Manual de usuario

Serie SpeedFace-V5L[QR]

Fecha: julio de 2021

Versión del documento: 1.0

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 tienen únicamente fines ilustrativos.

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

Marca comercial

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

Descargo de responsabilidad

Este manual contiene información sobre la operación 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 contenido del presente no debe ser utilizado ni 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 iniciar la operación y mantenimiento del equipo suministrado. Si alguno de los contenidos del manual parece poco claro o incompleto, comuníquese con ZKTeco antes de comenzar la operación y mantenimiento de dicho equipo.

Es un requisito previo esencial para una operación y mantenimiento satisfactorios que el personal de operación y mantenimiento esté completamente familiarizado con el diseño y que dicho personal haya recibido una capacitación exhaustiva 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, comprendido y seguido las instrucciones de seguridad contenidas en el manual.

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

ZKTeco no ofrece ninguna garantía ni representación con respecto a la integridad de la información contenida en este manual o cualquiera de las modificaciones realizadas en el mismo. ZKTeco no extiende la garantía de ningún tipo, incluyendo, entre otras, cualquier garantía de diseño, comerciabilidad o idoneidad para un determinado
objetivo.

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. Todo el riesgo sobre los resultados y rendimiento obtenidos del uso de la información es asumido por el usuario.

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

relacionados con el uso de la información contenida o referenciada en este manual, 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 aquí contenida, la cual se incorporará en nuevas adiciones/modificaciones al manual. ZKTeco se reserva el derecho de añadir, eliminar, enmendar o modificar periódicamente la información contenida en el manual en forma de circulares, cartas, notas, etc. para una mejor
funcionamiento y seguridad de la máquina/unidad/equipo. Dichas adiciones o modificaciones están destinadas a mejorar/mejorar el funcionamiento de la máquina/unidad/equipo y dichas modificaciones no darán ningún derecho a reclamar ninguna compensación o daños bajo ninguna circunstancia.

ZKTeco no será responsable de ninguna manera (i) en caso de que la máquina/unidad/equipo funcione mal debido al 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 procedimientos operativos más recientes y los documentos relevantes están disponibles en http://www.zkteco.com

Si hay algún problema relacionado con el producto, contáctenos.

Sede central de ZKTeco

DIRECCIÓN Parque Industrial ZKTeco, No. 32, Vía Industrial,

Ciudad de Tangxia, Dongguan, China.

Teléfono +86 769 - 82109991

Fax +86 755 - 89602394

Para consultas relacionadas con el negocio, escríbanos a: sales@zkteco.com.

Para saber más sobre nuestras sucursales globales, visite www.zkteco.com.

Sobre la empresa

ZKTeco es uno de los mayores fabricantes del mundo de lectores RFID y biométricos (huellas dactilares, faciales y venosos). Las ofertas de productos incluyen lectores y paneles de control de acceso, cámaras de reconocimiento facial de alcance cercano y lejano, controladores de acceso a ascensores/pisos, torniquetes, controladores de puertas con reconocimiento de matrículas (LPR) y productos de consumo que incluyen cerraduras de puertas con lector de huellas dactilares y rostro que funcionan con baterías. 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 700,000 pies cuadrados de ZKTeco, controlamos la fabricación, el diseño de productos, el ensamblaje de componentes y la logística/envío, todo bajo un mismo techo.

Los fundadores de ZKTeco estaban decididos a realizar investigación y desarrollo independientes de procedimientos de verificación biométrica y a 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 la gran cantidad de aplicaciones del 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, posee varias patentes y ha sido seleccionada como Empresa Nacional de Alta Tecnología durante 6 años consecutivos. Sus productos están protegidos por derechos de propiedad intelectual.

Acerca del Manual

Este manual presenta las operaciones de la serie SpeedFace-V5L[QR].

Todas las figuras mostradas son sólo para fines ilustrativos. Es posible que las cifras de este manual no coincidan exactamente con los productos reales.

Las funciones 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 la GUI

Para software	
Convención	Descripción
Negrita	Se utiliza para identificar nombres de interfaces de software, por ejemplo, Aceptar, Confirmar, Cancelar.
>	Los menús de varios niveles están separados por estos corchetes. Por ejemplo, Archivo > Crear > Carpeta.
Para dispositivo	
Convención	Descripción
< >	Nombres de botones o teclas para dispositivos. Por ejemplo, presione <Aceptar>.
[ ]	Los nombres de ventanas, elementos de menú, tablas de datos y nombres de campos están entre corchetes. Por ejemplo, abra la ventana [Nuevo usuario].
/	Los menús de varios niveles están separados por barras diagonales. Por ejemplo, [Archivo/Crear/ Carpeta].

Símbolos

Convención	Descripción
	Esto implica sobre el aviso o atención al que se encuentra 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 evento que advierte de algo o que sirve como ejemplo de advertencia.

Tabla de contenido

1 Medidas de seguridad

Las siguientes instrucciones tienen como objetivo garantizar que el usuario pueda utilizar el producto correctamente para evitar peligros o pérdidas de propiedad. Las siguientes precauciones son para mantener a los usuarios seguros y evitar cualquier daño. Lea atentamente antes de la instalación.

⚠ El incumplimiento de las instrucciones podría provocar daños al producto o lesiones físicas (incluso puede causar la muerte).

1. Lea, siga y conserve las instrucciones: todas las instrucciones operativas y de seguridad deben estar correctamente leer y seguir antes de poner el dispositivo en servicio.

2. No ignore las advertencias: respete todas las advertencias de la unidad y de las instrucciones de funcionamiento.

3. Accesorios: utilice únicamente accesorios recomendados por el fabricante o vendidos por el producto. No utilice ningún otro componente que no sean los materiales sugeridos por el fabricante.

4. Precauciones para la instalación: no coloque este dispositivo sobre un soporte o marco inestable. Puede caer y provocar lesiones graves a personas y daños al aparato.

5. Servicio: no intente reparar esta unidad usted mismo. Abrir o quitar las cubiertas puede exponerle a voltajes peligrosos u otros peligros.

6. Daños que requieren reparación: desconecte el sistema de la fuente de alimentación de CA o CC y remitir al personal de servicio bajo las siguientes condiciones:

   Cuando el control del cable o de la conexión se ve afectado.

   Cuando el líquido se derramó o un artículo cayó dentro del sistema.

   Si se expone al agua o debido a las inclemencias del tiempo (lluvia, nieve y más).

   Y si el sistema no funciona normalmente, según las instrucciones de funcionamiento.

   Simplemente cambie los controles definidos en las instrucciones de funcionamiento. Un ajuste inadecuado de los controles puede provocar daños y obligar a un técnico cualificado a devolver el dispositivo a su funcionamiento normal.

   Y no conecte varios dispositivos a un adaptador de corriente, ya que la sobrecarga del adaptador puede provocar sobrecalentamiento o peligro de incendio.

7. Piezas de repuesto: cuando se necesitan piezas de repuesto, los técnicos de servicio solo deben utilizar piezas de repuesto proporcionadas por el proveedor. Los sustitutos no autorizados pueden provocar quemaduras, shock, u otros peligros.

8. Verificación de seguridad: al finalizar el servicio o el trabajo de reparación en la unidad, solicite al técnico de servicio que realice verificaciones de seguridad para garantizar el funcionamiento adecuado del dispositivo.

9. Fuentes de energía: opere el sistema únicamente desde la fuente de energía indicada en la etiqueta. Si el tipo de poder suministro a utilizar no está claro, llame a su distribuidor.

10. Rayos: se pueden instalar pararrayos externos para proteger contra tormentas eléctricas. Para potenciadores destruyan el sistema.

Se recomienda instalar los dispositivos en áreas con acceso limitado.

Seguridad ELECTRICA

Antes de conectar un cable externo al dispositivo, complete la conexión a tierra correctamente y configure protección contra sobretensiones; de lo contrario, la electricidad estática dañará la placa base.

Asegúrese de que se haya desconectado la alimentación antes de cablear, instalar o desmontar el dispositivo.

Asegúrese de que la señal conectada al dispositivo sea una señal de corriente débil (interruptor); De lo contrario, se dañarán los componentes del dispositivo.

Asegúrese de que se cumpla el voltaje estándar aplicable en su país o región. Si no está seguro del voltaje estándar recomendado, consulte a su compañía de energía eléctrica local. La falta de coincidencia de energía puede causar un cortocircuito o daños al dispositivo.

En caso de daños en la fuente de alimentación, devuelva el dispositivo al personal técnico profesional o a su distribuidor para su manipulación.

Para evitar interferencias, mantenga el dispositivo alejado de dispositivos con alta radiación electromagnética, como generadores (incluidos generadores eléctricos), radios, televisores (especialmente monitores CRT) o parlantes.

Seguridad de operación

Si sale humo, olor o ruido del dispositivo, apáguelo de inmediato y desconéctelo. cable y luego comuníquese con el centro de servicio.

El transporte y otras causas impredecibles pueden dañar el hardware del dispositivo. Controlar si el dispositivo tiene algún daño intenso antes de la instalación.

Si el dispositivo tiene defectos importantes que no puede resolver, comuníquese con su distribuidor lo antes posible.

El polvo, la humedad y los cambios bruscos de temperatura pueden afectar la vida útil del dispositivo. Eres Se recomienda no conservar el dispositivo en tales condiciones.

No guarde el dispositivo en un lugar que vibre. Manipule el dispositivo con cuidado. no colocar objetos pesados encima del dispositivo.

No aplique colofonia, alcohol, benceno, pesticidas ni otras sustancias volátiles que puedan dañar la carcasa del dispositivo. Limpie los accesorios del dispositivo con un paño suave o una pequeña cantidad de producto limpiador.

Si tiene alguna pregunta técnica sobre el uso, comuníquese con personal técnico certificado o experimentado.

Nota

Asegúrese de que la polaridad positiva y la polaridad negativa de la fuente de alimentación de 12 V CC estén conectadas correctamente. Una conexión inversa puede dañar el dispositivo. No es recomendable conectar la fuente de alimentación de 24V CA al puerto de entrada de 12V CC.

Asegúrese de conectar los cables siguiendo la polaridad positiva y la polaridad negativa que se muestran en la placa de identificación del dispositivo.

El servicio de garantía no cubre daños accidentales, daños causados por un mal funcionamiento y daños debidos a la instalación o reparación independiente del producto por parte del usuario.

2 Descripción general

La serie SpeedFace-V5L[QR] es una versión completamente mejorada del terminal de reconocimiento facial de luz visible, utilizando algoritmos de reconocimiento facial de ingeniería inteligente y la última tecnología de visión por computadora. Admite verificación facial y de palma con gran capacidad y reconocimiento rápido, también admite código QR con sensor QR integrado con aplicación móvil y mejora el rendimiento de seguridad en todos los aspectos.
La serie SpeedFace-V5L[QR] tiene tres modelos, SpeedFace-V5L[QR][TD] es la versión mejorada de SpeedFace-V5L[QR] con función de medición de temperatura, SpeedFace-V5L[QR][TI] es la versión mejorada de SpeedFace-V5L[QR][TD] con algoritmo de reconocimiento facial de ingeniería inteligente de imágenes térmicas.

La serie SpeedFace-V5L[QR] adopta tecnología de reconocimiento sin contacto e identificación individual enmascarada que elimina eficazmente los problemas de higiene. También está equipado con el último algoritmo antispoofing para el reconocimiento facial contra casi todos los tipos de ataques de fotos y videos falsos. Es importante destacar que el reconocimiento de la palma 3 en 1 (forma de la palma, impresión de la palma y vena de la palma) se realiza en 0,35 segundos por mano; Los datos de la palma adquiridos se compararán con un máximo de 3000 plantillas de palma. Además, integró un sensor QR, que admite códigos QR, PDF417, Data Matrix, MicroPDF417, Aztec, etc., con la aplicación móvil ZKBiosecurity que admite códigos QR dinámicos para T&A/A&C.

El terminal con detección de máscara ayuda a reducir la propagación de gérmenes y ayuda a prevenir infecciones directamente en cada punto de acceso de cualquier local y área pública como hospitales, fábricas, escuelas, edificios comerciales y estaciones durante el reciente problema de salud pública mundial con su identificación individual enmascarada. Función durante la verificación facial y palmar.

Características

Reconocimiento facial en luz visible.

Mejor higiene con autenticación biométrica sin contacto, detección de temperatura y enmascaramiento.
identificación individual.

Detección de temperatura por imágenes térmicas, detección de alta velocidad de 0,1 s, distancia de medición de 30 a 120 cm.

Algoritmo anti-spoofing contra ataques de impresión (fotografías láser, color y B/N), ataques de vídeos y 3D.
ataque de máscara.

Múltiples métodos de verificación: Plam/ Face/ Código QR/ Tarjeta/ Contraseña.

Código QR, PDF417, Data Matrix, MicroPDF417, Aztec.

Código QR dinámico con aplicación móvil ZKBiosecurity.

Funciones especiales

Detección de mascarilla.

Detección de temperatura corporal.

Distancia de medición de temperatura: 30 cm a 120 cm (0,98 pies a 3,94 pies).

Precisión de medición de temperatura: ±0,3°C (±0,54°F)

(Probado a una distancia de 80 cm (2,63 pies) a una temperatura de 25 °C (77 °F))

Rango de medición de temperatura: 20 °C a 50 °C (68 °F a 122 °F)

3 Instrucciones de uso

Antes de entrar en las características del dispositivo y sus funciones, se recomienda familiarizarse con lo siguiente fundamentos.

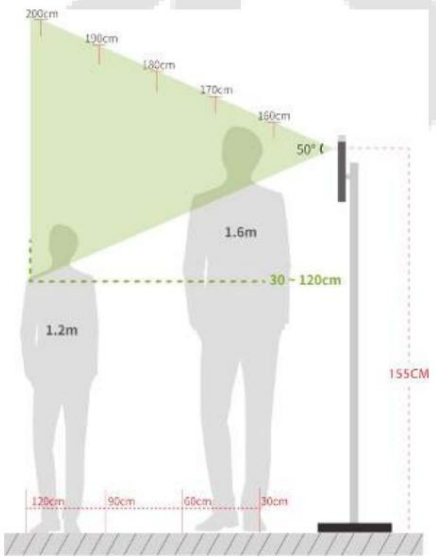
3.1 ¿Cómo escanear el código QR?

Abra la credencial móvil de la aplicación ZKBioSecurity y coloque en paralelo la pantalla del teléfono con el código QR del dispositivo escáner.

NOTA: Coloque su teléfono entre 15 y 50 cm del dispositivo (la distancia depende del tamaño de la pantalla del teléfono), no bloquee el escáner de códigos QR del dispositivo ni el código QR en la pantalla del teléfono.

3.2 Posición de pie, postura y expresión facial

La distancia recomendada



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

Postura de pie y expresión facial recomendadas

Postura de pie

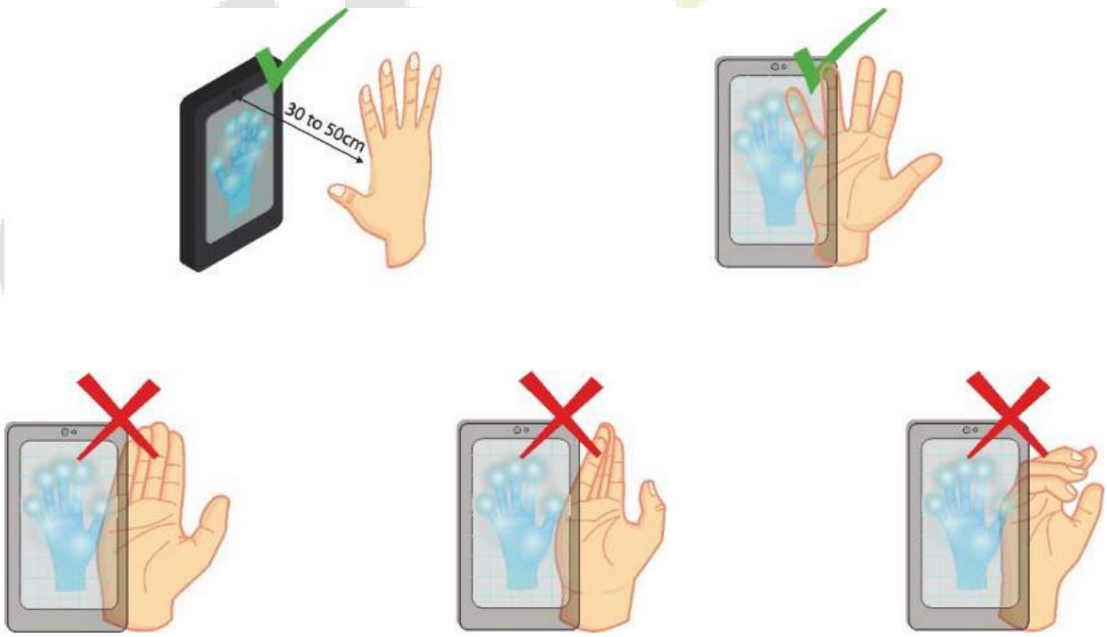
Expresión facial

NOTA: Mantenga su expresión facial y su postura de pie naturales durante la inscripción o verificación.

