

# MANUAL DE USUARIO

## SpeedFace-V5L [P]

Fecha: Abril 2020

Versión: 1.1

Español

# Copyright © 2020 ZKTECO CO., LTD. Todos los Derechos Reservados

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

## Marca Registrada

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

## Descargo de Responsabilidad

Este manual contiene información sobre la operación y mantenimiento del equipo ZKTeco. Los derechos de autor en todos los documentos, dibujos, etc. en relación con el equipo suministrado por ZKTeco se confieren y son propiedad de ZKTeco. El contenido del presente no debe ser utilizado o compartido por el receptor con ningún tercero sin el permiso expreso por escrito de ZKTeco.

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

Es un pre-requisito esencial para la operación y mantenimiento satisfactorios que el personal de operación y mantenimiento esté completamente familiarizado con el diseño y que dicho personal haya recibido capacitación exhaustiva sobre el funcionamiento y mantenimiento de la máquina / unidad / equipo. Es esencial para la operación segura 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 o representación con respecto a la integridad de cualquier información contenida en este manual o cualquiera de las modificaciones hechas al mismo. ZKTeco no extiende la garantía de ningún tipo, incluida, entre otras, cualquier garantía de diseño, comerciabilidad o idoneidad para un particular propósito.

ZKTeco no asume responsabilidad por ningún error u omisión en la información o documentos a los que se hace referencia o se vincula a este manual. El usuario asume todo el riesgo en cuanto a los resultados y el rendimiento obtenidos del uso de la información.

ZKTeco en ningún caso será responsable ante el usuario o un tercero por daños incidentales, consecuentes, indirectos, especiales o ejemplares, incluidos, entre otros, pérdida de negocios, pérdida de ganancias, interrupción de negocios, pérdida de información comercial o cualquier pérdida material derivada de, en relación con, o relacionada con el uso de la información contenida o referenciada en este manual, incluso si ZKTeco tiene, la posibilidad de tales daños.

Este manual y la información que contiene pueden incluir imprecisiones técnicas, de otro tipo o errores tipográficos. ZKTeco cambia periódicamente la información aquí contenida que se incorporará a nuevas adiciones / modificaciones 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 una mejor operación y seguridad de la máquina / unidad / equipo. Dichas adiciones o enmiendas están destinadas a mejorar las operaciones de la máquina / unidad / equipo y dichas enmiendas no otorgarán ningún derecho a reclamar compensación o daños bajo ninguna circunstancia.

ZKTeco no será responsable de ninguna manera (i) en caso de mal funcionamiento de la máquina / unidad / equipo 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 operación de la máquina y el equipo en condiciones diferentes a las prescritas en el manual.

El producto se actualizará periódicamente sin previo aviso. Los últimos procedimientos de operación y documentos relevantes están disponibles en <http://www.zkteco.com>.

Si hay algún problema relacionado con el producto, contáctenos.

## Sede Central de ZKTeco

**Dirección:** ZKTeco Industrial Park, No. 26, 188 Industrial Road, Tangxia Town, Dongguan, China.

**Teléfono:** +86 769 - 82109991

**Fax:** +86 755 - 89602394

Para consultas relacionadas con el negocio, escríbanos a: [sales@zkteco.com](mailto:sales@zkteco.com).

Para saber más sobre nuestras sucursales en el mundo, visite [www.zkteco.com](http://www.zkteco.com).

## Acerca de la Compañía

ZKTeco es uno de los mayores fabricantes de lectores de RFID y biométricos (huellas dactilares, faciales, venas digitales) más grandes del mundo. Las ofertas de productos incluyen Lectores y Paneles de Control de Acceso, Cámaras de Reconocimiento Facial de rango cercano y alejado, controladores de Ascensores, Torniquetes, Cámaras de Reconocimiento de Placas Vehiculares (LPR) y productos de Consumo, que incluyen cerraduras de puerta con lector de huellas digitales y cerraduras de puertas. Nuestras soluciones de seguridad son multilingües y están localizadas en más de 18 idiomas diferentes. En las modernas instalaciones de fabricación con certificación ISO9001 de 700,000 pies cuadrados de ZKTeco, controlamos la fabricación, el diseño de productos, el ensamblaje de componentes y la logística, todo bajo un mismo techo.

Los fundadores de ZKTeco se han determinado la investigación y el desarrollo independientes de los procedimientos y la producción del SDK de verificación biométrica, que inicialmente se aplicó ampliamente en los campos de seguridad de PC y autenticación de identidad. Con la mejora continua del desarrollo y muchas 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 las 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 es seleccionada como la Empresa Nacional de Alta Tecnología por 6 años consecutivos. Sus productos están protegidos por derechos de propiedad intelectual.

## Acerca del Manual

Este manual presenta las operaciones del producto SpeedFaceV5L[P].

Todas las imágenes mostradas son sólo para fines ilustrativos. Las cifras en este manual pueden no ser exactamente consistentes con los productos reales.

# Convenciones del Documento

La convención utilizada en este manual se enumeran a continuación:

## Convención Gráfica

Del Software	
Convención	Descripción
<b>Negrita</b>	Se utiliza para identificar nombres de interfaz de software, ejemplo OK, Confirmar, Cancelar
>	Niveles múltiples de los Menús están separados por estos corchetes. Ejemplo, Archivo > Crear > Carpeta

Del Dispositivo	
Convención	Descripción
< >	Nombre de botones o teclas en el dispositivo. Ejemplo, presione <OK>
[ ]	Nombres de ventana, elementos de menú, tabla de datos y nombres de campo están entre corchetes. Ejemplo, abra la ventana [Nuevo Usuario]
/	Menús de varios niveles están separados por barras diagonales. Ejemplo, [Archivo / Crear / Carpeta]

Símbolos	
Convención	Descripción
	Esto implica sobre el aviso o prestar atención, en el manual
	Información general que ayuda a realizar las operaciones más rápido
	Información que es importante
	Para evitar errores
	Declaración o evento de advertencia

# Contenido

<b>1. Visión General</b>	<b>07</b>
<b>2. Procedimiento Operacional</b>	<b>12</b>
Registro facial	12
Registro de palma	13
Modos de verificación	14
<b>3. Menú principal</b>	<b>22</b>
<b>4. Gestión de usuarios</b>	<b>23</b>
Agregar usuarios	23
Búsqueda de usuarios	26
Editar usuarios	26
Eliminar usuarios	27
<b>5. Rol de usuario</b>	<b>27</b>
<b>6. Configuración de comunicación</b>	<b>28</b>
Configuración de red	28
Conexión a PC	29
Configuración del servidor de nube	29
Configuración de Wiegand	30
<b>7. Configuración del sistema</b>	<b>33</b>
Fecha y hora	33
Ajustes de eventos de acceso	34
Parámetros de huella dactilares	35
Parámetros de rostro	36
Parámetros de palma	38
Restablecimiento de fábrica	38
<b>8. Personalización</b>	<b>39</b>
Configuración de la interfaz	39
Configuración de voz	40
Timbre	40
<b>9. Gestión de datos</b>	<b>42</b>
Eliminar datos	42
<b>10. Control de acceso</b>	<b>44</b>
Opciones de control de acceso	44
Horario	46
Configuración de vacaciones	47
Configuración de verificación combinada	47
Configuración Anti-Passback	49
Configuración de las opciones de amago	49
<b>11. Búsqueda de asistencia</b>	

<b>12. Autotest</b>	<b>50</b>
<b>13. Pruebas del sistema</b>	<b>51</b>
<b>14. Conectarse al Software ZKBioAccess / ZKBioSecurity</b>	<b>52</b>
Establecer la dirección de comunicación	
Agregar dispositivo al software	<b>53</b>
Agregar personal al software	53
	54
<b>Apéndice 1</b>	<b>55</b>
Requisitos para la recopilación en vivo y el registro de imágenes visible light	<b>56</b>
Requisitos para datos de imagen facial digital visible Light Digital	56
	57
<b>Apéndice 2</b>	
Declaración sobre el derecho a la privacidad	<b>58</b>
Eco-friendly operación	58
	59

# 1. Visión General

Este documento describe el procedimiento operativo del dispositivo SpeedFace-V5L Series. Los módulos operativos del dispositivo incluyen administración de usuarios, asignación de roles de usuario, comunicación del dispositivo, detección de temperatura y máscaras, 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.

## Instrucciones de uso

### Posición de huella y colocación de dedo

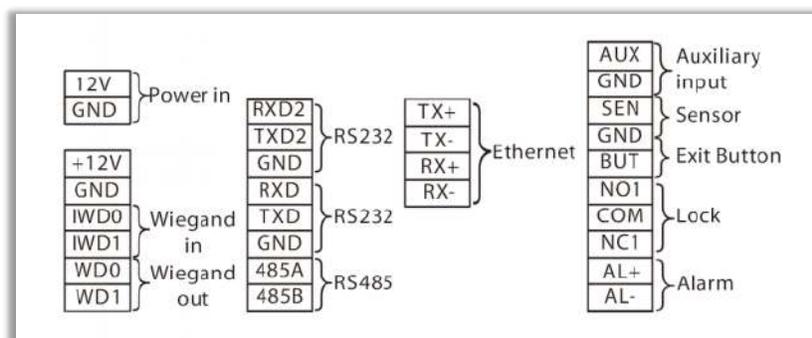
Dedos recomendados: dedos índice, medio o anular; Evite usar el pulgar o el meñique, ya que es difícil presionarlos con precisión sobre el lector de huellas dactilares.



**NOTA:** Utilice el método correcto al presionar con los dedos el lector de huellas dactilares 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.

Categoría	Característica	Descripción
<b>Cartas credenciales</b>	Biometría	Cara / Palma / Huella
	Tarjeta	ID o Mifare opcional
	Contraseña	Números (máximo 8 dígitos)
<b>General</b>	Tipo de LCD	LCD TFT de 5 pulgadas
	Resolución LCD	720 * 1280
	Temperatura de funcionamiento	0 ° C a 45 ° C (32 ° F a 113 ° F)
	Humedad de funcionamiento	20% a 80% de humedad relativa
	Dimensiones (AnxAlxPr)	92 (ancho) x203 (alto) x22.5 (profundidad) mm
	Usuarios máximos (1: N)	3000
<b>Capacidad</b>	Registros de transacciones máximas	1500
	Wifi	Soportadon opcional
<b>Eléctrico</b>	Energía	12 V, 3 A

## Diagrama de PIN del producto



## Configuración de la instalación

### Precauciones de seguridad

- Mantenga el dispositivo alejado del agua o la humedad. Evite que entre agua o humedad en el chasis del dispositivo de asistencia.
- No coloque el dispositivo sobre una caja o escritorio inestable. El dispositivo podría dañarse gravemente en caso de caída.
- Asegure la ventilación adecuada de la sala de equipos y mantenga las rejillas de ventilación del dispositivo libres de obstrucciones.
- Asegúrese de que el voltaje de operación sea el mismo que el etiquetado en el dispositivo de asistencia.
- No abra el chasis cuando el dispositivo de asistencia esté en funcionamiento o cuando existan peligros eléctricos para evitar descargas eléctricas.

### Lugar de instalación

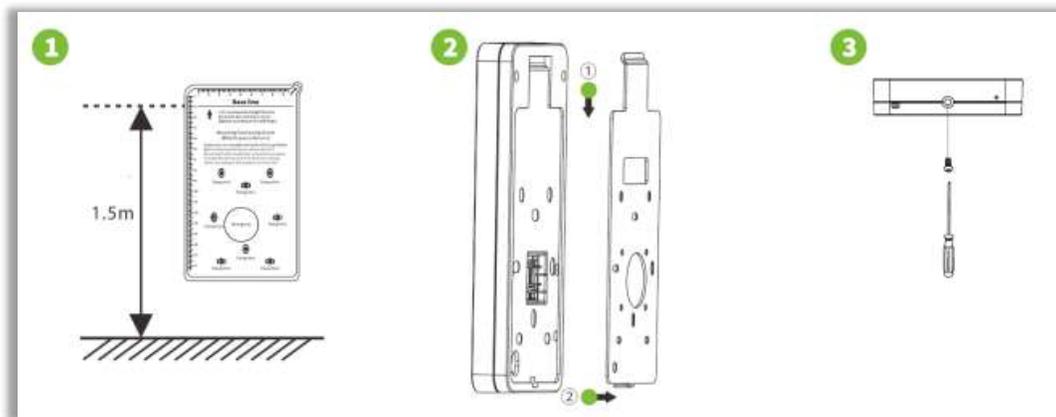
El dispositivo debe instalarse en interiores y debe reservarse un espacio suficiente en las rejillas de entrada / salida de aire para la disipación del calor.

### Herramientas de instalación

- Destornillador de punta plana
- Destornillador Phillips: P2-150mm

### Pasos de instalación

Asegúrese de que el dispositivo esté instalado según las instrucciones de instalación. Si desea abrir el chasis, debe comunicarse con el agente para obtener permiso. De lo contrario, sufrirá las consecuencias derivadas de sus acciones.



**Paso 1:** Pegue el adhesivo de la plantilla de montaje en la pared y taladre los orificios de acuerdo con el papel de montaje. Fije la placa trasera en la pared con tornillos de montaje en pared.

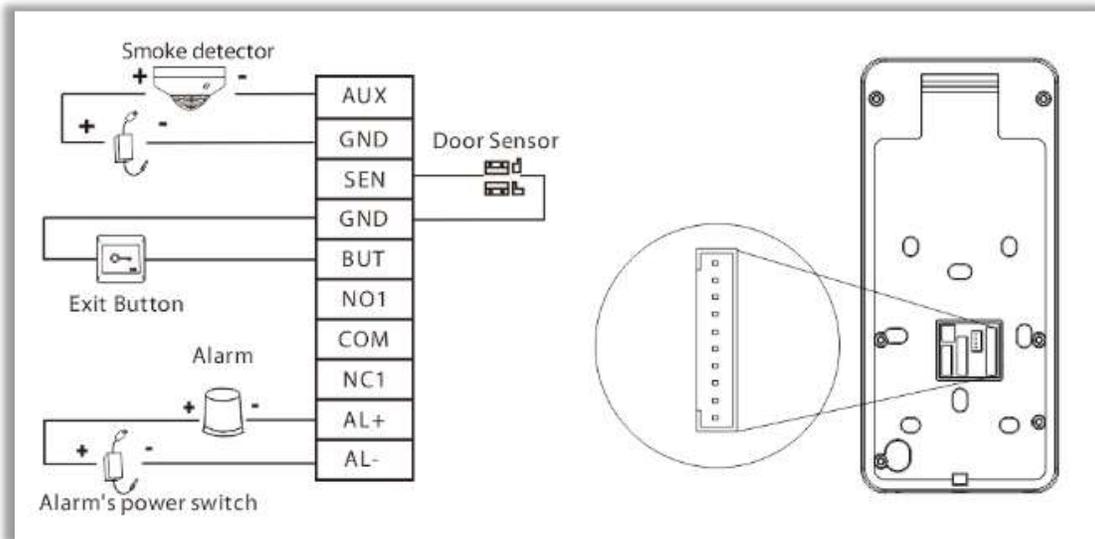
**Paso 2:** Coloque el dispositivo en la placa posterior.

