequisito 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, escribanos a [sales@zkteco.com](mailto:sales@zkteco.com) . Para saber más

sobre nuestras sucursales globales, visite [www.zkteco.com](http://www.zkteco.com) .

## Sobre la empresa

ZKTeco es uno de los fabricantes más grandes del mundo de lectores RFID y biométricos (huellas dactilares, faciales y de 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 a elevadores / pisos, torniquetes, controladores de puertas 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 las instalaciones de fabricación de última generación con certificación ISO9001 de ZKTeco de 700,000 pies cuadrados, 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 de la serie SpeedFace-V5L.

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 de GUI

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, abra la ventana [NewUser]
/	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

<b>1</b>	<b>VISIÓN GENERAL</b> .....	<b>7</b>
<b>2</b>	<b>INSTRUCCIONES DE USO</b> .....	<b>7</b>
<b>2.1</b>	<b>FINGER PAGES POSICIONAMIENTO</b> .....	<b>7 STAND BY PAGES POSICIÓN,</b>
<b>2.2</b>	<b>FACIAL MIPRESIÓN Y STAND BY PAGES POSICIÓN</b> .....	<b>8 PALM REGISTRO</b>
<b>2.3</b>	.....	<b>9 FAS REGISTRO</b> .....
<b>2.4</b>	.....	<b>10 STAND BY Y INTERFAZ</b> .....
<b>2.5</b>	.....	<b>11 VIRTUAL KEYBOARD</b> .....
<b>2.6</b>	<b>METRO ODA</b> .....	<b>14</b>
<b>2.7</b>		
2.7.1	VERIFICACIÓN DE LA PALMA .....	14
2.7.2	VERIFICACIÓN DE HUELLA DIGITAL .....	dieciséis
2.7.3	VERIFICACIÓN FACIAL .....	20
2.7.4	VERIFICACIÓN DE CONTRASEÑA .....	26
2.7.5	VERIFICACIÓN COMBINADA .....	29
<b>3</b>	<b>MENÚ PRINCIPAL</b> .....	<b>31</b>
<b>4</b>	<b>GESTIÓN DE USUARIOS</b> .....	<b>32</b>
<b>4.1</b>	<b>ADD USERS</b> .....	<b>32</b>
<b>4.2</b>	<b>SEARCH USERS</b> .....	<b>37</b>
<b>4.3</b>	<b>EDIT USERS</b> .....	<b>38</b>
<b>4.4</b>	<b>DELETE USERS</b> .....	<b>39</b>
<b>5</b>	<b>ROL DEL USUARIO</b> .....	<b>40</b>
<b>6</b>	<b>AJUSTES DE COMUNICACIÓN</b> .....	<b>43</b>
<b>6.1</b>	<b>NETWORK SETTINGS</b> .....	<b>43</b>
<b>6.2</b>	<b>PCC CONEXIÓN</b> .....	<b>45</b>
<b>6.3</b>	<b>LOUD SERVER SETTING</b> .....	<b>45</b>
<b>6.4</b>	<b>WIRELESS SETUP</b> .....	<b>46</b>
<b>7</b>	<b>AJUSTES DEL SISTEMA</b> .....	<b>50</b>
<b>7.1</b>	<b>RECOMENDADO Y TAYME</b> .....	<b>50 ACCESS LOGS SETTING</b>
<b>7.2</b>	.....	<b>51 FAS PARAMETROS</b> .....
<b>7.3</b>	.....	<b>52 FINGERPRINT PARAMETROS</b> .....
<b>7.4</b>	.....	<b>54 PALM PARAMETROS</b> .....
<b>7.5</b>	.....	<b>55 FACTORIA RESET</b> .....
<b>7.6</b>	<b>RETECCIÓN METRO GESTIÓN</b> .....	<b>57</b>
<b>7.7</b>		
<b>8</b>	<b>PERSONALIZAR AJUSTES</b> .....	<b>59</b>
<b>8.1</b>	<b>Y INTERFAZ AJUSTES</b> .....	<b>59</b>
<b>8.2</b>	<b>VOICE AJUSTES</b> .....	<b>61</b>

8,3	BANANAS CÓDULOS .....	61
8.4	PUNCH STATES OPCIONES .....	63
8.5	SHORTCUT KEYS METRO APLICACIONES .....	64
9	GESTIÓN DE DATOS .....	sesenta y cinco
9.1	DELETE re ATA .....	sesenta y cinco
10	CONTROL DE ACCESO.....	67
10,1	ACCESS CONTROL OPCIONES .....	68
10,2	toneladas YO ME SCHEDULE .....	69
10,3	HOLIDAY S AJUSTES .....	71
10,4	COMBINADO VERIFICACIÓN S AJUSTES .....	72
10,5	ANTI-PAGS Culo SETUP .....	74
10,6	DRESS OPCIONES S AJUSTES .....	75
11	BÚSQUEDA DE ASISTENCIA .....	76
12	AUTO PRUEBA .....	79
13	INFORMACIÓN DEL SISTEMA.....	80
14	CONECTARSE AL SOFTWARE ZKBIOACCESSMTD .....	81
14,1	SET EL COMUNICACIÓN UN DIRECCIÓN .....	81
14,2	ADD re EVICE AL SOFTWARE .....	82
14,3	ADD PAGS PERSONNEL EN EL SOFTWARE .....	83
14,4	RESEGUIMIENTO EN TIEMPO REAL DEL SOFTWARE .....	83
APÉNDICE 1	.....	85
	REQUIPOS PARA LHE COLLECTION Y REGISTRACIÓN DE VISIBLE LIGHT FAS y MAGES .....	85
	REQUIPOS PARA VISIBLE LIGHT re DIGITAL FAS y Mago re ATA .....	86
APÉNDICE 2	.....	88
	S DECLARACIÓN SOBRE EL RIGHT TO PRIVACY .....	88
	.....	89
		88 E CO-AMIGABLE OPERACIÓN

## 1 Visión general

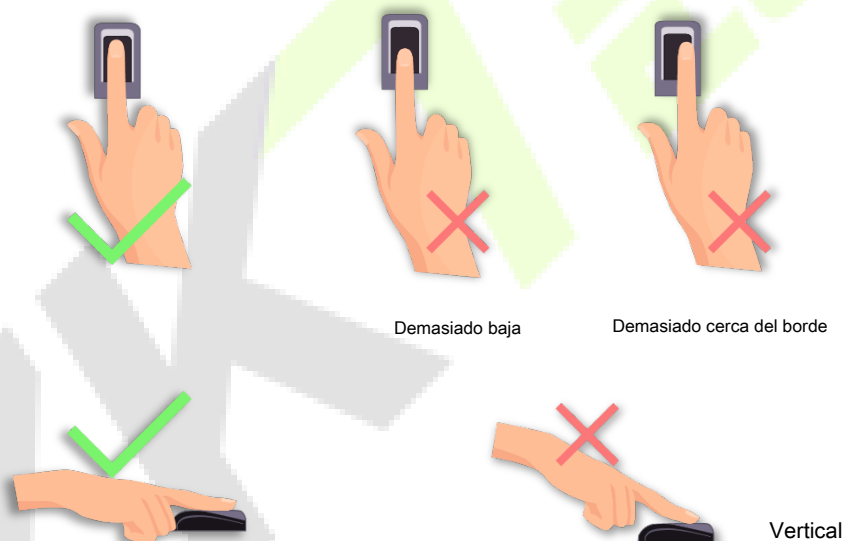
Este documento describe el procedimiento operativo de **Serie SpeedFace-V5L** dispositivo. Los módulos operativos del dispositivo incluyen administración de usuarios, asignación de roles de usuario, comunicación del dispositivo, detección de temperatura y máscara, control de acceso, etc. El dispositivo admite el acceso sin problemas de los usuarios a las instalaciones sin comprometer ningún aspecto de seguridad, lo que garantiza la protección.

**Nota:** No todos los productos tienen la función marcada con ★, prevalecerá el producto real.

## 2 Instrucciones de uso

### 2.1 Posicionamiento de dedos

**Dedos recomendados:** dedos índice, medio o anular; Evite usar el pulgar o el meñique, ya que es difícil presionarlos con precisión sobre el lector de huellas digitales.

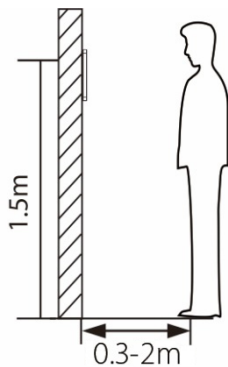


**Nota:** Utilice el método correcto cuando presione con los dedos el lector de huellas digitales para registrarse e identificarse. Nuestra empresa no asumirá ninguna responsabilidad por problemas de reconocimiento que puedan resultar del uso incorrecto del producto. Nos reservamos el derecho de interpretación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



## 2.2 Posición de pie, expresión facial y postura de pie

### Distancia recomendada



Se recomienda que la distancia entre el dispositivo y un usuario cuya altura esté entre 1,55 y 1,85 m sea de 0,3 a 2 m. Los usuarios pueden moverse ligeramente hacia adelante y hacia atrás para mejorar la calidad de las imágenes faciales capturadas.

### Expresión facial y postura de pie.

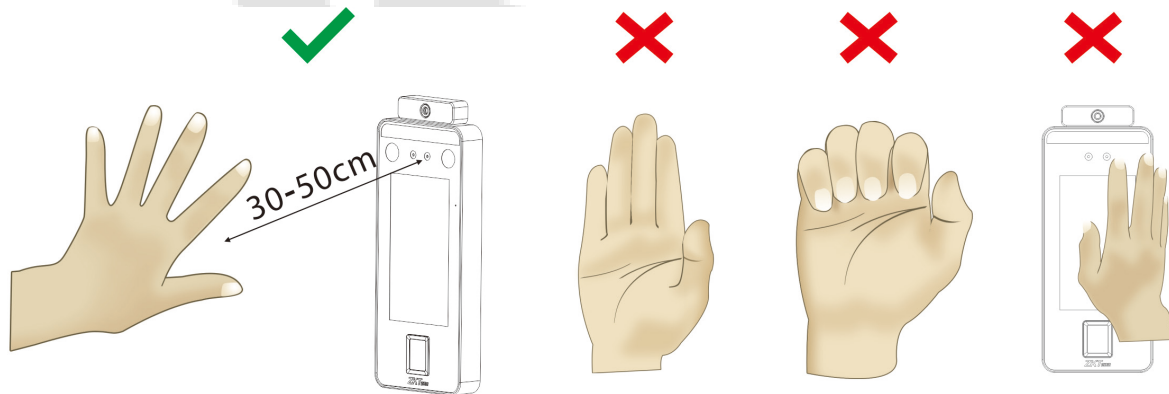




**Nota:** Durante la inscripción y la verificación, mantenga una expresión facial natural y una postura de pie.

### 2.3 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.

## 2.4 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 página se parece a la que se muestra a continuación:



### Métodos de autenticación y registro facial

#### Instrucciones 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 la expresión facial. (sonriendo, dibujado, guiñando un ojo, etc.)
- Si no sigue las instrucciones que aparecen en la 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 solo una persona a la vez.
- Se recomienda que un usuario con gafas registre ambos rostros con y sin gafas.

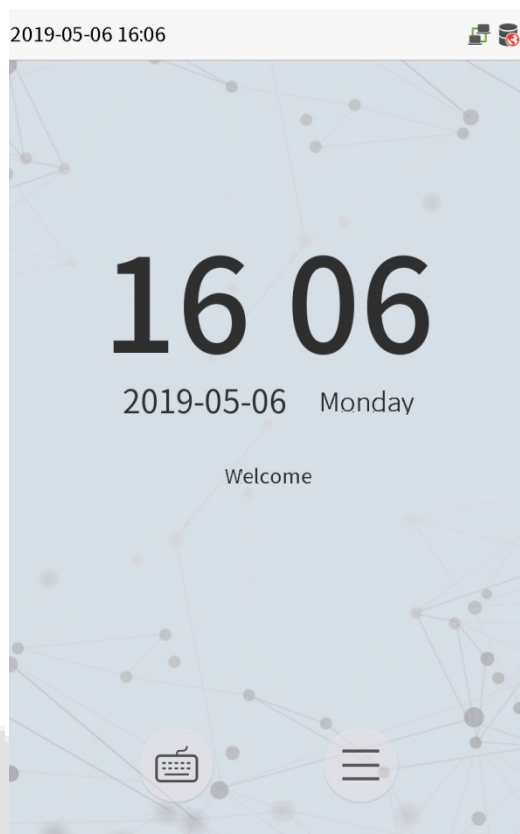
#### Instrucciones para autenticar un rostro

- Asegúrese de que la cara aparezca dentro del área de detección que se muestra en la pantalla del dispositivo.
- Si se han cambiado los anteojos, la autenticación puede fallar. Si se ha registrado la cara sin gafas, autentique la cara sin gafas. Si solo se ha registrado la cara con gafas, autentique nuevamente 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 anteojos de sol, la autenticación puede fallar. No cubra la cara, permita que el dispositivo reconozca tanto las cejas como la cara.


## 2.5 Interfaz de espera

Después de conectar la fuente de alimentación, la interfaz aparece como se muestra a continuación:

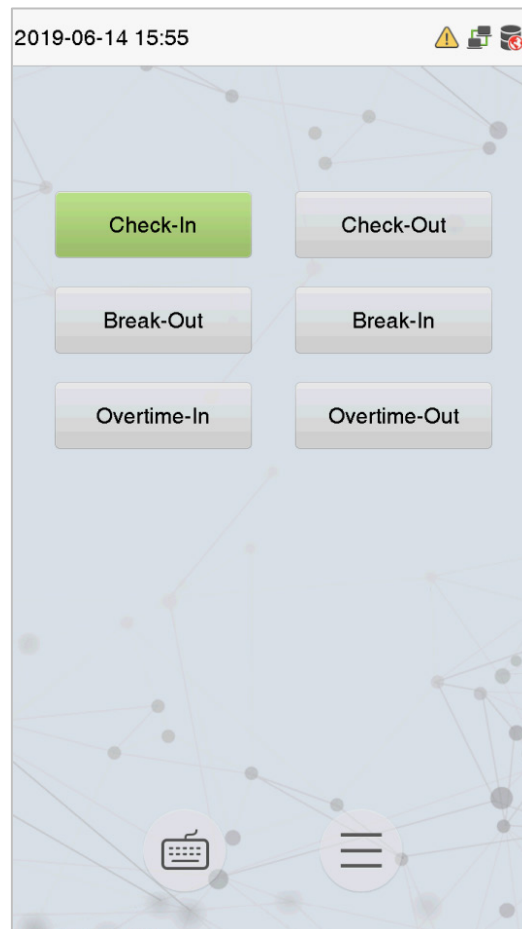


### Nota:

1 ) Hacer clic  para abrir la interfaz para ingresar el ID de usuario.

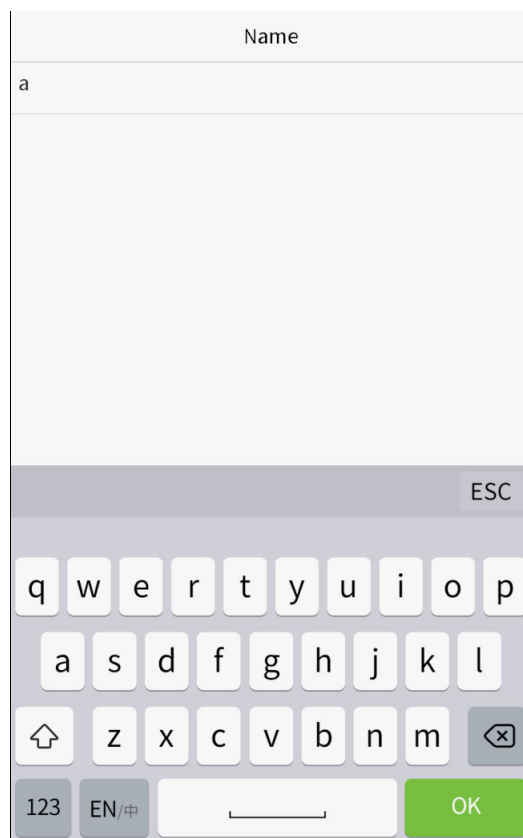
2 ) Cuando no haya ningún superadministrador registrado en el dispositivo, haga clic en  para entrar en el menú. Después al configurar el superadministrador, se requiere la verificación del superadministrador antes de ingresar a la operación del menú. Para la seguridad del dispositivo, se recomienda registrar un superadministrador la primera vez que use el dispositivo.

3 ) ★ El cambio de estado de perforación se puede realizar directamente utilizando las teclas de acceso directo de la pantalla. Haga clic en cualquier lugar en la pantalla sin iconos, y aparecen seis teclas de acceso directo, como se muestra en la siguiente figura:



Presione la tecla de método abreviado correspondiente para seleccionar el estado de perforación actual, que se muestra en verde. Por favor refiérase a "[8.5 Asignaciones de teclas de método abreviado](#)" a continuación para el método de operación específico.

## 2.6 Teclado virtual



**Nota:** El dispositivo admite la entrada de caracteres, números y símbolos chinos e ingleses. Haga clic en [ **En** ] para cambiar al teclado en inglés. Prensas [ **123** ] para cambiar al teclado numérico y de caracteres especiales, y haga clic en [ **A B C** ] para volver al teclado alfabético. Haga clic en el cuadro de entrada y aparecerá el teclado virtual. Haga clic en [ **ESC** ] para salir de la pantalla del teclado.

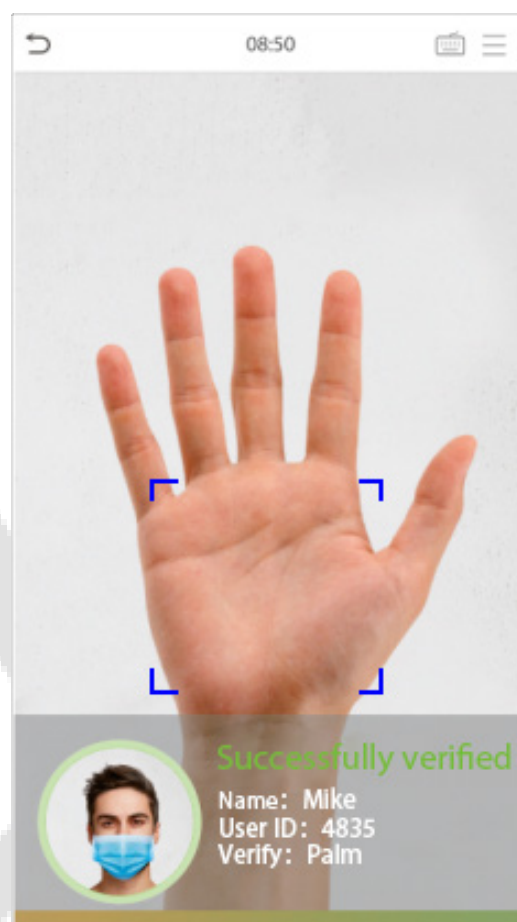
## 2.7 Modo de verificación

### 2.7.1 PalmVerification


#### 1: N (uno a muchos) modo de verificación de palma

Este modo de verificación compara la imagen de la palma recopilada por el módulo de la palma con toda la plantilla de datos de la palma del dispositivo.