3.3 Registro de palma

Coloque la palma de su mano en el área de recolección multimodo de la palma, de manera que quede paralela al dispositivo.

Asegúrate de dejar espacio entre tus dedos.



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

3.4 Registro de rostros

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

Método correcto de autenticación y registro de rostros

Recomendación para registrar una cara

Al registrar una cara, mantenga una distancia de 40 cm a 80 cm entre el dispositivo y el rostro.

Tenga cuidado de no cambiar su expresión facial. (cara sonriente, cara dibujada, guiño, etc.)

Si no sigue las instrucciones en pantalla, el registro facial puede tardar más o fallar.

Tenga cuidado de no tapar los ojos ni las cejas.

No use sombreros, máscaras, gafas de sol ni anteojos.

Tenga cuidado de no mostrar dos caras en la pantalla. Registre una persona a la vez.

Se recomienda que un usuario que usa gafas registre ambas caras con y sin gafas.

Recomendación para autenticar una cara

Asegúrese de que la cara aparezca dentro de la guía que se muestra en la pantalla del dispositivo.

Si se han cambiado las gafas, la autenticación puede fallar. Si se ha registrado el rostro sin gafas, autentifique aún más el rostro sin gafas. Si se ha registrado el rostro con gafas, autenticar el rostro con las gafas utilizadas anteriormente.

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

3.5 Interfaz de espera

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

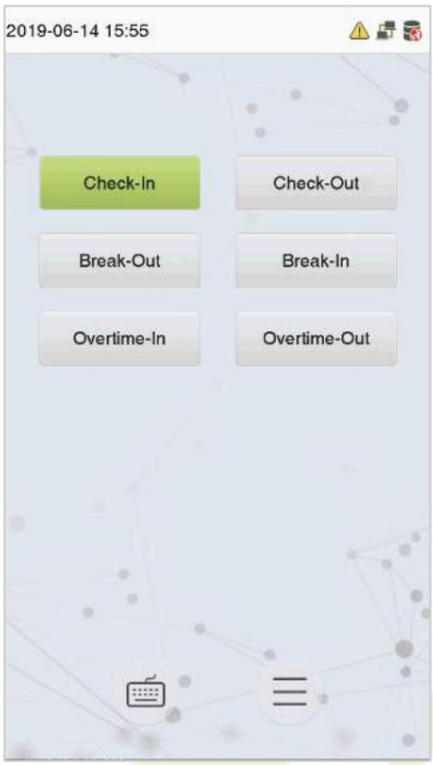
Haga clic para ingresar a la interfaz de entrada de ID de usuario.

Cuando no haya ningún superadministrador configurado en el dispositivo, toque para ir al menú.

Después de configurar el superadministrador en el dispositivo, se requiere la verificación del superadministrador antes de ingresar a las funciones del menú.

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

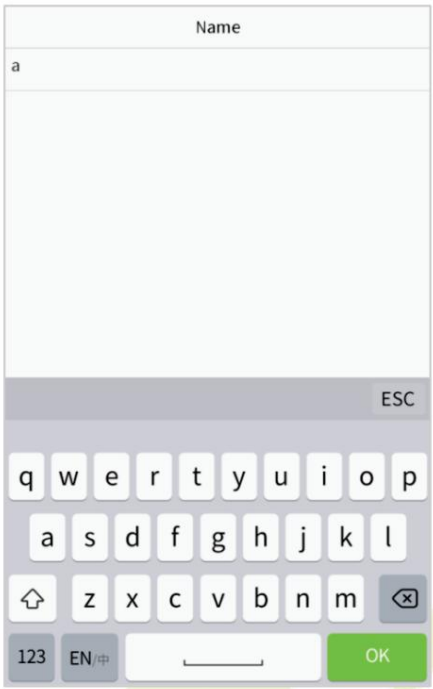
Las opciones de estado de perforación también se pueden mostrar y utilizar directamente en la interfaz de espera. Haga clic en cualquier lugar de la pantalla aparte de los íconos y aparecerán seis teclas de acceso directo en la pantalla, como se muestra en la siguiente figura:



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

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

3.6 Teclado virtual



NOTA:

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

Haga clic en [En] para cambiar al teclado en inglés.

Presione [123] para cambiar al teclado numérico y simbólico.

haga clic en [ABC] para regresar al teclado alfabético.

Haga clic en el cuadro de entrada y aparecerá el teclado virtual.

Haga clic en [ESC] para salir del teclado virtual.

3.7 Modo de verificación

3.7.1 Verificación del código QR

En este modo de verificación, el dispositivo compara la imagen del código QR recopilada por el recopilador de códigos QR con todos los datos del código QR en el dispositivo.

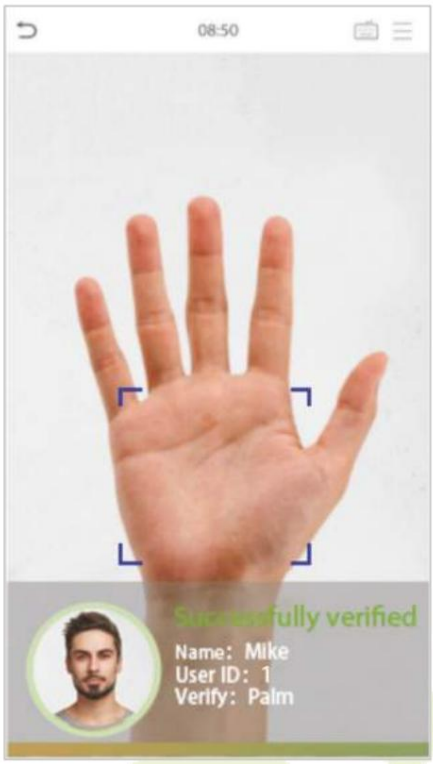
Toque [Credencial móvil] en la aplicación ZKBioSecurity y aparecerá un código QR que incluye información de identificación del empleado y número de tarjeta (el código QR estático solo incluye el número de tarjeta). El código QR puede reemplazar una tarjeta física en un dispositivo específico para lograr la autenticación sin contacto. Consulte 15.4 Móvil Credencial.

3.7.2 Verificación de la palma

1: N Modo de verificación de palma

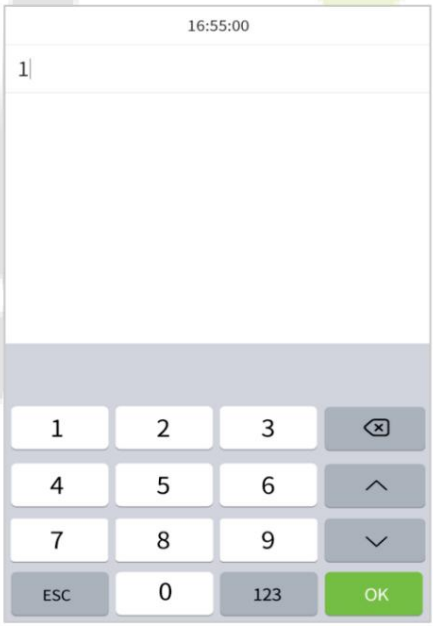
En este modo de verificación, el dispositivo compara la imagen de la palma recopilada por el recolector de palma con todos los datos de la palma en el dispositivo.

El dispositivo distingue automáticamente entre el modo de verificación de la palma y de la cara según el usuario coloca la palma de su mano en el área de escaneo. Luego, el recolector de palmas recopila la imagen de la palma y el dispositivo compara la imagen de la palma recopilada con todas las palmas registradas y devuelve una salida.



Modo de verificación de palma 1: 1

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



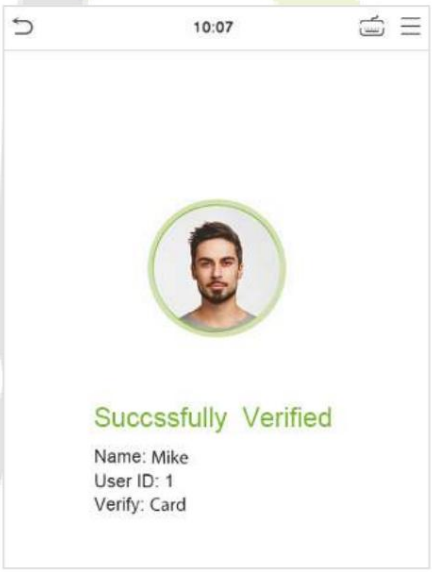
Si el usuario ha registrado la tarjeta, el rostro y la contraseña además de su palma, y el método de verificación está configurado en verificación de palma/tarjeta/cara/contraseña, aparecerá la siguiente pantalla. Seleccione la palma

icono para ingresar al modo de verificación de palma. Luego coloque la palma de su mano para verificar.

3.7.3 Verificación de tarjeta

1: modo de verificación de tarjeta N

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

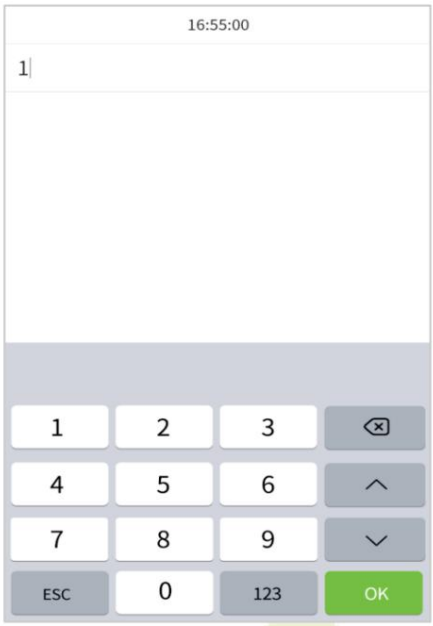


Verificación de tarjeta 1:1

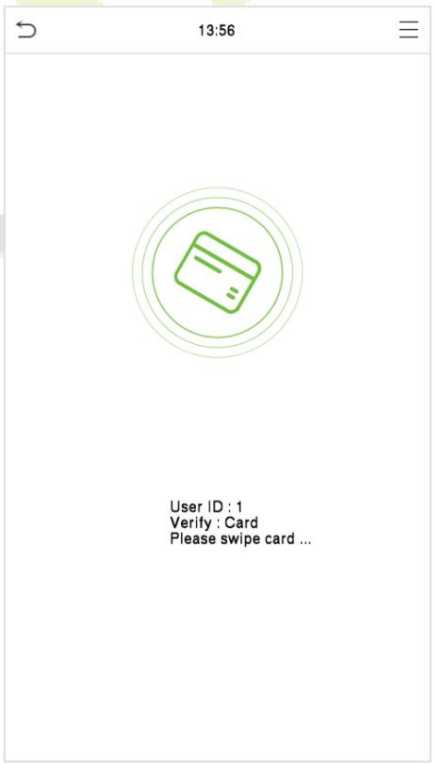
El modo de verificación de tarjeta 1:1 compara el número de tarjeta en el área de inducción de tarjeta con el número asociado con la identificación de usuario del empleado registrada en el dispositivo.

Prensa  en la interfaz principal para abrir el modo de verificación de tarjeta 1:1.

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



Si el usuario ha registrado palma, rostro y contraseña además de su tarjeta, y el método de verificación está configurado en verificación de palma/cara/tarjeta/contraseña, aparecerá la siguiente pantalla. Selecciona el  icono para ingrese al modo de verificación de tarjeta.

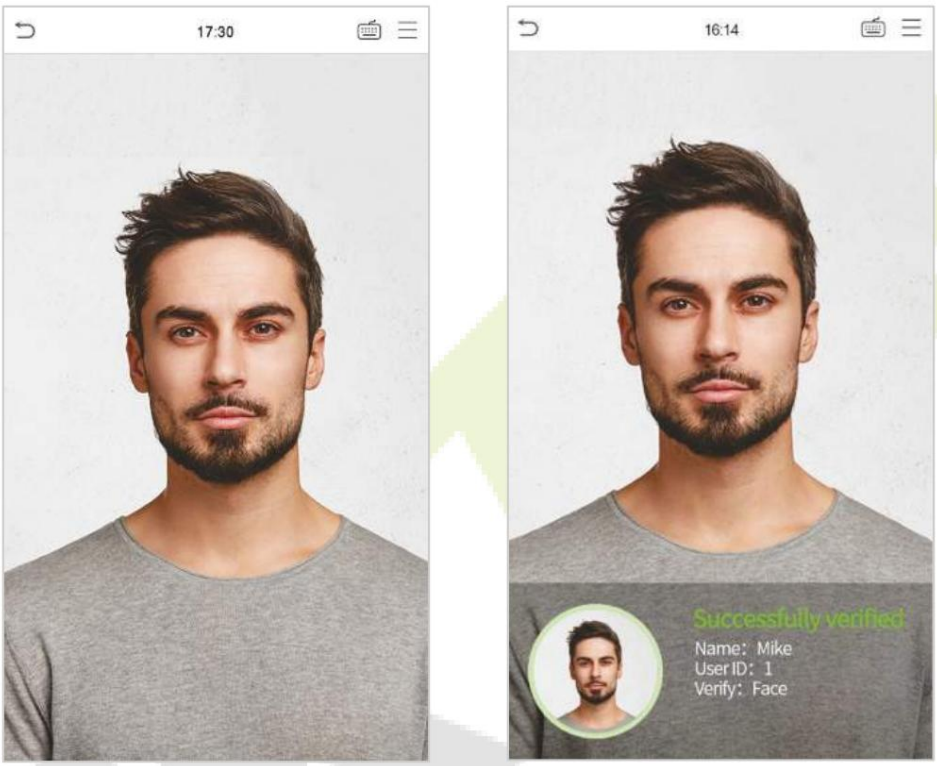


3.7.4 Verificación facial

Verificación facial 1:N

1. Verificación convencional

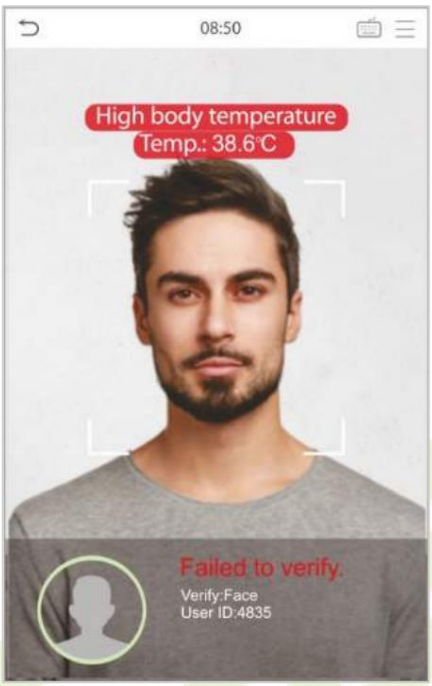
En este modo de verificación, el dispositivo compara las imágenes faciales recopiladas con todos los datos faciales registrados en el dispositivo. El siguiente es el mensaje emergente de un resultado de comparación exitoso.



2. Habilite el control de temperatura con infrarrojos

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

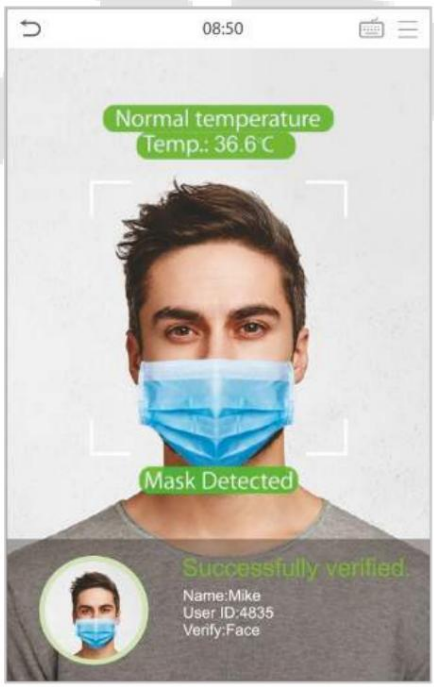
NOTA: Los datos de medición de temperatura son solo como referencia y no tienen fines médicos.



3. Habilite la detección de máscara

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

NOTA: Los datos de medición de temperatura son solo como referencia y no tienen fines médicos.