**Paso 3:** Fije el dispositivo a la placa posterior con un tornillo de seguridad.

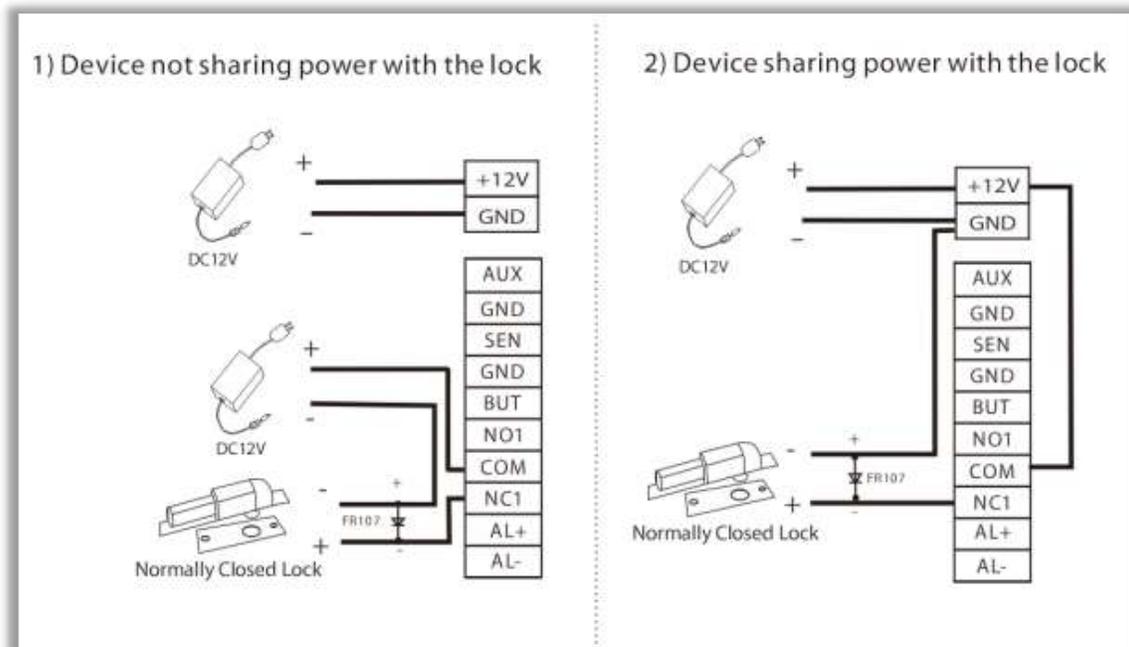
## Procedimiento de Conexión

### Conexión de botones y dispositivos auxiliares

- Conecte el botón Exit a los terminales GND y BUT
- Conecte el sensor de puerta a los terminales SEN y GND
- Conecte la alarma a los terminales AL + y AL-
- Conecte el dispositivo auxiliar a los terminales GND y AUX

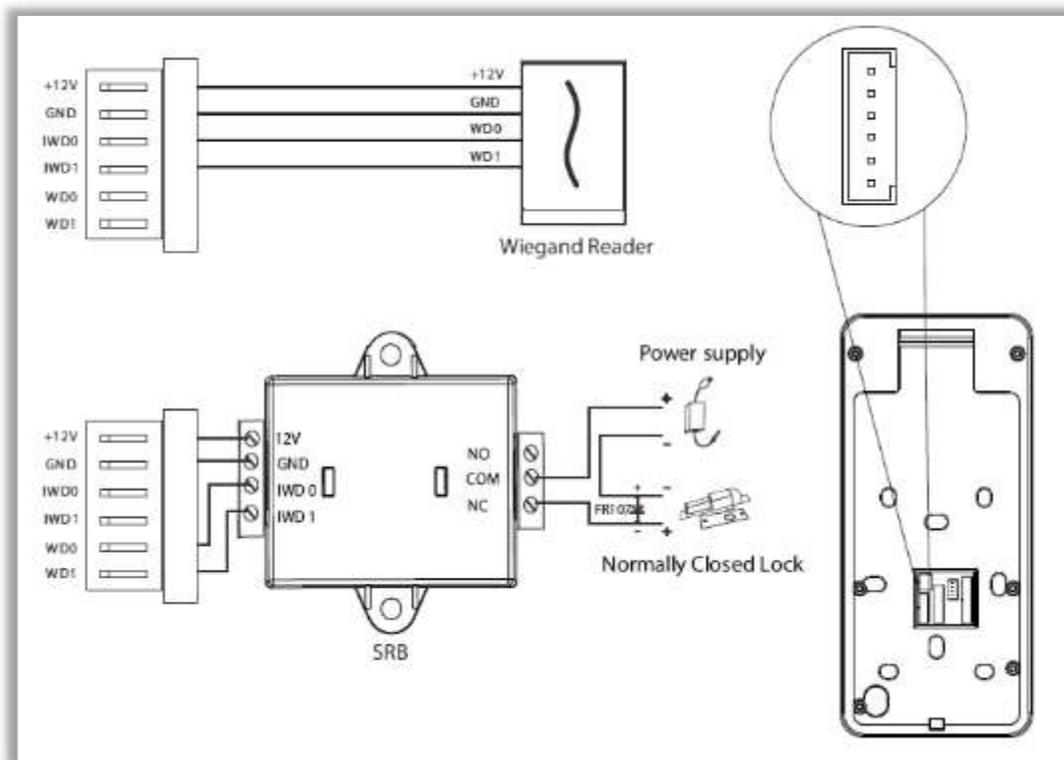


### Conexión de relé a cerradura



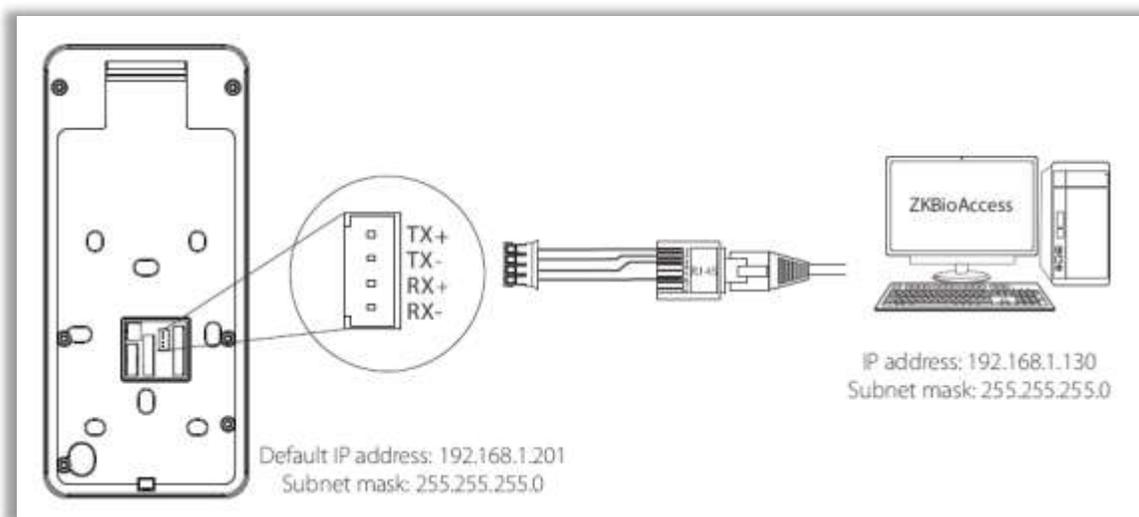
- El dispositivo admite condiciones normalmente abiertas y normalmente cerradas.
- La cerradura normalmente cerrada está conectada a los terminales NC 1 y COM.

## Conexión del lector Weigand / SRB



- Conecte los terminales WDO y WD1 al SRB .
- Conectar el IWD0, IWD1, GND, + 12V terminales hasta el lector de Weigand.

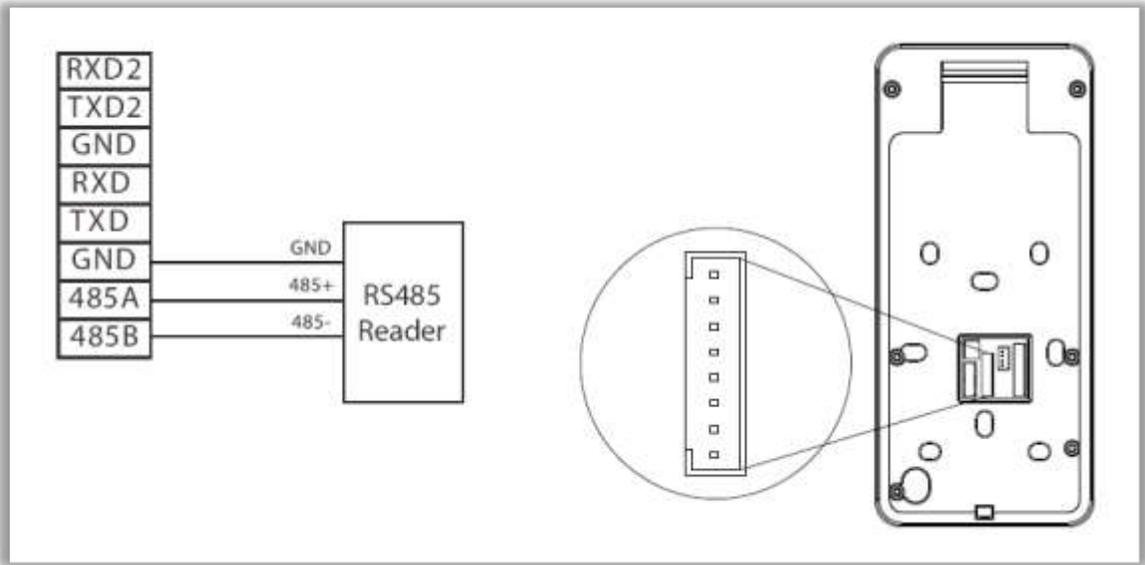
## Conexión a Ethernet



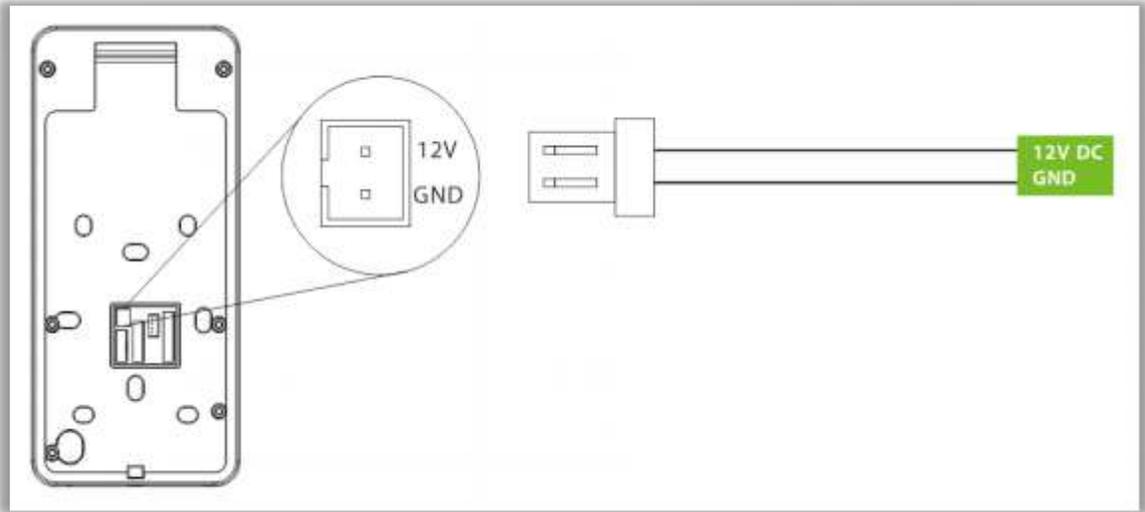
- Haga clic en [COM.] > [Ethernet] > [Dirección IP] , introduzca la dirección IP y haga clic en [Aceptar] .

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

Conexión RS485



Energía



## 2. Procedimiento Operacional

### 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 ve así:



#### Precauciones 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 a cambiar el rostro de expresión. ( cara sonriente , cara dibujada , guiño, etc.)
- Si usted que no sigue las instrucciones en la pantalla, el rostro de registro puede tomar más tiempo o puede fallar.
- Tenga cuidado de no a cubrir los ojos o cejas.
- No usar sombreros, máscaras, gafas de sol o gafas.
- Tenga cuidado de no a mostrar dos caras en la pantalla. Registre una persona en un tiempo.

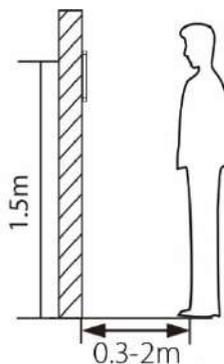
#### Precauciones para autenticar un rostro:

- Asegúrese de que los cara aparece dentro de la directriz en la pantalla de la dispositivo.
- Si se han cambiado las gafas, la autenticación puede fallar. Si se ha registrado la cara sin gafas, autentique la cara sin gafa 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 , no cubrir la cara; permitir que el dispositivo para reconocer tanto las cejas y la cara.

## Posiciones correctas e incorrectas

Posición de pie, expresión facial y postura:

- La distancia recomendada



Se recomienda tener un espacio de 0,5 m entre el dispositivo y el usuario cuya altura esté en un rango de 1,55m a 1,85 m. Los usuarios pueden moverse ligeramente hacia adelante o hacia atrás para mejorar el reconocimiento facial.