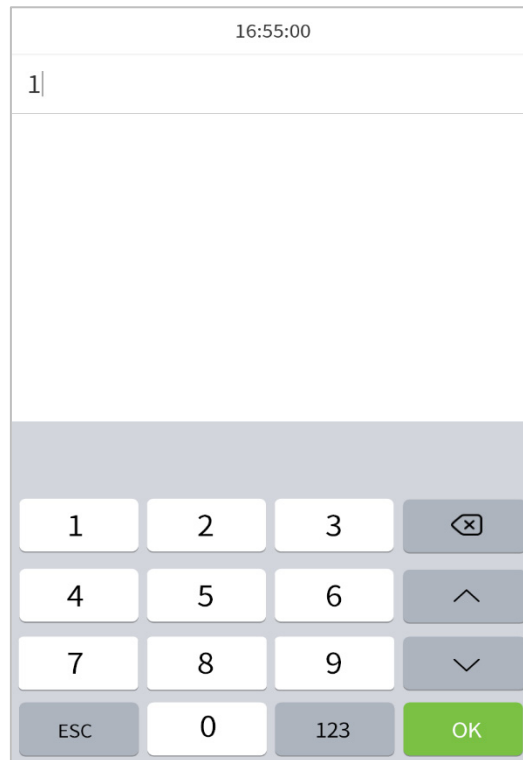
El dispositivo distinguirá automáticamente entre el modo de verificación de la palma y el rostro. Coloque la palma de la mano en el área que pueda recoger el módulo de la palma, de modo que el dispositivo cambie automáticamente al modo de verificación de la palma.



#### 1: 1 (uno a uno) modo de verificación de palma

Haga clic en el  en la pantalla principal para abrir el modo de verificación de palma 1: 1 (uno a uno).

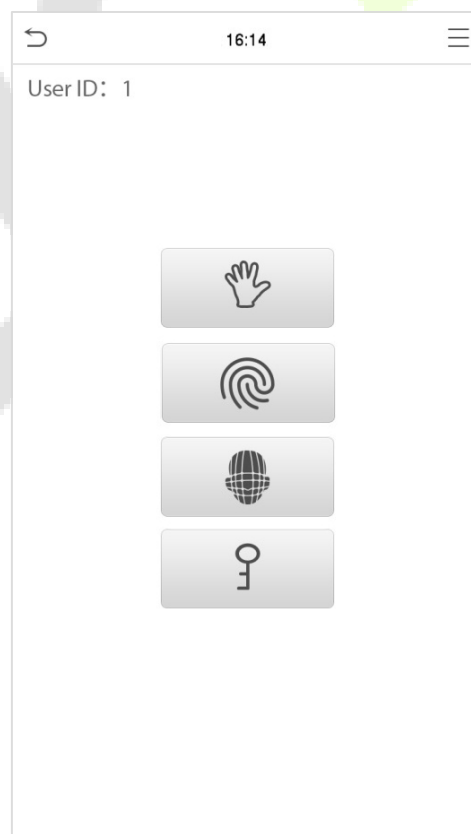
1. Ingrese el ID de usuario y presione [OK].



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



para ingresar al modo de verificación de palma.





## 2.7.2 Verificación de huellas dactilares

### Modo de verificación de huellas dactilares 1: N (uno a muchos)

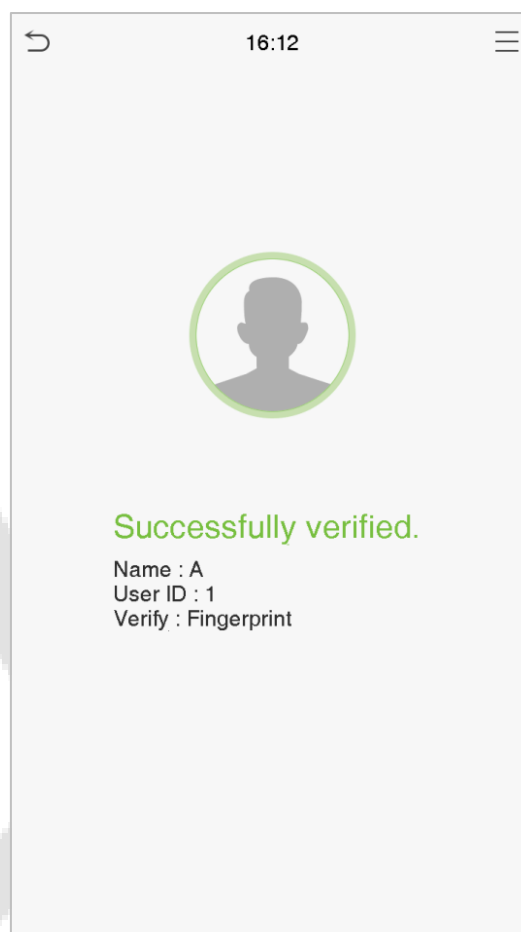
Compara la huella digital que se está presionando en el lector de huellas digitales con todos los datos de huellas digitales almacenados en el dispositivo.

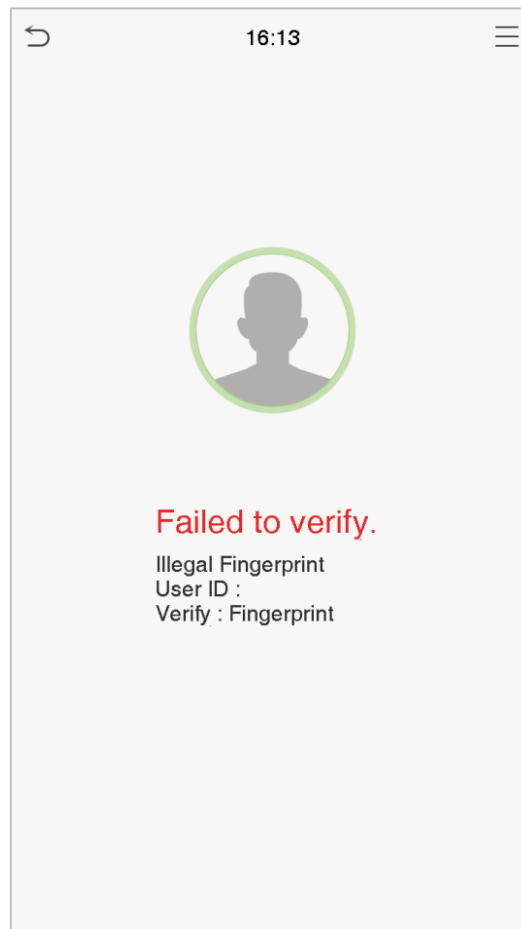
El dispositivo ingresará al modo de autenticación de huellas digitales cuando un usuario presione su dedo sobre el escáner de huellas digitales.

Siga la forma correcta de colocar el dedo en el sensor. Para obtener más información, consulte [2.1 Dedo](#)

[Posicionamiento.](#)

### La verificación es exitosa:



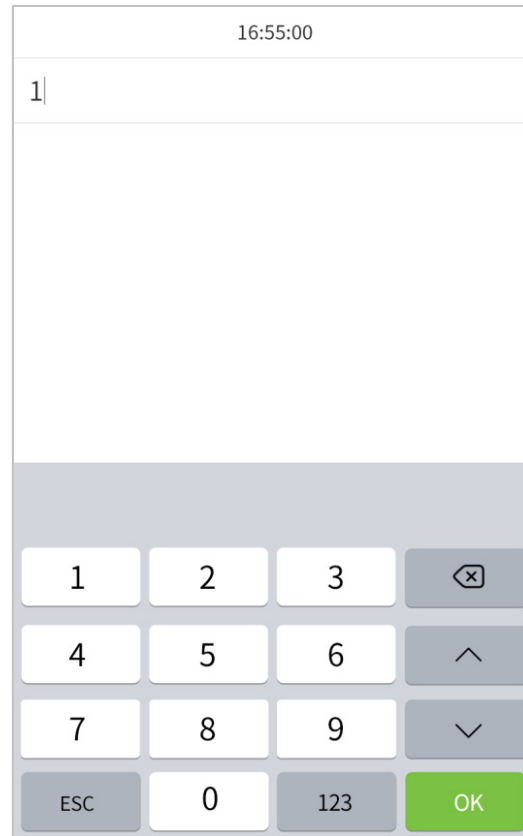
**Error de verificación:****Modo de verificación de huellas dactilares 1: 1 (uno a uno)**

Compara la huella dactilar que se presiona 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.

1. Ingrese el ID de usuario y presione [OK].



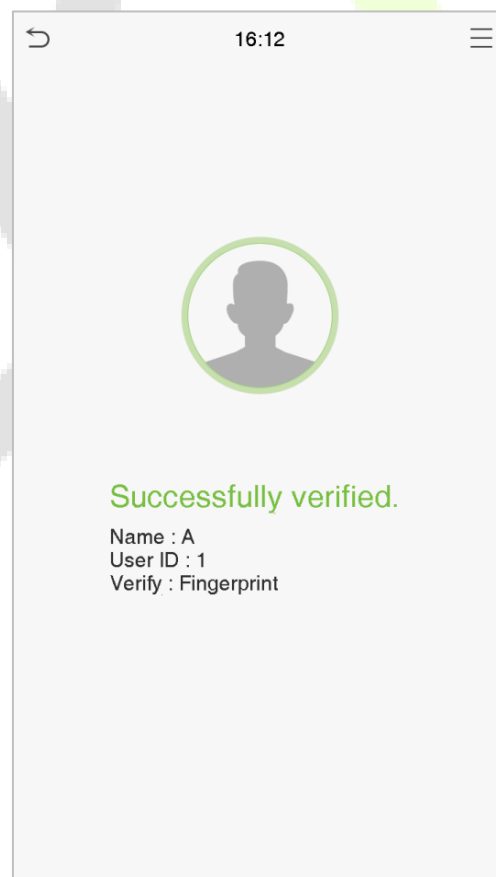
Si el usuario ha registrado plam, rostro y contraseña además de sus huellas dactilares, y el método de verificación está configurado como verificación de palma / huella dactilar / rostro / contraseña, aparecerá la siguiente pantalla. Selecciona el

icono de huella digital  para ingresar al modo de verificación de huellas dactilares.

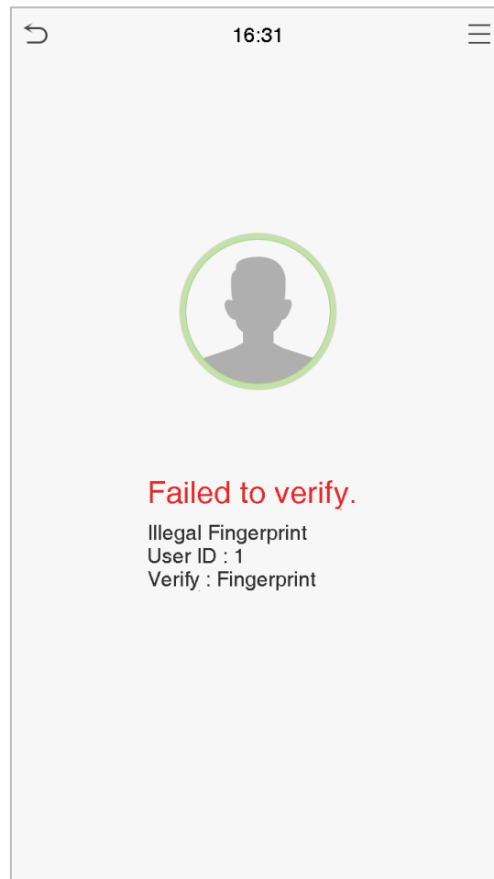


2. Presione la huella digital para verificar.

3. La verificación es exitosa.



#### 4. Error de verificación.

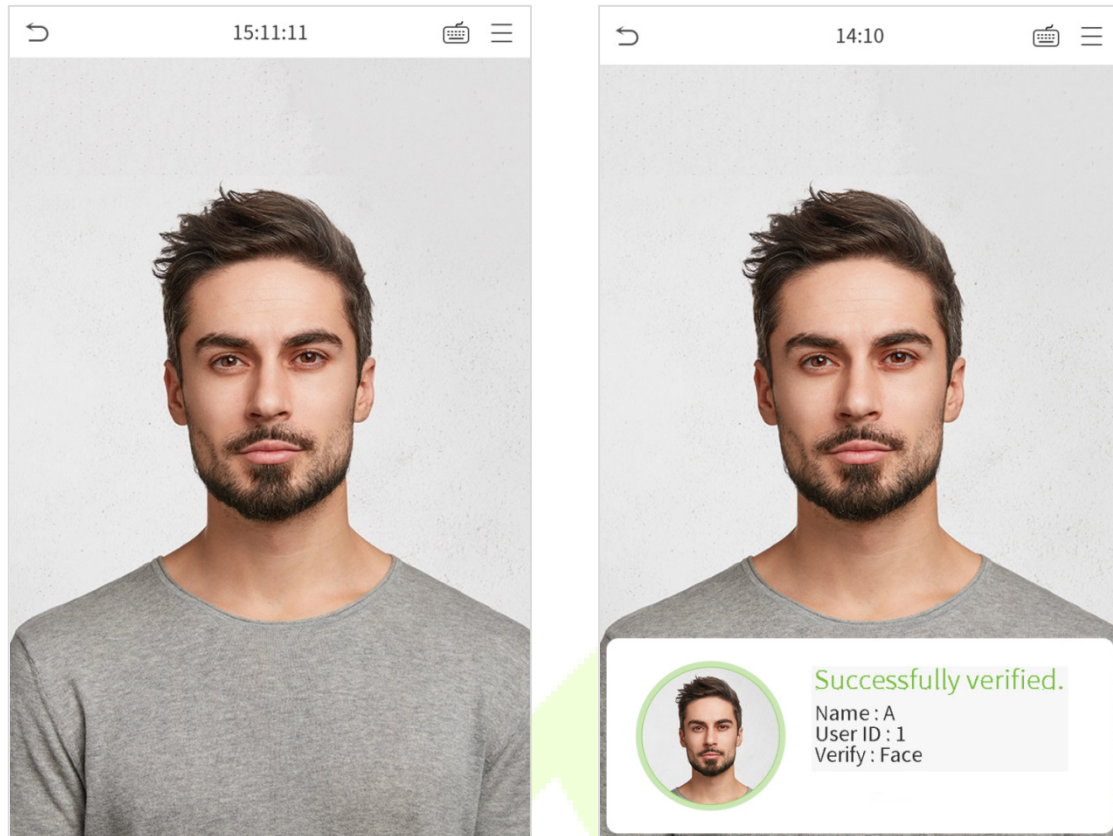


### 2.7.3 Verificación facial

#### Verificación facial 1: N (uno a muchos)

##### 1. Verificación convencional

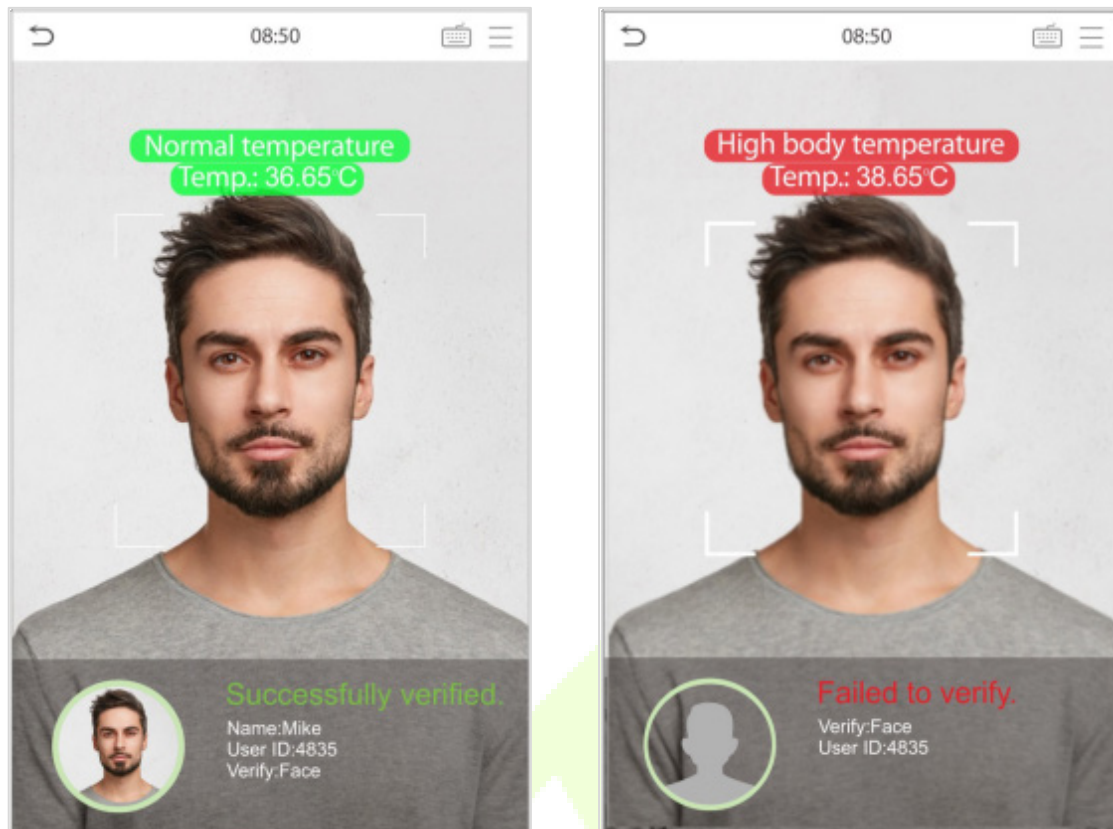
Este modo de verificación compara las imágenes faciales adquiridas con todos los datos faciales registrados en el dispositivo. A continuación, se muestra el cuadro de aviso emergente del resultado de la comparación.



## 2. Habilitar la detección de temperatura con infrarrojos ★

Cuando el usuario habilitó el **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 verificar la cara. La siguiente es la ventana emergente de la interfaz de solicitud de resultados de comparación.

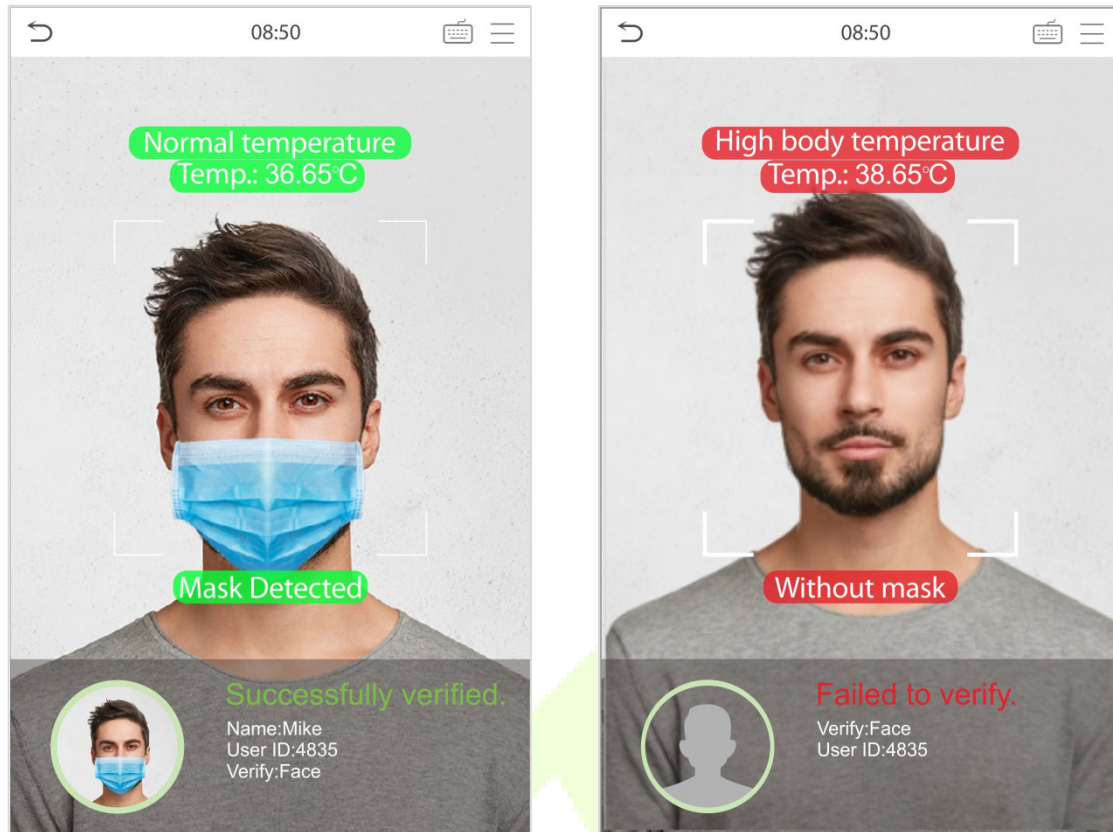
**Nota:** Esta función solo es aplicable a productos con módulo de detección de temperatura.