4. Mostrar la figura de termodinámica

Cuando el usuario habilita la función Mostrar figura termodinámica, se muestra la imagen térmica de la persona.

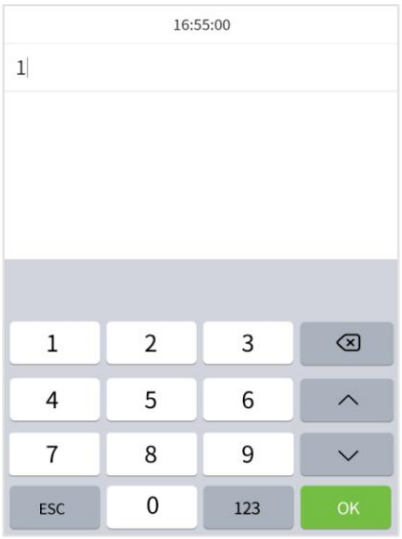
se muestra en la esquina superior izquierda del dispositivo, durante la verificación. Como se muestra en las imágenes a continuación: (Nota: esta función solo se aplica a productos con módulo de detección de temperatura por imagen térmica).

NOTA: Los datos de medición de temperatura son solo como referencia y no tienen fines médicos.

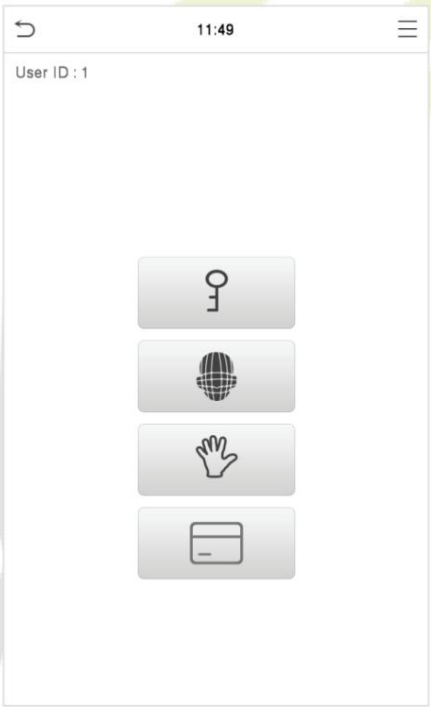
Verificación facial 1:1

En este modo de verificación, el dispositivo compara el rostro capturado por la cámara con la plantilla facial en la interfaz principal y ingresa al modo de relacionado con el ID de usuario ingresado. Prensa verificación facial 1:1.

e introduzca el ID de usuario y haga clic en [Aceptar].



Si el usuario ha registrado la palma, la tarjeta y la contraseña además de la cara, y el método de verificación está configurado en verificación de la palma/tarjeta/cara/ contraseña, aparecerá la siguiente pantalla. Seleccione el modo de verificación facial.  ícono para ingresar al



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

Si la verificación falla, aparecerá el mensaje "¡Ajuste su posición!".

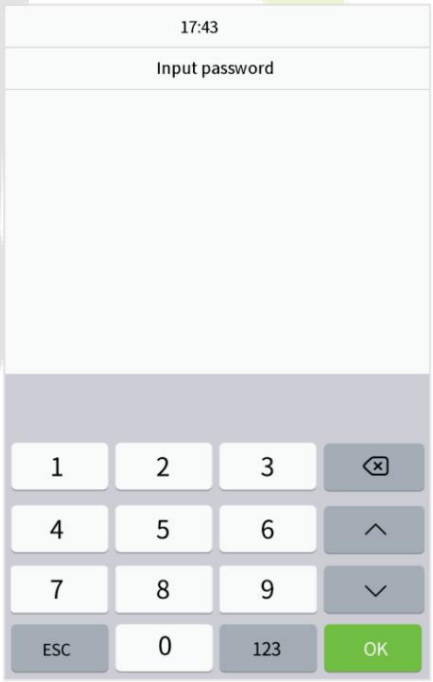
3.7.5 Verificación de contraseña

El dispositivo compara la contraseña ingresada con la contraseña registrada mediante la ID de usuario proporcionada.

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

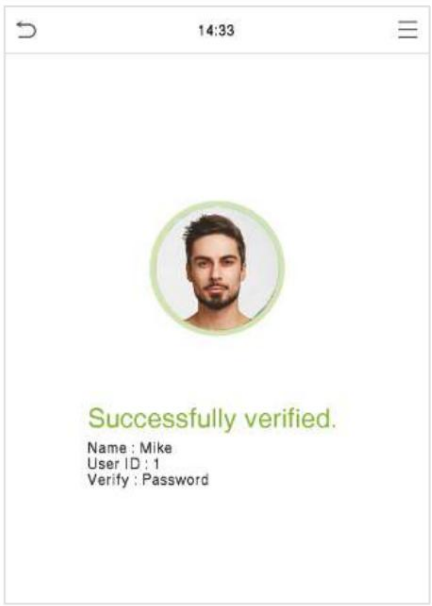
Si el usuario ha registrado la palma, la tarjeta y la cara además de la contraseña, y el método de verificación está configurado en verificación de la palma/tarjeta/cara/ contraseña, aparecerá la siguiente pantalla. Seleccione el modo de verificación de contraseña.  icono para entrar

Ingrese la contraseña y presione [OK].

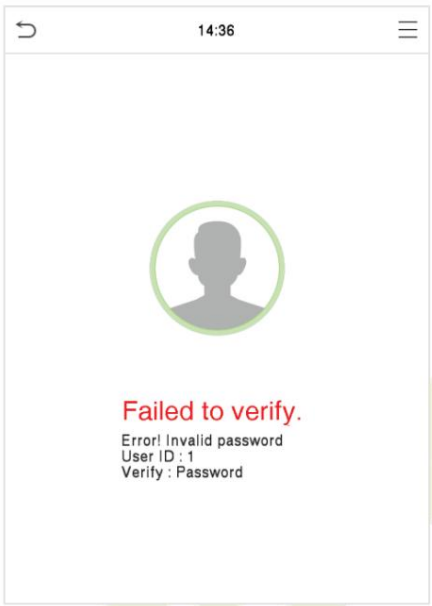


A continuación se muestra la pantalla de visualización después de ingresar una contraseña correcta y una contraseña incorrecta, respectivamente.

La verificación es exitosa:



La verificación ha fallado:

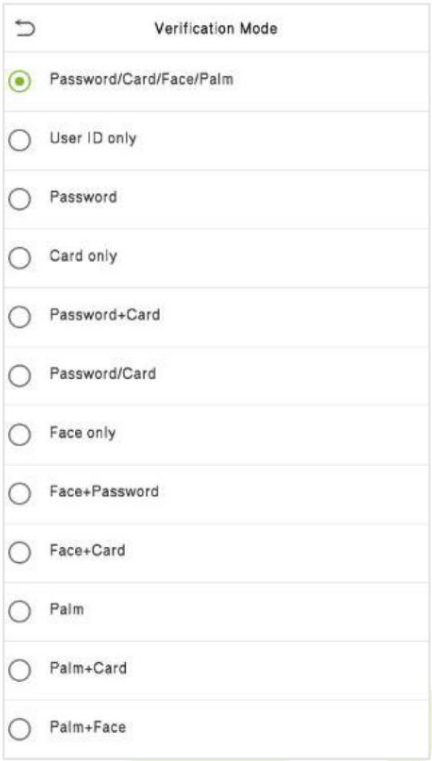


3.7.6 Verificación combinada

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:

Definición del símbolo de verificación combinado

Definición de símbolo		Explicación
/	o	Este método compara la verificación ingresada de una persona con la plantilla de verificación relacionada previamente almacenada en esa ID de personal en el Dispositivo.
+	y	Este método compara la verificación ingresada de una persona con todos los plantilla de verificación previamente almacenada en esa ID de personal en el Dispositivo.



Procedimiento para configurar el modo de verificación combinado

La verificación combinada requiere que el personal registre todos los diferentes métodos de verificación.

De lo contrario, los empleados no podrán verificar con éxito el proceso de verificación combinado.

Por ejemplo, cuando un empleado ha registrado solo los datos faciales, pero el modo de verificación del dispositivo está configurado como "Cara + Contraseña", el empleado no podrá completar el proceso de verificación con éxito.

Esto se debe a que el Dispositivo compara la plantilla de rostro de la persona con la plantilla de verificación registrada (tanto el Rostro como la Contraseña) previamente almacenada con esa ID de personal en el Dispositivo.

Pero como el empleado ha registrado sólo la Cara pero no la Contraseña, la verificación no se completa y el dispositivo muestra "Verificación fallida".

4 Menú principal

Prensa en la interfaz de espera para ingresar al menú principal, se mostrará la siguiente pantalla:

Función descriptiva

Menú	Descripciones
Gestión de usuarios	Agregar, editar, ver y eliminar información básica de un usuario.
Rol del usuario	Establecer el alcance del permiso de la función personalizada y el registrador para los usuarios, es decir, los derechos para operar el sistema.
COM.	Para configurar los parámetros relevantes de Red, Comunicación serie, Conexión de PC, Red inalámbrica, Servidor en la nube, Wiegand y Diagnóstico de red.
Sistema	Para configurar los parámetros relacionados con el sistema, incluida la fecha y hora, la configuración de registros de acceso, el parámetro de rostro y palma, el restablecimiento de fábrica, la configuración del tipo de dispositivo y la gestión de detección.
Personalizar	Esto incluye configuración de interfaz de usuario, voz, horarios de timbre, opciones de estado de marcado y asignaciones de teclas de acceso directo.
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 relevante, incluidas opciones como Regla de tiempo, Configuración de vacaciones, Verificación combinada, Configuración anti-passback y Configuración de opciones de coacción.
Asistencia Buscar	Para consultar los registros de eventos especificados, consulte Fotos de asistencia y Fotos de asistencia de la lista de bloqueo.
Autotest	Para probar automáticamente si cada módulo funciona correctamente, incluida la pantalla LCD, el audio, la cámara y el reloj en tiempo real.
Información del sistema	Para ver la capacidad de datos y la información del dispositivo y del firmware del dispositivo actual.

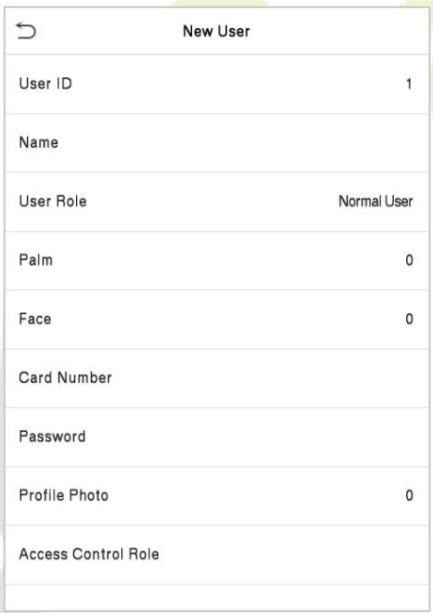
5 Gestión de usuarios

5.1 Registro de Usuario

Haga clic en Gestión de usuarios. en el menú principal.

5.1.1 ID de usuario y nombre

Toca Nuevo usuario. Ingrese la ID de usuario y el nombre.



NOTA:

1Un nombre puede tener hasta 31 caracteres.

2La ID de usuario puede contener entre 1 y 9 dígitos de forma predeterminada.

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

4Si aparece el mensaje "¡Duplicado!" aparece, debe elegir otra ID como ingresar ID de usuario ya existe

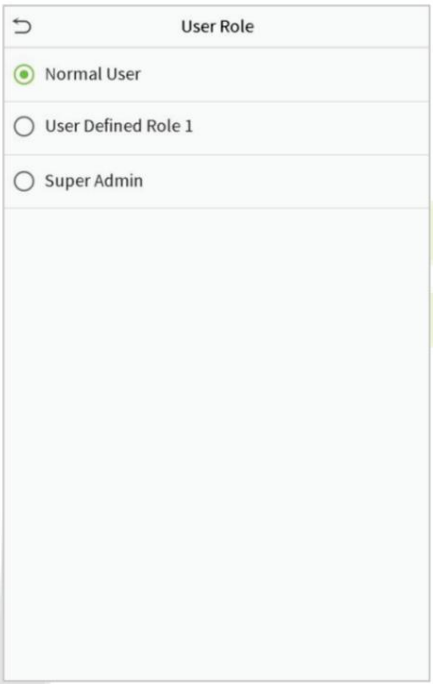
5.1.2 Función de usuario

En la interfaz Nuevo usuario, toque Función de usuario para establecer la función del usuario como Usuario normal o Super Administración.

Superadministrador: el superadministrador posee todos los privilegios de administración en el dispositivo.

Usuario normal: si el superadministrador ya está registrado en el dispositivo, los usuarios normales no tendrán los privilegios para administrar el sistema y solo podrán acceder a las verificaciones de autenticación.

Roles definidos por el usuario: el usuario normal también se puede configurar con roles definidos por el usuario, que son los roles personalizados que se pueden configurar para el usuario normal.



NOTA: Si el rol de usuario seleccionado es el de 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 3.7 Método de verificación.

5.1.3 Palma

Toque Palm en la interfaz Nuevo usuario para ingresar a la página de registro de Palm.

Seleccione la palma que desea registrar.

Coloque la palma de su mano dentro de la caja guía y manténgala quieta mientras se registra.

Aparece una barra de progreso mientras se registra la palma y se muestra "Inscrito exitosamente" como la barra de progreso se completa.

Si la palma ya está registrada, aparecerá el mensaje "Palm repetida". La interfaz de registro es la siguiente:

5.1.4 Cara

Toque Cara en la interfaz Nuevo usuario para ingresar a la página de registro de caras.

Mire hacia la cámara y coloque su cara dentro del cuadro guía blanco y quédese quieto.
durante el registro facial.

Aparece una barra de progreso mientras se registra la cara y se muestra "Inscrito exitosamente" como
la barra de progreso se completa.

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

5.1.5 Tarjeta

Toque Tarjeta en la interfaz Nuevo usuario para ingresar a la página de registro de la tarjeta.

En la interfaz de Tarjeta, pase la tarjeta debajo del área de lectura de tarjetas. El registro de la tarjeta será exitoso.

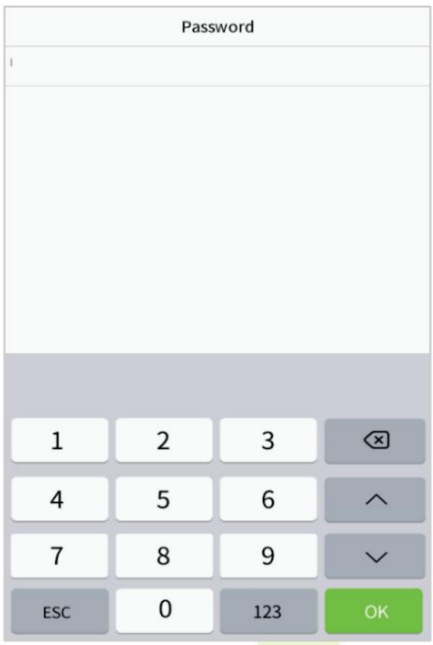
Si la tarjeta ya está registrada, aparecerá el mensaje “¡Error! Aparece el mensaje "Tarjeta ya registrada". El La interfaz de registro es la siguiente:

5.1.6 Contraseña

Toque Contraseña en la interfaz Nuevo usuario para ingresar a la página de registro de contraseña.

En la interfaz Contraseña, ingrese la contraseña requerida y vuelva a ingresarla para confirmarla y toque Aceptar.

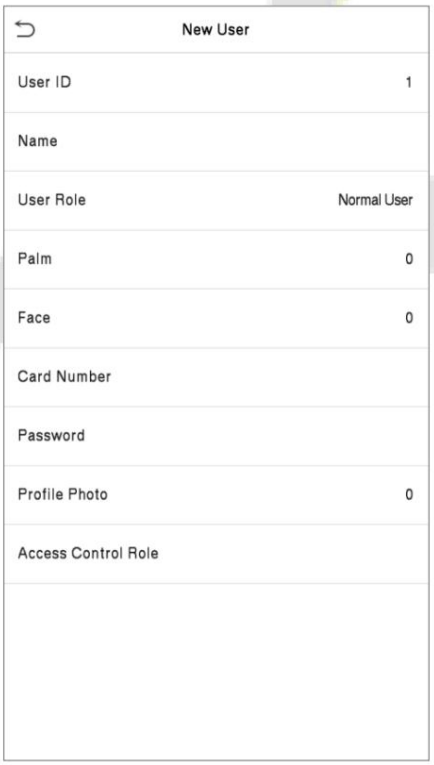
Si la contraseña reingresada es diferente de la contraseña ingresada inicialmente, el dispositivo muestra el mensaje "¡La contraseña no coincide!", donde el usuario debe volver a confirmar la contraseña.