- Expresión facial y postura de pie

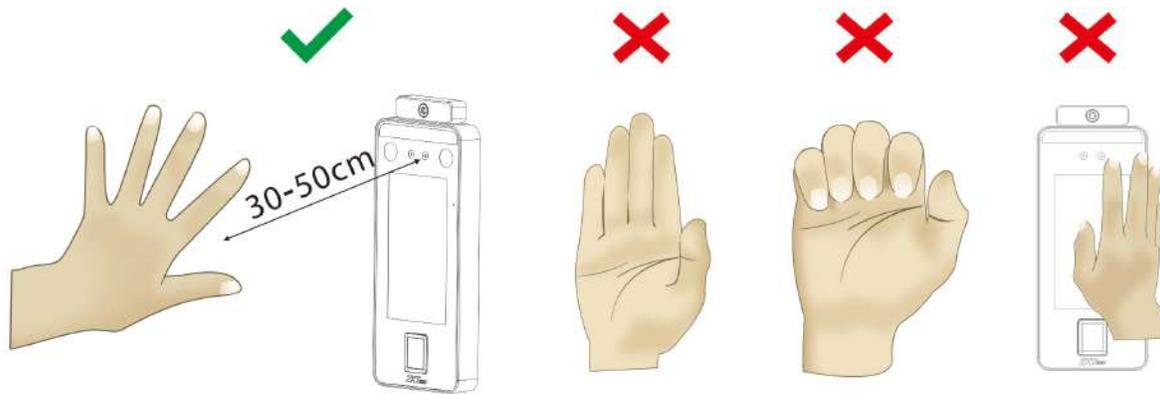


NOTA : Durante la inscripción y la verificación, por favor, mantener naturales facial expresión y de pie postura.

## Registro de Palma

Coloque la Palma de la mano en el área de recolección multimodo de la Palma, de modo que la Palma quede paralela al dispositivo.

Asegúrate de dejar espacio entre tus dedos.



## Modos de verificación

### Verificación de huellas dactilares

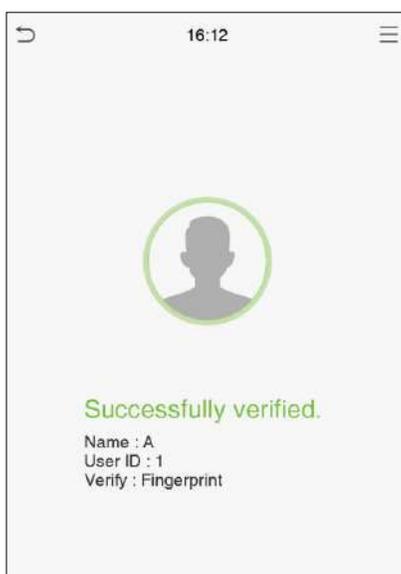
Modo de verificación de huellas dactilares 1: N (uno a muchos)

Compara la huella dactilar que se presiona en el lector de huellas dactilares con todos los datos de huellas dactilares que se almacenan en el dispositivo.

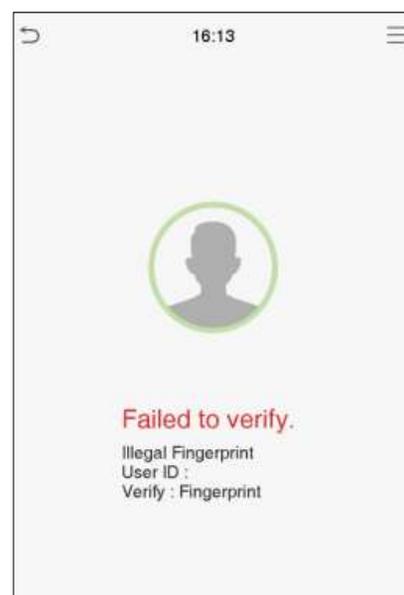
El dispositivo entrará en el modo de autenticación de huellas dactilares cuando un usuario presione su dedo sobre el escáner de huellas dactilares.

Siga la forma correcta de colocar el dedo en el sensor. Para obtener más información, consulte 2.1 Colocación de los dedos.

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.

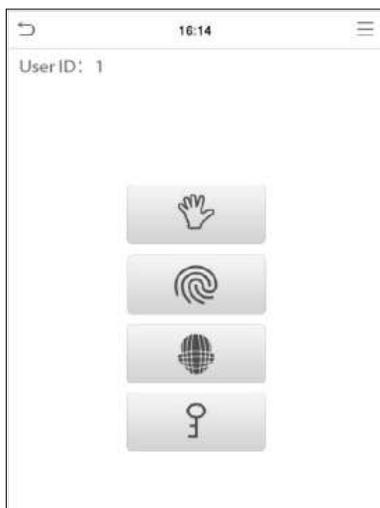
Los usuarios pueden intentar verificar sus identidades con el modo de verificación 1: 1 cuando no pueden obtener acceso con el método de autenticación 1: N.

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

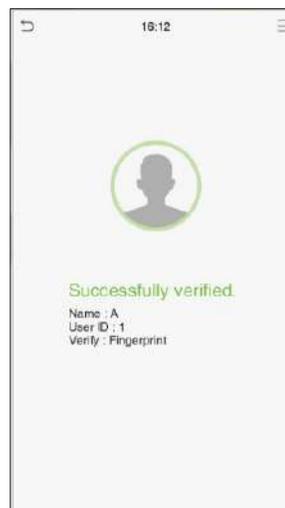
Si el usuario ha registrado palma, rostro y contraseña además de sus huellas dactilares, y el método de verificación está configurado como verificación de palma / huella dactilar / rostro / contraseña, aparecerá la siguiente pantalla. Selecciona el Icono de huella digital para ingresar al modo de verificación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



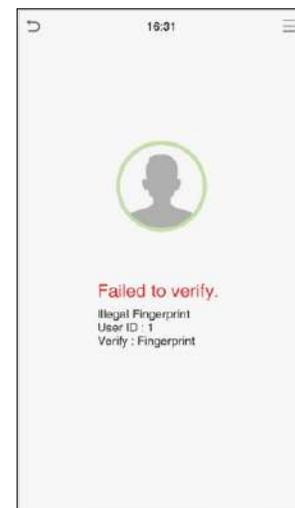
Presione la huella digital para verificar



La verificación es exitosa



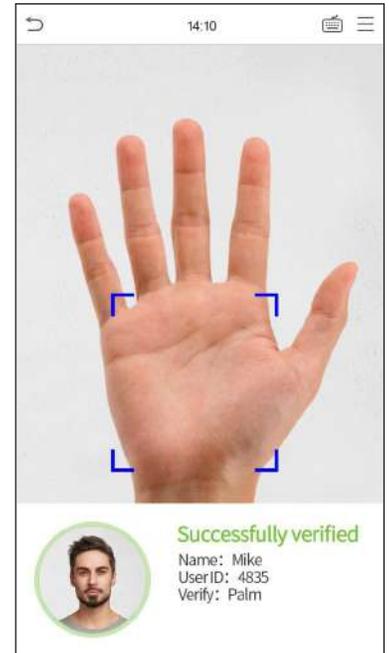
Verificación Fallida



## Palma

### Modo de verificación de Palma 1:N

Compare la imagen de la palma recopilada por el colector de palma con todos los datos de la palma del dispositivo. El dispositivo distinguirá automáticamente entre la palma y el modo de verificación facial, y colocará la palma en el área que puede ser recolectada por el recolector de palma, y el dispositivo detectará automáticamente el modo de verificación de la palma.



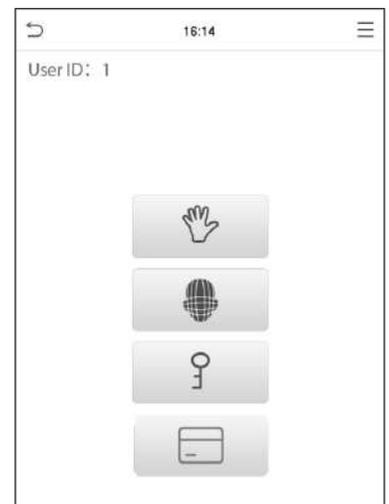
### Modo de verificación de Palma1:1

Haga clic en el botón  de la pantalla principal para abrir el modo de verificación de Palma1:1 (uno a uno).

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



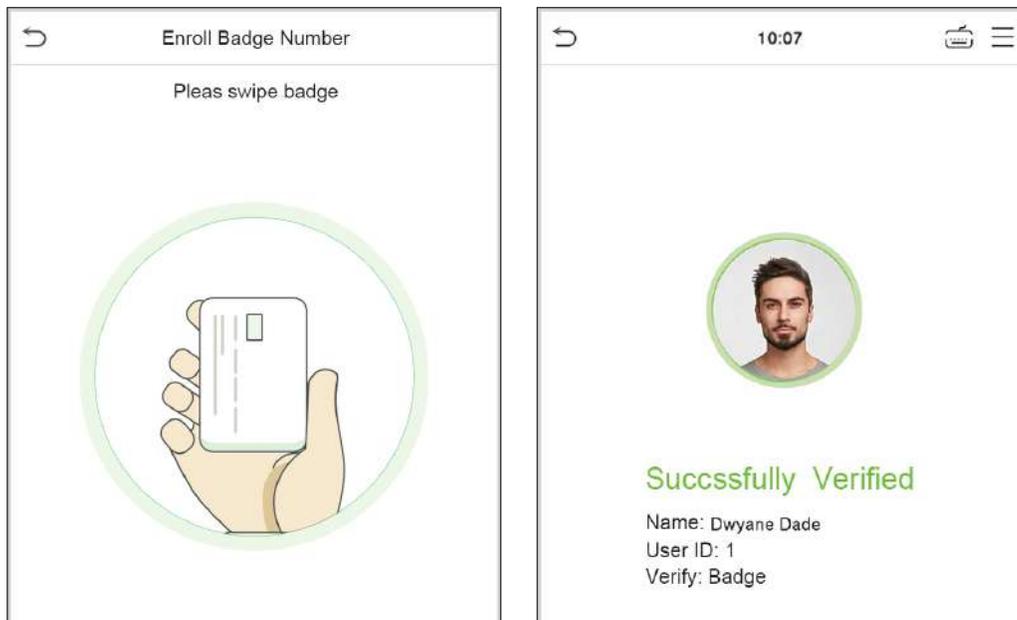
Si el usuario ha registrado tarjeta, rostro y contraseña además de la Palma, y el método de verificación está configurado en Contraseña / Tarjeta / Rostro / Palma, aparecerá la siguiente pantalla. Seleccione el icono de la Palma  para ingresar al modo de verificación de la Palma.



## Tarjeta \*

### Verificación de tarjeta 1: N

Coloque la tarjeta registrada en el área de lectura de tarjetas.



### Verificación de tarjeta 1: 1

Presione  en la pantalla principal para ingresar la verificación de tarjeta 1:1:

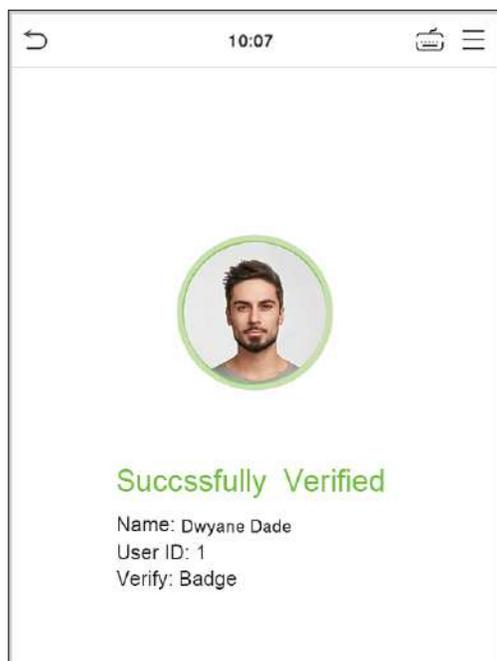
1. Ingrese su ID de usuario y haga clic en Aceptar.



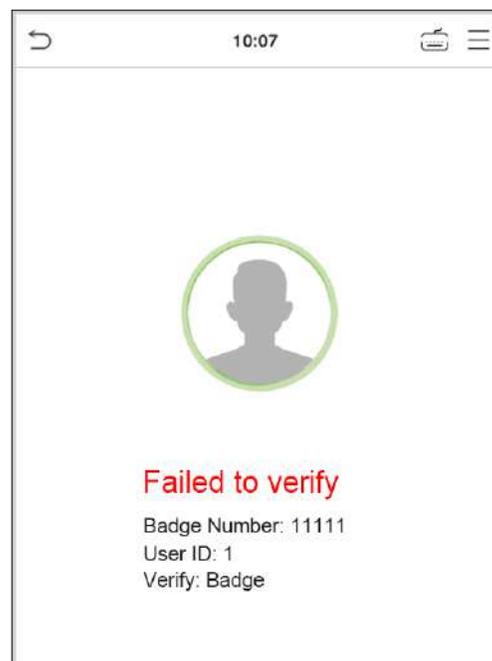
2. Si el empleado registra cara, contraseña y palma además de tarjeta, aparecerá la siguiente pantalla. Seleccione el icono para ingresar al modo de verificación de credencial.



Verificación es exitosa



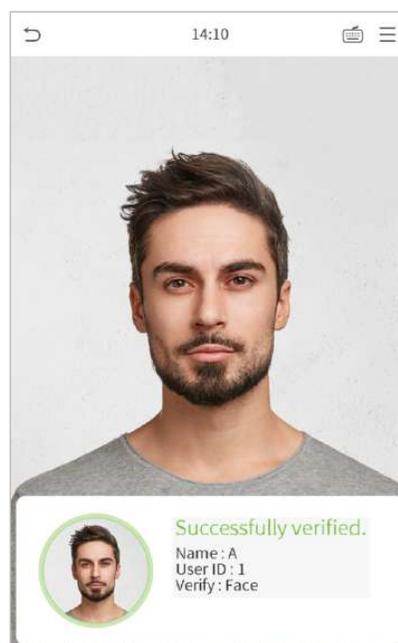
Verificación Fallida



## Rostro

### Verificación facial 1: N

Compare las imágenes faciales adquiridas con todos los datos faciales registrados en el dispositivo. A continuación se muestra el cuadro emergente del resultado de la comparación.



## Verificación facial 1: 1

Compare el rostro capturado por la cámara con la plantilla facial relacionada con el ID de usuario ingresado.

Presione  en la interfaz principal e ingrese al modo de verificación facial 1: 1.



Introduzca la ID de usuario y haga clic en Aceptar.

Si un empleado registra contraseña ,credencial y palma, además de rostro, aparecerá la siguiente pantalla. Seleccione el icono  para ingresar al modo de verificación facial.