### 3. Habilitar detección de máscara ★


Cuando el usuario habilitó el **Habilitar la detección de máscara** función, el dispositivo identificará si el usuario está usando una máscara o no. La siguiente es la ventana emergente de la interfaz de solicitud de resultados de comparación.

**Nota:** Esta función solo es aplicable a productos con módulo de detección de temperatura.



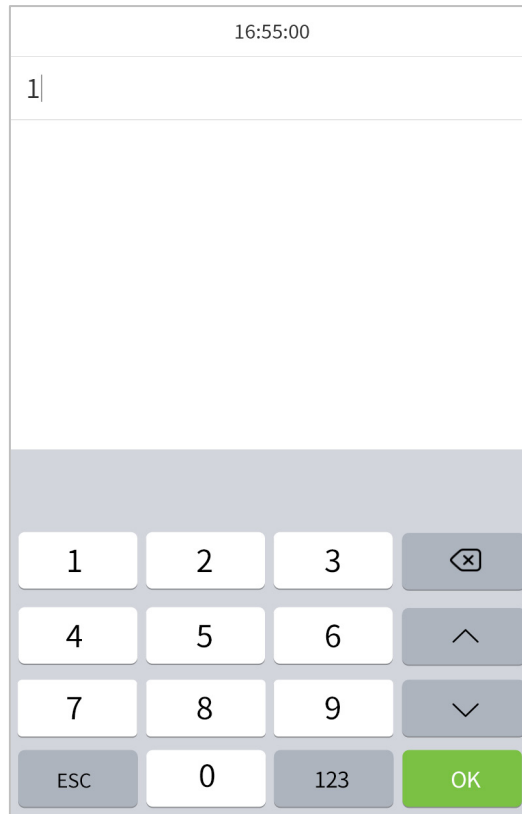
### **Verificación facial 1: 1 (uno a uno)**

Este modo de verificación compara la cara capturada por la cámara con la plantilla facial relacionada con la ID de usuario ingresada.


prensa  en la interfaz principal e ingrese al modo de verificación facial 1: 1 (uno a uno).

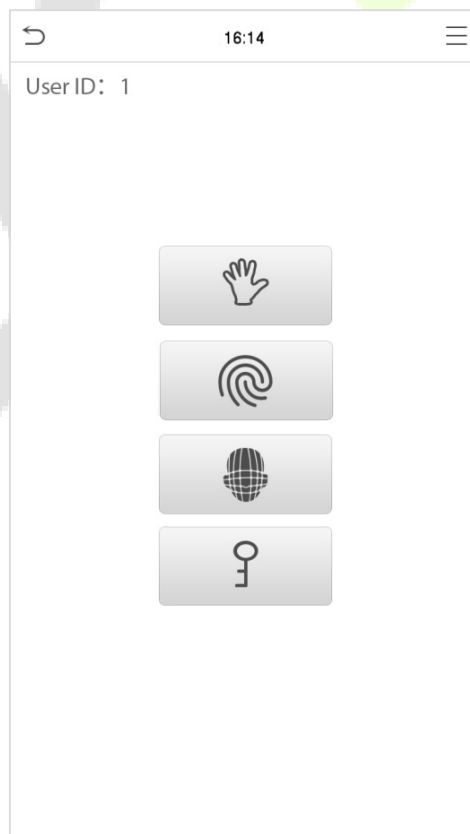
Introduzca la ID de usuario y haga clic en [Aceptar].



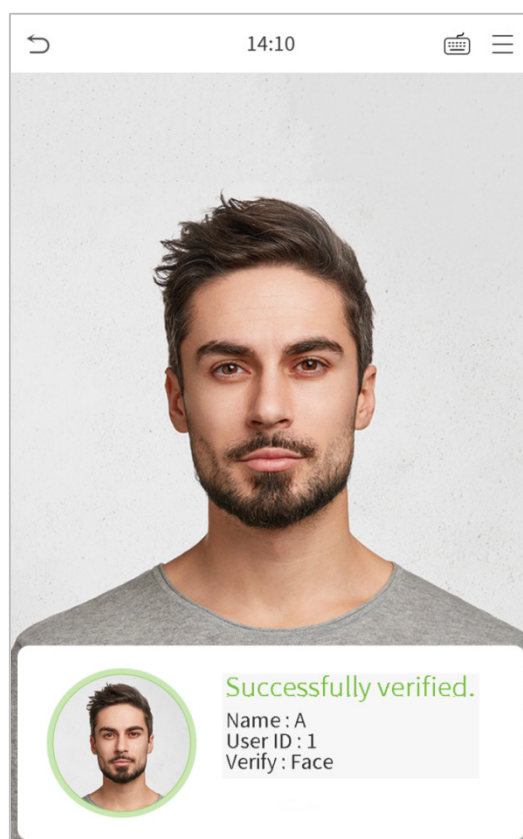


Si un empleado registra palma, huella digital y contraseña además del rostro, aparecerá la siguiente pantalla

Aparecer. Selecciona el  para ingresar al modo de verificación facial.




Después de una verificación exitosa, aparecerá el cuadro de aviso "verificado exitosamente".



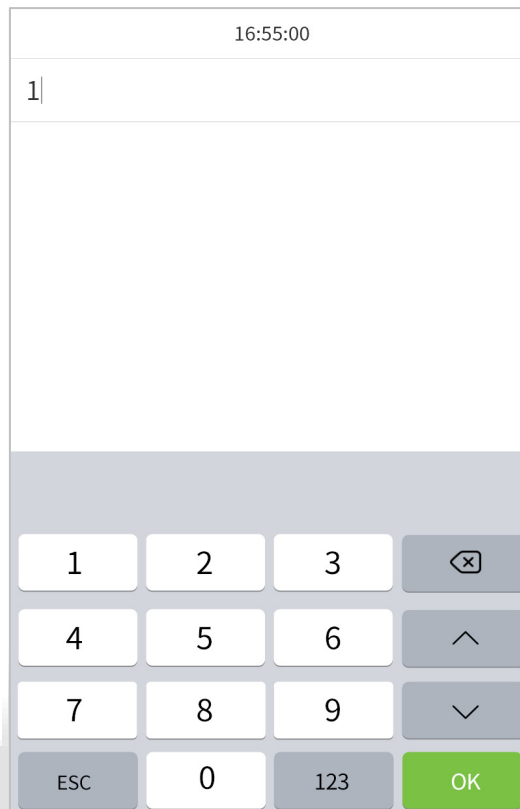
Si la verificación falla, aparecerá el mensaje "¡Por favor, ajuste su posición!".

## 2.7.4 Verificación de contraseña


El modo de verificación de contraseña compara la contraseña ingresada con el ID de usuario y la contraseña registrados.

Haga clic en el  en la pantalla principal para abrir el modo de verificación de contraseña 1: 1 (uno a uno).

1. Ingrese el ID de usuario y presione [OK].

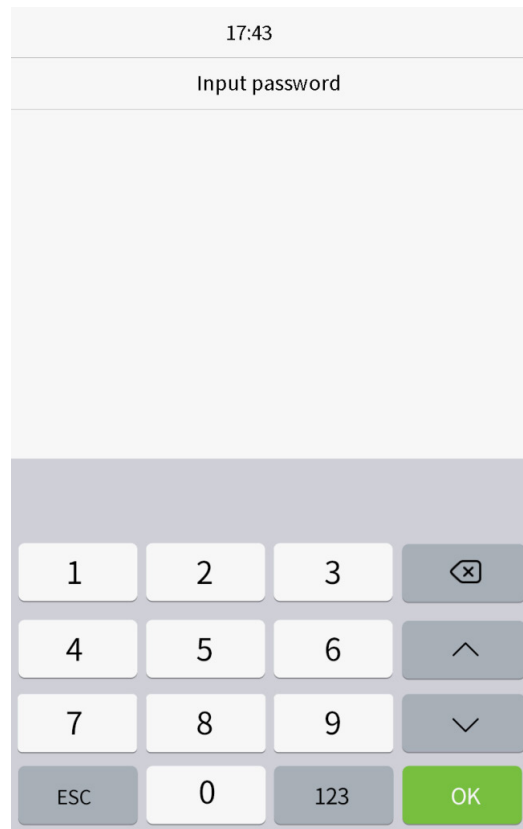


Si un empleado registra palma, huella digital y rostro además de la contraseña, aparecerá la siguiente pantalla

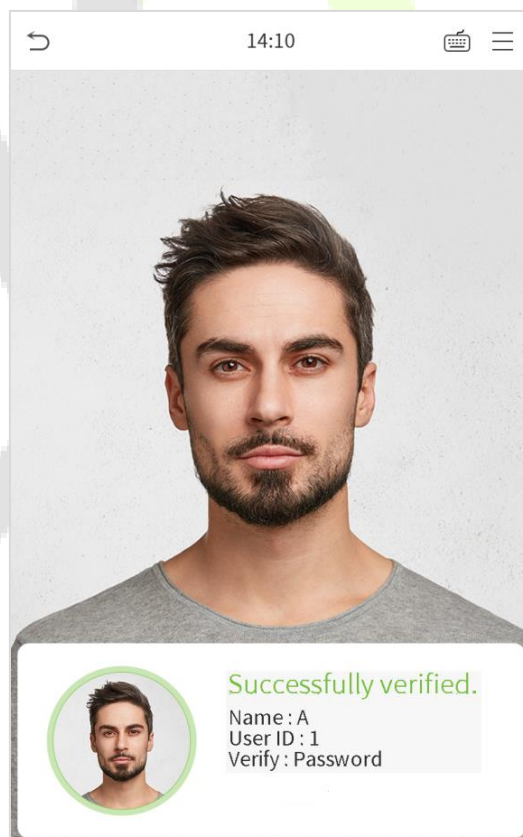
Aparecer. Selecciona el  para ingresar al modo de verificación de contraseña.

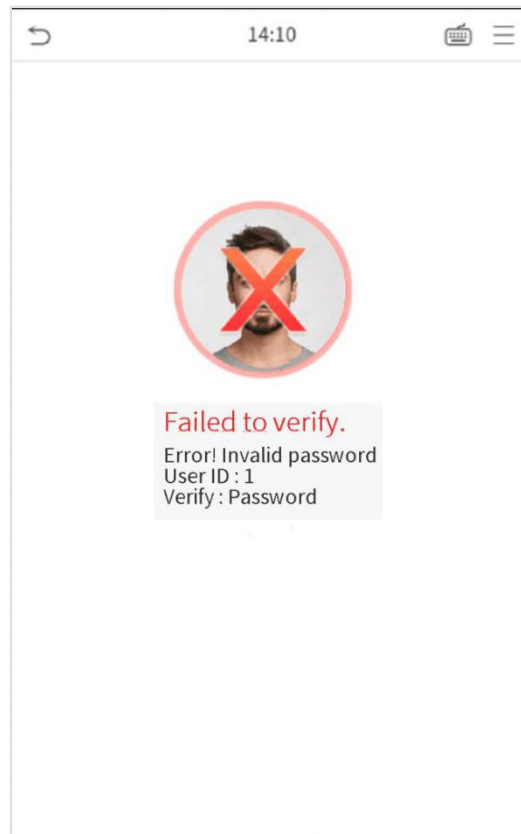


2. Ingrese la contraseña y presione [OK].

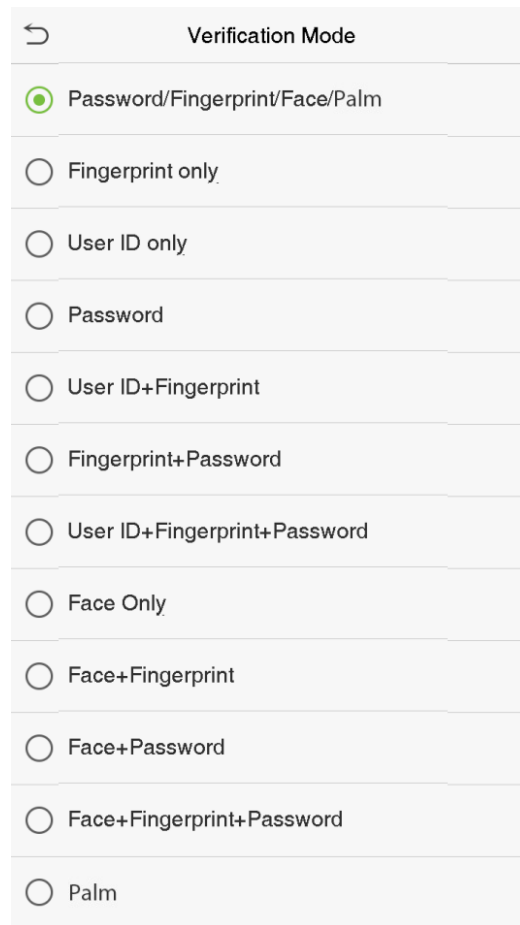


**Verificación exitosa:**



**Verificación fallida:****2.7.5 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 12 combinaciones de verificación diferentes, como se muestra a continuación:



Verification Mode

- Password/Fingerprint/Face/Palm
- Fingerprint only
- User ID only
- Password
- User ID+Fingerprint
- Fingerprint+Password
- User ID+Fingerprint+Password
- Face Only
- Face+Fingerprint
- Face+Password
- Face+Fingerprint+Password
- Palm


**Nota:**

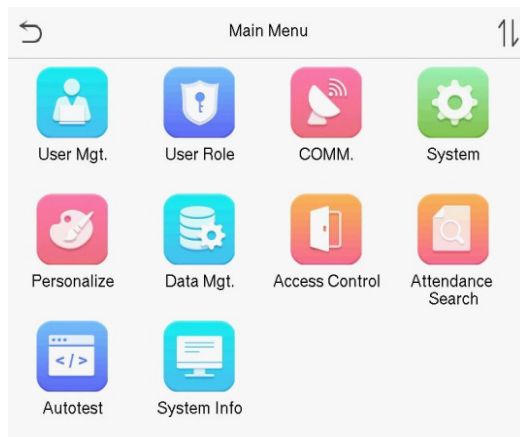
1 ) "/" significa "o" y "+" significa "y".

2 ) Debe registrar la información de verificación requerida antes de usar la verificación de combinación

modo, de lo contrario, la verificación puede fallar. Por ejemplo, si un usuario usa Registro facial pero el modo de verificación es Cara + Contraseña, este usuario nunca pasará la verificación.

### 3 Menú principal

presiona  en la interfaz inicial para ingresar al menú principal, como se muestra a continuación:





Menú	Descripción
<b>Administrador de usuarios</b>	Para agregar, editar, ver y eliminar la información básica sobre un usuario.
<b>Rol del usuario</b>	Para establecer el alcance del permiso del rol personalizado y el registrador, es decir, los derechos para operar el sistema.
<b>COMM.</b>	Para configurar los parámetros relevantes de la red, la conexión de la PC, el servidor en la nube y Wiegand.
<b>Sistema</b>	Para configurar los parámetros relacionados con el sistema, incluyendo fecha y hora, registros de acceso, plantillas faciales, plantillas de palma, plantillas de huellas dactilares, restablecimiento a la configuración de fábrica, gestión de temperatura y gestión de detección.
<b>Personalizar</b>	Esto incluye la interfaz de usuario, voz, timbre, opciones de estado de marcado y configuraciones de asignaciones de teclas de acceso directo.
<b>DataMgt.</b>	Para eliminar todos los datos relevantes en el dispositivo.
<b>Control de acceso</b>	Para configurar los parámetros de la cerradura y el dispositivo de control de acceso correspondiente.
<b>Asistencia Buscar</b>	Consulte el registro de acceso especificado, verifique las fotos de asistencia y las fotos de la lista de bloqueo.
<b>Auto prueba</b>	Para probar automáticamente si cada módulo funciona correctamente, incluida la pantalla, el audio, la cámara y el reloj en tiempo real.
<b>Información del sistema</b>	Para ver la capacidad de datos, el dispositivo y la información de firmware del dispositivo actual.



## 4 Gestión de usuarios

### 4.1 Agregar usuarios

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

User Mgt.	
	New User
	All Users
	Display Style

Hacer clic **Nuevo Usuario**.

#### Registrar una identificación de usuario y un nombre

Ingrese la identificación de usuario y el nombre.

New User	
User ID	1
Name	Mike
User Role	Normal User
Palm	1
Fingerprint	1
Face	1
Password	*****
User Photo	1
Access Control Role	

#### Notas:

- 1 ) Un nombre de usuario puede contener 17 caracteres.
- 2 ) El ID de usuario puede contener de 1 a 9 dígitos por defecto.

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

4 ) Si aparece un mensaje "ID duplicado", debe elegir otro ID.

#### Configuración de la función del usuario

Hay dos tipos de cuentas de usuario: **Usuario normal** y **Super administrador**. Si ya hay un administrador registrado, los usuarios normales no tienen derechos para administrar el sistema y solo pueden acceder a las verificaciones de autenticación. El administrador posee todos los privilegios de administración. Si se establece una función personalizada, también puede seleccionar **rol definido por el usuario** permisos para el usuario.

Hacer clic **Rol del usuario** para seleccionar Usuario normal o Superadministrador.

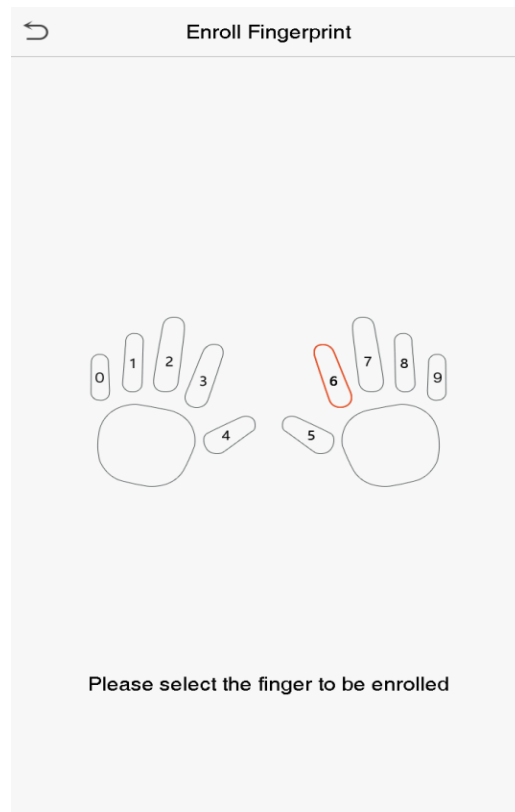


User Role	
<input checked="" type="radio"/>	Normal User
<input type="radio"/>	User Defined Role 1
<input type="radio"/>	Super Admin

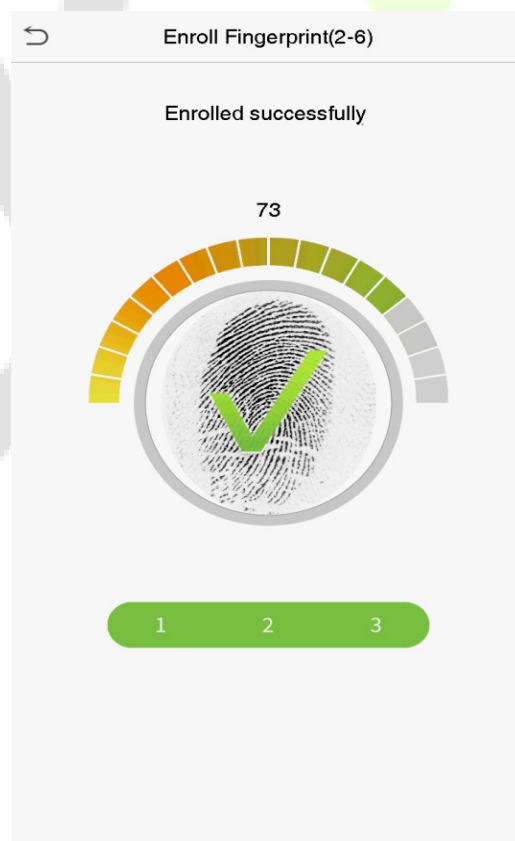
**Nota:** Si el rol de usuario seleccionado es el superadministrador, el usuario debe pasar la autenticación de identidad para acceder al menú principal. La autenticación se basa en los métodos de autenticación que ha registrado el superadministrador. Consulte [2.7 Método de verificación](#).