NOTA: La contraseña puede contener de 1 a 8 dígitos de forma predeterminada.

5.1.7 Foto de perfil

Toque Foto de perfil en la interfaz Nuevo usuario para ir a la página de registro de Foto de perfil.



Cuando un usuario registrado con una foto pasa la autenticación, la foto registrada será desplegado.

Toque Foto de perfil, se abrirá la cámara del dispositivo, luego toque el ícono de la cámara para tomar una foto. El

La foto capturada se muestra en la esquina superior izquierda de la pantalla y la cámara se abre nuevamente para tomar una nueva foto, después de tomar la foto inicial.

NOTA: Al registrar una cara, el sistema captura automáticamente una imagen como foto de perfil. Si no registra una foto de perfil, el sistema establece automáticamente la imagen capturada durante el registro como la foto predeterminada.

5.1.8 Función de control de acceso

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

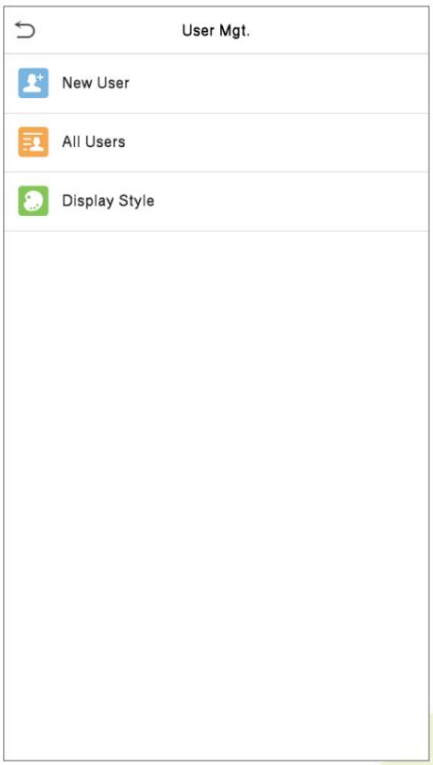
Toque Función de control de acceso > Grupo de acceso para asignar los usuarios registrados a diferentes grupos para una mejor administración. Los nuevos usuarios pertenecen al Grupo 1 de forma predeterminada y pueden reasignarse a otros grupos. El dispositivo admite hasta 99 grupos de control de acceso.

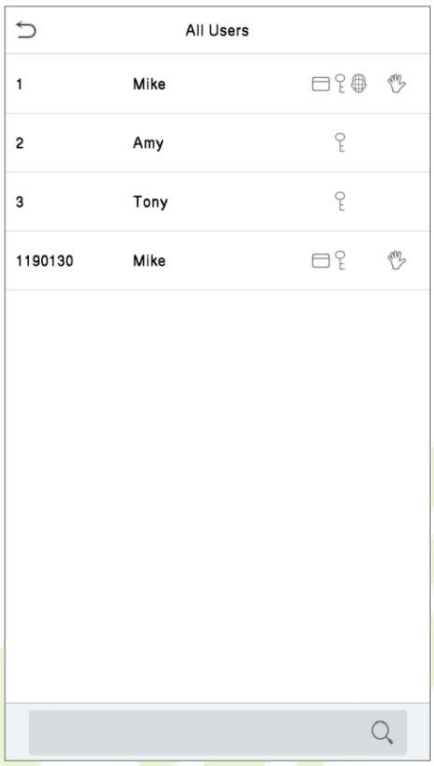
Toque Período de tiempo para seleccionar el período de tiempo que desea utilizar.

5.2 Búsqueda de usuarios

En el menú principal, toque Gestión de usuarios y luego toque Todos los usuarios para buscar un usuario.

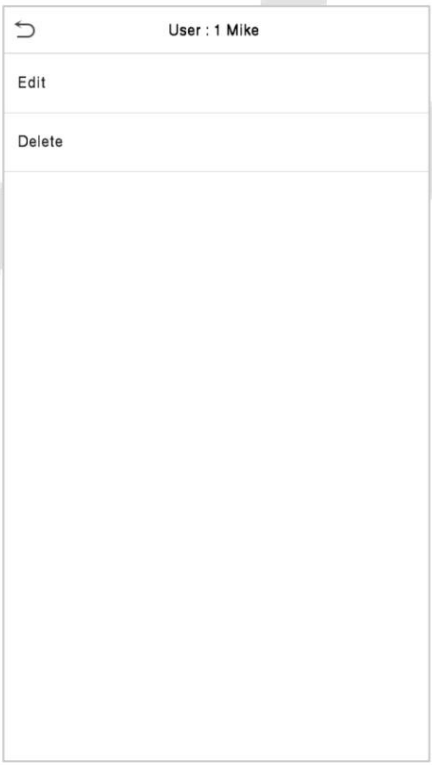
En la interfaz Todos los usuarios, toque la barra de búsqueda en la lista de usuarios para ingresar la palabra clave de recuperación requerida (donde la palabra clave puede ser la identificación del usuario, el apellido o el nombre completo) y el sistema buscará la información del usuario relacionada.

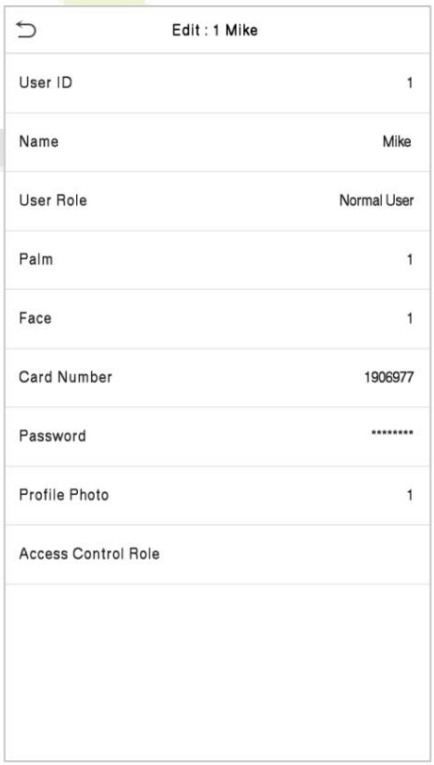




5.3 Editar usuario

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





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

5.4 Eliminar usuario

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

Eliminar operaciones

Eliminar Usuario: Elimina toda la información del usuario (elimina el Usuario seleccionado en su totalidad) del Dispositivo.

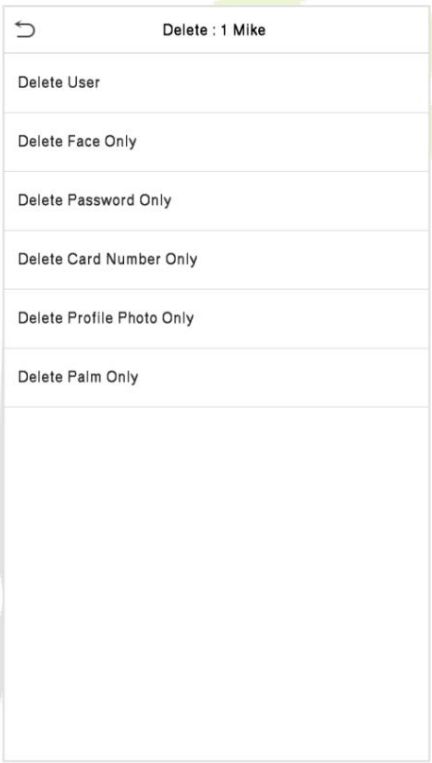
Eliminar solo rostro: elimina la información del rostro del usuario seleccionado.

Eliminar solo contraseña: elimina la información de contraseña del usuario seleccionado.

Eliminar solo número de tarjeta: elimina el número de tarjeta del usuario seleccionado.

Eliminar solo foto de perfil: elimina la foto de perfil del usuario seleccionado.

Eliminar solo Palm: elimina la información de Palm del usuario seleccionado.

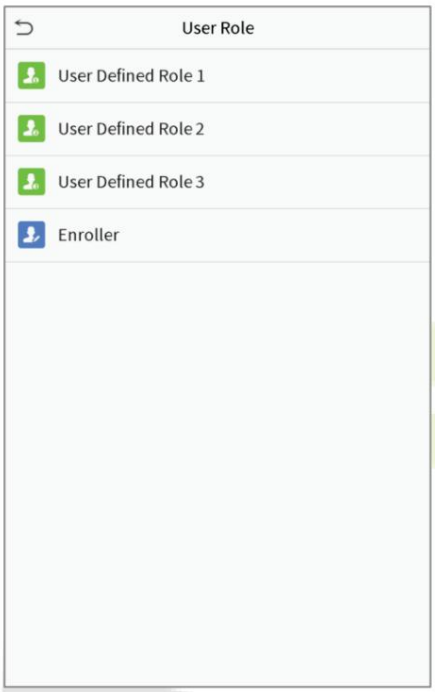


6 Rol de usuario

El rol de usuario facilita asignar algunos permisos específicos a ciertos usuarios, según el requisito.

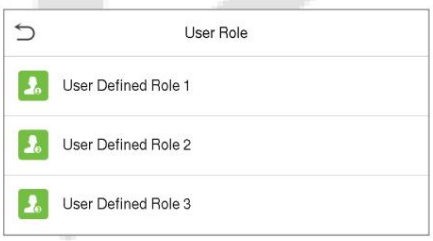
En el menú principal, toque Función de usuario y luego toque Función definida por el usuario para configurar la función definida por el usuario. permisos.

El alcance del permiso de la función personalizada se puede configurar en hasta 3 funciones, es decir, la función operativa personalizada. alcance de las funciones del menú del usuario.



En la interfaz Rol definido por el usuario, active Habilitar rol definido para habilitar o deshabilitar el usuario. rol definido.

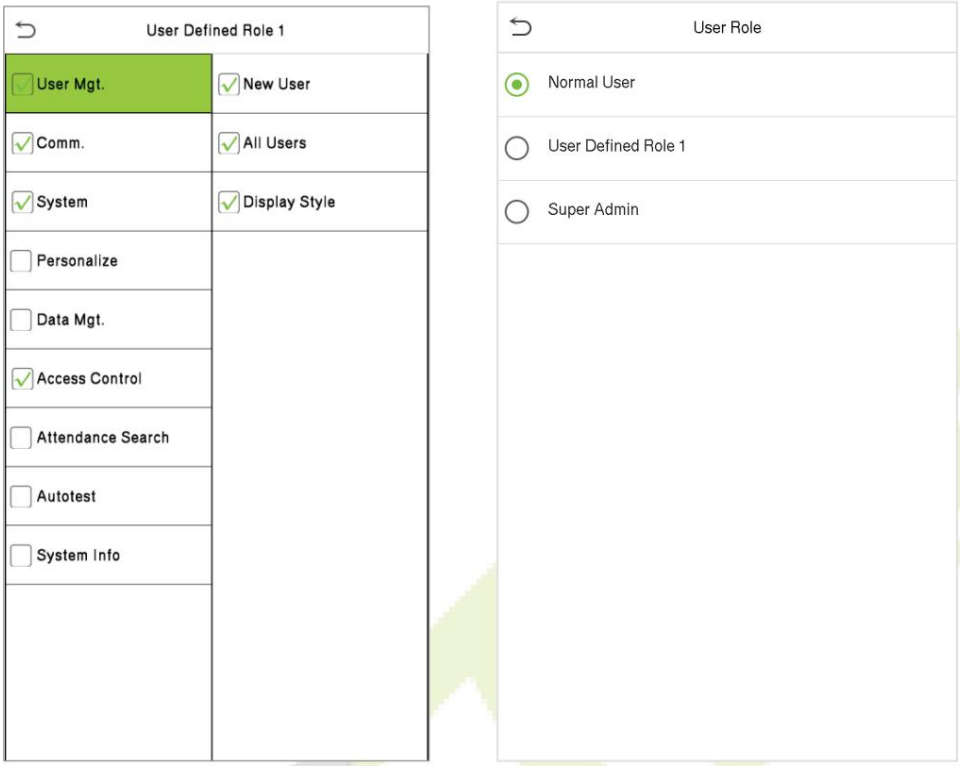
Toque Nombre e ingrese el nombre personalizado del rol.



Luego, toque Definir rol de usuario y seleccione los privilegios requeridos para asignar al nuevo rol, y luego toque el botón Volver.

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

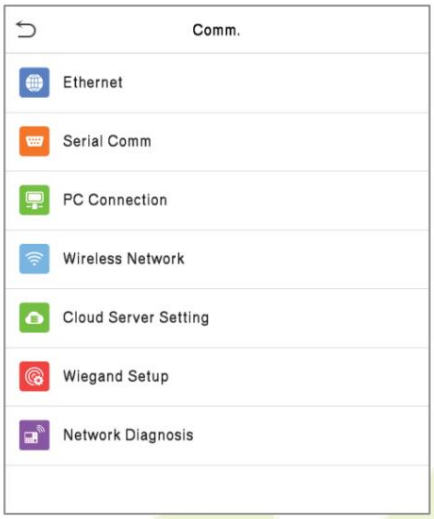
Primero toque el nombre de la función del Menú principal requerido y luego seleccione los submenús requeridos en la lista.



NOTA: Si la función de usuario está habilitada para el dispositivo, toque Gestión de usuarios. > Nuevo usuario > Rol de usuario para asignar los roles creados a los usuarios requeridos. Pero si no hay ningún superadministrador registrado en el dispositivo, el dispositivo indicará "¡Inscriba al superadministrador primero!". al habilitar la función de rol de usuario.

7 configuraciones de comunicación

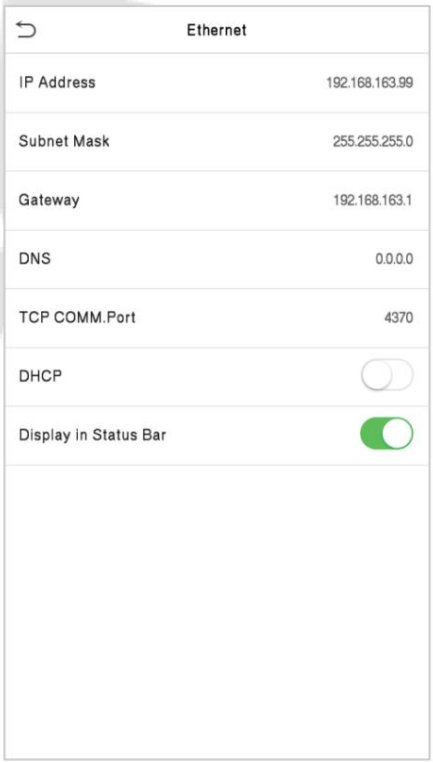
Toca COMUNICACIÓN. en el menú principal para configurar Ethernet, comunicación serie, conexión a PC, red inalámbrica, servidor en la nube, Wiegand y diagnóstico de red.



7.1 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.

Toque Ethernet en Comm. Interfaz de configuración para configurar los ajustes.



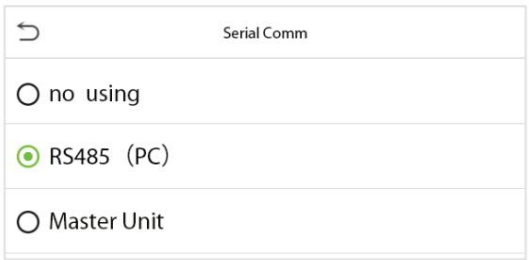
Función descriptiva

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

7.2 Comunicaciones en serie

La función Serial Comm facilita establecer comunicación con el dispositivo a través de un puerto serie (RS485/Unidad maestra).

Toque Comunicación en serie. en la comunicación. Interfaz de configuración.



Función descriptiva

Nombre de la función	Descripciones
Puerto serial	sin uso: No se comunique con el dispositivo a través del puerto serie. RS485(PC): Se comunica con el dispositivo a través del puerto serie RS485. Unidad maestra: cuando se utiliza RS485 como función de “Unidad maestra”, el dispositivo actuará como una unidad maestra y se puede conectar a una tarjeta y huella digital RS485.

	lector.
Tasa de baudios	Para la velocidad a la que se comunican los datos con la PC, existen 4 opciones de velocidad en baudios: 115200 (predeterminada), 57600, 38400 y 19200. Cuanto mayor sea la velocidad en baudios, más rápida será la velocidad de comunicación, pero también menos fiable. Por lo tanto, se puede utilizar una velocidad de transmisión más alta cuando la distancia de comunicación es corta; Cuando la distancia de comunicación es larga, sería más confiable elegir una velocidad de transmisión más baja.