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

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

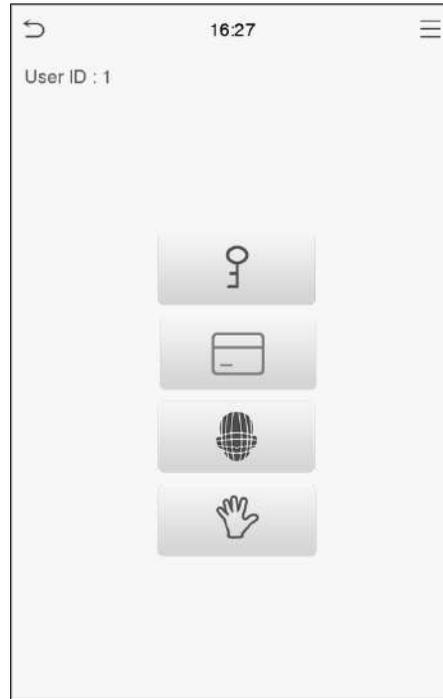
## Contraseña

Compare la contraseña ingresada con el ID de usuario y la contraseña registrados.

Haga clic en el botón  en la pantalla principal para ingresar al modo de verificación de contraseña 1: 1.



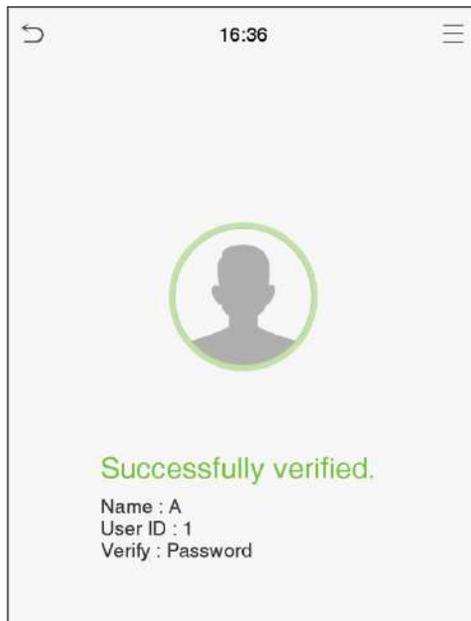
Ingrese el ID de usuario y haga clic en Aceptar.



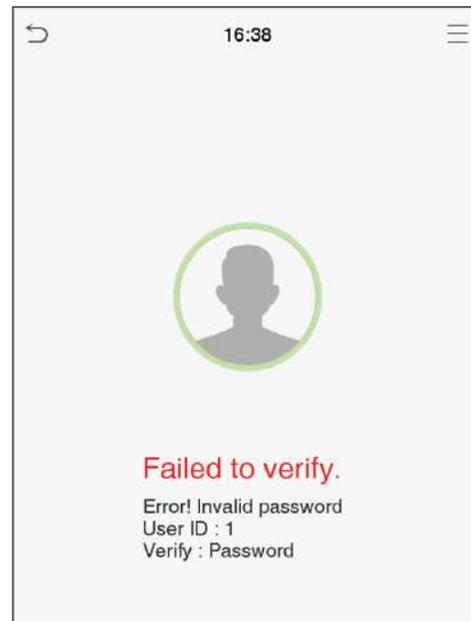
Si un empleado registra cara , credencial y palma además de la contraseña, aparecerá la siguiente pantalla. Seleccione el icono  para ingresar al modo de verificación de contraseña.



Introduzca la contraseña y haga clic en Aceptar.



Verificación es exitosa



Error de Verificación

## Combinación

Para aumentar la seguridad, este dispositivo ofrece la opción de utilizar múltiples formas de métodos de verificación.

Verification Mode	
<input checked="" type="radio"/>	Password/Badge/Face/Palm
<input type="radio"/>	User ID only
<input type="radio"/>	Password
<input type="radio"/>	Badge only
<input type="radio"/>	Password+Badge
<input type="radio"/>	Password/Badge
<input type="radio"/>	Face Only
<input type="radio"/>	Face+Password
<input type="radio"/>	Face+Badge
<input type="radio"/>	Palm

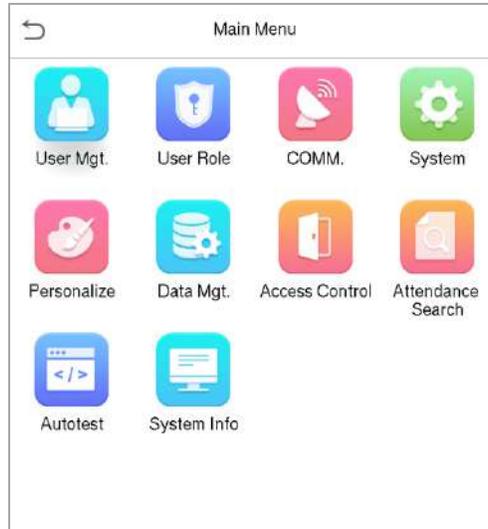
### Notas:

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

2). Debe registrar la información de verificación requerida antes de usar el modo de verificación de combinación; 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

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



Menú	Descripción
Admin. de Usuarios	Para agregar, editar, ver y eliminar información básica sobre un usuario.
Rol de Usuario	Para establecer el alcance del permiso del rol personalizado y el registrador, es decir, los derechos para operar el sistema.
Red - COMM	Para configurar los parámetros relevantes de red, comunicación en serie, conexión a PC, WIFI, nube servidor y Wiegand.
Sistema	Para configurar los parámetros relacionados con el sistema, incluida la fecha y la hora, los registros de acceso, las plantillas faciales, restablecimiento de la configuración de fábrica.
Personalizar	Para personalizar la configuración de la pantalla de la interfaz, el audio y el timbre.
Gestión de Datos	Para eliminar todos los datos relevantes en el dispositivo.
Control de Acceso	Para configurar los parámetros de la cerradura y el dispositivo de control de acceso correspondiente.
Búsqueda de Asistencia	Consulte el registro de acceso especificado, verifique las fotos de asistencia y las fotos de la lista negra.
Pruebas	Para probar automáticamente si cada módulo funciona correctamente, incluida la pantalla LCD, la voz, la cámara y el reloj en tiempo real.
Inf. del Sistema	Para ver la capacidad de datos, el dispositivo y la información de firmware del dispositivo actual.

## 4. Gestión de Usuarios

### Agregar usuarios

Haga clic en User Mgt. en el menú principal.

Haga clic en Nuevo usuario.

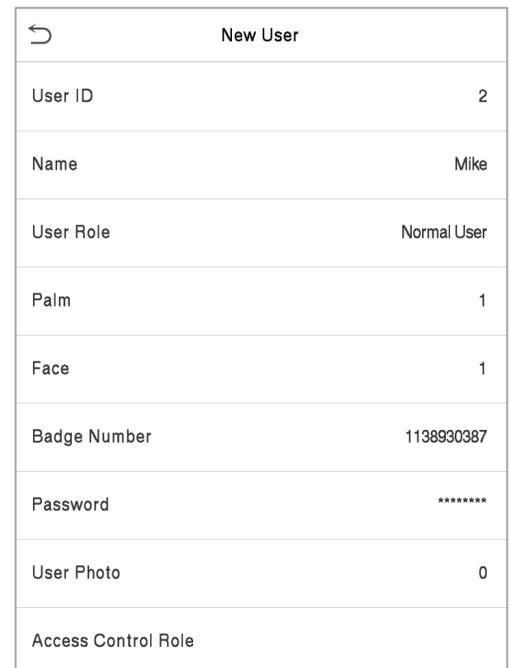
Registrar un ID de usuario y un nombre

Ingrese el ID de usuario y el nombre



### Notas:

1. Un nombre de usuario puede contener 17 caracteres.
2. El ID de usuario puede contener de 1 a 9 dígitos predeterminadamente.
3. Durante el registro inicial, puede modificar su ID, que no se puede modificar después del registro.
4. Si aparece un mensaje "El ID ya existe", debe elegir otro ID.



New User	
User ID	2
Name	Mike
User Role	Normal User
Palm	1
Face	1
Badge Number	1138930387
Password	*****
User Photo	0
Access Control Role	

### Configuración de la función del usuario

Hay dos tipos de cuentas de usuario: los usuarios normales y el superadministrador. 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 gestión. Si se establece un rol personalizado, también puede seleccionar permisos de rol personalizados para el usuario.

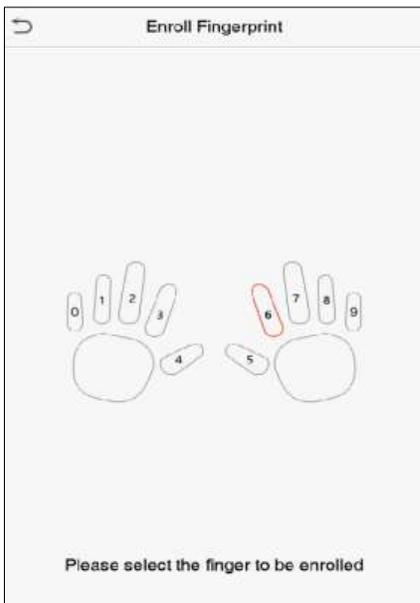
Haga clic en función de usuario para seleccionar Usuario normal o Super administrador.



**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 2.4 Método de verificación.

## Registrar Huella Digital

Haga clic en Huella digital para abrir la página de registro de huellas digitales. Seleccione la huella digital que desea registrar.



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



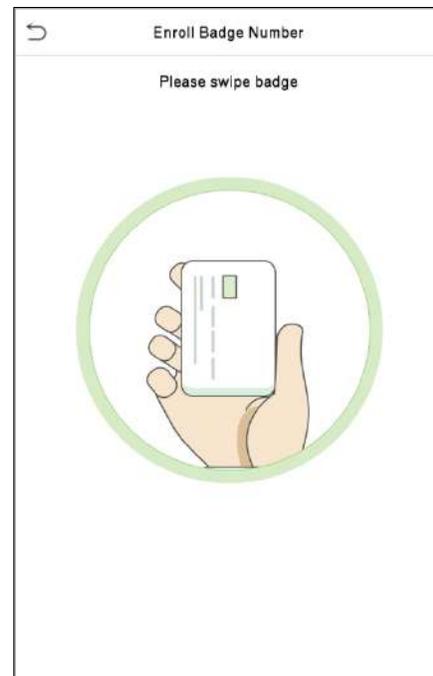
## Registrar Palma

Haga clic en palma para entrar en la página de registro de palma. Seleccione la palma que desea enrolar.



## Registrar Tarjeta\*

Haga clic en Badge number para ingresar a la página de registro de la tarjeta y coloque la tarjeta en el área de lectura de tarjetas. La interfaz de registro es la siguiente:



## Registrar Rostro

Haga clic en Rostro para ingresar a la página de registro de rostros. Mire hacia la cámara y quédese quieto durante el registro facial. La interfaz de registro es la siguiente:



## Registrar Contraseña

Haga clic en Contraseña para ingresar a la página de registro de contraseña. Ingrese una contraseña y vuelva a ingresarla. Haga clic en Aceptar . Si las dos contraseñas ingresadas son diferentes, aparecerá el mensaje "La contraseña no coincide".

**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.

Haga clic en 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 capturará 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.

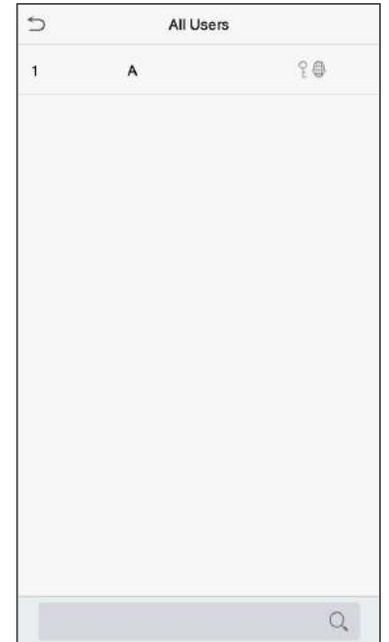
## Rol de Control de Acceso

El control de acceso del usuario establece los derechos de desbloqueo de la puerta de cada persona, incluido el grupo al que pertenece el usuario, el modo de verificación y si se aplica el período de tiempo del grupo.

Haga clic en Función de control de acceso > Grupo de acceso , asigne 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.

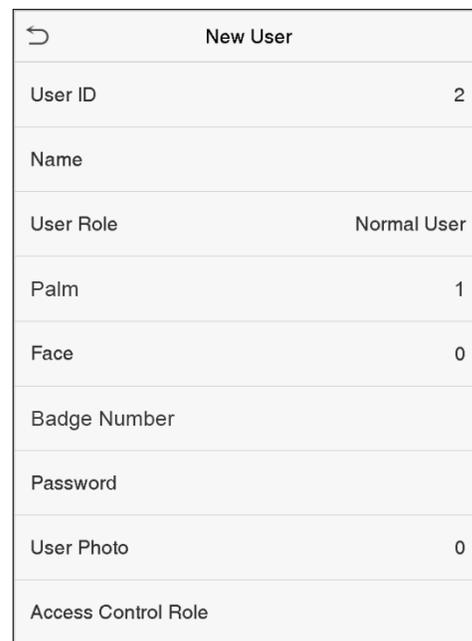
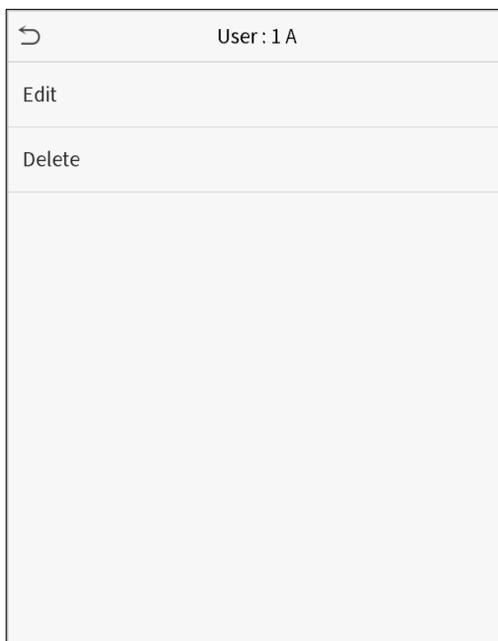
## Búsqueda de usuarios

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



## Editar usuarios

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



**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 “43.1 Agregar usuarios”.

## Eliminar usuarios

Seleccione un usuario de la lista y haga clic en Eliminar para ingresar a la interfaz de eliminación de usuario. Seleccione la información de usuario que desee eliminar y haga clic en Aceptar.