#### Registrar huella digital

Hacer clic **Huella dactilar** para abrir la página de registro de huellas digitales. Seleccione la huella dactilar que desea registrar.



Presione el mismo dedo en el lector de huellas dactilares tres veces. El verde indica que la huella digital se registró correctamente.



### Registrar palma

Hacer clic **Palma** para abrir la página de registro de la palma. Seleccione la palma que desea inscribir.



### Cara de registro

Hacer clic **Cara** para ingresar a la página de registro facial. Mire hacia la cámara y quédese quieto durante el registro facial. La interfaz de registro es la siguiente:



### Registrar contraseña

Hacer clic **Contraseña** para abrir la página de registro de contraseña. Ingrese una contraseña y vuelva a ingresarla. Hacer clic **OKAY**. Si las dos contraseñas ingresadas son diferentes, aparecerá el mensaje "La contraseña no coincide".

A screenshot of a mobile application interface for password registration. The title is "Password". Below the title is a text input field containing a single character. At the bottom of the screen is a numeric keypad with buttons for digits 1-9, 0, and 123. There are also buttons for backspace (x), up arrow, down arrow, and an "OK" button in green.

**Nota:** La contraseña puede contener de uno a ocho dígitos por defecto.

#### Registrar foto de usuario

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

Hacer clic **Foto de usuario**; haga clic en el icono de la cámara para tomar una foto. El sistema volverá a la interfaz de nuevo usuario después de tomar una foto.

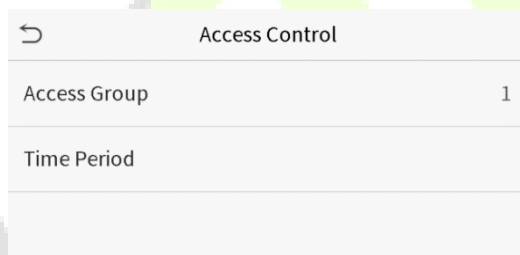
**Nota:** Al registrar un rostro, el sistema capturaré automáticamente una imagen como foto de usuario. Si no desea registrar una foto de usuario, el sistema establecerá automáticamente la imagen capturada como la foto predeterminada.

#### Rol de control de acceso

El control de acceso de usuario establece los derechos de desbloqueo de puertas de cada persona, incluido el grupo y el período de tiempo al que pertenece el usuario.

Hacer clic **Función de control de acceso** > **Grupo de acceso**, asignar 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.

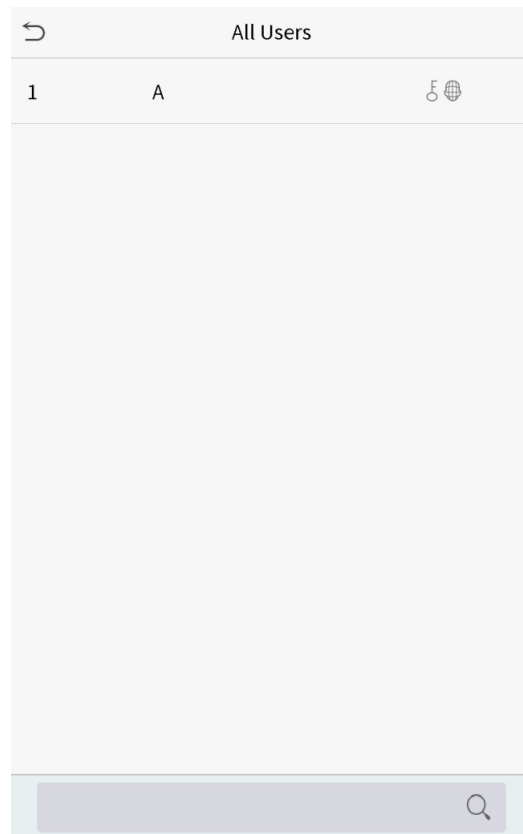
Hacer clic **Periodo de tiempo**, seleccione el período de tiempo a utilizar.



Access Control	
Access Group	1
Time Period	

## 4.2 Buscar usuarios

Haga clic en la barra de búsqueda en la lista de usuarios e ingrese la palabra clave de recuperación (la palabra clave puede ser una identificación, apellido o nombre completo). El sistema buscará los usuarios relacionados con la información.



### 4.3 Editar usuarios

Seleccione un usuario de la lista y haga clic en **Editar** para ingresar a la interfaz de usuario de edición.

User : 1 A	
Edit	
Delete	

Edit : 1 A	
User ID	1
Name	A
User Role	Normal User
Palm	1
Face	1
Password	*****
User Photo	0
Access Control Role	

**Nota:** La operación de editar un usuario es la misma que la de agregar un usuario, excepto que el ID de usuario no se puede modificar al editar un usuario. Para más detalles, consulte "[4.1 Agregar usuarios](#)".

#### 4.4 Eliminar usuarios

Seleccione un usuario de la lista y haga clic en **Eliminar** para ingresar a la interfaz de borrado de usuario. Seleccione la información de usuario que desea eliminar y haga clic en **OKAY**.

**Nota:** Si selecciona **Borrar usuario**, toda la información del usuario será eliminada.

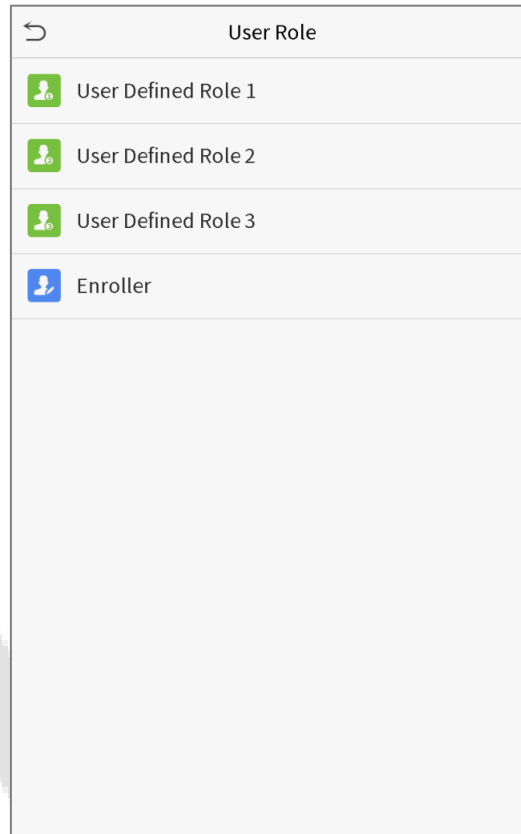


## 5 Rol del usuario

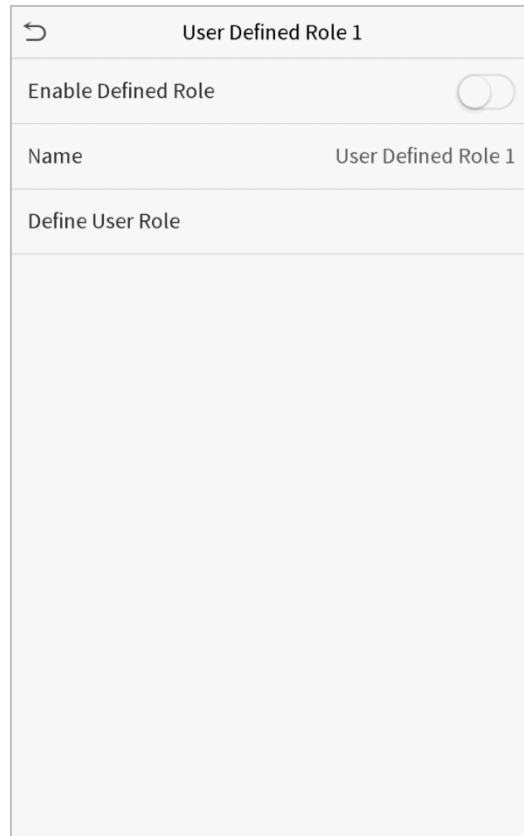
Si necesita asignar algunos permisos específicos a ciertos usuarios, puede editar el "Rol definido por el usuario" en el **Rol del usuario** menú.

Puede establecer el alcance del permiso del rol personalizado (hasta 3 roles) y el registrador, es decir, el alcance del permiso del menú de operaciones.

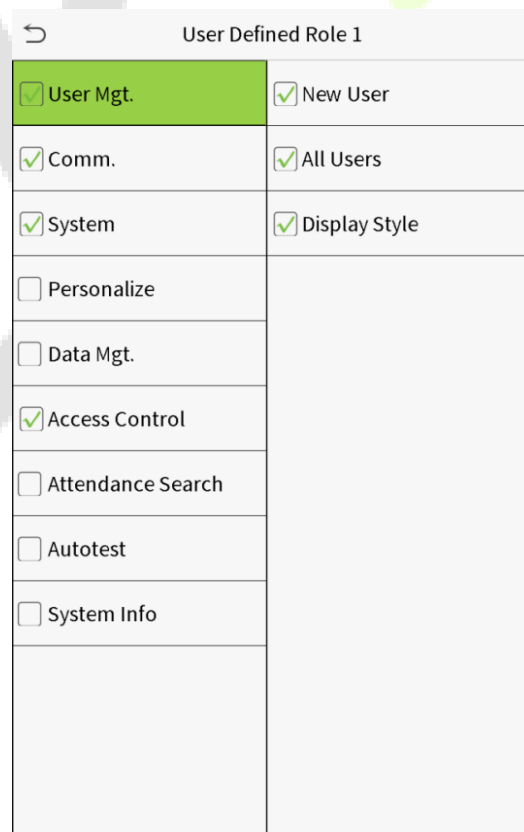
Hacer clic **Rol del usuario** en la interfaz del menú principal.



1. Haga clic en cualquier rol de usuario para establecer un rol definido. Alternar el **Habilitar rol definido** botón para habilitar esto papel definido. Hacer clic **Nombre** e ingrese el nombre del rol.



2. Hacer clic **Definir rol de usuario** para asignar privilegios al rol. Una vez que se completa la asignación de privilegios, hacer clic **Regreso**.



**Nota:** Durante la asignación de privilegios, el menú principal está a la izquierda y sus submenús están a la derecha. Solo necesita seleccionar las funciones en los submenús. Si el dispositivo tiene una función habilitada, puede asignar las funciones que estableció a los usuarios haciendo clic en **Administrador de usuarios > NewUser> Rol de usuario**.

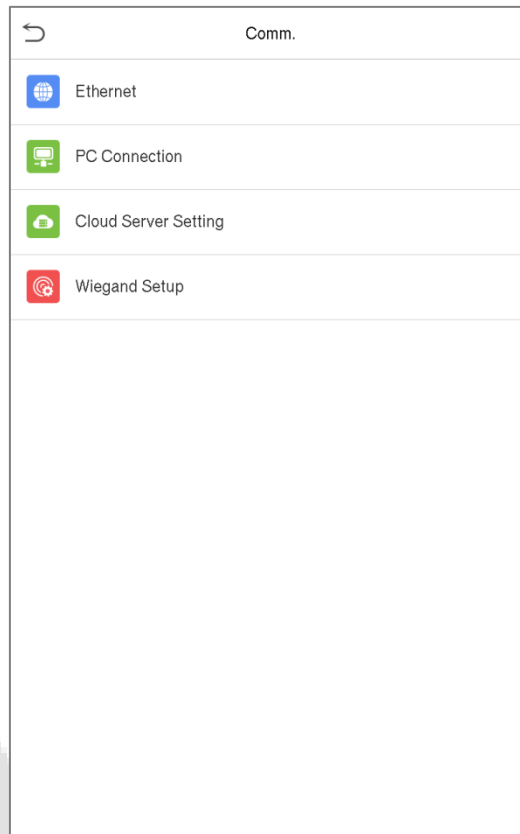
↩	User Role
<input checked="" type="radio"/>	Normal User
<input type="radio"/>	Enroller
<input type="radio"/>	User Defined Role 1
<input type="radio"/>	Super Admin

Si no hay ningún superadministrador registrado, el dispositivo le preguntará "¡Registre primero el usuario superadministrador!" después de hacer clic en la barra de habilitación.

## 6 Configuración de comunicación

La configuración de comunicación se utiliza para establecer los parámetros de la red, la conexión de la PC, el servidor en la nube y Wiegand.

Grifo **COMM.** en el menú principal.



### 6.1 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.

Hacer clic **Ethernet** en el Comm. Interfaz de configuración.

Ethernet	
IP Address	192.168.163.150
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	0.0.0.0
TCP COMM.Port	4370
DHCP	<input type="checkbox"/>
Display in Status Bar	<input checked="" type="checkbox"/>

Característica	Descripción
<b>Dirección IP</b>	El valor predeterminado de fábrica es 192.168.1.201. Configure la dirección IP según los requisitos.
<b>Máscara de subred</b>	El valor predeterminado de fábrica es 255.255.255.0. Establezca el valor según los requisitos.
<b>Puerta</b>	La dirección predeterminada de fábrica es 0.0.0.0. Establezca el valor según los requisitos.
<b>DNS</b>	La dirección predeterminada de fábrica es 0.0.0.0. Establezca el valor según los requisitos.
<b>TCP COMM. Puerto</b>	El valor predeterminado de fábrica es 4370. Configure el valor según los requisitos.
<b>DHCP</b>	Protocolo de configuración dinámica de host, que consiste en asignar dinámicamente direcciones IP para clientes a través del servidor.
<b>Mostrar en la barra de estado</b>	Para configurar si se muestra el icono de red en la barra de estado.

## 6.2 Conexión a PC

Para mejorar la seguridad de los datos, establezca un **Clave de comunicación** para la comunicación entre el dispositivo y la PC.

Si se establece una clave de comunicación, esta contraseña de conexión debe ingresarse antes de que el dispositivo se pueda conectar al software de PC.

Hacer clic **Conexión a PC** en el Comm. Interfaz de configuración.

PC Connection	
Comm Key	0
Device ID	1

Nombre del menú	Descripción
<b>CommKey</b>	Clave de comunicación: la contraseña predeterminada es 0, que se puede cambiar. La clave de comunicación puede contener de 1 a 6 dígitos.
<b>ID del dispositivo</b>	El número de identidad del dispositivo, que varía 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.

## 6.3 Configuración del servidor en la nube

Esto representa la configuración utilizada para conectar el servidor ADMS. Hacer clic **Configuración**

**del servidor en la nube** en el Comm. Interfaz de configuración.

Cloud Server Setting	
Server mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	0.0.0.0
Server port	8081
Enable Proxy Server	<input type="checkbox"/>

Menú		Descripción
Habilitar Dominio Nombre	Dirección del servidor	Cuando esta función está habilitada, se usará el modo de nombre de dominio "http: // ...", como http://www.XYZ.com, mientras que "XYZ" indica el nombre de dominio cuando este modo está encendido.
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.

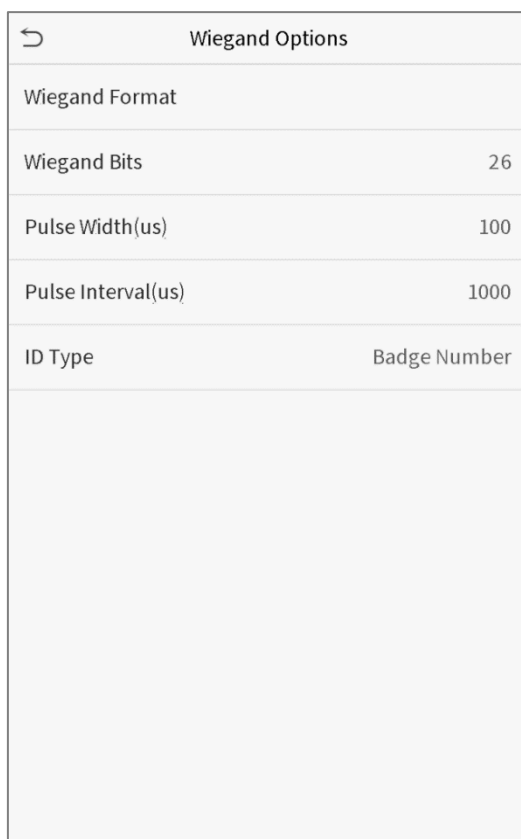
#### 6.4 Configuración de Wiegand

El menú se usa para configurar los parámetros de entrada y salida Wiegand. Hacer clic **Configuración**

de **Wiegand** en el Comm. Interfaz de configuración.