7.3 Conexión a PC

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

Toque Conexión de PC en Comm. Interfaz de configuración para configurar los ajustes de comunicación.

Función descriptiva

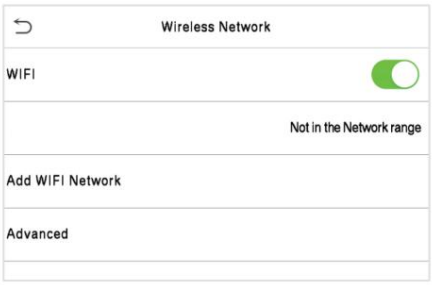
Nombre de la función	Descripciones
Tecla de comunicación	La contraseña predeterminada es 0, que se puede cambiar. La clave de comunicación puede contener de 1 a 6 dígitos.
ID del dispositivo	Número de identidad del dispositivo, que oscila entre 1 y 254. Si el método de comunicación es RS232/RS485, deberá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

7.4 Red inalámbrica

El dispositivo proporciona un módulo Wi-Fi, que puede integrarse dentro del molde del dispositivo o puede ser externo.
conectado.

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

Toque Red inalámbrica en Comm. Interfaz de configuración para configurar los ajustes de WiFi.



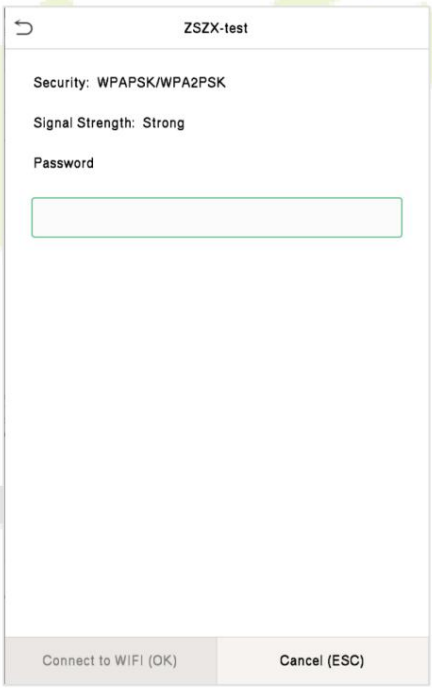
Buscar en la Red WIFI

WIFI está habilitado en el dispositivo de forma predeterminada. Activar Botón para habilitar o deshabilitar WIFI.

Una vez que el Wi-Fi esté encendido, el dispositivo buscará el WIFI disponible dentro del alcance de la red.

Toque el nombre de WiFi apropiado de la lista disponible e ingrese la contraseña correcta en el interfaz de contraseña y luego toque Conectar a WIFI (Aceptar).

WIFI habilitado: toque la red requerida de la red buscada lista.

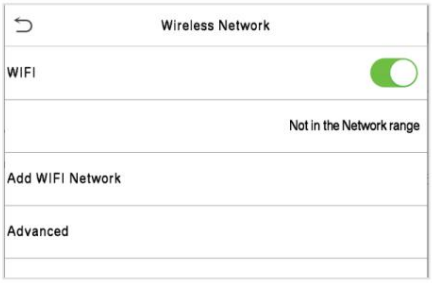


Toque el campo de contraseña para ingresar la contraseña y luego toque Conectarse a WIFI (Aceptar).

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

Agregar red WIFI manualmente

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



Toque Agregar red WIFI para agregar el WIFI manualmente.

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

NOTA: Después de agregar exitosamente el WIFI manualmente, siga el mismo proceso para buscar el nombre del WIFI agregado. Haga clic aquí para ver el proceso para buscar la red WIFI.

Configuración avanzada

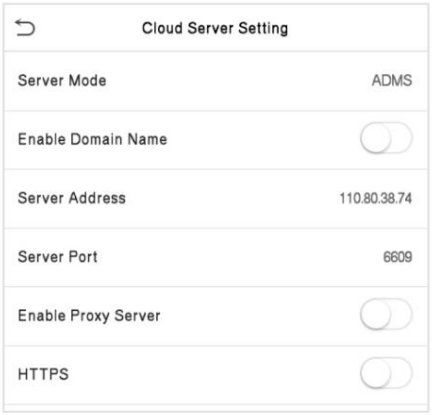
En la interfaz de red inalámbrica, toque Avanzado para configurar los parámetros relevantes según sea necesario.

Función descriptiva

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

7.5 Configuración del servidor en la nube

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



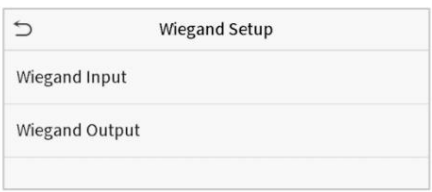
Función descriptiva

Nombre de la función		Descripción
Permitir Dominio Nombre	Dirección del servidor	Una vez habilitada esta función, se utilizará el modo de nombre de dominio “http://...”, como http://www.XYZ.com, mientras que “XYZ” denota el nombre de dominio (cuando este modo está activado).
Desactivar Dominio Nombre	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.
HTTPS		Basado en HTTP, el cifrado de transmisión y la autenticación de identidad garantizan la seguridad del proceso de transmisión.

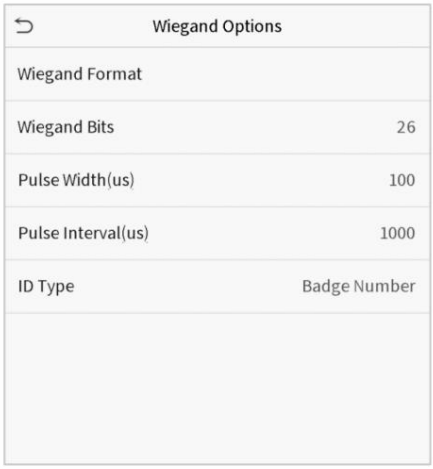
7.6 Configuración Wiegand

Para configurar los parámetros de entrada y salida Wiegand.

Toque Configuración de Wiegand en Comm. Interfaz de configuración para configurar los parámetros de entrada y salida Wiegand.



7.6.1 Entrada Wiegand



Función descriptiva

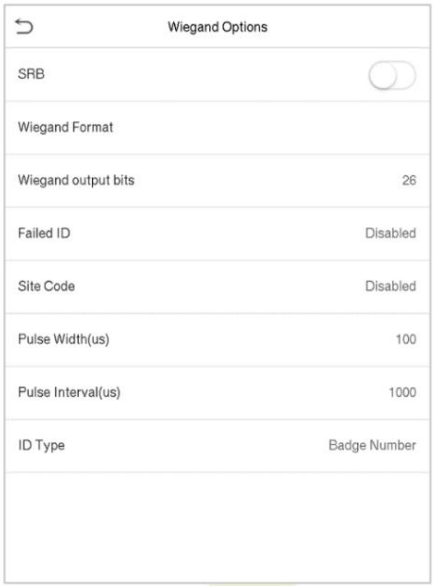
Nombre de la función	Descripciones
Los valores del formato Wiegand varían entre 26 bits, 32 bits, 34 bits, 36 bits, 37 bits, 50 bits y 64 bits.	
Puntas Wiegand	Número de bits de datos Wiegand.
Ancho de pulso (nosotros)	El valor del ancho de pulso enviado por Wiegand es de 100 microsegundos por defecto, el cual se puede ajustar dentro del rango de 20 a 100 microsegundos.
Legumbres Intervalo (nosotros)	El valor predeterminado es 1000 microsegundos, que se puede ajustar dentro del rango de 200 a 20000 microsegundos.
tipo de identificación	Seleccione entre ID de usuario y número de tarjeta.

Varios formatos Wiegand comunes Descripción:

Formato Wiegand	Descripción
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El primer bit es el bit de paridad par del 2 al 13. bits, mientras que el bit 26 es el bit de paridad impar de los bits 14 al 25. Los bits del 2 al 25 son los números de tarjeta.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El primer bit es el bit de paridad par del 2 al 13. bits, mientras que el bit 26 es el bit de paridad impar de los bits 14 al 25. Los bits del 2 al 9 son los códigos de sitio, mientras que los bits del 10 al 25 son los números de tarjeta.

Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El primer bit es el bit de paridad par de los bits 2 al 17, mientras que el bit 34 es el bit de paridad impar de los bits 18 al 33. Los bits del 2 al 25 son los números de tarjeta.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El primer bit es el bit de paridad par de los bits 2 al 17, mientras que el bit 34 es el bit de paridad impar de los bits 18 al 33. Los bits del 2 al 9 son los códigos de sitio, mientras que los bits del 10 al 25 son los números de tarjeta.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El primer bit es el bit de paridad impar de los bits 2 al 18, mientras que el bit 36 es el bit de paridad par de los bits 19 al 35. Los bits del 2 al 17 son los códigos de dispositivo. Los bits 18 al 33 son los números de tarjeta y los bits 34 al 35 son los códigos del fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCO Consta de 36 bits de código binario. El primer bit es el bit de paridad par de los bits 2 al 18, mientras que el bit 36 es el bit de paridad impar de los bits 19 al 35. Los bits del 2 al 19 son los códigos del dispositivo y los bits del 20 al 35 son los números de tarjeta.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCE Consta de 37 bits de código binario. El primer bit es el bit de paridad impar de los bits 2 al 18, mientras que el bit 37 es el bit de paridad par de los bits 19 al 36. Los bits 2.º a 4.º son los códigos del fabricante. Los bits del 5 al 16 son los códigos de sitio y los bits del 21 al 36 son los números de tarjeta.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCO Consta de 37 bits de código binario. El primer bit es el bit de paridad par de los bits 2 al 18, mientras que el bit 37 es el bit de paridad impar de los bits 19 al 36. Los bits 2.º a 4.º son los códigos del fabricante. Los bits del 5 al 14 son los códigos de dispositivo, los bits del 15 al 20 son los códigos de sitio y los bits del 21 al 36 son los números de tarjeta.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 50 bits de código binario. El primer bit es el bit de paridad par de los bits 2 al 25, mientras que el bit 50 es el bit de paridad impar de los bits 26 al 49. Los bits del 2 al 17 son los códigos de sitio y los bits del 18 al 49 son los números de tarjeta.
"C" indica el número de tarjeta; "E" denota el bit de paridad par; "O" denota el bit de paridad impar; "F" indica el código de instalación; "M" indica el código del fabricante; "P" denota el bit de paridad; y "S" indica el código del sitio.	

7.6.2 Salida Wiegand



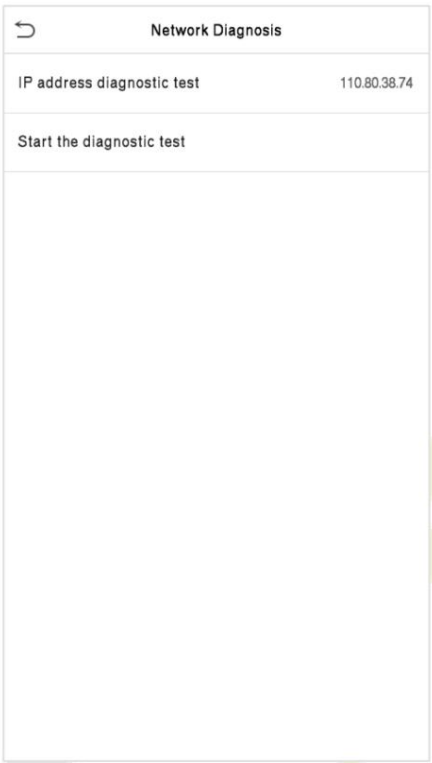
Función descriptiva

Nombre de la función	Descripciones
SRB	Cuando SRB está habilitado, el SRB controla el bloqueo para evitar que se abra debido a la extracción del dispositivo.
Formato Wiegand	Los valores varían entre 26 bits, 32 bits, 34 bits, 36 bits, 37 bits, 50 bits y 64 bits.
Bits de salida Wiegand	Después de seleccionar el formato Wiegand requerido, seleccione los dígitos de bits de salida correspondientes del formato Wiegand.
Identificación fallida	Si la verificación falla, el sistema enviará la identificación fallida al dispositivo y reemplazará el número de tarjeta o la identificación del personal por uno nuevo.
Código del sitio	Es similar a la ID del dispositivo. La diferencia es que un código de sitio se puede configurar manualmente y se puede repetir en un dispositivo diferente. El valor válido oscila entre 0 y 256 de forma predeterminada.
Ancho de pulso (nosotros)	El ancho de tiempo representa los cambios de la cantidad de carga eléctrica con capacitancia regular de alta frecuencia dentro de un tiempo específico.
Intervalo de pulso (nosotros)	El intervalo de tiempo entre pulsos.
tipo de identificación	Seleccione los tipos de ID como ID de usuario o número de tarjeta.

7.7 Diagnóstico de red

Para configurar los parámetros de diagnóstico de la red.

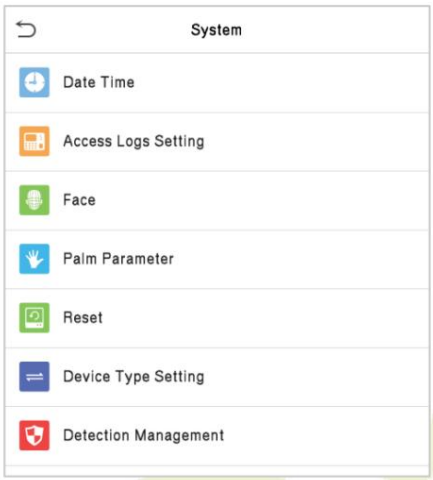
Toque Diagnóstico de red en el menú Comm. Interfaz de configuración para configurar el diagnóstico de la dirección IP e iniciar los parámetros de diagnóstico.



8 Configuración del sistema

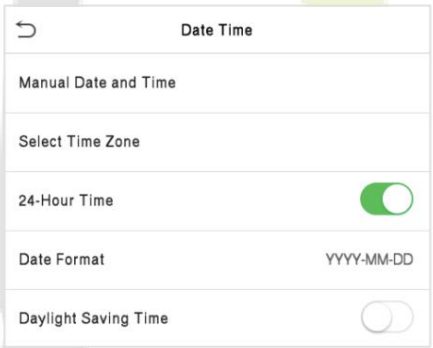
Configure los parámetros relacionados del sistema para optimizar el rendimiento del dispositivo.

Toque Sistema en la interfaz del Menú principal para configurar los parámetros relacionados del sistema a fin de optimizar el rendimiento del dispositivo.



8.1 Fecha y hora

Toque Fecha y hora en la interfaz del Sistema para configurar la fecha y la hora.

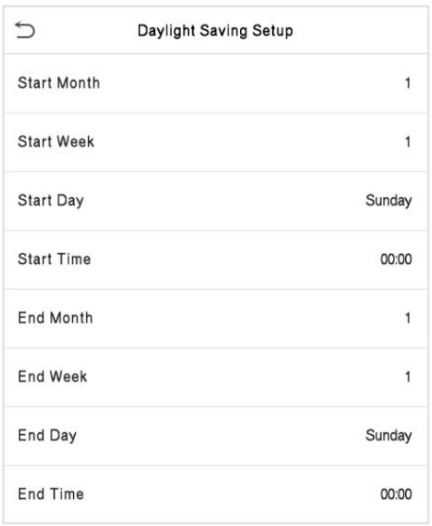


Toque Configuración de hora manual para configurar manualmente la fecha y la hora y toque Confirmar para guardar.

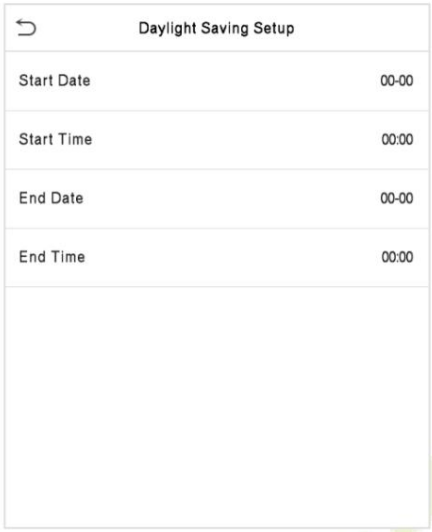
Toque Seleccionar zona horaria para seleccionar manualmente la zona horaria donde se encuentra el dispositivo.

Toque Hora de 24 horas para habilitar o deshabilitar este formato. Si está habilitado, seleccione el formato de fecha para configurar el formato de fecha.

Toque Horario de verano para habilitar o deshabilitar la función. Si está habilitado, toque Horario de verano Modo para seleccionar un modo de horario de verano y luego toque Configuración de horario de verano para configurar el interruptor. tiempo.