**Nota:** Si selecciona Eliminar usuario, se eliminará toda la información del usuario.

## 5. Rol de Usuario

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

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

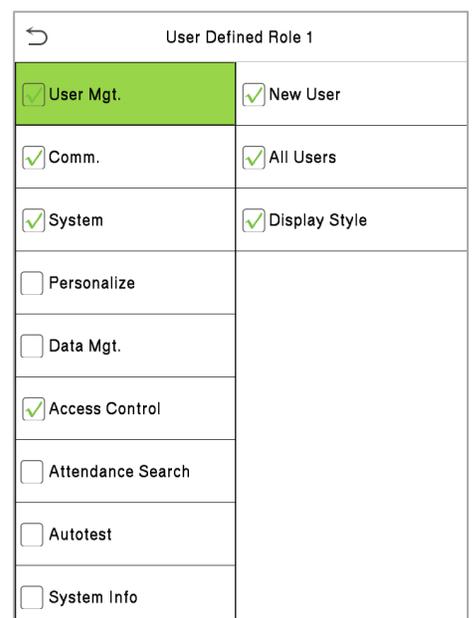
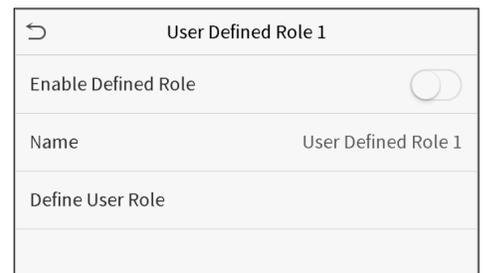
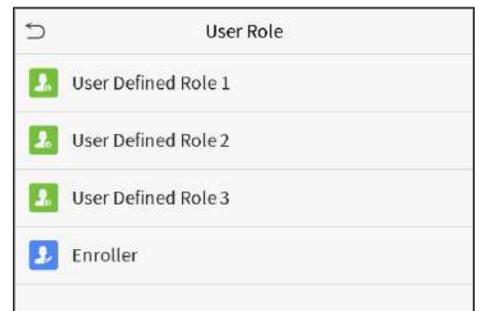
Haga clic en Rol de usuario en la interfaz del menú principal.

1. Haga clic en cualquier rol de usuario para establecer un rol definido. Alterne el botón Habilitar rol definido para habilitar este rol definido. Haga clic en Nombre e ingrese el nombre del rol.

2. Haga clic en Definir función de usuario para asignar privilegios a la función. Una vez que se complete la asignación de privilegios, haga clic en Volver.

**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 ha s una función activada, puede asignar las funciones que establezca para los usuarios haciendo clic con el usuario Mgt. > Nuevo usuario> Rol de usuario.



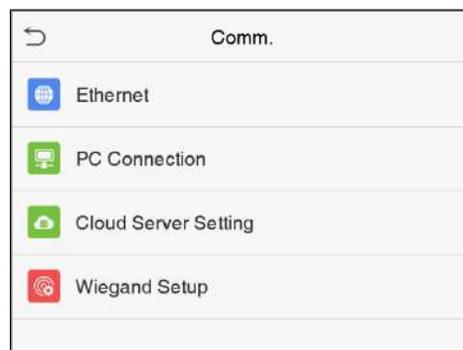
Si no hay ningún superadministrador registrado, el dispositivo le preguntará “¡Primero enrole al superadministrador!” después de hacer clic en la barra de habilitar.



## 6. Configuración de Comunicación

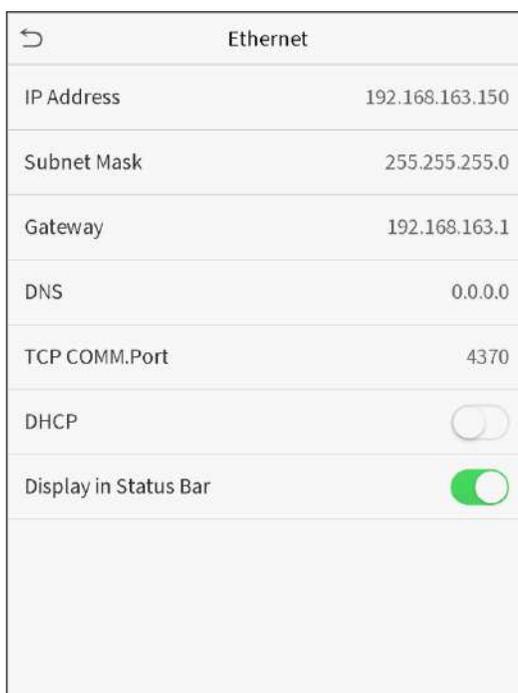
Configure los parámetros de la red, la conexión a la PC, el servidor en la nube y Wiegand.

Toque COMM. en el menú principal.



### Configuración de 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. Haga clic en Ethernet en Comm. Interfaz de configuración



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

## Conexión a PC

Para mejorar la seguridad de los datos, configure una clave de comunicación para la comunicación entre el dispositivo y la PC. Si se configura una clave de comunicación, se debe ingresar esta contraseña de conexión antes de que el dispositivo se pueda conectar al software de la PC.

Haga clic en Conexión a PC en RED. Interfaz de configuración .

PC Connection	
Comm Key	0
Device ID	1

Menú	Descripción
Clave de comunicación	Clave de comunicación: la contraseña predeterminada es 0, que se puede cambiar. La clave de comunicación puede contener de 1 a 6 dígitos.
ID del dispositivo	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 .

## Configuración del servidor de nube

Esto representa la configuración utilizada para conectarse con el servidor ADMS. Haga clic en Configuración del servidor en la nube en 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 nombre de dominio	Dirección del servidor	Cuando esta función está habilitada, se utilizará 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.
Deshabilitar el nombre de dominio	Dirección del servidor	Dirección IP del servidor ADMS
	Puerto de servicio	Puerto 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.

## Configuración de Wiegand

Para configurar los parámetros de entrada y salida de Wiegand. Haga clic en Configuración de Wiegand en Comm. Interfaz de configuración.

←
**Wiegand Setup**

Wiegand Input

---

Wiegand Output

## Entrada Wiegand

←
**Wiegand Options**

Wiegand Format

---

Wiegand Bits 26

---

Pulse Width(us) 100

---

Pulse Interval(us) 1000

---

ID Type Badge Number

Menú	Descripción
Formato Wiegand	Los valores oscilan entre 26 bits, 34 bits, 36 bits, 37 bits y 50 bits.
Bits de salida Wiegand	Después de elegir el formato Wiegand, puede seleccionar uno de los dígitos de salida correspondientes en el formato Wiegand
Identificación Fallida	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.
Código del Sitio	Es similar al ID del dispositivo. La diferencia es que un código de sitio se puede configurar manualmente y es repetible en un dispositivo diferente. El valor válido varía de 0 a 256 de forma predeterminada.
Ancho de Pulso (EE.UU.)	El ancho de tiempo representa los cambios de la cantidad de carga eléctrica con capacitancia de alta frecuencia regularmente dentro de un tiempo especificado.
Intervalo de Pulso (EE.UU.)	El intervalo de tiempo entre pulsos.
Tipo de identificación	Seleccione entre ID de usuario y número de placa.

Definiciones de varios formatos Wiegand comunes:

Formato Wiegand	Definiciones
Wiegand26	<p>ECCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 26 bits de código binario. El primer bit es el bit de paridad par de los bits 2º a 13º, mientras que el bit 26º es el bit de paridad impar de los bits 14º a 25º. Los bits 2 a 25 son los números de tarjeta.</p>
Wiegand26a	<p>ESSSSSSSCCCCCCCCCCCCCCCCCO</p> <p>Consta de 26 bits de código binario. El primer bit es el bit de paridad par de los bits 2º a 13º, mientras que el bit 26º es el bit de paridad impar de los bits 14º a 25º. Los bits 2 a 9 son los códigos de sitio, mientras que los bits 10 a 25 son los números de tarjeta.</p>
Wiegand34	<p>ECCCCCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 34 bits de código binario. El primer bit es el bit de paridad par de los bits segundo a 17, mientras que el bit 34 es el bit de paridad impar de los bits 18 a 33. Los bits 2 a 25 son los números de tarjeta.</p>
Wiegand34a	<p>ESSSSSSSCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 34 bits de código binario. El primer bit es el bit de paridad par de los bits segundo a 17, mientras que el bit 34 es el bit de paridad impar de los bits 18 a 33. Los bits 2 a 9 son los códigos de sitio, mientras que los bits 10 a 25 son los números de tarjeta.</p>
Wiegand36	<p>OFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME</p> <p>Consta de 36 bits de código binario. El primer bit es el bit de paridad impar del segundo al décimo octavo bit, mientras que el bit 36 es el bit de paridad par del decimonoveno al treinta y cinco bits. Los bits 2 a 17 son los códigos de dispositivo. Los bits 18 a 33 son los números de tarjeta y los bits 34 a 35 son los códigos del fabricante.</p>



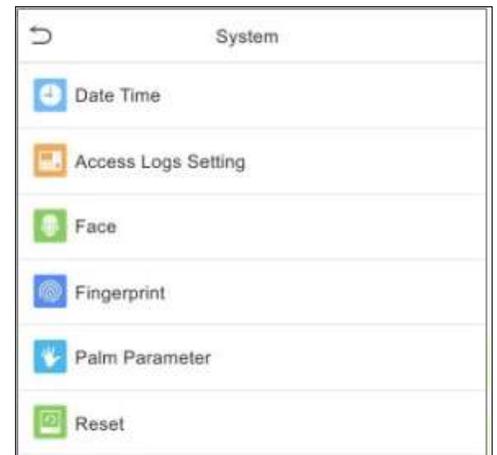
Menú	Descripción
Formato Wiegand	Los valores oscilan entre 26 bits, 34 bits, 36 bits, 37 bits y 50 bits.
Bits de salida Wiegand	Después de elegir el formato Wiegand, puede seleccionar uno de los dígitos de salida correspondientes en el formato Wiegand
Identificación Fallida	Si la verificación falla, el sistema enviará la identificación fallida al dispositivo y reemplazará el número de tarjeta o la identificación del personal por los nuevos.
Código del Sitio	Es similar al ID del dispositivo. La diferencia es que un código de sitio se puede configurar manualmente y es repetible en un dispositivo diferente. El valor válido varía de 0 a 256 de forma predeterminada.
Ancho de Pulso (EE.UU.)	El ancho de tiempo representa los cambios de la cantidad de carga eléctrica con capacitancia de alta frecuencia regularmente dentro de un tiempo especificado.
Intervalo de Pulso (EE.UU.)	El intervalo de tiempo entre pulsos.
Tipo de identificación	Seleccione entre ID de usuario y número de placa.

## 7. Configuración del Sistema

### Configuración del sistema

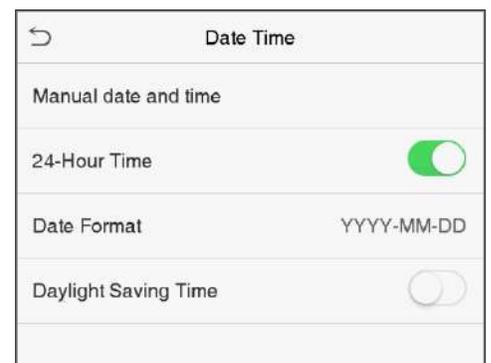
Configure los parámetros del sistema relacionados para optimizar el rendimiento del dispositivo.

Haga clic en Sistema en la interfaz del menú principal.



### Fecha y hora

Haga clic en Fecha y hora en la interfaz del sistema.



1. Puede configurar manualmente la fecha y la hora y hacer clic en Confirmar para guardar.

2. Puede configurar manualmente la fecha y la hora y hacer clic en Confirmar para guardar.

3. Haga clic en Horario de verano para habilitar o deshabilitar la función. Si está habilitado, seleccione un modo de horario de verano y configure la hora de cambio.

Daylight Saving Setup	
Start Month	1
Start Week	1
Start Day	Sunday
Start Time	00:00
End Month	1
End Week	1
End Day	Sunday
End Time	00:00

Modo semana

Daylight Saving Setup	
Start Date	00-00
Start Time	00:00
End Date	00-00
End Time	00:00

Modo fecha

Al restaurar a fábrica los justes, el tiempo (24 -Hora ) y formato de fecha (AAAA-MM-DD) pueden ser restauradas, pero la fecha y la hora del dispositivo no se pueden recuperar.

**Nota:** Por ejemplo, el usuario ajusta el tiempo del dispositivo (18:35 el 15 de marzo, 2019) a las 18:30 horas del 1 de enero de 2020. Después de la restauración de la configuración de fábrica s , el tiempo del dispositivo cambiará a 18: 30, 1 de enero de 2020.

## Ajuste de eventos de acceso

Haga clic en 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 Blacklist Photo	99
Confirm Screen Delay(s)	3
Face comparison interval(s)	1

Menú	Descripción
Modo cámara	Ya sea para capturar y guardar la imagen instantánea actual durante la verificación. Hay 5 modos: Sin foto: no se toma ninguna foto durante la verificación del usuario. <b>Tomar foto, no guardar:</b> la foto se toma pero no se guarda durante la verificación. <b>Tomar una foto y guardar:</b> la foto se toma y se guarda durante la verificación. <b>Guardar en la verificación exitosa:</b> se toma una foto y se guarda para cada verificación exitosa. <b>Guardar en verificación fallida:</b> la foto se toma y se guarda durante cada verificación fallida.
Mostrar foto de usuario	Si mostrar la foto del usuario cuando el usuario pasa la verificación.
Advertencia de registros de acceso	Cuando 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.
Eliminar registros de acceso	Cuando 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.
Eliminación cíclica de foto ATT	Cuando 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.
Eliminación cíclica de foto en lista negra	Cuando las fotos de la lista negra hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un valor establecido de las fotos antiguas de la lista negra. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Confirmar el retraso de la pantalla	El período de tiempo que se muestra el mensaje de verificación exitosa. Valor válido: 1 ~ 9 segundos.
Intervalo (s) de comparación de caras	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.