Wiegand Setup	
Wiegand Input	
Wiegand Output	

**Entrada Wiegand**



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

**Definiciones de varios formatos Wiegand comunes: Definiciones**

de formato Wiegand	
Wiegand26	<p>ECCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 26 bits de código binario. El 1<sup>er</sup> bit es el bit de paridad par del 2<sup> Dakota del Norte</sup> a 13<sup>th</sup> bits, mientras que los 26<sup>th</sup> bit es el bit de paridad impar del 14<sup>th</sup> hasta 25<sup>th</sup> bits. El 2<sup> Dakota del Norte</sup> hasta 25<sup>th</sup> los bits son los números de las tarjetas.</p>



<p>Wiegand26a</p>	<p>ESSSSSSSSCCCCCCCCCCCCCCCCCO</p> <p>Consta de 26 bits de código binario. El 1<sup>er</sup> bit es el bit de paridad par del 2<sup>o</sup> Dakota del Norte a 13<sup>er</sup> bits, mientras que los 26<sup>er</sup> bit es el bit de paridad impar del 14<sup>er</sup> hasta 25<sup>er</sup> bits. El 2<sup>o</sup> Dakota del Norte al 9<sup>er</sup> bits son los códigos de sitio, mientras que los 10<sup>er</sup> hasta 25<sup>er</sup> los bits son los números de las tarjetas.</p>
<p>Wiegand34</p>	<p>ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 34 bits de código binario. El 1<sup>er</sup> bit es el bit de paridad par del 2<sup>o</sup> Dakota del Norte hasta 17<sup>er</sup> bits, mientras que el 34<sup>er</sup> bit es el bit de paridad impar del 18<sup>er</sup> hasta 33<sup>er</sup> bits. El 2<sup>o</sup> Dakota del Norte hasta 25<sup>er</sup> los bits son los números de las tarjetas.</p>
<p>Wiegand34a</p>	<p>ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 34 bits de código binario. El 1<sup>er</sup> bit es el bit de paridad par del 2<sup>o</sup> Dakota del Norte hasta 17<sup>er</sup> bits, mientras que el 34<sup>er</sup> bit es el bit de paridad impar del 18<sup>er</sup> hasta 33<sup>er</sup> bits. El 2<sup>o</sup> Dakota del Norte al 9<sup>er</sup> bits son los códigos de sitio, mientras que los 10<sup>er</sup> hasta 25<sup>er</sup> los bits son los números de las tarjetas.</p>
<p>Wiegand36</p>	<p>APAGADOFFFFFFFFFCCCCCCCCCCCCCMMME</p> <p>Consta de 36 bits de código binario. El 1<sup>er</sup> bit es el bit de paridad impar del 2<sup>o</sup> Dakota del Norte hasta 18<sup>er</sup> bits, mientras que los 36<sup>er</sup> bit es el bit de paridad par del 19<sup>er</sup> hasta 35<sup>er</sup> bits. El 2<sup>o</sup> Dakota del Norte hasta 17<sup>er</sup> los bits son los códigos de dispositivo. El 18<sup>er</sup> hasta 33<sup>er</sup> los bits son los números de la tarjeta, y los 34<sup>er</sup> hasta 35<sup>er</sup> los bits son los códigos del fabricante.</p>
<p>Wiegand36a</p>	<p>EEEEEEEEEEEEEEEECCCCCCCCCCCCCO</p> <p>Consta de 36 bits de código binario. El 1<sup>er</sup> bit es el bit de paridad par del 2<sup>o</sup> Dakota del Norte hasta 18<sup>er</sup> bits, mientras que los 36<sup>er</sup> bit es el bit de paridad impar del 19<sup>er</sup> hasta 35<sup>er</sup> bits. El 2<sup>o</sup> Dakota del Norte al 19<sup>er</sup> bits son los códigos de dispositivo y los 20<sup>er</sup> hasta 35<sup>er</sup> los bits son los números de las tarjetas.</p>
<p>Wiegand37</p>	<p>OMMMMSSSSSSSSSSCCCCCCCCCCCCCCCCCE</p> <p>Consta de 37 bits de código binario. El 1<sup>er</sup> bit es el bit de paridad impar del 2<sup>o</sup> Dakota del Norte hasta 18<sup>er</sup> bits, mientras que el 37<sup>er</sup> bit es el bit de paridad par del 19<sup>er</sup> hasta 36<sup>er</sup> bits. El 2<sup>o</sup> Dakota del Norte para 4<sup>er</sup> los bits son los códigos del fabricante. El 5<sup>er</sup> hasta 16<sup>er</sup> bits son los códigos de sitio, y los 21<sup>er</sup> hasta 36<sup>er</sup> los bits son los números de las tarjetas.</p>
<p>Wiegand37a</p>	<p>EMMMFFFFFFFSSSSSSCCCCCCCCCCCCCO</p> <p>Consta de 37 bits de código binario. El 1<sup>er</sup> bit es el bit de paridad par del 2<sup>o</sup> Dakota del Norte hasta 18<sup>er</sup> bits, mientras que el 37<sup>er</sup> bit es el bit de paridad impar del 19<sup>er</sup> hasta 36<sup>er</sup> bits. El 2<sup>o</sup> Dakota del Norte para 4<sup>er</sup> los bits son los códigos del fabricante. El 5<sup>er</sup> hasta 14<sup>er</sup> los bits son los códigos de dispositivo, y 15<sup>er</sup> hasta 20<sup>er</sup> bits son los códigos de sitio, y los 21<sup>er</sup> hasta 36<sup>er</sup> los bits son los números de las tarjetas.</p>
<p>Wiegand50</p>	<p>ESSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 50 bits de código binario. El 1<sup>er</sup> bit es el bit de paridad par del 2<sup>o</sup> Dakota del Norte hasta 25<sup>er</sup> bits, mientras que los 50<sup>er</sup> bit es el bit de paridad impar del 26<sup>er</sup> hasta 49<sup>er</sup> bits. El 2<sup>o</sup> Dakota del Norte hasta 17<sup>er</sup> bits son los códigos de sitio, y los 18<sup>er</sup> hasta 49<sup>er</sup> los bits son los números de las tarjetas.</p>
<p>"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; "PAGS" denota el bit de paridad; y "S" denota el código del sitio.</p>	

## Salida Wiegand

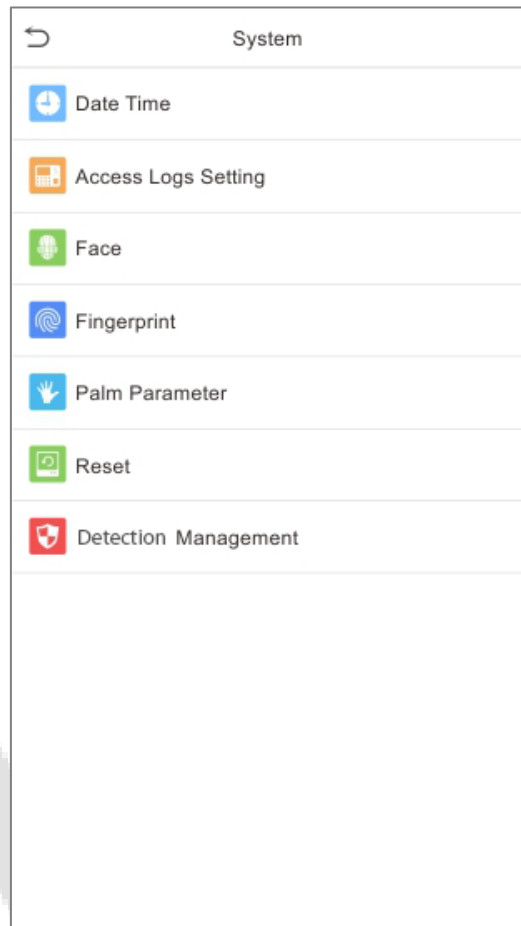
Wiegand Options	
SRB	<input type="checkbox"/>
Wiegand Format	
Wiegand output bits	26
Failed ID	Disabled
Site Code	Disabled
Pulse Width(us)	100
Pulse Interval(us)	1000
ID Type	Badge Number

Nombre del menú	Descripciones
<b>SRB</b>	Cuando SRB está habilitado, el bloqueo es controlado por el SRB para evitar que se abra debido a la extracción del dispositivo.
<b>Formato Wiegand</b>	Los valores oscilan entre 26 bits, 34 bits, 36 bits, 37 bits y 50 bits.
<b>Bits de salida Wiegand</b>	Después de elegir el formato Wiegand, puede seleccionar uno de los dígitos de salida correspondientes en el formato Wiegand
<b>Identificación fallida</b>	Si la verificación falla, el sistema enviará la identificación fallida al dispositivo y reemplazará el número de tarjeta o la identificación del personal por los nuevos.
<b>Código del sitio</b>	Es similar a la 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.
<b>PulseWidth (nosotros)</b>	El ancho de pulso representa los cambios en la cantidad de carga eléctrica con capacitancia de alta frecuencia regularmente dentro de un tiempo especificado.
<b>Intervalo de pulso (nosotros)</b>	El intervalo de tiempo entre pulsos.
<b>tipo de identificación</b>	Seleccione entre el ID de usuario y el número de placa.

## 7 Ajustes del sistema

La configuración del sistema se utiliza para establecer los parámetros del sistema relacionados para optimizar el rendimiento del dispositivo.

Hacer clic **Sistema** en la interfaz del menú principal.



### 7.1 Fecha y hora

Hacer clic **Fecha y hora** en la interfaz del sistema.



1. Puede configurar manualmente la fecha y la hora y hacer clic en **Confirmar** ahorrar.
2. Haga clic en 24 horas para habilitar o deshabilitar este formato y seleccione el formato 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. Después de restaurar la configuración de fábrica, la hora del dispositivo cambiará a las 18:30, 1 de enero de 2020.

## 7.2 Configuración de registros de acceso

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

Access Logs Setting	
Camera Mode	No photo
Display User Photo	<input checked="" type="checkbox"/>
Access Logs Warning	99
Circulation Delete Access Records	Disabled
Cyclic Delete ATT Photo	99
Cyclic Delete Blocklist Photo	99
Confirm Screen Delay(s)	3
Face comparison interval(s)	1

Nombre del menú	Descripción
<b>Modo cámara</b>	<p>Ya sea para capturar y guardar la imagen instantánea actual durante la verificación. Hay 5 modos:</p> <p><b>Sin fotografía:</b> No se toma ninguna foto durante la verificación del usuario.</p> <p><b>Tomar una foto, no guardar:</b> Se toma una foto, pero no se guarda durante la verificación.</p> <p><b>Tomar una foto y guardar:</b> La foto se toma y se guarda durante la verificación.</p> <p><b>Ahorre en la verificación exitosa:</b> Se toma una foto y se guarda para cada verificación exitosa.</p> <p><b>Guardar en verificación fallida:</b> La foto se toma y se guarda durante cada verificación fallida.</p>
<b>Mostrar foto de usuario</b>	Si mostrar la foto del usuario cuando el usuario pasa la verificación.

<b>Registros de acceso</b>	Quando el espacio de registro restante alcanza un valor preestablecido, el dispositivo mostrará automáticamente una advertencia. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999.
<b>Eliminación de circulación Registros de acceso</b>	Quando los registros de acceso hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un valor establecido de registros de acceso antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 999.
<b>Eliminación cíclica ATT Foto</b>	Quando las fotos de asistencia hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un valor establecido de las fotos de asistencia antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
<b>Lista de bloqueo de eliminación cíclica Foto</b>	Quando las fotos de la lista de bloqueo hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un valor establecido de las fotos antiguas de la lista de bloqueo. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
<b>Confirmar Pantalla Retraso (s)</b>	El tiempo que el mensaje de éxito se muestra en la pantalla. El rango válido es de 1 a 9 segundos.
<b>Comparación de caras Intervalo (s)</b>	Para configurar el intervalo de tiempo de coincidencia de la plantilla facial según sea necesario. El intervalo de tiempo válido es de 0 a 9 segundos.

### 7.3 Parámetros faciales

Hacer clic **Cara** en la interfaz del sistema.

↶	Face	↷	↶	Face	↷
	1:N Match Threshold	75		Face Enrollment Threshold	70
	1:1 Match Threshold	63		Face Pitch Angle	35
	Face Enrollment Threshold	70		Face Rotation Angle	25
	Face Pitch Angle	35		Image Quality	40
	Face Rotation Angle	25		Minimum Face Size	80
	Image Quality	40		LED Light Triggered Threshold	80
	Minimum Face Size	80		Motion Detection Sensitivity	4
	LED Light Triggered Threshold	80		Live Detection	<input checked="" type="checkbox"/>
	Motion Detection Sensitivity	4		Live Detection Threshold	70
	Live Detection	<input checked="" type="checkbox"/>		Anti-counterfeiting with NIR	<input type="checkbox"/>
	Live Detection Threshold	70		WDR	<input type="checkbox"/>
	Anti-counterfeiting with NIR	<input type="checkbox"/>		Anti-flicker Mode	50HZ

Nombre del menú	Descripción
<b>1: N (uno a muchos)</b> <b>Umbral de coincidencia</b>	<p>En el modo de verificación 1: N (uno a muchos), 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.</p> <p>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 el valor predeterminado de 75.</p>
<b>1: 1 (uno a uno)</b> <b>Umbral de coincidencia</b>	<p>En el modo de verificación 1: 1 (uno a uno), la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y las plantillas faciales registradas en el dispositivo sea mayor que el valor establecido.</p> <p>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 el valor predeterminado de 63.</p>
<b>Inscripción facial</b> <b>Límite</b>	<p>Durante el registro facial, se utiliza la comparación 1: N (uno a muchos) para determinar si el usuario ya se ha registrado antes.</p> <p>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.</p>
<b>Ángulo de inclinación de la cara</b>	<p>La tolerancia del ángulo de inclinación de una cara para el registro facial y la comparación.</p> <p>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.</p>
<b>Ángulo de rotación de la cara</b>	<p>La tolerancia del ángulo de rotación de una cara para el registro y la comparación de plantillas faciales.</p> <p>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.</p>
<b>Calidad de la imagen</b>	<p>Calidad de imagen para registro facial y comparación. Cuanto mayor sea el valor, más clara será la imagen.</p>
<b>Tamaño mínimo de la cara</b>	<p>Requerido para el registro facial y la comparación.</p> <p>Si el tamaño de un objeto es menor que este valor establecido, el objeto se filtrará y no se reconocerá como una cara.</p> <p>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.</p>
<b>Luz LED activada</b> <b>Límite</b>	<p>Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, con más frecuencia se encenderá la luz LED.</p>

<b>Detección de movimiento</b> <b>Sensibilidad</b>	Una medida de la cantidad de cambio en el campo de visión de una cámara que califica como posible detección de movimiento 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 se activa con frecuencia.
<b>Detección en vivo</b>	Detectar un intento de falsificación determinando si la fuente de una muestra biométrica es un ser humano vivo o una representación falsa utilizando imágenes de luz visible.
<b>Detección en vivo</b> <b>Límite</b>	Ayudar a juzgar si la imagen visible proviene de un cuerpo vivo. Cuanto mayor sea el valor, mejor será el rendimiento anti-spoofing de la luz visible.
<b>Lucha contra la falsificación con NIR</b>	Uso de imágenes de espectros de infrarrojo cercano para identificar y prevenir ataques de fotos y videos falsos.
<b>WDR</b>	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.
<b>Modo anti-parpadeo</b>	Se usa cuando WDR está apagado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea a la misma frecuencia que la luz.
<b>Notas</b>	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.

## 7.4 Parámetros de huellas dactilares

Hacer clic **Huella dactilar** en la interfaz del sistema.

Fingerprint	
1:1 Match Threshold	15
1:N Match Threshold	35
FP Sensor Sensitivity	Low
1:1 Retry Times	3
Fingerprint Image	Always show

FRR	LEJOS	Coincidencia recomendada umbrales	
		1: N	1: 1
Alto	Bajo	45	25
Medio	Medio	35	15
Bajo	Alto	25	10

Nombre del menú	Descripción
<b>Partido 1: 1</b> <b>Límite</b>	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 el ID de usuario ingresado inscrito en el dispositivo sea mayor que el valor establecido.

<b>1: NMatch Límite</b>	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.
<b>Sensor FP Sensibilidad</b>	Para establecer la sensibilidad de la adquisición de huellas dactilares. Se recomienda utilizar el nivel predeterminado " <b>Medio</b> ". Cuando el ambiente está seco, lo que resulta en una detección lenta de huellas dactilares, puede establecer el nivel en " <b>Alto</b> " elevar la sensibilidad; cuando el ambiente es húmedo, lo que dificulta la identificación de la huella digital, puede establecer el nivel en " <b>Bajo</b> ".
<b>1: 1 Reintentar Veces</b>	En la Verificación 1: 1, los usuarios pueden olvidar la huella digital registrada o presionar el dedo de manera incorrecta. Para reducir el proceso de volver a ingresar la ID de usuario, se permite reintentar.
<b>Huella dactilar Imagen</b>	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:  <b>Mostrar para inscribirse:</b> para mostrar la imagen de la huella digital en la pantalla solo durante el registro.  <b>Mostrar para el partido:</b> para mostrar la imagen de la huella digital en la pantalla solo durante la verificación.  <b>Siempre muestra:</b> para mostrar la imagen de la huella digital en la pantalla durante el registro y la verificación.  <b>Ninguna:</b> no mostrar la imagen de la huella digital.

## 7.5 Parámetros de la palma

Hacer clic **Palma** en la interfaz del sistema.

Palm Parameter	
Palm 1:1 Matching Threshold	576
Palm 1:N Matching Threshold	576

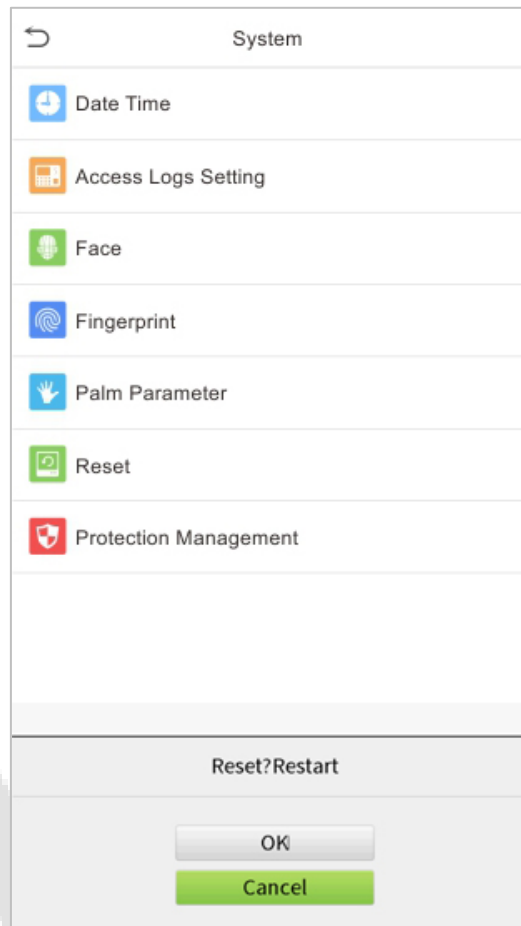
Nombre del menú	Descripción
<b>Palma 1: 1 (uno a Uno) Pareo Límite</b>	Bajo el método de verificación 1: 1 (uno a uno), solo cuando la similitud entre la palma de verificación y la palma registrada del usuario es mayor que este valor, la verificación se realiza correctamente.
<b>Palma 1: N (uno a Muchos) Pareo Límite</b>	Bajo el método de verificación 1: N (uno a muchos), solo cuando la similitud entre la palma verificadora y toda la palma registrada es mayor que este valor, la verificación se realiza correctamente.



## 7,6 Restablecimiento de fábrica

Esta opción restaura el dispositivo, como la configuración de comunicación y la configuración del sistema, a la configuración de fábrica (no borra los datos de usuario registrados).

Hacer clic **Reiniciar** en la interfaz del sistema.



Hacer clic **Okay** reiniciar.

## 7.7 Gestión de detección de temperatura

Hacer clic **Gestión de detección** en la interfaz del sistema.