Modo semana



Modo de fecha

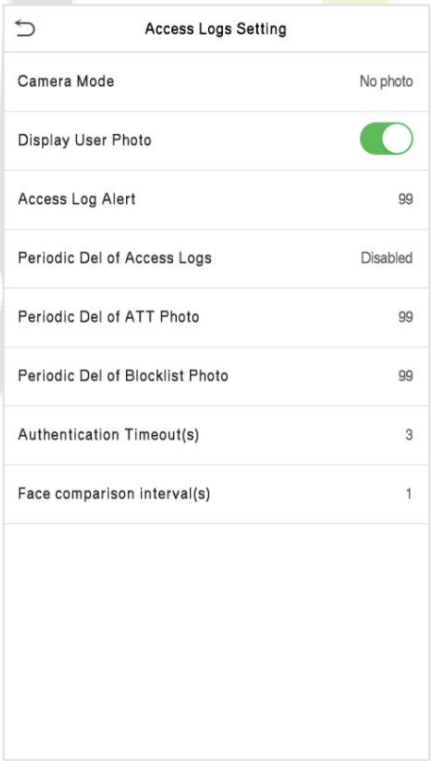
Al restaurar la configuración de fábrica, se pueden cambiar la hora (24 horas) y el formato de fecha (AAAA-MM-DD).

restaurar, pero la fecha y 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 de 2020. Luego de restaurar la configuración de fábrica, la hora del equipo seguirá siendo las 18:30 del 1 de enero de 2020.

8.2 Configuración de registros de acceso

Haga clic en Configuración de registros de acceso en la interfaz del sistema.

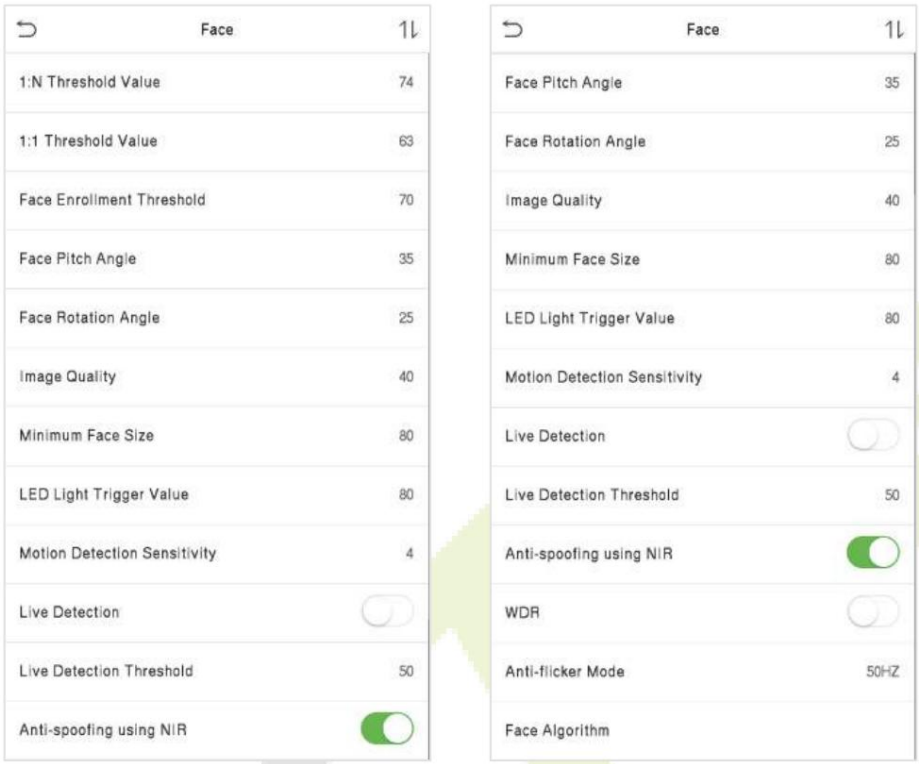


Función descriptiva

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

8.3 Parámetros de la cara

Toque Cara en la interfaz del Sistema para ir a la configuración de parámetros de la cara.



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

Función descriptiva

Nombre de la función	Descripción
Valor umbral 1:N	En el modo de verificación 1:N, la verificación solo será exitosa cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas sea mayor que el valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será la tasa de errores de juicio, mayor será la tasa de rechazo y viceversa. Se recomienda establecer el valor predeterminado de 74.

Valor umbral 1:1	En el modo de verificación 1:1, la verificación solo será exitosa cuando la similitud entre la imagen facial adquirida y las plantillas faciales del usuario registradas en el dispositivo sea mayor que el valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será la tasa de 55nrolment55nt, mayor será la tasa de rechazo y viceversa. Se recomienda establecer el valor predeterminado de 63.
Inscripción facial Límite	Durante la inscripción facial, se utiliza la comparación 1:N para determinar si el usuario ya se ha registrado anteriormente. Cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas es mayor que este umbral, indica que el rostro ya ha sido registrado.
Ángulo de paso de la cara	La tolerancia del ángulo de paso de una cara para el registro y comparación facial. Si el ángulo de inclinación de una cara excede este valor establecido, el algoritmo lo filtrará, es decir, el terminal lo ignorará y, por lo tanto, no se activará ninguna interfaz de registro y comparación.
Ángulo de rotación de la cara	La tolerancia del ángulo de rotación de una cara para el registro y comparación de plantillas faciales. Si el ángulo de rotación de una cara excede este valor establecido, el algoritmo lo filtrará, es decir, el terminal lo ignorará y, por lo tanto, no se activará ninguna interfaz de registro y comparación.
Calidad de la imagen	Calidad de imagen para registro y comparación facial. Cuanto mayor sea el valor, más clara será la imagen.
Tamaño mínimo de la cara	Requerido para el registro y comparación facial. Si el tamaño mínimo de la figura capturada es menor que este valor establecido, se filtrará y no se reconocerá como una cara. Este valor puede entenderse como la distancia de comparación de caras. Cuanto más lejos esté la persona, más pequeña será la cara y el algoritmo obtendrá el píxel de la cara más pequeño. Por lo tanto, ajustar este parámetro puede ajustar la distancia de comparación más lejana de las caras. Cuando el valor es 0, la distancia de comparación de caras no está limitada.
Luz LED activada Valor	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, más frecuentemente se encenderá la luz LED.
Detección de movimiento Sensibilidad	Se trata de establecer el valor de la cantidad de cambio en el campo de visión de una cámara, lo que se conoce como detección de movimiento potencial que activa el terminal desde el modo de espera a la interfaz de comparación. Cuanto mayor sea el valor, más sensible será el sistema, es decir, si un valor mayor Se establece el valor, la interfaz de comparación es mucho más fácil y la detección de movimiento frecuentemente desencadenado.

Detección en vivo	Intento de detección de la falsificación utilizando imágenes de luz visible para determinar si la muestra de fuente biométrica proporcionada es realmente una persona (un ser humano vivo) o una representación falsa.
Detección en vivo Límite	Facilita juzgar si la imagen visible capturada es realmente una persona (un ser humano vivo). Cuanto mayor sea el valor, mejor será el rendimiento contra la suplantación de identidad utilizando luz visible.
Uso antisuplantación de identidad 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 amplía la visibilidad de la imagen para vídeos de vigilancia en escenas de iluminación de alto contraste y mejora la identificación de objetos en entornos brillantes y oscuros.
Modo antiparpadeo	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.
Algoritmo facial	Información relacionada con el algoritmo facial y pausar la actualización de la plantilla facial.

NOTA: Un ajuste inadecuado de los parámetros de exposición y calidad puede afectar gravemente el rendimiento del dispositivo. Ajuste el parámetro de exposición únicamente bajo la guía del personal de servicio posventa de nuestra empresa.

Proceso para modificar la Precisión del Reconocimiento Facial

En la interfaz del Sistema, toque Cara y luego alterne para habilitar Anti-Spoofing usando NIR para configurar la anti-suplantación de identidad.

Luego, en el Menú principal, toque Prueba automática > Probar rostro y realice la prueba facial.

Toque tres veces para ver las puntuaciones en la esquina superior derecha de la pantalla y el cuadro rectangular rojo. Aparece para comenzar a ajustar el modo.

Mantenga la distancia de un brazo entre el dispositivo y la cara, y se recomienda no mover la cara en amplio rango

8.4 Parámetros de la palma

Toque Palm en la interfaz del Sistema para configurar los ajustes de Palm.

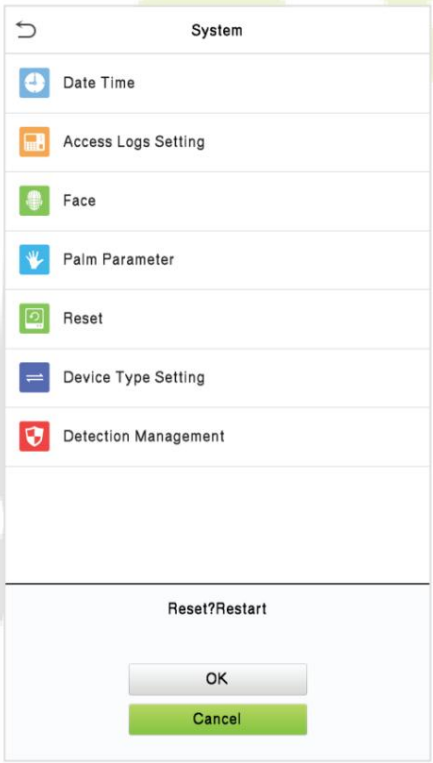
Función descriptiva

Nombre de la función	Descripción
Umbral de coincidencia 1:1 de Palm	Solo cuando la similitud entre la palma de verificación y la palma registrada del usuario sea mayor que este valor, la verificación podrá tener éxito.
Umbral coincidente Palm 1:N	Según el método de verificación 1:N, la verificación solo puede tener éxito cuando la similitud entre la palma verificada y todas las palmas registradas es mayor que este valor.

8.5 Restablecimiento de fábrica

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

Toque Restablecer en la interfaz del Sistema y luego toque Aceptar para restaurar la configuración predeterminada de fábrica.



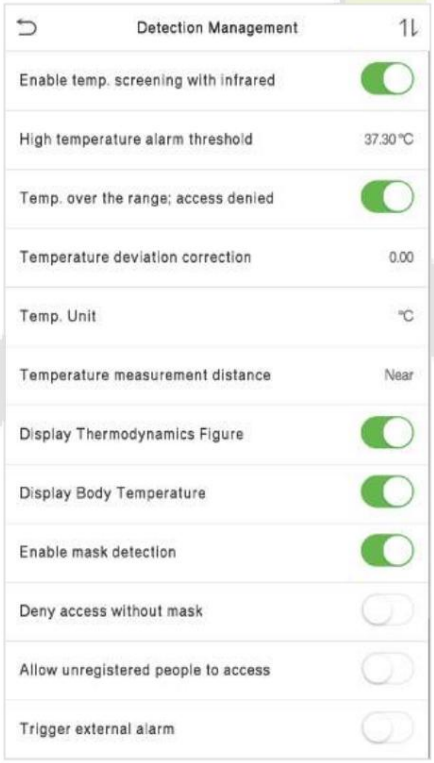
8.6 Configuración del tipo de dispositivo

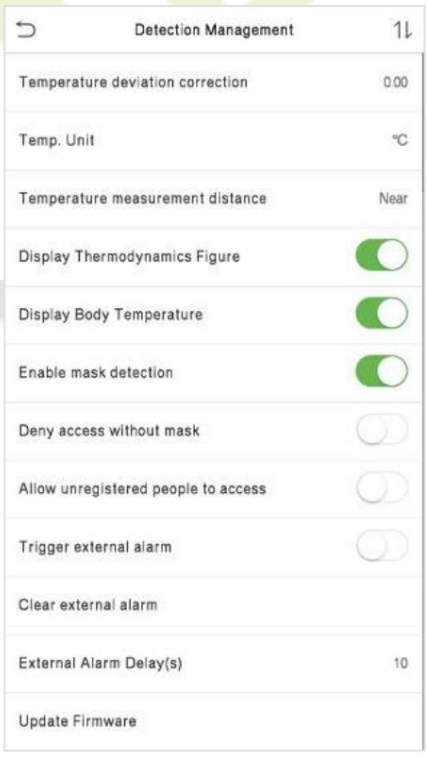
Toque Configuración del tipo de dispositivo en la interfaz del Sistema.

Nombre de la función	Descripción
Protocolo de comunicación	Configure el protocolo de comunicación del dispositivo.
Tipo de dispositivo	Configure el dispositivo como terminal de control de acceso.

8.7 Gestión de detección

Haga clic en Gestión de detección en la interfaz del sistema para configurar los ajustes de Gestión de detección.





Función descriptiva

Nombre de la función	Descripción
Habilitar tem. cribado con infrarrojos	Para habilitar o deshabilitar la medición de temperatura por infrarrojos. Cuando esta función está habilitada, los usuarios deben pasar el control de temperatura además de la verificación de identidad antes de que se les conceda el acceso. Para medir la temperatura corporal, las caras del usuario deben estar alineadas con el área de medición de temperatura.
Umbral de alarma de alta temperatura	Para configurar el valor del umbral de alarma por temperatura corporal alta. Cuando la temperatura medida durante la verificación es superior al valor establecido, el dispositivo emitirá una alarma sonora y rápida. El umbral de alarma predeterminado es 37,30 °C.
Tem. en el rango; acceso denegado	Cuando está habilitado, si la temperatura corporal del usuario medida está por encima (o por debajo) del umbral de alarma, no se le otorgará acceso al usuario incluso si se verifica su identidad. Cuando está deshabilitado, se otorga acceso al usuario si se verifica su identidad, independientemente de su temperatura corporal.
Corrección de desviación de temperatura	Como el módulo de medición de temperatura lee un pequeño rango de variación de un valor observado en ambientes inusuales (humedad, temperatura ambiente extrema y similares), los usuarios pueden configurar el valor de desviación aquí para reflejar la temperatura real de la persona.
Temperatura. Unidad	La unidad de temperatura corporal se puede alternar entre Celsius (°C) y Fahrenheit (°F).
Temperatura medición distancia	Hay tres modos al medir la temperatura durante el proceso de verificación: Cerca, Cerca y Lejos.
Mostrar Termodinámica Cifra	Para habilitar o deshabilitar la visualización de la imagen térmica de una persona. Cuando está habilitado, la imagen térmica de la persona se muestra en la esquina superior izquierda del dispositivo durante el proceso de detección.
Cuerpo de visualización Temperatura	Para habilitar o deshabilitar la visualización de la temperatura corporal. Cuando esté habilitado, el dispositivo mostrará el valor de temperatura corporal del usuario durante el proceso de verificación.
Habilitar máscara detección	Para habilitar o deshabilitar la función de detección de máscara. Cuando esté habilitado, el dispositivo identificará si el usuario lleva una máscara o no durante la verificación.

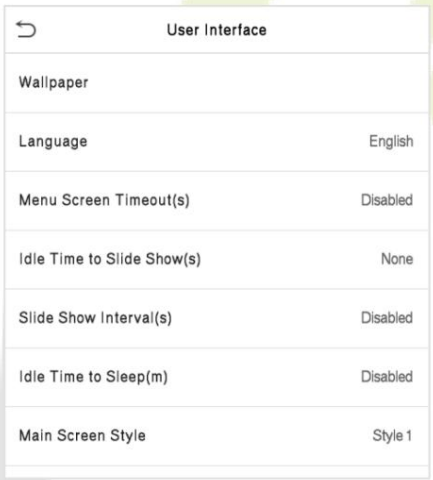
Denegar acceso sin máscara	Para habilitar o deshabilitar el acceso de una persona sin máscara. Cuando esté habilitado, el dispositivo negará el acceso a una persona que no use una máscara.
Permitir el acceso a personas no registradas	Para habilitar o deshabilitar el acceso de personas no registradas. Cuando está habilitado, el dispositivo permite que la persona ingrese sin registrarse, siempre y cuando la persona pase la detección.
Habilitar captura de persona no registrada	Para habilitar o deshabilitar la función de captura de persona no registrada. Cuando está habilitada, el dispositivo capturará automáticamente la foto de la persona no registrada; para habilitar esta función es necesario habilitar Permitir el acceso a personas no registradas.
Activar alarma externa	Cuando está habilitado, si la temperatura del usuario es superior al valor umbral establecido o la detección de máscara está habilitada, pero la persona no usa la máscara, se activará una alarma.
Borrar alarma externa	Borra los registros de alarma activada del dispositivo.
Alarma externa Retraso(s)	El tiempo de retardo para activar una alarma externa. Se puede configurar en segundos. Los usuarios pueden desactivar la función o establecer un valor entre 1 y 255.
Actualice el firmware	Elija si desea actualizar la versión del software del módulo de detección de temperatura de imágenes térmicas.