## Parámetros de Huellas Dactilares

Haga clic en Huella digital 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	FAR	Umbrales de coincidencia recomendados	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Menú	Descripción
Umbral de coincidencia 1: 1	Bajo el método de verificación 1: 1, la verificación solo será exitosa cuando la similitud entre los datos de huellas dactilares adquiridos y la plantilla de huellas dactilares asociada con la ID de usuario ingresada inscrita en el dispositivo sea mayor que el valor establecido.
Umbral de coincidencia 1: N	Bajo el método de verificación 1: N, la verificación solo será exitosa cuando la similitud entre los datos de huellas dactilares adquiridos y las plantillas de huellas dactilares registradas en el dispositivo sea mayor que el valor establecido.
Sensibilidad del sensor FP	Para establecer la sensibilidad de la adquisición de huellas dactilares. Se recomienda utilizar el nivel predeterminado "Medio". Cuando el ambiente está seco, lo que resulta en una detección lenta de huellas dactilares, puede establecer el nivel en "Alto" para aumentar la sensibilidad; cuando el ambiente es húmedo, lo que dificulta la identificación de la huella digital, puede establecer el nivel en "Bajo".
Tiempos de reintento 1: 1	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.
Imagen de huella digital	Para configurar si se muestra la imagen de la huella digital en la pantalla durante el registro o la verificación de la huella digital. Hay cuatro opciones disponibles: <b>Mostrar para enrolar:</b> para mostrar la imagen de la huella digital en la pantalla solo durante la inscripción. <b>Mostrar por coincidencia:</b> para mostrar la imagen de la huella digital en la pantalla solo durante la verificación. <b>Mostrar siempre:</b> para mostrar la imagen de la huella digital en la pantalla durante el registro y la verificación. <b>Ninguno:</b> no mostrar la imagen de la huella digital.

## Parámetros de Rostro

Haga clic en Rostro en la interfaz del sistema .

		Umbral de coincidencia recomendados	
FRR	FAR	1: N	1: 1
Alto	Bajo	85	80
Medio	Medio	82	75
Bajo	Alto	80	70

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

Menú	Descripción
Umbral de Verificación 1: N (uno a muchos)	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. 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.
Umbral de Verificación 1: 1 (uno a uno)	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. El valor válido varía de 55 a 120. Cuanto más altos son los umbrales, menor es la tasa de errores de juicio, mayor es la tasa de rechazo y viceversa. Se recomienda el valor predeterminado de 63.
Umbral de enrolado de rostros	Durante el registro facial, se utiliza la comparación 1: N (uno a muchos) para determinar si el usuario ya se ha registrado antes. Cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas es mayor que este umbral, indica que la cara ya ha sido registrada.
Ángulo de inclinación de rostro	La tolerancia del ángulo de inclinación de una cara para el registro facial y la comparación. Si una cara 's ángulo de paso supera este valor de ajuste, se filtra por el algoritmo, es decir, ignorada por el terminal por lo tanto no interfaz de registro y la comparación se activará.
Angulo de rotación de rostro	La tolerancia del ángulo de rotación de una cara para el registro y la comparación de plantillas faciales. Si una cara 's ángulo de rotación supera este valor de ajuste, se filtra por el algoritmo, es decir, ignorada por el terminal por lo tanto no interfaz de registro y la comparación se activará.
Calidad de la imagen	Calidad de imagen para registro facial y comparación. Cuanto mayor sea el valor, más clara será la imagen.
Tamaño mínimo de la cara	Requerido para el registro facial y la comparación. Si un objeto ' tamaño s es menor que este valor de ajuste, el objeto se filtró y no se reconoce como una cara. Este valor puede entenderse como la distancia de comparación de caras. Cuanto más lejos esté la persona, más pequeña será la cara y el algoritmo obtendrá el píxel de la cara más pequeño. Por lo tanto, ajustar este parámetro puede ajustar la distancia de comparación más lejana de caras. Cuando el valor es 0, la distancia de comparación de caras no está limitada.
Umbral de activación de luz LED	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, con mayor frecuencia se encenderá la luz LED.
Sensibilidad de detección de movimiento	Una medida de la cantidad de cambio en el campo de visión de una cámara que califica como detección de movimiento potencial que activa el terminal desde el modo de espera a la interfaz de comparación. Cuanto mayor sea el valor, más sensible será el sistema, es decir, si se establece un valor mayor, la interfaz de comparación es mucho más fácil y se activa con frecuencia.
Detección de vida	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.
Umbral de detección de vida	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.
Detección de rostro falso con NIR	Uso de imágenes de espectros de infrarrojo cercano para identificar y prevenir ataques de fotos y videos falsos.
WDR	Amplio rango dinámico (WDR), que equilibra la luz y extiende la visibilidad de la imagen para videos de vigilancia en escenas de iluminación de alto contraste y mejora la identificación de objetos en ambientes brillantes y oscuros.
Modo anti-parpadeo	Se utiliza cuando WDR está desactivado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea con la misma frecuencia que la luz.
Notas	Un ajuste inadecuado de los parámetros de exposición y calidad puede afectar gravemente al rendimiento del dispositivo. Ajuste el parámetro de exposición solo bajo la guía del personal de servicio posventa de nuestra empresa.

## Parámetros de Palma

Haga clic en Palma en la interfaz del sistema.

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

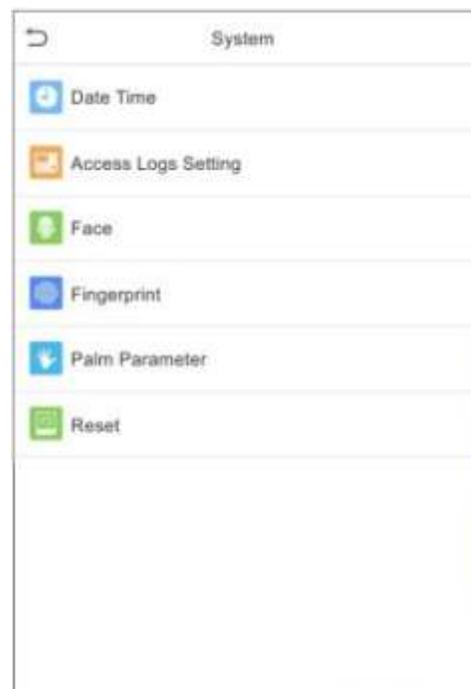
Menú	Descripción
Umbral de verificación de Palma 1: 1 (uno a uno)	En el método de verificación 1: 1, solo cuando la similitud entre la palma de verificación y la palma registrada del usuario es mayor que este valor, la verificación puede tener éxito.
Umbral de verificación de Palma 1:N (uno a muchos)	En el método de verificación 1: N, solo cuando la similitud entre la palma verificadora y toda la palma registrada es mayor que este valor, la verificación puede tener éxito.

## 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).

Haga clic en Restablecer en la interfaz del sistema .

Haga clic en Aceptar para restablecer.



## 8. Configuración de Personalización

Puede personalizar la configuración de la interfaz, voz, timbre.

Haga clic en Personalizar en la interfaz del menú principal.



### Configuración de la interfaz

Puede personalizar el estilo de visualización de la interfaz principal.

Haga clic en Interfaz de usuario en la interfaz Personalizar.



Menú	Descripción
Fondo de pantalla	Para seleccionar el fondo de pantalla de la pantalla principal según sus preferencias personales.
Idioma	Para seleccionar el idioma del dispositivo.
Tiempo de espera del menú (s)	Cuando no hay operación y el tiempo excede el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. Puede deshabilitar la función o establecer el valor entre 60 y 99999 segundos.
Tiempo para protector de pantalla	Cuando no se realiza 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.
Intervalo de imágenes	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.
Tiempo para reposo (m)	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.
Estilo de pantalla principal	Para seleccionar el estilo de la pantalla principal según sus preferencias personales.

## Configuración de voz

Haga clic en Voz en la interfaz Personalizar.



Menú	Descripción
Mensaje de Voz	Seleccione si desea habilitar las indicaciones de voz durante el funcionamiento.
Toque Indicación	Seleccione si desea habilitar los sonidos del teclado.
Volumen	Ajuste el volumen del dispositivo; valor válido: 0-100.

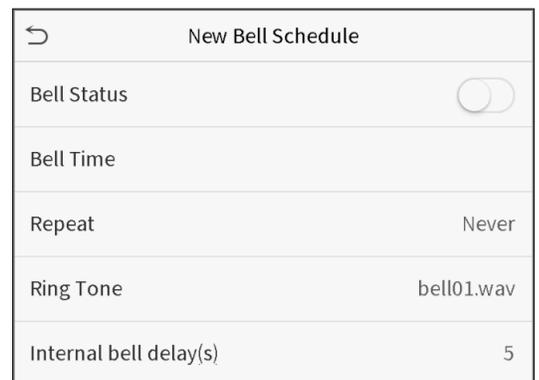
## Horarios de Timbre

Haga clic en Programación de timbre en la interfaz Personalizar.



## Agregar un timbre

1. Haga clic en New Bell Schedule para ingresar a la interfaz de adición:



Menú	Descripción
Estado del timbre	Establezca si desea habilitar el timbre.
Tiempo de Timbre	A esta hora del día, el dispositivo hará sonar el timbre automáticamente.
Repetir	Configure el ciclo de repetición de la campana.
Tono	Seleccione un tono de timbre.
Duración del timbre	Configure la duración del timbre interno. Los valores válidos oscilan entre 1 y 999 segundos.

2. Regrese a la interfaz de Horarios de Campana, haga clic en Todos los Horarios de Campana para ver la campana recién agregada.

### Editar un timbre

En la interfaz Horarios de Timbre, toque el timbre para editarlo.

- Haga clic en Editar, el método de edición es el mismo que las operaciones de agregar un timbre.

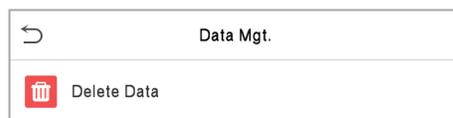
### Eliminar una campana

- En la interfaz de Todos los horarios de timbre, toque el timbre para eliminarlo.
- Toque Eliminar y seleccione [SÍ] para eliminar la campana.

## 9. Gestión de Datos

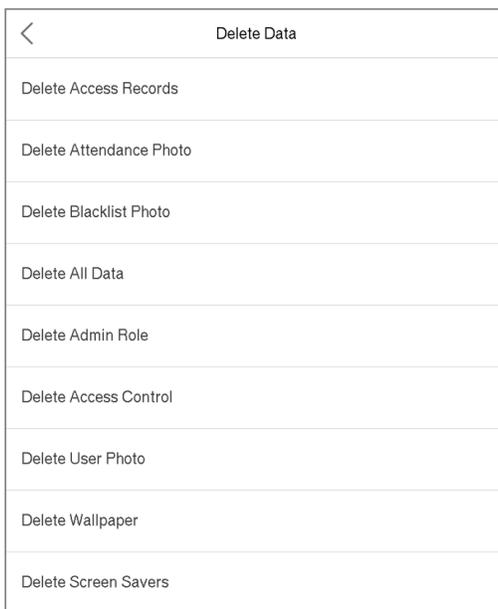
Para eliminar los datos relevantes en el dispositivo.

Haga clic en Data Mgt. en la interfaz del menú principal.



### Eliminar datos

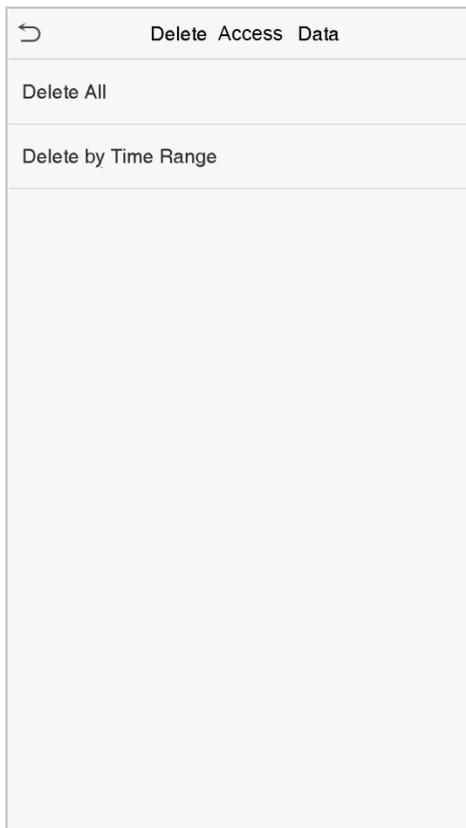
Haga clic en Borrar Datos en el Administrador de datos.



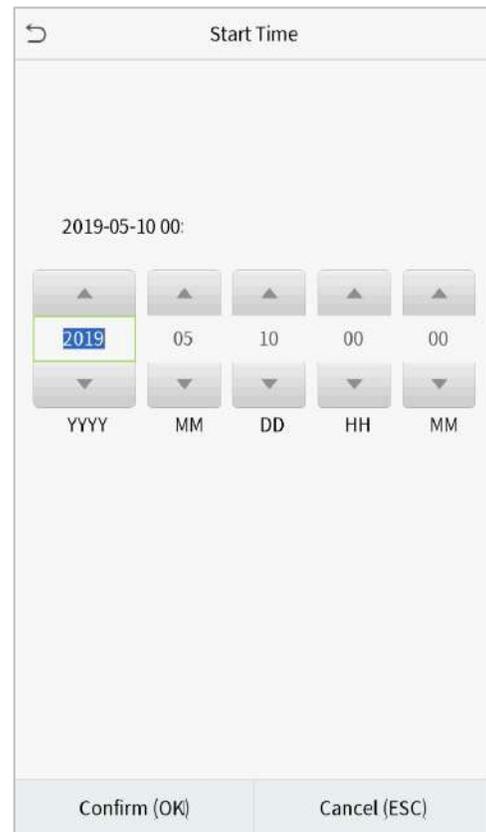
Menú	Descripción
Borrar Eventos de acceso	Eliminar registros de acceso condicionalmente.
Borrar Fotos de Eventos	Eliminar las fotos de asistencia del personal designado.
Borrar Fotos, No aprobados	Para eliminar las fotos tomadas durante verificaciones fallidas.
Borrar Todo	Eliminar información y registros de acceso de todos los usuarios registrados.
Borrar Privilegio de Administrador	Para eliminar los privilegios de administrador.
Eliminar control de acceso	Eliminar todos los datos de acceso.
Eliminar foto de usuario	Para eliminar todas las fotos de usuario en el dispositivo.

Menú	Descripción
Eliminar fondo de pantalla	Para eliminar todos los fondos de pantalla del dispositivo.
Borrar Protectores de pantalla	Para eliminar los protectores de pantalla del dispositivo.