Detection Management	
Enable temperature screening with infrared	<input checked="" type="checkbox"/>
High temperature alarm threshold	37.30 °C
Temperature over the range; access denied	<input checked="" type="checkbox"/>
Temperature deviation correction	0.00
Temp. Unit	°C
Temperature measurement distance	Far
Enable palm temp. detection	<input checked="" type="checkbox"/>
Temperature calibration	
Display Body Temperature	<input checked="" type="checkbox"/>
Enable mask detection	<input checked="" type="checkbox"/>
Deny access without mask	<input checked="" type="checkbox"/>
Allow unregistered people to access	<input checked="" type="checkbox"/>

Detection Management	
High temperature alarm threshold	37.30 °C
Temperature over the range; access denied	
Temperature deviation correction	0.00
Temp. Unit	°C
Temperature measurement distance	Far
Enable palm temp. detection	<input checked="" type="checkbox"/>
Temperature calibration	
Display Body Temperature	<input checked="" type="checkbox"/>
Enable mask detection	<input checked="" type="checkbox"/>
Deny access without mask	<input checked="" type="checkbox"/>
Allow unregistered people to access	<input checked="" type="checkbox"/>
Enable capture of unregistered person	<input checked="" type="checkbox"/>

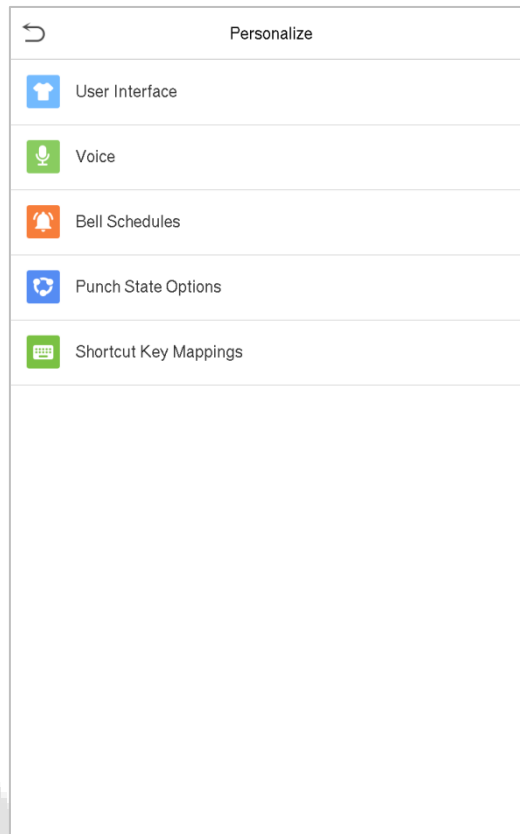
Nombre del menú	Descripción
<b>Habilitar temperatura proyección con infrarrojo</b>	<p>Para habilitar o deshabilitar la función de medición de temperatura por infrarrojos.</p> <p>Cuando esta función está habilitada, antes de que se conceda el acceso, los usuarios deben pasar el control de temperatura además de la verificación de identidad.</p> <p>Para medir la temperatura corporal, las caras de los usuarios deben estar alineadas con el área de medición de temperatura.</p>
<b>Alta temperatura umbral de alarma</b>	<p>Para establecer el valor del umbral de alarma de temperatura corporal alta.</p> <p>Cuando la temperatura medida durante la verificación es más alta que el valor establecido, el dispositivo emitirá un aviso y una alarma sonora.</p> <p>El umbral de alarma predeterminado es 37,30 °C.</p>
<b>Temperatura sobre el rango; acceso negado</b>	<p>Cuando esta función está habilitada, 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.</p> <p>Si esta función está deshabilitada, el usuario puede acceder al área restringida cuando se verifica su identidad, independientemente de su temperatura corporal.</p>

<b>Temperatura</b> corrección de desviación	Dado que el módulo de medición de temperatura permite una pequeña gama de errores (perturbación) de un valor observado en diferentes entornos (humedad, temperatura ambiente y similares), los usuarios pueden establecer aquí el valor de desviación.
<b>Temperatura. Unidad</b>	La unidad de temperatura corporal se puede cambiar entre Celsius ( °C) y Fahrenheit ( °F).
<b>Temperatura medición distancia</b>	Al medir la temperatura durante el proceso de verificación, hay tres modos: Cerca, Cerca y Lejos.
<b>Habilite la temperatura de la palma. detección ★</b>	Para habilitar o deshabilitar la función de detección de temperatura de la palma. Cuando está habilitado, el dispositivo mostrará la temperatura de la palma del usuario durante el proceso de verificación. Nota: esta función no está habilitada de forma predeterminada y se puede actualizar para admitir.
<b>Temperatura calibración</b>	Calibre la temperatura comparando el valor de temperatura actual con el valor de temperatura de la superficie del dispositivo.
<b>Enablemask detección</b>	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.
<b>Cuerpo de la pantalla Temperatura</b>	Para habilitar o deshabilitar la función de visualización de la temperatura corporal. Cuando está habilitado, el dispositivo mostrará el valor de temperatura específico del usuario durante el proceso de verificación.
<b>Enablemask detección</b>	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.
<b>Denegar el acceso sin máscara</b>	Para habilitar o deshabilitar la función denegar acceso sin máscara. Cuando está habilitado, incluso si la temperatura corporal es normal, la persona que no usa máscara no permitirá que ingrese.
<b>Permitir no registrados personas para acceder</b>	Para habilitar o deshabilitar la función de acceso de personas no registradas. Cuando está habilitado, siempre y cuando la persona que pasa la detección, el dispositivo permite que el personal ingrese sin registrarse.
<b>Habilitar captura de persona no registrada</b>	Para habilitar o deshabilitar la función de captura de personas no registradas. Cuando está habilitado, el dispositivo capturará automáticamente la foto del persona no registrada, habilitar esta función requiere habilitar <b>Permitir personas no registradas para acceder</b> .

## 8 Personalizar la configuración

Puede personalizar la configuración de la interfaz, el audio y el timbre. Hacer clic **Personalizar**

en la interfaz del menú principal.



### 8.1 Configuración de la interfaz

Puede personalizar el estilo de visualización de la interfaz principal. Hacer clic **Interfaz**

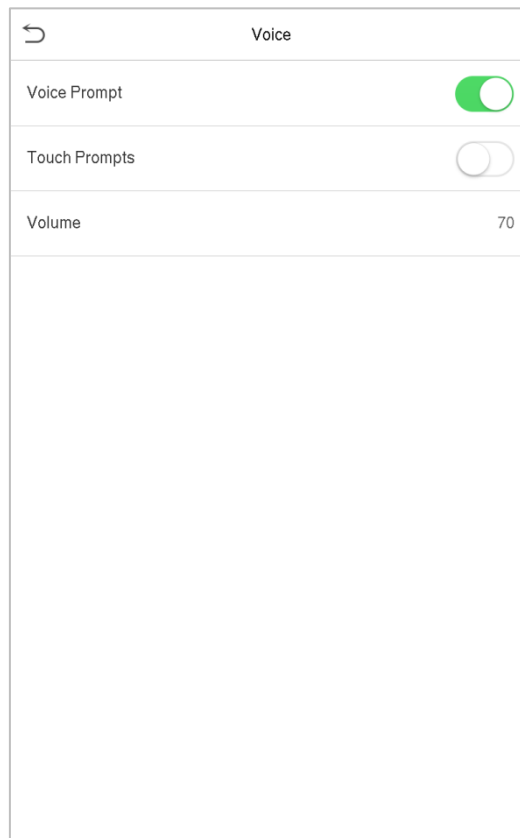
**de usuario** en la interfaz Personalizar.

User Interface	
Wallpaper	
Language	English
Menu Screen Timeout(s)	99999
Idle Time To Slide Show(s)	60
Slide Show Interval(s)	30
Idle Time To Sleep(m)	Disabled
Main Screen Style	Style 1

Menú	Descripción
<b>Fondo de pantalla</b>	Para seleccionar el fondo de pantalla de la pantalla principal de acuerdo con sus preferencias personales. Para
<b>Idioma</b>	seleccionar el idioma del dispositivo.
<b>Pantalla de menú Tiempo de espera (s)</b>	Cuando no hay operación y el tiempo excede el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. Puede desactivar la función o establecer el valor entre 60 y 99999 segundos.
<b>Tiempo de inactividad para la presentación de diapositivas</b>	Cuando no hay ninguna operación y el tiempo excede el valor establecido, se reproducirá una presentación de diapositivas. Puede desactivarse o puede establecer el valor entre 3 y 999 segundos.
<b>Intervalo de presentación de diapositivas (s)</b>	Esto se refiere al intervalo de tiempo que cambia diferentes imágenes de presentación de diapositivas. La función puede desactivarse o puede establecer el intervalo entre 3 y 999 segundos.
<b>Tiempo inactivo para dormir (m)</b>	Si ha activado el modo de suspensión, cuando no haya ninguna operación, el dispositivo entrará en el modo de espera. Presione cualquier tecla o dedo para reanudar el modo de trabajo normal. Puede desactivar esta función o establecer un valor entre 1 y 999 minutos.
<b>Estilo de pantalla principal</b>	Para seleccionar el estilo de la pantalla principal según sus preferencias personales.

## 8.2 Configuración de voz

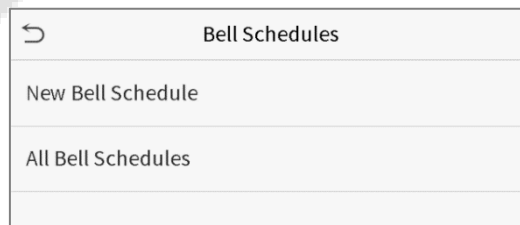
Hacer clic **Voz** en la interfaz Personalizar.



Nombre del menú	Descripción
<b>Mensaje de voz</b>	Seleccione si desea habilitar las indicaciones de voz durante la operación. Seleccione si
<b>Toque Indicación</b>	desea habilitar los sonidos del teclado.
<b>Volumen</b>	Ajuste el volumen del dispositivo; valor válido: 0 a 100.

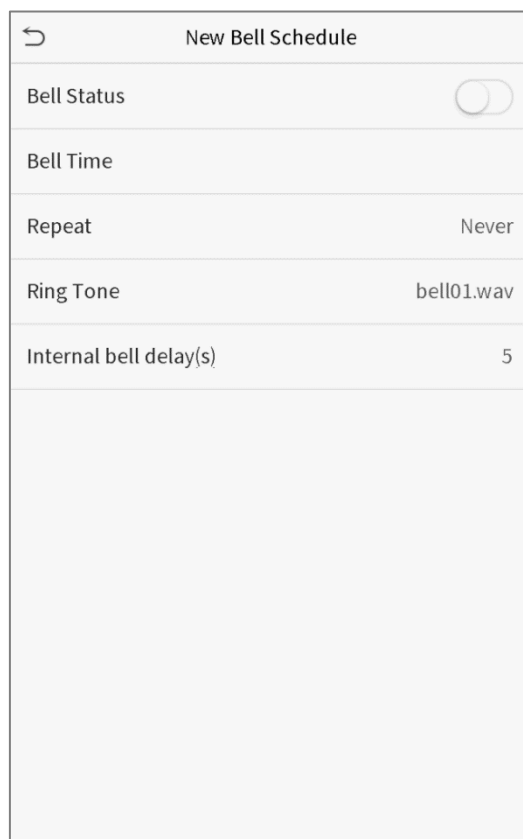
## 8.3 Horarios de campana

Hacer clic **Horarios de campana** en la interfaz Personalizar.



### Agregar una campana

1. Hacer clic **Horario NewBell** para ingresar a la interfaz de adición:



The screenshot shows a mobile application interface titled "New Bell Schedule". It features a list of settings:

- Bell Status:** A toggle switch that is currently turned off.
- Bell Time:** A field for setting the time.
- Repeat:** A dropdown menu currently set to "Never".
- Ring Tone:** A dropdown menu currently set to "bell01.wav".
- Internal bell delay(s):** A numeric input field set to "5".

Nombre del menú	Descripción
<b>Estado de la campana</b>	Establezca si habilitar el estado de la campana.
<b>Tiempo de campana</b>	A esta hora del día, el dispositivo hace sonar el timbre automáticamente. Configure
<b>Repetir</b>	el ciclo de repetición de la campana.
<b>Tono de llamada</b>	Seleccione un tono de llamada.
<b>Retardo de campana interna</b>	Establezca la duración de la campana interna. Los valores válidos oscilan entre 1 y 999 segundos.

2. Volver a la interfaz de Bell Schedules; hacer clic **Todos los horarios de campana** para ver la campana recién agregada.

### Editar una campana

En la interfaz Todos los horarios de timbre, toque el timbre para editarlo. Hacer clic **Editar**, El método de edición

es el mismo que el de agregar una campana.

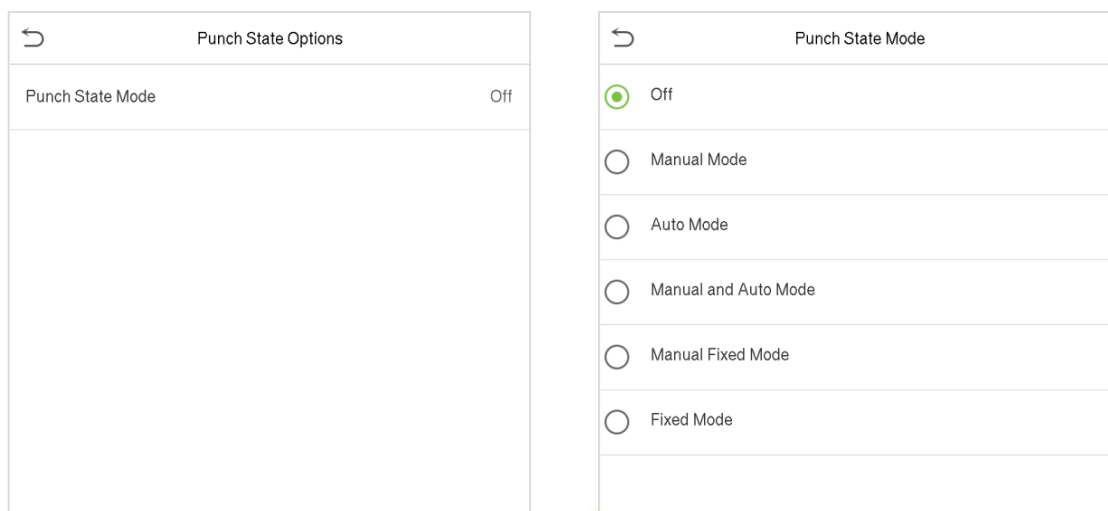
### Eliminar una campana

En la interfaz de Todos los horarios de timbre, toque el timbre para eliminarlo. Grifo **Eliminar** y

seleccione [ **Si**] para eliminar la campana.

## 8.4 Opciones de estados de perforación

Hacer clic **Opciones de estados de perforación** en la interfaz Personalizar.



Nombre del menú	Descripción
<b>Modo de estado de perforación</b>	<p>Seleccione un modo de estado de perforación, que puede ser:</p> <p><b>Apagado:</b> Para deshabilitar la función de tecla de estado de perforación. La clave de estado de perforación establecida en <b>Asignaciones de teclas de método abreviado</b> el menú dejará de ser válido.</p> <p><b>Modo manual:</b> Para cambiar la tecla de estado de perforación manualmente, y la tecla de estado de perforación desaparecerá después <b>Tiempo de espera del estado de perforación</b>.</p> <p><b>Modo automático:</b> Después de elegir este modo, configure <b>la</b> tiempo de conmutación de la tecla de estado de perforación en <b>Asignaciones de teclas de acceso directo</b>; cuando se alcanza el tiempo de conmutación, la tecla de estado de perforación establecida se cambiará automáticamente.</p> <p><b>Modo manual y automático:</b> En este modo, la interfaz principal mostrará la clave de estado de perforación de conmutación automática, mientras que admite el cambio manual de la clave de estado de perforación. Después del tiempo de espera, la tecla de estado de perforación de conmutación manual se convertirá en una tecla de estado de perforación de conmutación automática.</p> <p><b>Modo fijo manual:</b> Después de que la clave de estado de perforación se cambie manualmente, la clave de estado de perforación permanecerá sin cambios hasta que se cambie manualmente la próxima vez.</p> <p><b>Modo fijo:</b> Solo se mostrará la clave de estado de perforación fija y no se puede cambiar.</p>



## 8.5 Asignaciones de teclas de acceso directo

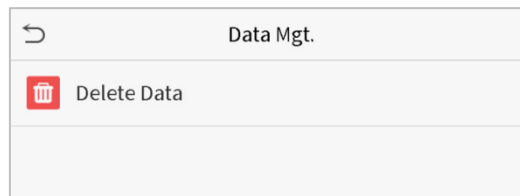
Los usuarios pueden definir accesos directos como estado de asistencia o teclas funcionales. En la interfaz principal, cuando se presionan las teclas de acceso directo, se mostrará rápidamente el estado de asistencia correspondiente o la interfaz de función.

Hacer clic **Asignaciones de teclas de método abreviado** en la interfaz Personalizar.

Shortcut Key Mappings	
F1	Check-In
F2	Check-Out
F3	Break-Out
F4	Break-In
F5	Overtime-In
F6	Overtime-Out

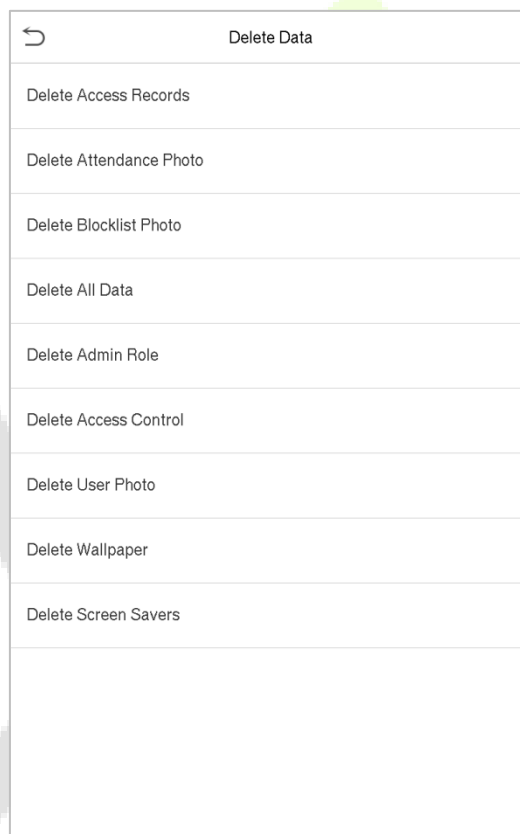
## 9 Gestión de datos

La gestión de datos se utiliza para eliminar los datos relevantes en el dispositivo. Hacer clic **DataMgt.** en la interfaz del menú principal.



### 9.1 Borrar datos

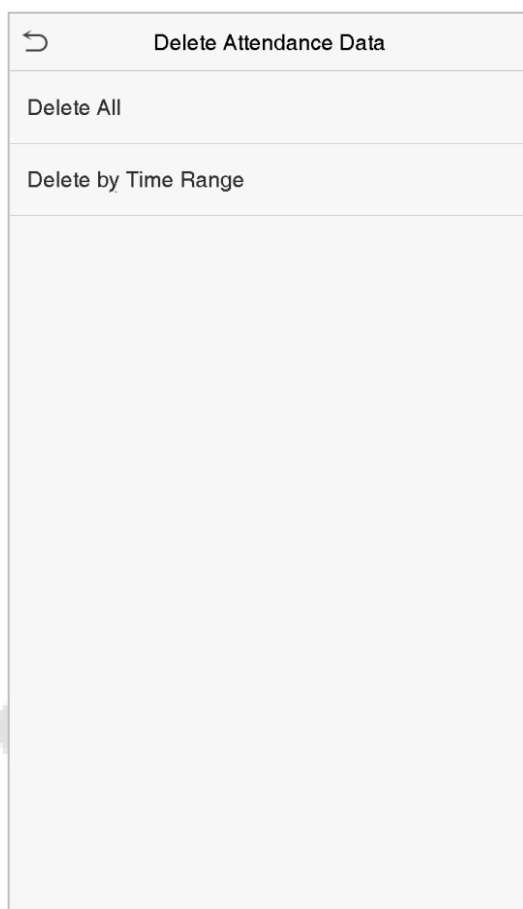
Hacer clic **Borrar datos** en el Data Mgt. interfaz.



Nombre del menú	Descripción
<b>Eliminar registros de acceso</b>	Eliminar los datos de asistencia / registros de acceso condicionalmente.
<b>Eliminar asistencia Foto</b>	Eliminar las fotos de asistencia del personal designado.
<b>Eliminar foto de la lista de bloqueo</b>	Para borrar las fotos tomadas durante las verificaciones fallaron.
<b>Eliminar todos los datos</b>	Para eliminar la información y los registros de asistencia / registros de acceso de todos los registrados

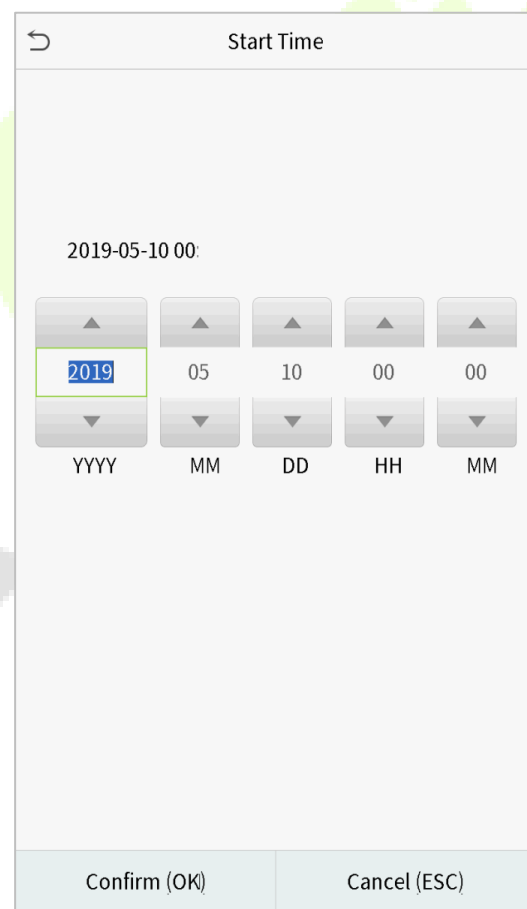
	usuarios.
<b>Eliminar función de administrador</b>	Para eliminar los privilegios de administrador.
<b>Eliminar control de acceso</b>	Eliminar todos los datos de acceso.
<b>Eliminar foto de usuario</b>	Para eliminar todas las fotos de usuario en el dispositivo. Para
<b>Eliminar fondo de pantalla</b>	eliminar todos los fondos de pantalla del dispositivo. Para eliminar
<b>Eliminar protectores de pantalla</b>	los protectores de pantalla del dispositivo.