9 Personalizar configuraciones

Toque Personalizar en la interfaz del Menú principal para personalizar la configuración de la interfaz, voz, timbre, opciones de estado de marcado y asignaciones de teclas de acceso directo.

9.1 Configuración de la interfaz

Toque Interfaz de usuario en la interfaz Personalizar para personalizar el estilo de visualización de la interfaz principal.



Función descriptiva

Nombre de la función	Descripción
Fondo de pantalla	El fondo de pantalla de la pantalla principal se puede seleccionar según las preferencias del usuario.
Idioma	Seleccione el idioma del dispositivo.
Pantalla de menú Tiempos de espera	Cuando no se realiza ninguna operación y el tiempo excede el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. La función se puede desactivar o establecer el valor requerido entre 60 y 99999 segundos.

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

9.2 Configuración de voz

Toque Voz en la interfaz Personalizar para configurar los ajustes de voz.

Función descriptiva

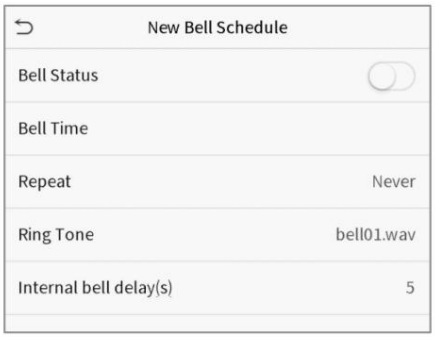
Nombre de la función	Descripción
Mensaje de voz	Cambie para habilitar o deshabilitar las indicaciones de voz durante las operaciones de funciones.
Aviso táctil	Alternar para habilitar o deshabilitar los sonidos del teclado.
Volumen	Ajuste el volumen del dispositivo, que se puede configurar entre 0 y 100.

9.3 Horarios de timbre

Toque Horarios de timbre en la interfaz Personalizar para configurar los ajustes del timbre.

Nuevo horario de campana

Toque Nuevo horario de timbre en la interfaz Horario de timbre para agregar un nuevo horario de timbre.



Función descriptiva

Nombre de la función	Descripción
Estado de la campana	Alterne para habilitar o deshabilitar el estado de la campana.
Hora de la campana	Una vez establecido el tiempo requerido, el dispositivo se activará automáticamente para sonar el timbre durante ese tiempo.
Repetir	Establezca el número requerido de conteos para repetir la campana programada.
Tono de llamada	Seleccione un tono de timbre.
Retardo(s) de timbre interno	Configure el tiempo de reproducción de la campana interna. Los valores válidos oscilan entre 1 y 999 segundos.

Todos los horarios de timbre

Una vez programada la campana, en la interfaz Horarios de timbre, toque Todos los horarios de timbre para ver los nuevos campana programada.

Editar la campana programada

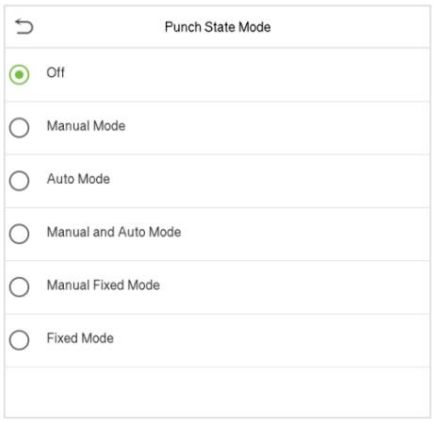
En la interfaz Todos los horarios de timbre, toque el horario de timbre requerido y toque Editar para editar el horario de timbre seleccionado. El método de edición es el mismo que el de agregar un nuevo horario de campana.

eliminar una campana

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

9.4 Opciones de estados de perforación

Toque Opciones de estados de perforación en la interfaz Personalizar para configurar los ajustes del estado de perforación.



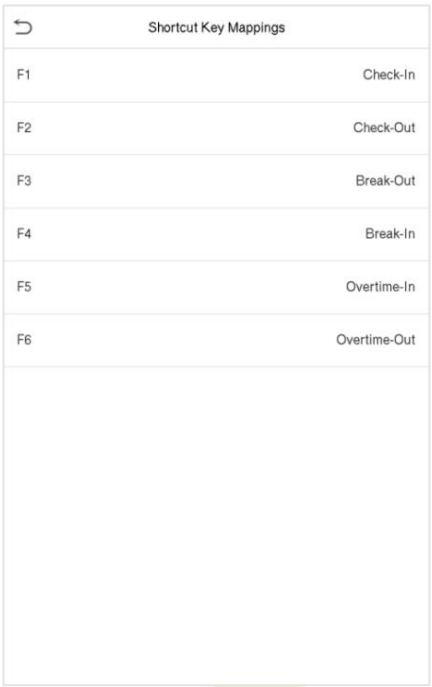
Función descriptiva

Nombre de la función	Descripción
Modo de estado de perforación	Apagado: Desactiva la función de estado de perforación. Por lo tanto, la clave de estado de perforación configurada en el menú Asignaciones de teclas de acceso directo dejará de ser válida. Modo manual: cambie la tecla de estado de perforación manualmente y la tecla de estado de perforación desaparecerá después del tiempo de espera del estado de perforación. Modo automático: la tecla de estado de marcado cambiará automáticamente a un estado de marcado específico de acuerdo con el horario predefinido que se puede configurar en las asignaciones de teclas de acceso directo. Modo manual y automático: la interfaz principal mostrará la clave de estado de perforación de cambio automático. Sin embargo, los usuarios aún podrán seleccionar una alternativa que es el estado de asistencia manual. Después del tiempo de espera, la tecla de estado de marcado de cambio manual se convertirá en la clave de estado de marcado de cambio automático. Modo fijo manual: después de que la tecla de estado de perforación se configura manualmente en un estado de perforación particular, la función permanecerá sin cambios hasta que se cambie manualmente nuevamente. Modo fijo: solo se mostrará la clave de estado de perforación fijada manualmente. Los usuarios no pueden cambiar el estado presionando ninguna otra tecla.

9.5 Asignaciones de teclas de acceso directo

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

Toque Asignaciones de teclas de acceso directo en la interfaz Personalizar para configurar las teclas de acceso directo requeridas.



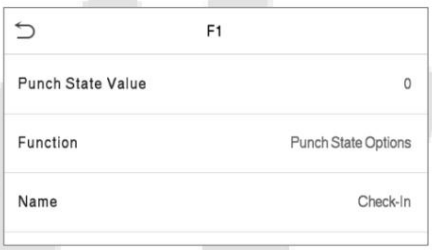
En la interfaz de Asignaciones de teclas de acceso directo, toque la tecla de acceso directo requerida para configurar los ajustes de la tecla de acceso directo.

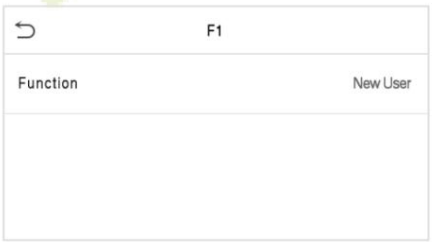
En la interfaz de la tecla de acceso directo (es decir, “F1”), toque función para configurar el proceso funcional del

tecla de acceso directo ya sea como tecla de estado de perforación o tecla de función.

Si la tecla de acceso directo se define como una tecla de función (como Nuevo usuario, Todos los usuarios, etc.), la configuración se completa como se muestra en la

imagen a continuación.





Si la tecla de acceso directo está configurada como una tecla de estado de marcado (como registro de entrada, salida, etc.), entonces es necesario

para configurar el valor del estado de perforación (valor válido 0~250), el nombre y el tiempo de conmutación.

Establecer el tiempo de cambio

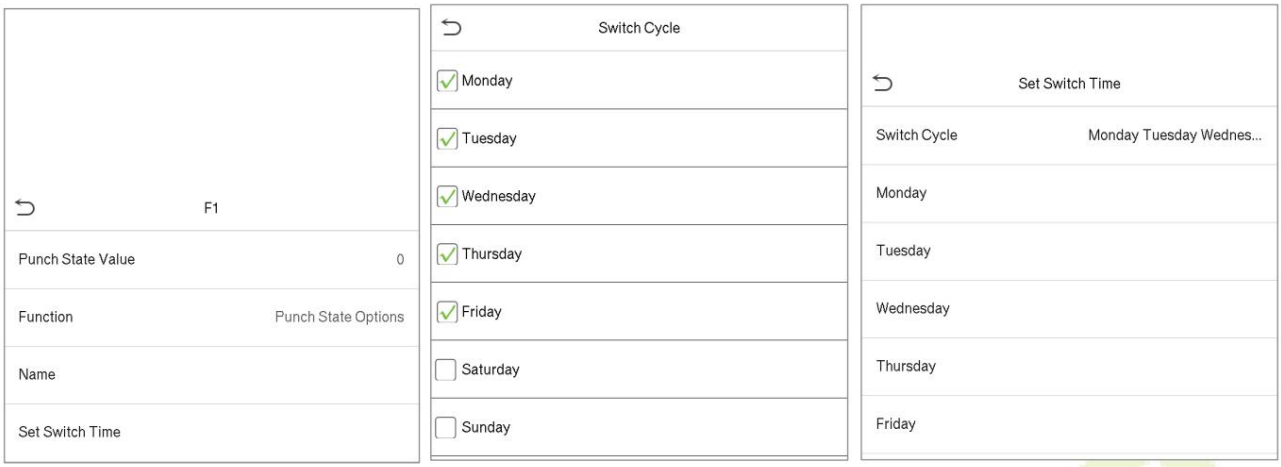
El tiempo de cambio se establece de acuerdo con las opciones de estado de perforación.

Cuando el modo de estado de perforación está configurado en modo automático, se debe configurar el tiempo de cambio.

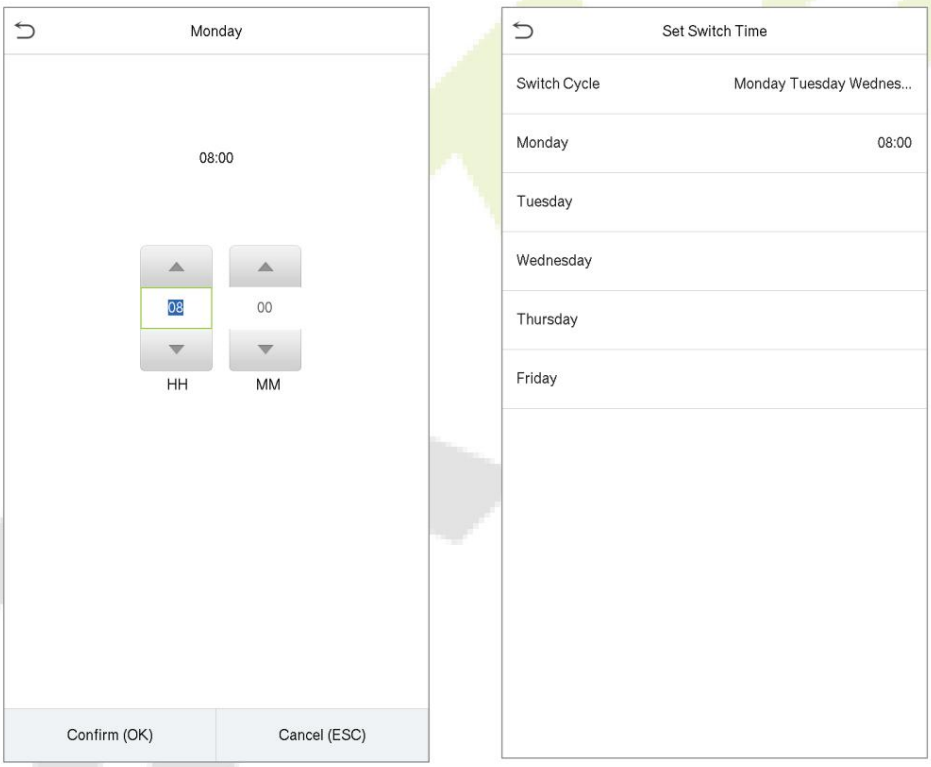
En la interfaz de la tecla de acceso directo, toque Establecer hora de cambio para configurar la hora de cambio.

En la interfaz Switch Cycle, seleccione el ciclo de cambio (lunes, martes, etc.) como se muestra en la

imagen a continuación.



Una vez seleccionado el ciclo de cambio, configure la hora de cambio para cada día y toque Aceptar para confirmar, como se muestra en la imagen de abajo.



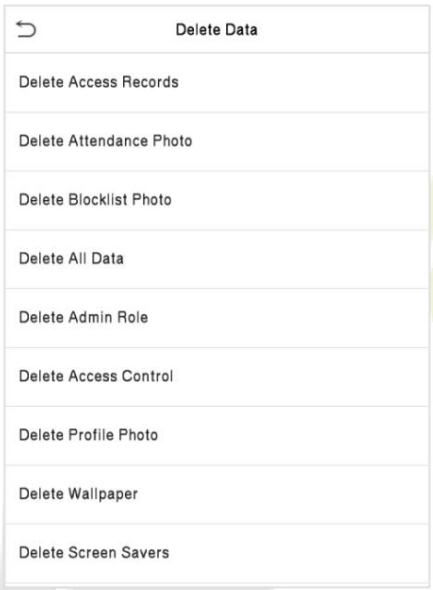
NOTA: Cuando la función está configurada en Indefinido, el dispositivo no habilitará la tecla de estado de perforación.

10 Gestión de datos

En el menú principal, toque Gestión de datos. para eliminar los datos relevantes en el dispositivo.

10.1 Eliminar datos

Toque Eliminar datos en Gestión de datos. interfaz para eliminar los datos requeridos.

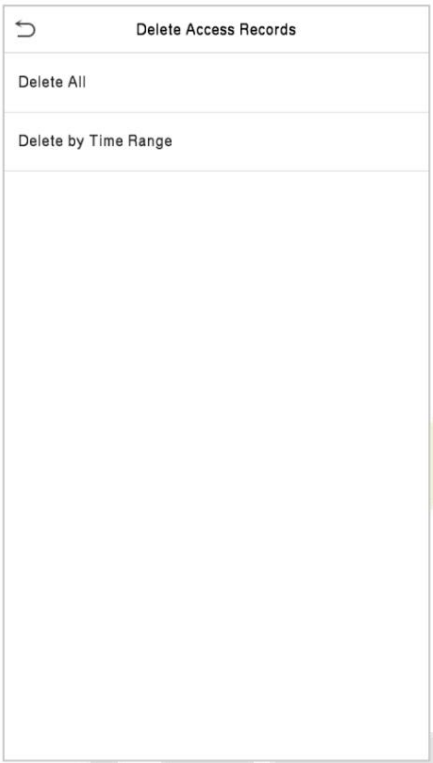


Función descriptiva

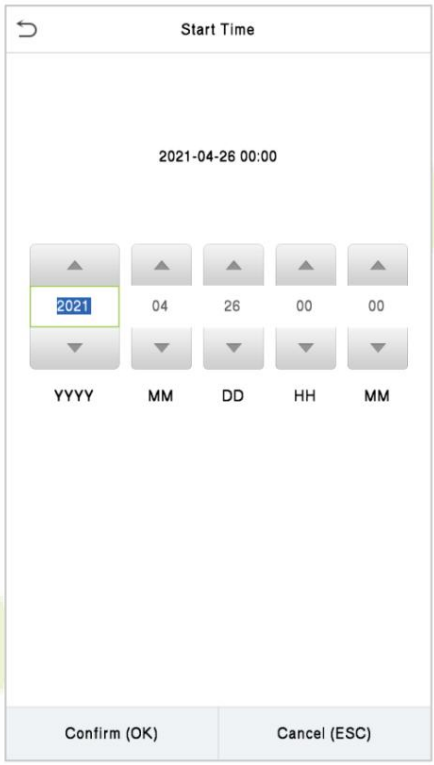
Nombre de la función	Descripción
Eliminar registros de acceso	Eliminar datos de asistencia/registros de acceso de forma condicional.
Eliminar foto de asistencia	Para eliminar fotos de asistencia del personal designado.
Eliminar foto de la lista de bloqueo	Para eliminar las fotos tomadas durante las verificaciones fallidas.
Eliminar todos los datos	Para eliminar información y registros de asistencia/registros de acceso de todos los registrados usuarios.
Eliminar función de administrador	Para eliminar todos los privilegios de administrador.
Eliminar control de acceso	Eliminar todos los datos de acceso.
Eliminar foto de perfil	Para eliminar todas las fotos de perfil en el dispositivo.