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



Seleccione Eliminar por rango de tiempo.



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.

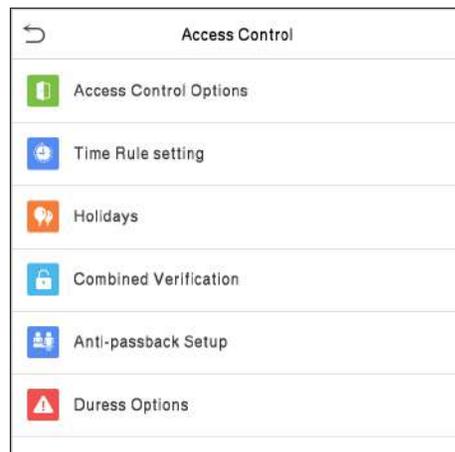
Haga clic en Control de acceso en la interfaz del menú principal.

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.

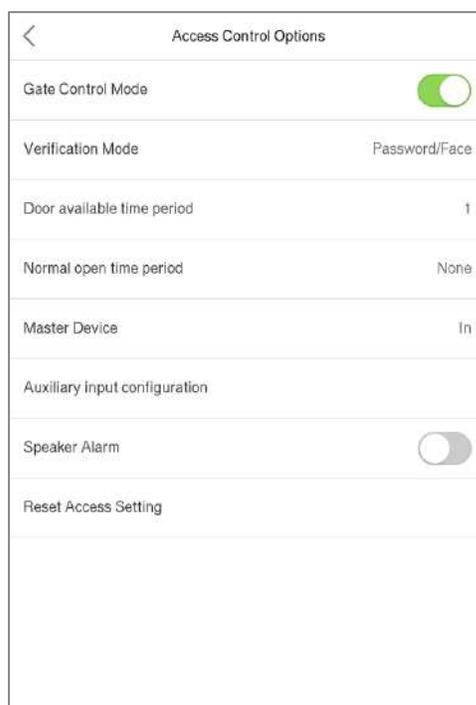
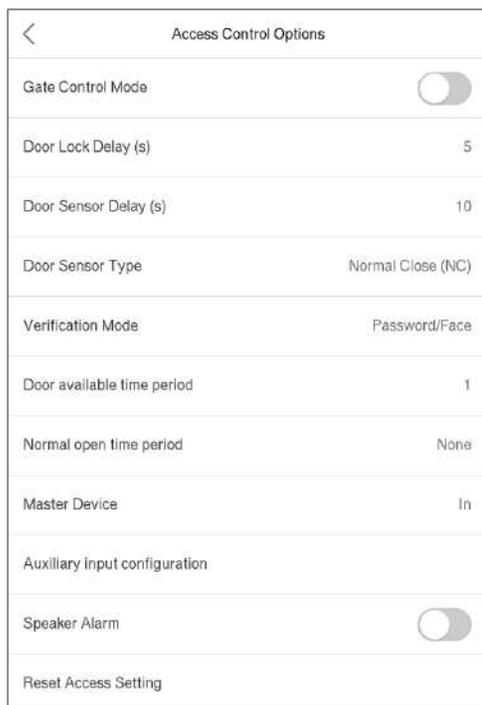
2.El grupo del usuario debe estar en la combinación de desbloqueo de la puerta (cuando hay otros grupos en el mismo combo de acceso, también se requiere la verificación de los miembros de esos grupos para desbloquear la puerta).

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.



### Opciones de control de acceso

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



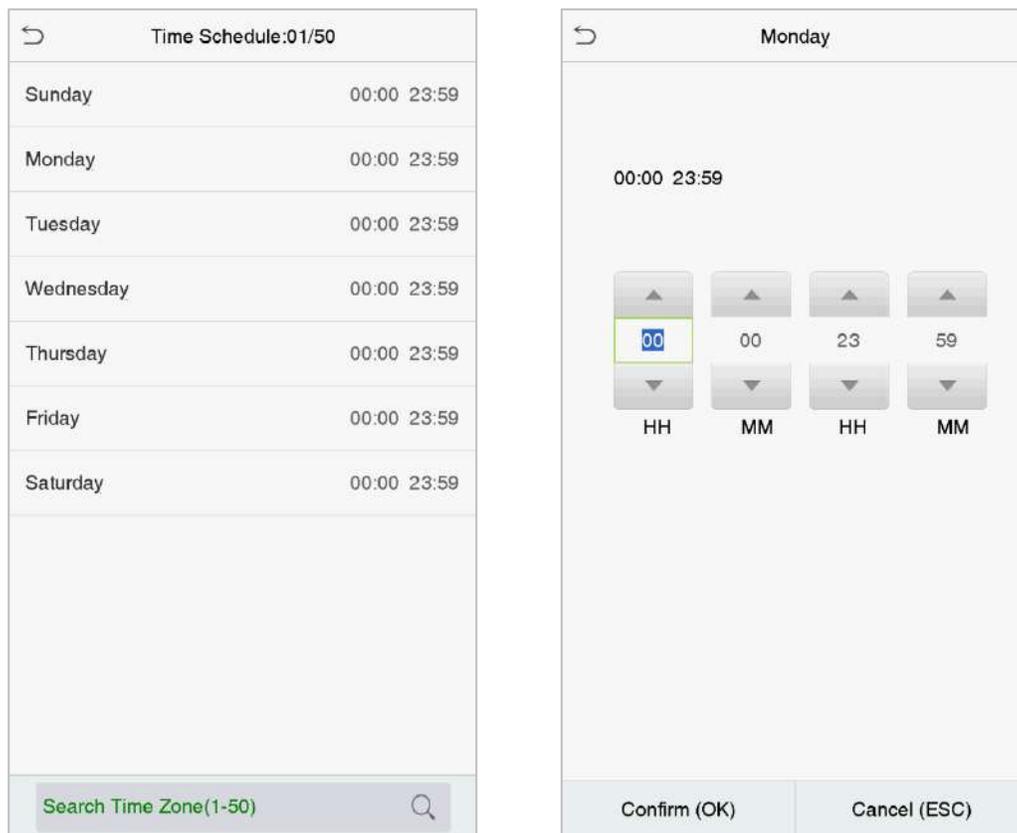
Menú	Descripción
Modo de control de puerta	Seleccione si desea habilitar el modo de control de puerta. Cuando está habilitado, el relé de bloqueo de puerta, el relé de sensor de puerta y el tipo de sensor de puerta no se mostrarán.
Retardo de bloqueo de puerta	El tiempo que el dispositivo controla la cerradura eléctrica para abrir. Valor válido: 1 a 10 segundos; 0 segundos representa la desactivación de la función.
Retardo del sensor de puerta	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.
Tipo de sensor de puerta	Hay tres tipos: Ninguno, Normalmente Abierto y Normalmente 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.
Modo de verificación	El modo de verificación admitido incluye contraseña / rostro, solo ID de usuario, contraseña, solo rostro y rostro + contraseña.
Horario de puerta habilitada	Para establecer un período de tiempo para la puerta, de modo que la puerta sea accesible solo durante este período de tiempo.
Periodo disponible	El período de tiempo en el que el usuario puede abrir la puerta, se puede establecer en cualquiera de las 50 reglas de tiempo.
Periodo normalmente abierto	Tiempo programado para el modo de "apertura normal", de modo que la puerta siempre esté desbloqueada durante este período.
Dispositivo maestro	Al configurar el maestro y el esclavo, el estado del maestro se puede configurar en fuera o en. Fuera: El registro verificado en el host es el registro de salida. En: El registro verificado en el host es el registro de entrada.
Ajustes de entrada auxiliar	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.
Altavoz de alarma	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.
Restablecer configuración de acceso	Los parámetros de control de acceso restaurados incluyen el retardo del bloqueo de la puerta, el retardo del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el período de tiempo disponible de la puerta, el período de tiempo de apertura normal, un dispositivo maestro y una alarma. Sin embargo, los datos de control de acceso borrados en Data Mgt. está excluido. a; Normalmente cerrado significa que la puerta siempre está cerrada cuando la electricidad está encendida.

## Horario

Todo el sistema puede definir hasta 50 períodos de tiempo. Cada período de tiempo representa siete zonas horarias, es decir, una semana, y cada zona horaria es un período de tiempo válido dentro de las 24 horas del día. El usuario solo puede verificar dentro del período de tiempo válido. Cada formato de zona horaria del período de tiempo: HH MM-HH MM, que tiene una precisión de minutos según el reloj de 24 horas.

Haga clic en Horario 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).
2. Haga clic en la fecha en la que se requiere la configuración de la zona horaria. Ingrese la hora de inicio y finalización y luego presione OK.



### 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 durante 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: abrir todo el día (00: 00 ~ 23: 59) o cuando la hora de finalización es posterior a la hora de inicio, como 08: 00 ~ 23: 59.
3. La zona horaria predeterminada 1 indica que la puerta está abierta todo el día.

## 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.

Haga clic en Días Festivos en la interfaz de Control de acceso .

Holidays	
Add Holiday	
All Holidays	

### Agregar un nuevo día festivo

Haga clic en Agregar Día Festivo en la interfaz de vacaciones y configure los parámetros de vacaciones.

Holidays	
No.	1
Start Date	Undefined
End Date	Undefined
Time Period	1

### Editar un día festivo

En la interfaz de vacaciones, seleccione un elemento de vacaciones para modificarlo. Haga clic en 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. Haga clic en Aceptar para confirmar la eliminación. Después de la eliminación, este día festivo ya no se muestra en la interfaz de Todos los días festivos.

## 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 puerta, 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.

Haga clic en Verificación combinada en la interfaz de Control de acceso.

Haga clic en 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.

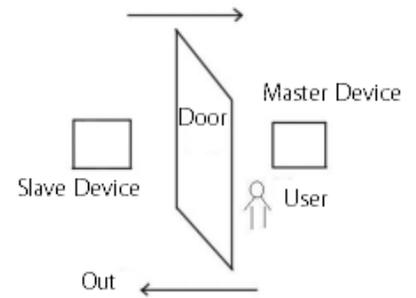
### Eliminar una combinación de desbloqueo de puertas

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

## Configuración Anti-Passback

Para evitar que algunas personas sigan a los usuarios y entren por la puerta sin verificación, lo que resultará en un problema de seguridad, los usuarios pueden habilitar la función anti-passback. El registro de entrada debe coincidir con el registro de salida para poder abrir la puerta.

Esta función requiere dos dispositivos para trabajar juntos: uno está instalado dentro de la puerta (dispositivo maestro), 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.



↶
Anti-passback Setup

---

Anti-passback Direction
No Anti-passback

↶
Anti-passback Direction

---

No Anti-passback

---

Out Anti-passback

---

In Anti-passback

---

In/Out Anti-passback

Menú	Descripción
Sin Anti-passback	La función Anti-Passback está deshabilitada, lo que significa que pasar la verificación en el dispositivo maestro o en el dispositivo esclavo puede desbloquear la puerta. El estado de asistencia no está reservado.
Fuera Anti-passback	Después de que un usuario se retira, solo si el último registro es un registro de entrada, el usuario puede volver a retirarse; de lo contrario, se activará la alarma. Sin embargo, el usuario puede registrarse libremente.
En Anti-passback	Después de que un usuario se registra, solo si el último registro es un registro de salida, el usuario puede registrarse nuevamente; de lo contrario, se activará la alarma. Sin embargo, el usuario puede salir libremente.
Antirretorno de entrada / salida	Después de que un usuario se registra de entrada / salida, solo si el último registro es un registro de salida, el usuario puede volver a registrarse, o un registro de entrada puede volver a retirarse; de lo contrario, se activará la alarma.

## Configuración de las opciones de amago

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.

Haga clic en Opciones de coacción en la interfaz de Control de acceso.

←
Duress Options

---

Alarm on Password

---

Alarm Delay(s)
10

---

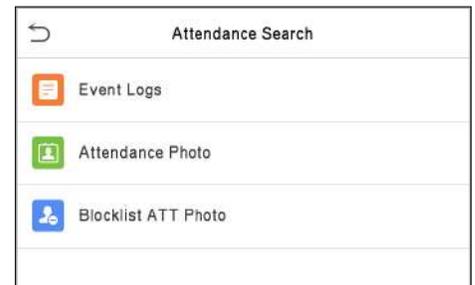
Duress Password
None

Menú	Descripción
Alarma por contraseña	Cuando un usuario usa el método de verificación de contraseña, se generará una señal de alarma; de lo contrario, no habrá señal de alarma.
Retardo de alarma (s)	La señal de alarma no se transmitirá hasta que haya transcurrido el tiempo de retardo de la alarma. El valor varía de 1 a 999 segundos.
Contraseña de amago	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.

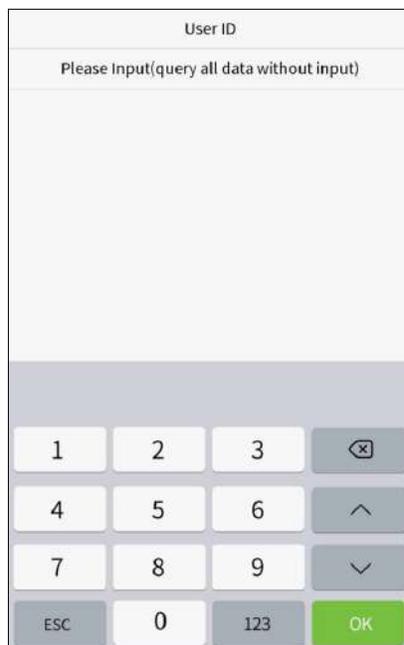
Haga clic en Búsqueda de asistencia en la interfaz del menú principal.



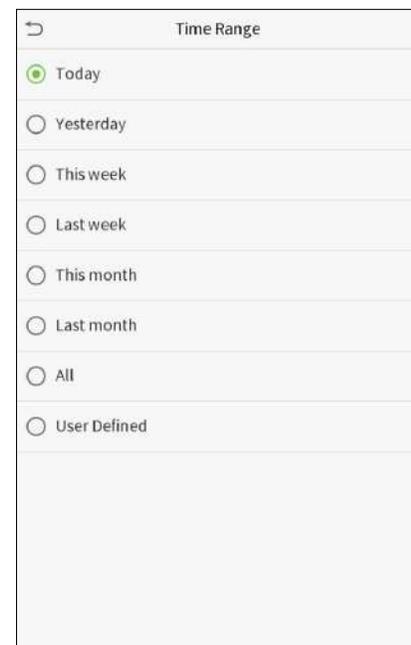
El proceso de búsqueda de asistencia y blocklist Photos es similar a la de la búsqueda de registro de eventos. El siguiente es un ejemplo de búsqueda de registro de eventos.