**Nota:** Al eliminar los registros de acceso, las fotos de asistencia o las fotos de la lista de bloques, puede seleccionar Eliminar todo o Eliminar por intervalo de tiempo. Si selecciona Eliminar por rango de tiempo, debe establecer un rango de tiempo específico para eliminar todos los datos con el período.



The screenshot shows a mobile application interface with a back arrow and the title "Delete Attendance Data". Below the title, there are two menu options: "Delete All" and "Delete by Time Range". The "Delete by Time Range" option is highlighted with a light blue background, indicating it is the selected option.

Seleccione Eliminar por rango de tiempo



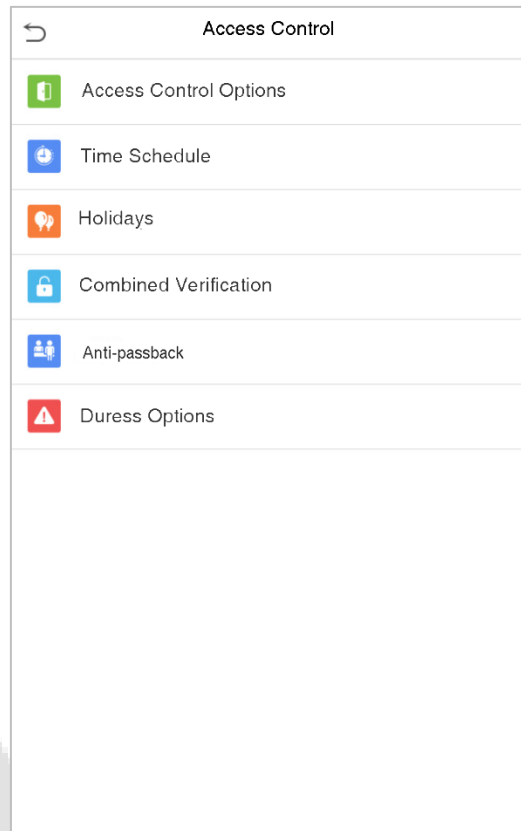
The screenshot shows a mobile application interface with a back arrow and the title "Start Time". Below the title, the date and time "2019-05-10 00:" are displayed. Below this, there are five columns of spinners for selecting the year, month, day, hour, and minute. The year spinner is currently set to "2019". Below the spinners, the labels "YYYY", "MM", "DD", "HH", and "MM" are displayed. At the bottom of the screen, there are two buttons: "Confirm (OK)" and "Cancel (ESC)".

Establezca el rango de tiempo y haga clic en Aceptar

## 10 Control de acceso

El control de acceso se utiliza para establecer el horario de apertura de una puerta, control de cerraduras y otros ajustes de parámetros relacionados con el control de acceso.

Hacer clic **Control de acceso** en la interfaz del menú principal.



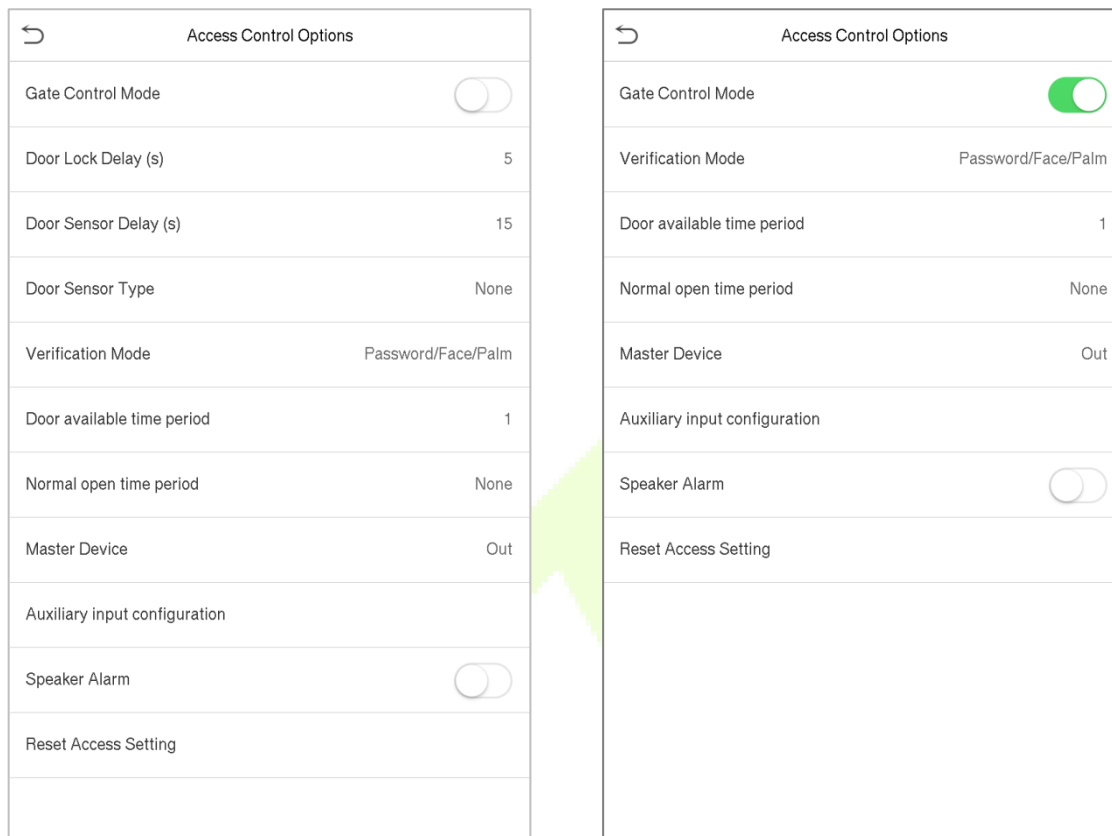
**Para acceder, el usuario registrado debe cumplir las siguientes condiciones:**

1. El tiempo de desbloqueo de la puerta actual debe estar dentro de cualquier zona horaria válida del período de tiempo del usuario.
2. El grupo de usuarios debe estar en la combinación de desbloqueo de puertas (cuando hay otros grupos en la misma combinación de acceso, también se requiere la verificación de los miembros de esos grupos para desbloquear la puerta).

En la configuración predeterminada, los nuevos usuarios se asignan al primer grupo con la zona horaria del grupo predeterminado y el combo de acceso como "1" y se establecen en un estado de desbloqueo.

## 10.1 Opciones de control de acceso

Esta opción se utiliza para configurar los parámetros del bloqueo de control del dispositivo y los parámetros relacionados. Hacer clic **Opciones de control de acceso** en la interfaz de control de acceso.



Nombre del menú	Descripción
<b>Modo de control de puerta</b>	Ya sea para activar el modo de control de puerta o no. Cuando se establece en ON, en esta interfaz se eliminará el relé de bloqueo de puerta, el relé de sensor de puerta y la función de tipo de sensor de puerta.
<b>Retraso de bloqueo de puerta (s)</b>	El tiempo que el dispositivo controla la cerradura eléctrica para desbloquear. Valor válido: 1 a 10 segundos; 0 segundos representa la desactivación de la función.
<b>Retraso del sensor de puerta (s)</b>	Si la puerta no está cerrada y bloqueada después de abrirse durante un tiempo determinado (retardo del sensor de puerta), se activará una alarma. El valor válido del retardo del sensor de puerta varía de 1 a 255 segundos.
<b>Tipo de sensor de puerta</b>	Hay tres tipos: Ninguno, Normal Abierto y Normal Cerrado. Ninguno significa que el sensor de la puerta no está en uso; Normalmente abierto significa que la puerta siempre está abierta cuando la electricidad está encendida; Normalmente cerrado significa que la puerta siempre está cerrada cuando hay electricidad.
<b>VerificationMode</b>	El modo de verificación admitido incluye contraseña / rostro, solo ID de usuario, contraseña, solo rostro y rostro y contraseña.

<b>Puerta disponible tiempo período</b>	Para establecer un período de tiempo para la puerta, de modo que la puerta sea accesible solo durante este período de tiempo.
<b>Tiempo abierto normal Período</b>	Período de tiempo programado para el modo de "apertura normal", de modo que la puerta siempre esté desbloqueada durante este período.
<b>Dispositivo maestro</b>	Al configurar el maestro y el esclavo, el estado del maestro se puede configurar para salir o entrar.  <b>Salida:</b> El registro verificado en el host es el registro de salida.  <b>Entrar:</b> El registro verificado en el host es el registro de entrada.
<b>Entrada auxiliar configuración</b>	Configure 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.
<b>Alarma de altavoz</b>	Para transmitir 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.
<b>Restablecer configuración de acceso</b>	Los parámetros de control de acceso restaurados incluyen retardo de bloqueo de puerta, retardo de sensor de puerta, tipo de sensor de puerta, modo de verificación, período de tiempo disponible de puerta, período de tiempo de apertura normal, un dispositivo maestro y alarma. Sin embargo, los datos de control de acceso borrados en Data Mgt. está excluido.

## 10,2 Horario

Todo el sistema puede definir hasta 50 reglas de tiempo. Cada regla de tiempo representa diez zonas horarias, es decir, una semana y 3 días festivos, y cada zona horaria es un período de tiempo válido dentro de las 24 horas del día. Puede establecer un máximo de 3 períodos de tiempo para cada zona horaria. La relación entre estos períodos de tiempo es "o". Cuando el tiempo de verificación cae en cualquiera de estos períodos de tiempo, la verificación es válida. Cada formato de período de tiempo de la zona horaria: HHMM-HHMM, que tiene una precisión de minutos según el reloj de 24 horas.

Hacer clic **Configuración de la regla de tiempo** en la interfaz de control de acceso.

1. Haga clic en el cuadro gris para ingresar una zona horaria para buscar. Ingrese el número de zona horaria (máximo: 50 zonas).

Time Rule[2/50]	
Sunday	[00:00 23:59] [00:00 23:...
Monday	[00:00 23:59] [00:00 23:...
Tuesday	[00:00 23:59] [00:00 23:...
Wednesday	[00:00 23:59] [00:00 23:...
Thursday	[00:00 23:59] [00:00 23:...
Friday	[00:00 23:59] [00:00 23:...
Saturday	[00:00 23:59] [00:00 23:...
holiday type 1	[00:00 23:59] [00:00 23:...
holiday type 2	[00:00 23:59] [00:00 23:...
holiday type 3	[00:00 23:59] [00:00 23:...
<input type="text"/> <input type="button" value="Q"/>	

- Haga clic en la fecha en la que se requieren los ajustes de zona horaria. Ingrese la hora de inicio y finalización, y luego presione OK.

Time Period 1			
00:00 23:59			
▲	▲	▲	▲
00	00	23	59
▼	▼	▼	▼
HH	MM	HH	MM
Confirm (OK)		Cancel (ESC)	

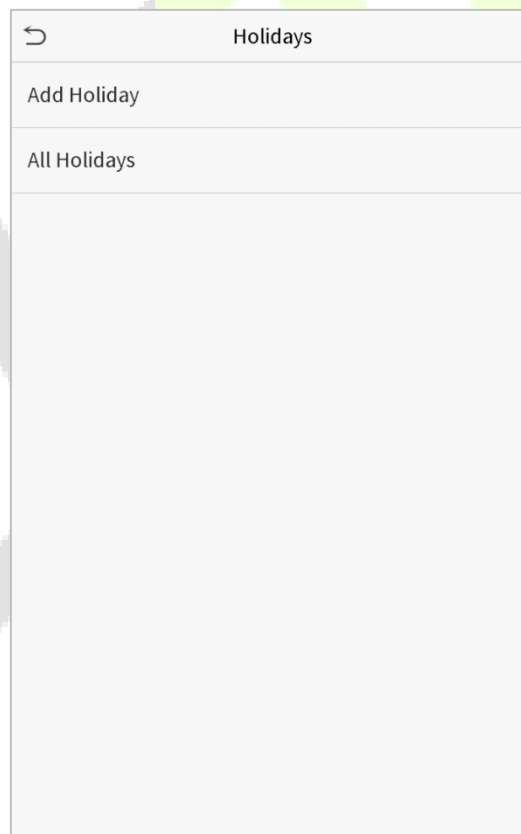
**Notas:**

- 1 ) Cuando la hora de finalización es anterior a la hora de inicio, como 23: 57 ~ 23: 56, indica que el acceso está prohibido todo el día; cuando la hora de finalización es posterior a la hora de inicio, como 00: 00 ~ 23: 59, indica que el intervalo es válido.
- 2 ) El período de tiempo efectivo para desbloquear la puerta: abierta todo el día (00: 00 ~ 23: 59) o cuando la hora de finalización es posterior a la hora de inicio, por ejemplo, 08: 00 ~ 23: 59.
- 3 ) La zona horaria predeterminada 1 indica que la puerta está abierta todo el día.

**10,3 Configuración de vacaciones**

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 se aplique a todos los empleados, y el usuario podrá abrir la puerta durante las vacaciones.

Hacer clic **Días festivos** en la interfaz de control de acceso.





### Agregar un nuevo feriado

Hacer clic **Agregar feriado** en la interfaz de vacaciones y configure los parámetros de vacaciones.

Holidays	
No.	1
Date	Undefined
holiday type	holiday type 1
Looping or not	<input checked="" type="checkbox"/>

### Editar un feriado

En la interfaz de vacaciones, seleccione un elemento de vacaciones para modificarlo. Hacer clic **Editar** para modificar los parámetros de vacaciones.

### Eliminar un feriado

En la interfaz de vacaciones, seleccione un elemento de vacaciones para eliminar y haga clic en **Eliminar**. Hacer clic **Okay** para confirmar la eliminación. Después de la eliminación, este día festivo ya no se muestra en la interfaz de Todos los días festivos.

## 10,4 Configuración de 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 puertas, el rango del número combinado N es  $0 \leq N \leq 5$ , y el número de miembros N pueden pertenecer todos a un grupo de acceso o pueden pertenecer a cinco grupos de acceso diferentes.

Hacer clic **Verificación combinada** en la interfaz de control de acceso.

Combined Verification	
1	01 02 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00
6	00 00 00 00 00
7	00 00 00 00 00
8	00 00 00 00 00
9	00 00 00 00 00
10	00 00 00 00 00
<input type="text"/>	

Haga clic en la combinación de desbloqueo de puertas que desee configurar. Haga clic en las flechas hacia arriba y hacia abajo para ingresar el número de combinación, luego presione OK.

### Ejemplos:

La combinación de desbloqueo de puerta 1 se establece como (01 03 05 06 08), lo que indica que la combinación de desbloqueo 1 consta de 5 personas y las 5 personas pertenecen a 5 grupos, es decir, grupo de control de acceso 1 (grupo de CA 1), CA grupo 3, grupo de CA 5, grupo de CA 6 y grupo de CA 8, respectivamente.

La combinación de desbloqueo de puerta 2 se establece como (02 02 04 04 07), lo que indica que la combinación de desbloqueo 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.

La combinación de desbloqueo de puertas 3 se establece como (09 09 09 09 09), lo que indica que hay 5 personas en esta combinación; todos los cuales son del grupo AC 9.

La combinación de desbloqueo de puerta 4 se establece como (03 05 08 00 00), lo que indica que la combinación de desbloqueo 4 consta de 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.

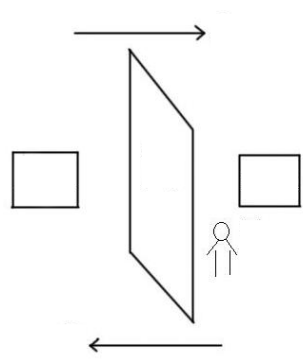
### Eliminar una combinación de desbloqueo de puertas

Configure todos los números de grupo como 0 si desea eliminar las combinaciones de desbloqueo de puertas.

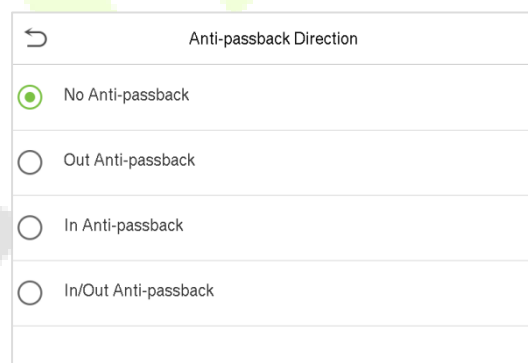
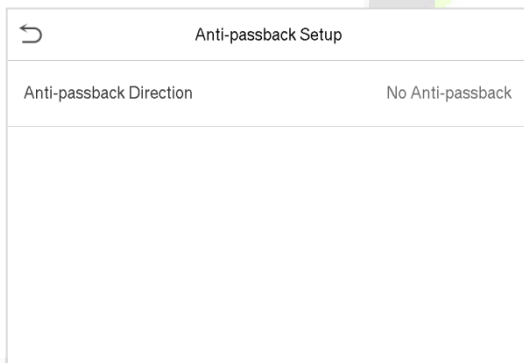
### 10,5 Configuración de Anti-Passback

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

Esta función requiere dos dispositivos para trabajar juntos: uno está instalado dentro de la puerta (dispositivo maestro), 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 placa) adoptados por el dispositivo maestro y el dispositivo esclavo deben ser consistentes.



Hacer clic **Configuración anti-passback** en la interfaz de control de acceso.



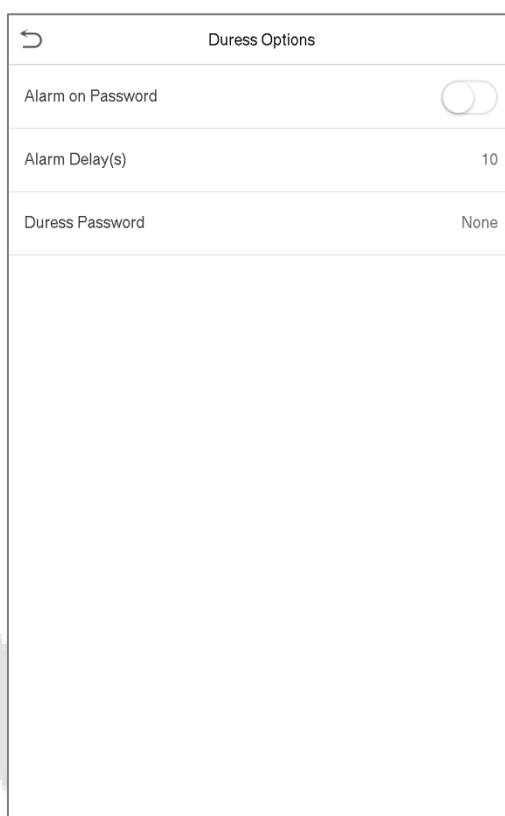
Nombre del menú	Descripción
<p><b>Anti-passback dirección</b></p>	<p><b>Sin Anti-passback:</b> La función anti-passback está desactivada, lo que significa que la verificación exitosa a través del dispositivo maestro o esclavo puede desbloquear la puerta. El estado de asistencia no se guarda.</p> <p><b>Fuera Anti-passback:</b> 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.</p> <p><b>En Anti-passback:</b> 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 salir libremente.</p> <p><b>Anti-passback de entrada / salida:</b> Después de que un usuario se registra de entrada / salida, solo si el último registro es un registro de salida, el usuario puede registrarse nuevamente; o un registro de registro, el usuario</p>

puede salir de nuevo; de lo contrario, se activará la alarma.