En la interfaz de búsqueda de asistencia, haga clic en Registro de eventos.

1. Ingrese el ID de usuario a buscar y haga clic en Aceptar. Si desea buscar registros de todos los usuarios, haga clic en Aceptar sin ingresar ningún ID de usuario.



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



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

Date	User ID	Time
10-09		Number of Records:18
		14:18 14:13
	2	16:47 16:44 16:43 15:03 14:58
		14:56 14:55 14:55 14:53 14:43
		14:41 14:38
	1000702	14:55 14:54 14:27 14:18

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

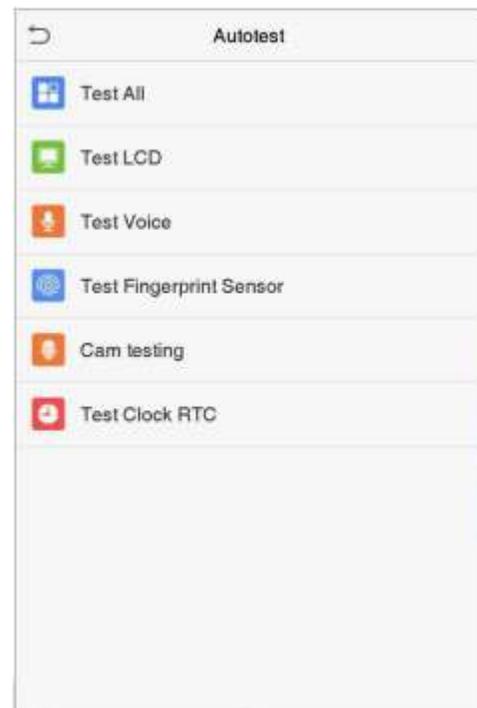
User ID	Name	Time	Mode	State
2	Mike	10-09 16:47	15	255
2	Mike	10-09 16:44	15	255
2	Mike	10-09 16:43	15	255
2	Mike	10-09 15:03	15	255
2	Mike	10-09 14:58	15	255
2	Mike	10-09 14:56	25	255
2	Mike	10-09 14:55	15	255
2	Mike	10-09 14:55	15	255
2	Mike	10-09 14:53	25	255
2	Mike	10-09 14:43	15	255
2	Mike	10-09 14:41	15	255
2	Mike	10-09 14:38	15	255

Verification Mode : Face Punch State : 255

## 12. Autotest

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

Haga clic en Autotest en la interfaz del menú principal.

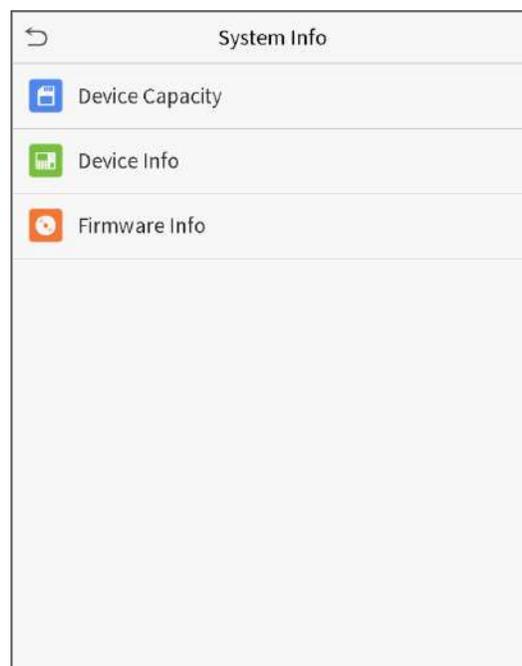


Menú	Descripción
Probar todo	Para probar automáticamente si la pantalla LCD, el audio, la cámara y el RTC son normales.
Prueba de LCD	Para probar automáticamente el efecto de visualización de la pantalla LCD mostrando a todo color, blanco puro y negro puro para verificar si la pantalla muestra los colores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

## 13. Pruebas de Sistema

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

Haga clic en Información del sistema en la interfaz del menú principal.



Menú	Descripción
Capacidad del dispositivo	Muestra el espacio de almacenamiento del dispositivo actual , palma, contraseña y la Rostro, los administradores, registros de acceso, asistencia fotos de no permitidos, y fotos de usuario.
Información del dispositivo	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.
Información de firmware	Muestra la versión de firmware y otra información de la versión del dispositivo.

## 14. Conectarse al Software ZKBioAccess / ZKBioSecurity

### Establecer la dirección de comunicación

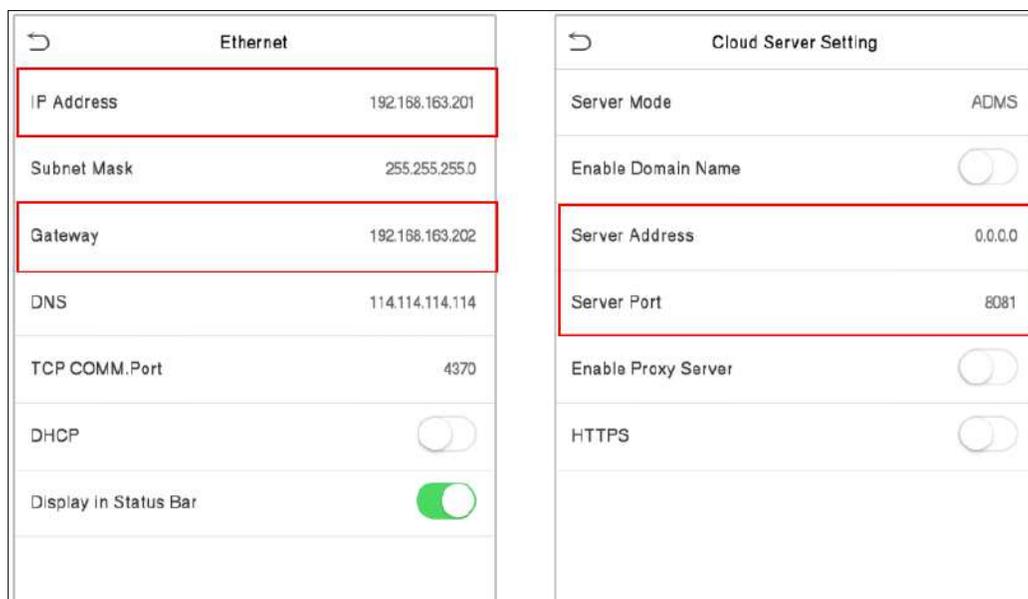
#### Lado del dispositivo

1. Hacer clic RED.> Ethernet en el menú principal para configurar la dirección IP y la puerta de enlace de el dispositivo. (Nota: La dirección IP debe poder comunicarse con el servidor ZKBioAccess, preferiblemente en el mismo segmento de red con la dirección del servidor..)

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

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

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



## Lado del software

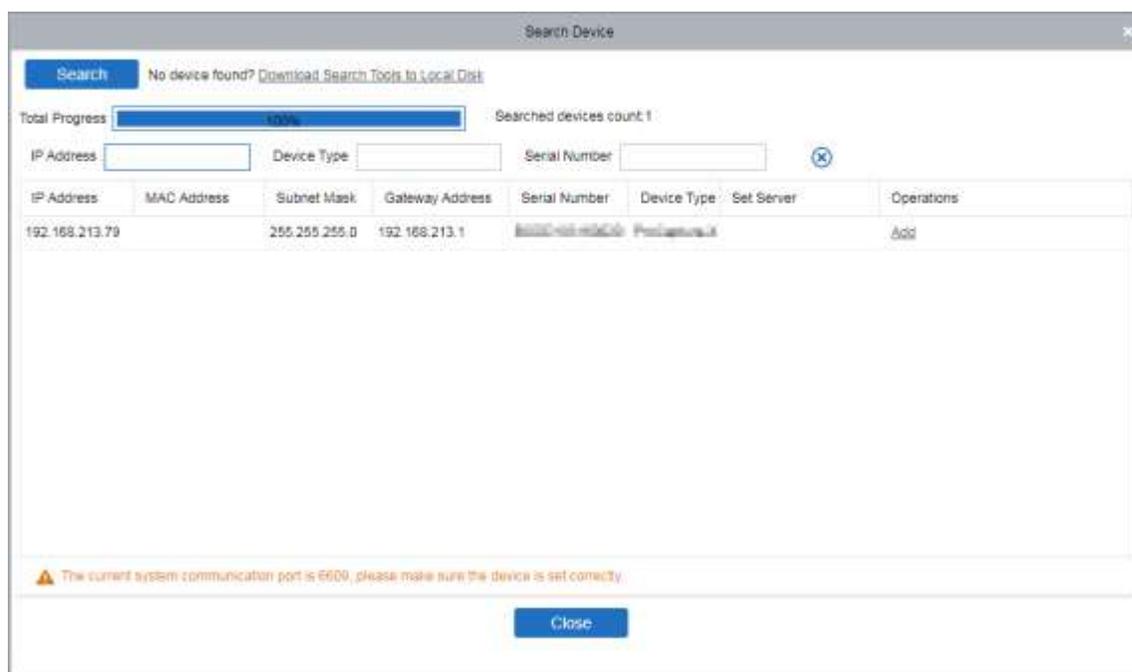
Inicie sesión en el software ZKBioAccess, haga clic en Sistema> Comunicación> Monitor de comunicación para configurar el puerto de servicio ADMS, como se muestra en la siguiente figura:



## Agregar dispositivo al software

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

1. Haga clic en Control de acceso> Dispositivo> Buscar dispositivo, para abrir la interfaz de búsqueda.
2. Haga clic en Buscar y aparecerá [Buscando .....].
3. Después de la búsqueda, se mostrará la lista y el número total de controladores de acceso..



4. Haga clic en Agregar para agregar el dispositivo específico al software.

## Agregar personal al software

1. Haga clic en Personal > Persona > Nuevo.

The screenshot shows a 'New' personnel form with the following fields and sections:

- Personal Information:** Personnel ID\* (2), Department\* (Department Name), First Name, Last Name, Gender, Mobile Phone, Certificate Type (ID), Certificate Number, Birthday, Email, Device Verification (password), Card Number.
- Biological Template:** Selection of icons and Quantity.
- Photo:** Placeholder image with 'Browse' and 'Capture' buttons. Note: (Optimal Size 120\*140).
- Access Control:** Levels Settings (General selected).
- Time Attendance:** Add, Select All, Unselect All buttons.
- Personnel Detail:** Superuser (No), Device Operation Role (Ordinary User), Disabled (checkbox), Set Valid Time (checkbox).
- Buttons:** Save and New, OK, Cancel.

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

## Apéndice 1

### Requisitos para la recopilación en vivo y el registro de imágenes visible light

- 1) Se recomienda realizar el registro en un entorno interior con una fuente de luz adecuada sin subexposición o sobreexposición.
- 2) No apunte hacia fuentes de luz exteriores como puertas o ventanas u otras fuentes de luz fuertes.
- 3) Se recomienda que en el registro las prendas de color sean diferentes del color de fondo.
- 4) Muestre su cara y frente, y no cubra su cara y cejas con su cabello, lentes de sol o lentes de aumento.
- 5) Se recomienda mostrar una expresión facial sencilla. Sonreír es aceptable, pero no cierre los ojos ni incline la cabeza en ninguna orientación. Se requieren dos imágenes para personas con anteojos, una imagen con anteojos y otra sin anteojos simultáneamente.
- 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 se muestra en la Imagen 1.
- 8) No incluya más de una cara en el área de captura.
- 9) Se recomienda una distancia de captura de 50 cm a 80 cm, ajustable en función de la altura del cuerpo.



Área de captura de rostro de Imagen 1

## Requisitos para datos de imagen facial digital visible Light Digital

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 deberán enrolarse con los anteojos para la captura de fotografías.

### Distancia de los ojos

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

### Expresión facial

Se recomienda un Rostro sencillo 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 cubrebocas y anteojos de colores. El marco de los anteojos no debe cubrir los ojos y no debe reflejar la luz. Para personas con montura de anteojos gruesa, se recomienda capturar dos imágenes, una con anteojos y la otra sin anteojos.

### Rostro

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.

### Requerimientos 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 un Rostro sencillo o una sonrisa, no se prefiere mostrar los dientes.

La persona capturada debe ser vista claramente, de color natural y sin un giro obvio de la imagen, sin sombras, puntos de luz o reflejos en el Rostro o el fondo, y un nivel de contraste y luminosidad apropiado..

## Apéndice 2

### Declaración sobre el derecho a la privacidad

#### Estimados 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..

#### Nosotros declaramos que:

- 1.Todos nuestros dispositivos de reconocimiento de huellas dactilares civiles 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.

Si desea disputar cuestiones de derechos humanos o privacidad relacionadas 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;

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

Como punto final, nos gustaría enfatizar aún más que el reconocimiento biométrico es una tecnología avanzada que ciertamente será utilizada en el comercio electrónico, banca, seguros, judicial y otros sectores en el futuro. Cada año el mundo sufre grandes pérdidas debido a la inseguridad de Contraseñas. Los productos biométricos sirven para proteger su identidad en entornos de alta seguridad.



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 operativo 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.

Nombre del Componente	Sustancias peligrosas o tóxicas y sus cantidades					
	Sustancia / elemento peligroso / tóxico					
	Plomo (Pb)	Mercurio (Hg)	Cadmio (Cd)	Cromo hexavalente (Cr6 +)	Bifenilos polibromados (PBB)	Éteres de difenilo polibromados (PBDE)
Resistencia	×	o	o	o	o	o
Condensador	×	o	o	o	o	o
Inductor	×	o	o	o	o	o
Diodo	×	o	o	o	o	o
Componente ESD	×	o	o	o	o	o
Buzzer/Bocina	×	o	o	o	o	o
Adaptador	×	o	o	o	o	o
Tornillos	o	o	o	×	o	o

o 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.



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



[www.zktecolatinoamerica.com](http://www.zktecolatinoamerica.com)



Derechos de Autor © 2021, ZKTeco CO, LTD. Todos los derechos reservados.  
ZKTeco puede, en cualquier momento y sin previo aviso, realizar cambios o mejoras en los productos y servicios o detener su producción o comercialización.  
El logo ZKTeco y la marca son propiedad de ZKTeco CO, LTD.