## 10,6 Configuración de opciones de coacción

Si un usuario activó la función de verificación de coacción con métodos de autenticación específicos, cuando esté bajo coacción durante la autenticación con dicho método, el dispositivo desbloqueará la puerta como de costumbre, pero al mismo tiempo se enviará una señal para activar la alarma.

Hacer clic **Opciones de coacción** en la interfaz de control de acceso.



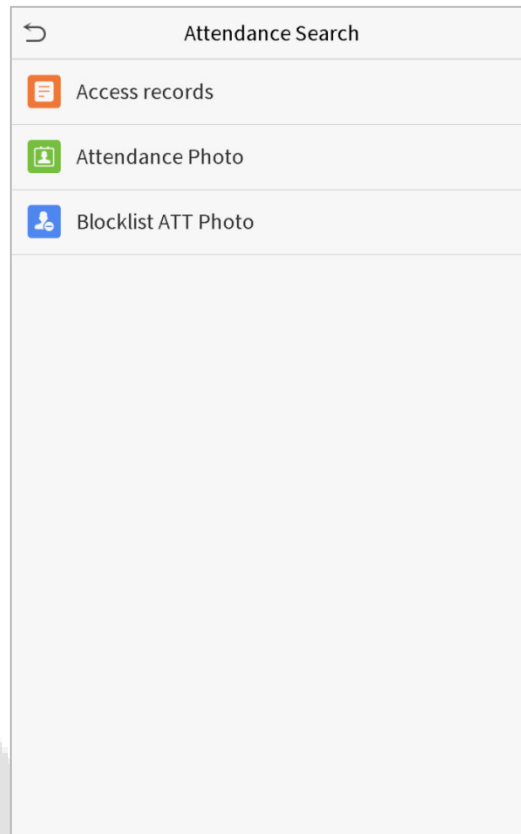
Duress Options	
Alarm on Password	<input type="checkbox"/>
Alarm Delay(s)	10
Duress Password	None

Menú	Descripción
<b>Alarmon Password</b>	Cuando un usuario utiliza el método de verificación de contraseña, se generará una señal de alarma; de lo contrario, no habrá señal de alarma.
<b>Retraso de alarma (s)</b>	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.
<b>Contraseña de coacción</b>	Configure la contraseña de coacción de 6 dígitos. Cuando el usuario ingresa esta contraseña de coacción para verificación, se generará una señal de alarma.

## 11 Búsqueda de asistencia

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

Hacer clic **Búsqueda de asistencia** en la interfaz del menú principal.



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.

En la interfaz de búsqueda de asistencia, haga clic en **Registros de acceso**.

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.

User ID			
Please Input(query all data without input)			
1	2	3	✕
4	5	6	^
7	8	9	∨
ESC	0	123	OK

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

←	Time Range
<input checked="" type="radio"/>	Today
<input type="radio"/>	Yesterday
<input type="radio"/>	This week
<input type="radio"/>	Last week
<input type="radio"/>	This month
<input type="radio"/>	Last month
<input type="radio"/>	All
<input type="radio"/>	User Defined

3. La búsqueda de registros se realiza correctamente. Haga clic en el registro en verde para ver sus detalles.

Personal Record Search		
Date	User ID	Access records
05-10		Number of Records:01
	0	09:09
05-09		Number of Records:02
	1	12:25
	0	08:53
05-08		Number of Records:03
	1	09:17 09:15
	0	09:03
05-07		Number of Records:01
	0	16:06
05-06		Number of Records:04
	0	18:20 15:55
	1	17:28 17:28
05-05		Number of Records:01
	0	10:12
04-30		Number of Records:01
	0	13:56
04-29		Number of Records:05
	1	10:06 10:06 10:06 10:06
	0	08:56
04-28		Number of Records:01
	0	08:57
04-27		Number of Records:06
	0	18:00 17:58 17:57 17:56 17:44 17:40

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

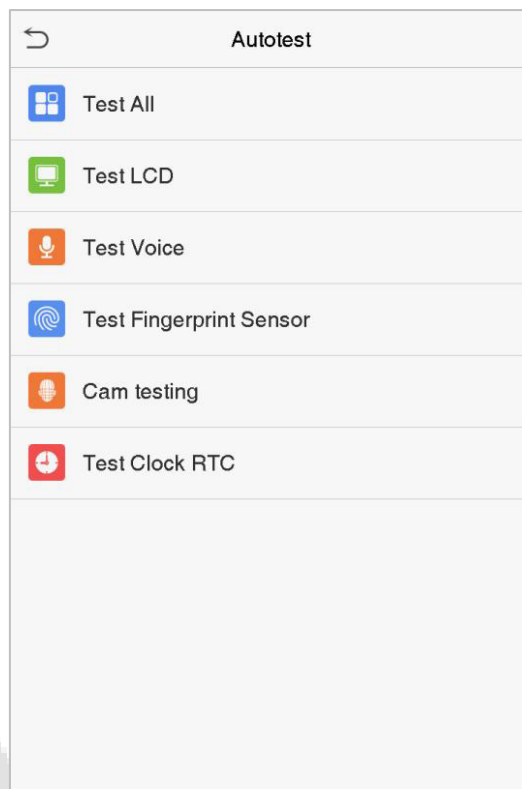
Personal Record Search				
User ID	Name	Access record	Mode	State
1	A	05-09 12:25	15	0

Verification Mode : Face Status : In

## 12 Auto prueba

Para probar automáticamente si todos los módulos del dispositivo funcionan correctamente, que incluyen la pantalla LCD, el audio, la cámara y el reloj en tiempo real (RTC).

Hacer clic **Auto prueba** en la interfaz del menú principal.



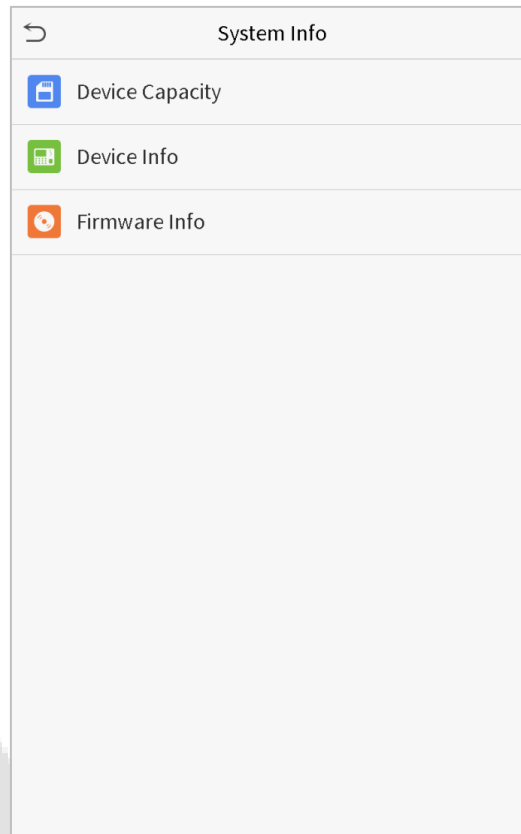
Menú	Descripción
<b>Probar todo</b>	Para probar automáticamente si la pantalla LCD, el audio, la cámara y el RTC son normales.
<b>Prueba de LCD</b>	Para probar automáticamente el efecto de visualización de la pantalla LCD mostrando a todo color, blanco puro y negro puro para verificar si la pantalla muestra los colores normalmente.
<b>Prueba de voz</b>	Para probar automáticamente si los archivos de audio almacenados en el dispositivo están completos y la calidad de voz es buena.
<b>Prueba de huella digital Sensor</b>	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.
<b>Prueba de cámara</b>	Para probar si la cámara funciona correctamente, verifique las imágenes tomadas para ver si son lo suficientemente claras.
<b>Prueba de reloj RTC</b>	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.



## 13 Información del sistema

Con la opción de información del sistema, puede ver el estado del almacenamiento, la información de la versión del dispositivo, etc.

Hacer clic **Información del sistema** en la interfaz del menú principal.



Nombre del menú	Descripción
<b>Dispositivo Capacidad</b>	Muestra el almacenamiento de usuario del dispositivo actual, el almacenamiento de la palma, la contraseña y el rostro, los administradores, los registros de acceso, las fotos de listas de asistencia y de bloqueo y las fotos de los usuarios.
<b>Información del dispositivo</b>	Muestra el nombre del dispositivo, el número de serie, la dirección MAC, la información de la versión del algoritmo facial, la información de la plataforma y el fabricante.
<b>Información de firmware</b>	Muestra la versión de firmware y otra información de versión del dispositivo.

## 14 Conéctese al software MTD ZKBioAccess

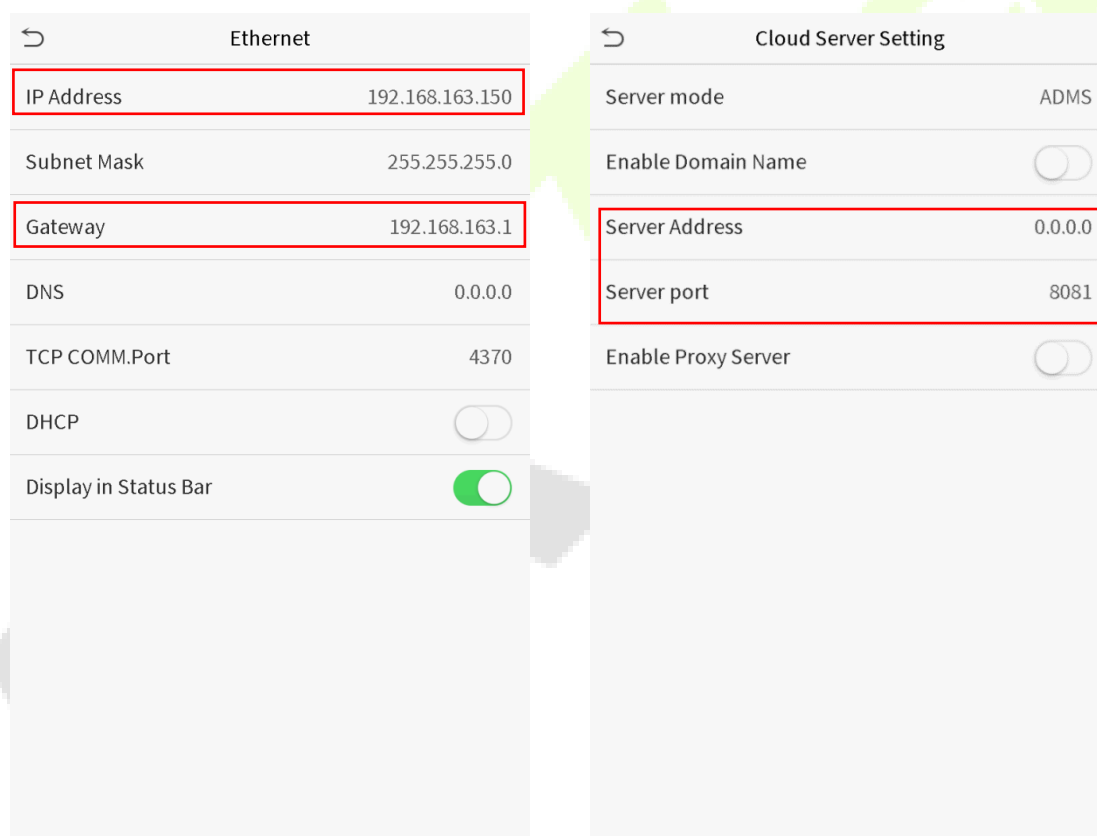
### 14.1 Establecer la dirección de comunicación

#### Lado del dispositivo

1. Hacer clic **COM.> 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 del servidor y el puerto del servidor.

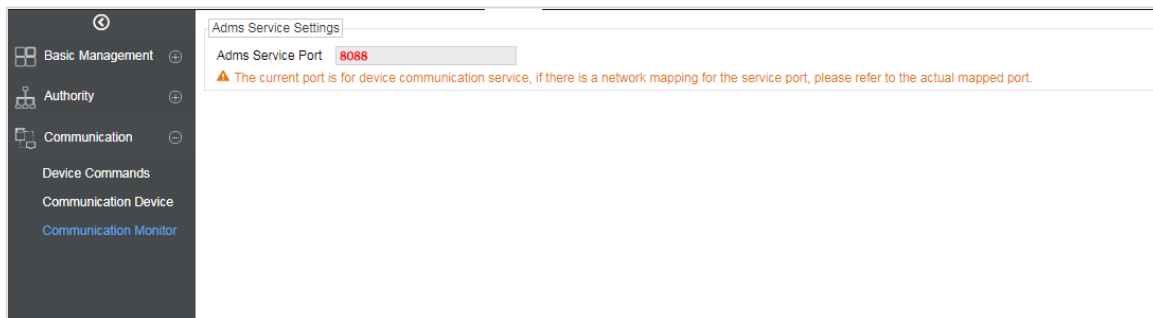
**Dirección del servidor:** Establecer como la dirección IP del servidor MTD ZKBioAccess.

**Puerto de servicio:** Establecer como puerto de servicio de ZKBioAccess MTD (el valor predeterminado es 8088).



#### Lado del software

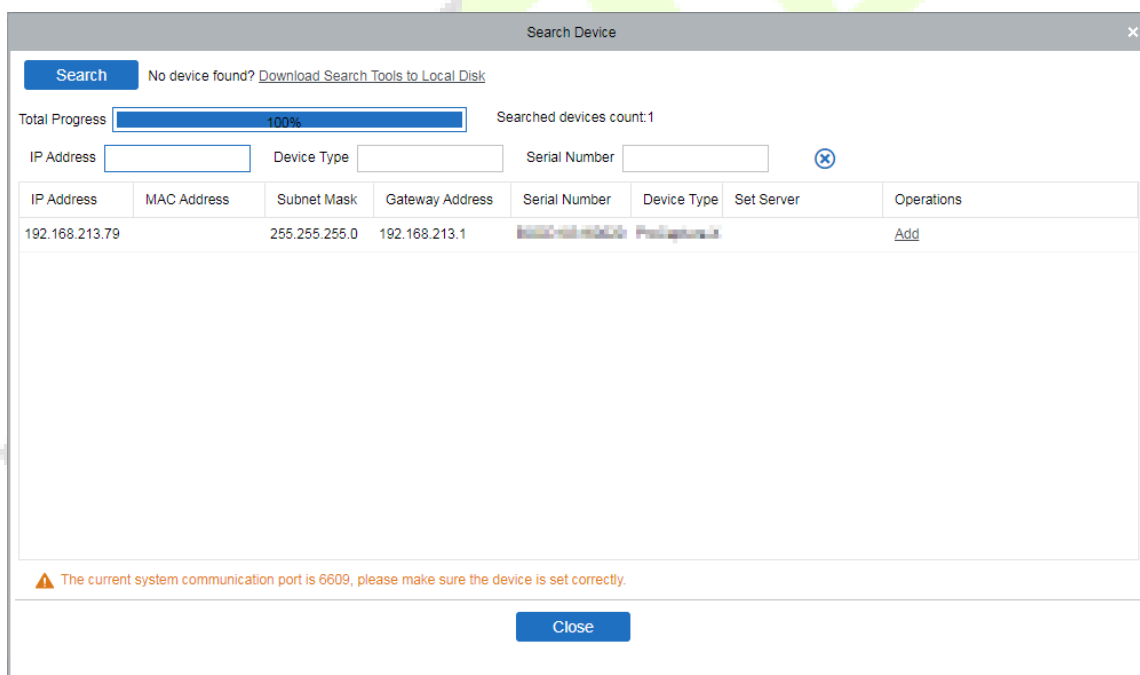
Inicie sesión en el software ZKBioAccess MTD, haga clic en **Sistema> Comunicación> Monitor de comunicación** para configurar el puerto de servicio ADMS, como se muestra en la siguiente figura:



## 14,2 Agregar dispositivo al software

Puede agregar un dispositivo buscando. El proceso es el siguiente:

- 1 ) Hacer clic **Control de acceso> Dispositivo> Dispositivo de búsqueda**, para abrir la interfaz de búsqueda.
- 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 ) Hacer clic **Añadir** para agregar el dispositivo específico al software.

## 14.3 Agregar personal al software

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

2. Después de configurar todos los parámetros, haga clic en **OKAY**.

## 14.4 Supervisión en tiempo real del software

Una vez instalado el software ZKBioAccess MTD, los usuarios pueden realizar varias operaciones de monitoreo:

1. Configure la dirección IP y la dirección del servidor del servicio en la nube en el dispositivo y agregue el dispositivo al software.
2. Haga clic en [ **Detección de temperatura** ]> [ **Gestión de temperatura** ]> [ **Monitorización en tiempo real** ] a 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.

3. Haga clic en [ **Gestión de temperatura** ]> [ **Panel de estadísticas** ] para ver el análisis de datos estadísticos 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.

### Monitoreo en tiempo real

### Panel de estadísticas

Personnel ID	First Name	Department Number	Department Name
3		1	Sales
2		1	Sales

**Nota:** Para otras operaciones específicas, consulte *Manual del usuario de ZKBioAccess MTD*.

## **Apéndice 1**

### **Requisitos para la recopilación en vivo y el registro de imágenes de caras con luz**

#### **visible**

- 1 ) Se recomienda realizar el registro en un entorno interior con una luz adecuada fuente sin subexposición o sobreexposición.
- 2 ) No apunte hacia fuentes de luz exteriores como puertas o ventanas u otras fuentes de luz fuertes.
- 3 ) Se recomiendan prendas de colores oscuros que sean diferentes del color de fondo para registro.
- 4 ) Muestre su cara y frente, y no se cubra la cara y las cejas con el cabello.
- 5 ) Se recomienda mostrar una expresión facial sencilla. Sonreír es aceptable, pero no cierre la ojos, o inclinar la cabeza hacia cualquier orientación. Se requieren dos imágenes para personas con anteojos, una imagen con anteojos y otra sin anteojos.
- 6 ) No use accesorios como bufandas o mascarillas que puedan cubrir su boca o barbilla.
- 7 ) Mire a la derecha hacia el dispositivo de captura y ubique su rostro en el área de captura de imágenes como mostrado en la Imagen 1.
- 8 ) No incluya más de una cara en el área de captura.
- 9 ) Se recomiendan 50 cm a 80 cm como distancia de captura, sujeto a la altura del cuerpo ajustable.



Área de captura de rostro Image1

## Requisitos para datos de imagen facial digital con luz visible

La foto digital debe ser de bordes rectos, coloreada, retratada a medias con una sola persona, y la persona debe ser inexplorada y sin uniforme. 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 una cara sencilla o una sonrisa con los ojos naturalmente abiertos.

### Gesto y ángulo

El ángulo de rotación horizontal no debe exceder  $\pm 10^\circ$ , la elevación no debe exceder  $\pm 10^\circ$  y el ángulo de depresión no debe exceder  $\pm 10^\circ$ .

### Accesorios

No se permiten máscaras y anteojos de colores. El marco de los anteojos no debe proteger 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**

La imagen debe tener un contorno claro, una escala real, una 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 ) Tasa de definición entre 358 x 441 y 1080 x 1920.
- 5 ) La escala vertical de la cabeza y el cuerpo debe ser 2: 1.
- 6 ) La foto debe incluir los hombros de la persona capturada al mismo nivel horizontal.
- 7 ) La persona capturada debe tener los ojos abiertos y el iris claramente visible.
- 8 ) Se prefiere una cara sencilla o una sonrisa, no se prefiere mostrar los dientes.
- 9 ) La persona capturada debe verse claramente, de color natural y sin un giro obvio de la imagen, no sombra, punto de luz o reflejo en la cara o el fondo, y el nivel de luminosidad y contraste adecuados.



## **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 civiles de reconocimiento de huellas dactilares capturan solo características, no imágenes de huellas dactilares, y no involucran 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 de los ciudadanos. 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 china 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 período de 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)	Cadmio (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	×	○	○	○	○	○
Empulveras	○	○	○	×	○	○

○ 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](http://www.zkteco.com)