Eliminar fondo de pantalla	Para eliminar todos los fondos de pantalla del dispositivo.
Eliminar protectores de pantalla	Para eliminar los protectores de pantalla del dispositivo.

El usuario puede seleccionar Eliminar todo o Eliminar por rango de tiempo al eliminar los registros de acceso, las fotos de asistencia o las fotos bloqueadas. Al seleccionar Eliminar por rango de tiempo, debe establecer un rango de tiempo específico para eliminar todos los datos dentro de un período específico.



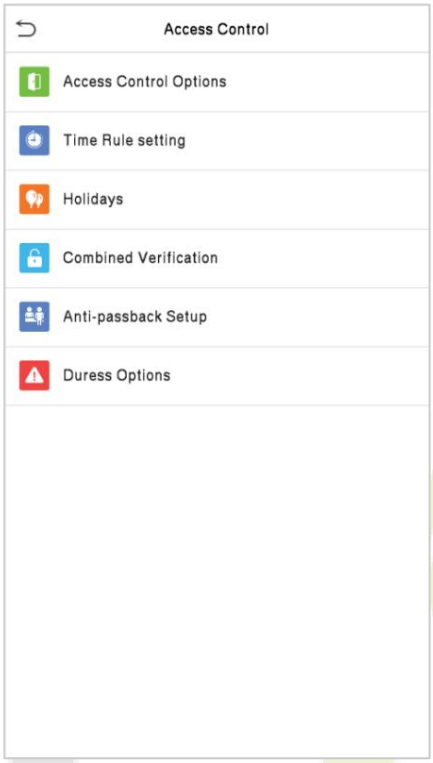
Seleccione Eliminar por rango de tiempo.



Establezca el rango de tiempo y haga clic en Aceptar.

11 Control de acceso

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



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

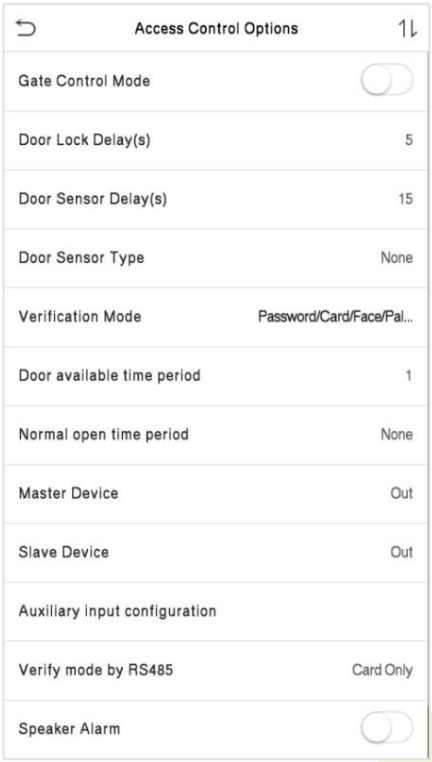
La hora de desbloqueo actual de la puerta correspondiente debe estar dentro de cualquier zona horaria válida de la hora del usuario. período.

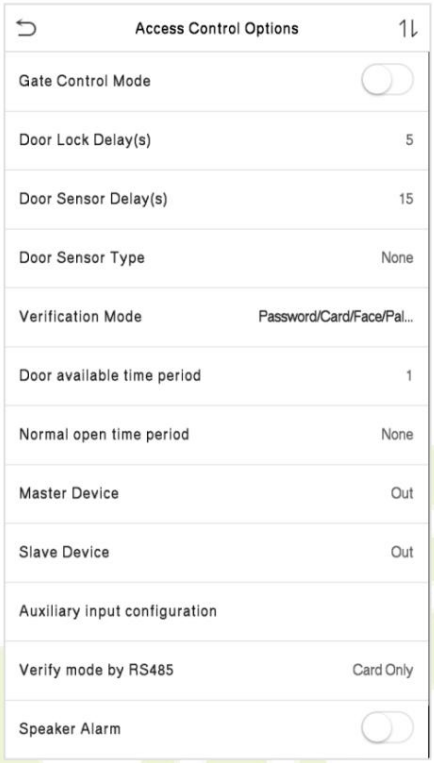
El grupo de usuario correspondiente ya debe estar configurado en la combinación de desbloqueo de puertas (y si hay otros grupos, estando configurados en el mismo combo de acceso, entonces la verificación de esos grupos los miembros también deben desbloquear la puerta).

En la configuración predeterminada, los nuevos usuarios se asignan al primer grupo con la zona horaria predeterminada del grupo. donde el combo de acceso es "1" y está configurado en estado de desbloqueo de forma predeterminada.

11.1 Opciones de control de acceso

Toque Opciones de control de acceso en la interfaz de Control de acceso para configurar los parámetros del bloqueo de control del terminal y el equipo relacionado.





Función descriptiva

Nombre de la función	Descripción
Modo de control de puerta	Cambie entre el interruptor ON o OFF para entrar o no en el modo de control de puerta. Cuando se configura en ON, en esta interfaz se eliminarán las opciones Relé de bloqueo de puerta, Relé de sensor de puerta y Tipo de sensor de puerta.
Retardo(s) de bloqueo de puerta	El período de tiempo que el dispositivo controla que la cerradura eléctrica esté en estado de desbloqueo. Valor válido: 1 a 99 segundos; 0 segundos representa la desactivación de la función.
Retardo(s) del sensor de puerta	Si la puerta no está bloqueada y se deja abierta durante un período determinado (Retardo del sensor de puerta), se activará una alarma. El valor válido del retardo del sensor de puerta oscila entre 1 y 255 segundos.
Tipo de sensor de puerta	Hay tres tipos de sensores: Ninguno, Normal abierto y Normal cerrado. Ninguno: Significa que el sensor de puerta no está en uso. Abierto Normal: Significa que la puerta siempre se deja abierta cuando hay energía eléctrica. Normal Cerrado: Significa que la puerta siempre se deja cerrada cuando hay energía eléctrica encendida.
Modo de verificación	El modo de verificación admitido incluye Contraseña/Tarjeta/Cara/Palm, Sólo ID de usuario, Contraseña, Sólo tarjeta, Contraseña + Tarjeta, Contraseña/Tarjeta, Sólo cara, Cara + Contraseña, Palma, Palma + Tarjeta y Palma + Cara.

Tiempo de disponibilidad de puerta período	Para establecer el período de tiempo para la puerta, de modo que la puerta esté disponible solo durante ese período.
horario normal de apertura Período	Periodo de tiempo programado para el modo “Apertura Normal”, de manera que la puerta quede siempre abierta durante este periodo.
Dispositivo maestro	Al configurar el maestro, el estado del maestro se puede configurar para salir en ingresar. Salida: el registro verificado en el host es el registro de salida. En: El registro verificado en el host es el registro de entrada.
Dispositivo esclavo	Al configurar el esclavo, el estado del esclavo se puede configurar para salir al ingresar. Salida: el registro verificado en el host es el registro de salida. En: El registro verificado en el host es el registro de entrada.
Configuración de entrada auxiliar	Establece el período de tiempo de desbloqueo de la puerta y el tipo de salida auxiliar del dispositivo terminal auxiliar. Los tipos de salida auxiliar incluyen Ninguno, Activador de puerta abierta, Activador de alarma, Activador de puerta abierta y Alarma.
Verificar el modo por RS485	T El modo de verificación se utiliza cuando el dispositivo se utiliza como host o esclavo. El modo de verificación admitido incluye Solo Tarjeta, Tarjeta + Contraseña.
Alarma de altavoz	Transmite una alarma sonora o alarma de desmontaje desde el local. Cuando la puerta esté cerrada o la verificación sea exitosa, el sistema cancelará la alarma del local.
Restablecer configuración de acceso	Los parámetros de restablecimiento del control de acceso incluyen el retraso del bloqueo de la puerta, el retraso del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el período de tiempo disponible de la puerta, el período de tiempo normal de apertura, el dispositivo maestro y la alarma. Sin embargo, se borraron los datos de control de acceso en Data Mgt. está excluido.

11.2 Configuración de la regla de tiempo

Toque Configuración de regla de tiempo en la interfaz de Control de acceso para configurar los ajustes de tiempo.

Todo el sistema puede definir hasta 50 períodos de tiempo.

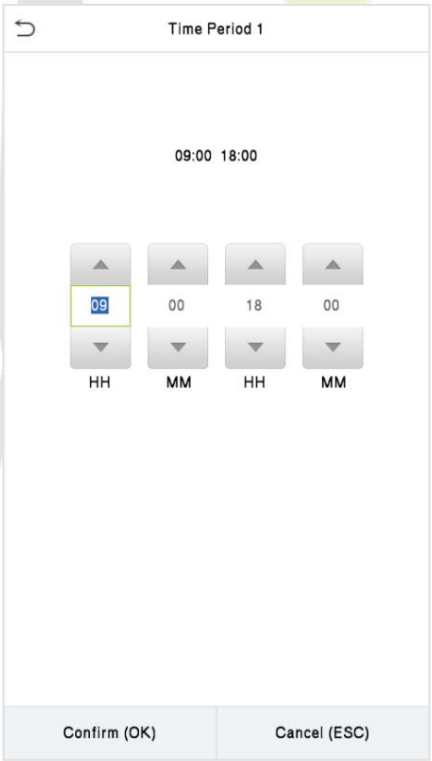
Cada período de tiempo representa 10 zonas horarias, es decir, 1 semana y 3 días festivos, y cada zona horaria es un período estándar de 24 horas por día y el usuario solo puede verificar dentro del período de tiempo válido.

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

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

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

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



Especifique la hora de inicio y finalización y luego toque Aceptar.

NOTA:

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

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

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

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

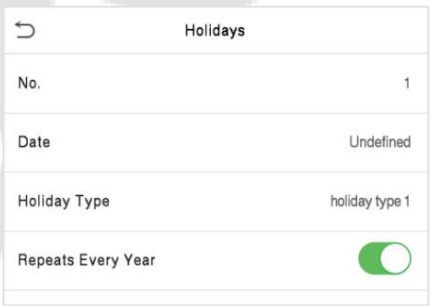
11.3 Vacaciones

Siempre que haya un día festivo, es posible que necesites 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 durante los días festivos que sea aplicable a todos los empleados, y el usuario podrá abrir la puerta durante los días festivos.

Toque Días festivos en la interfaz de Control de acceso para configurar el acceso durante los días festivos.

Agregar un nuevo día festivo

Toque Agregar vacaciones en la interfaz de vacaciones y configure los parámetros de vacaciones.



Editar un día festivo

En la interfaz de Días festivos, seleccione un elemento festivo para modificar. Toca Editar para modificar las vacaciones parámetros

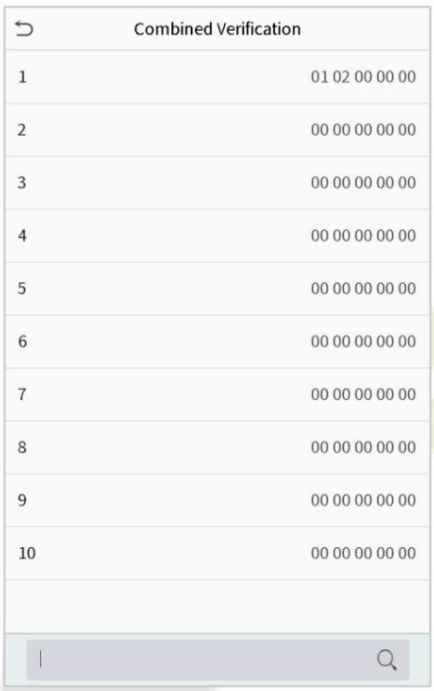
Eliminar un día festivo

En la interfaz de Días festivos, seleccione un elemento de vacaciones para eliminar y toque Eliminar. Presione Aceptar para confirmar la eliminación. Después de la eliminación, este día festivo ya no se muestra en la interfaz Todos los días festivos.

11.4 Verificación combinada

Los grupos de acceso están organizados 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 ≤ N ≤ 5, y el número de miembros N pueden pertenecer todos a un grupo de acceso o pueden pertenecer a cinco diferentes.
grupos de acceso.

Toque Verificación combinada en la interfaz de Control de acceso para configurar la configuración de verificación combinada.



En la interfaz de verificación combinada, toque la combinación de desbloqueo de puerta que desea configurar y toque las flechas hacia arriba y hacia abajo para ingresar el número de combinación y luego presione OK.

Por ejemplo:

La combinación de desbloqueo de puerta 1 está configurada 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, a saber, Grupo de control de acceso 1 (grupo AC 1), AC grupo 3, AC grupo 5, AC grupo 6 y AC grupo 8, respectivamente.

La combinación de desbloqueo de puerta 2 está configurada 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 AC, los dos siguientes son del grupo 4 de AC y la última persona es del grupo 7 de AC.

La combinación de desbloqueo de puerta 3 está configurada 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 está configurada como (03 05 08 00 00), lo que indica que la combinación de desbloqueo 4 consta de solo tres personas. La primera persona es del grupo AC 3, la segunda persona es del grupo AC 5 y la tercera persona es del grupo AC 8.

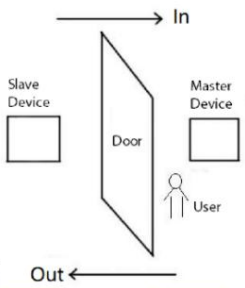
Eliminar una combinación de desbloqueo de puertas

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

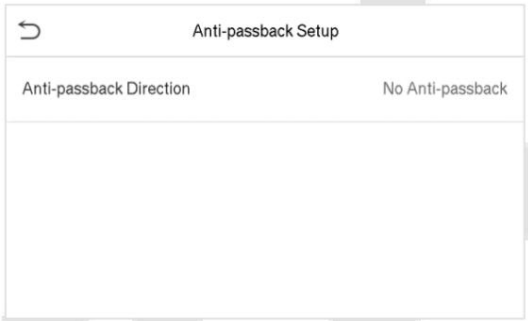
11.5 Configuración anti-passback

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

Esta función requiere que dos dispositivos funcionen juntos: uno está instalado dentro de la puerta (dispositivo maestro) y el otro está instalado fuera de la puerta (dispositivo esclavo). Los dos dispositivos se comunican mediante la señal Wiegand. El formato Wiegand y el tipo de salida (ID de usuario/Número de tarjeta) adoptado por el dispositivo maestro y
El dispositivo esclavo debe ser consistente.



Toque Configuración anti-passback en la interfaz de Control de acceso.



Función descriptiva

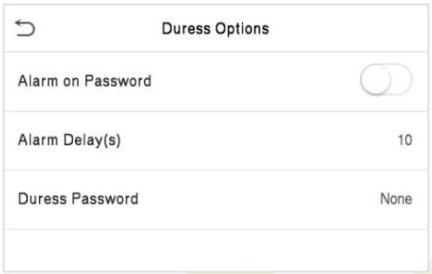
Nombre de la función	Descripción
Dirección anti-passback	Sin Anti-passback: La función Anti-passback está deshabilitada, lo que significa que la verificación exitosa a través del dispositivo maestro o esclavo puede desbloquear la puerta. El estado de asistencia no se guarda en esta opción. Anti-passback de salida: después de que un usuario realiza el check-out, solo si el último registro es un registro de check-in, el usuario puede realizar el check-out nuevamente; de lo contrario, se activará la alarma. No obstante, el usuario podrá realizar el check-in libremente. En Anti-passback: después de que un usuario se registra, solo si el último registro es un registro de salida, el usuario puede registrarse nuevamente; de lo contrario, se activará la alarma. Sin embargo, el usuario puede realizar el pago libremente.

	Anti-passback de entrada/salida: después de que un usuario realiza el registro de entrada/salida, solo si el último registro es un registro de salida, el usuario puede realizar el registro de entrada nuevamente; o si es un registro de check-in, el usuario puede volver a realizar check-out; de lo contrario, se activará la alarma.

11.6 Opciones de coacción

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

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



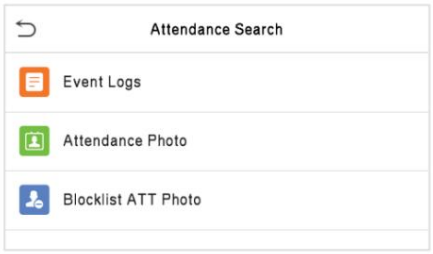
Función descriptiva

Nombre de la función	Descripción
Alarma en Contraseña	Cuando un usuario utiliza el método de verificación de contraseña, se generará una señal de alarma solo cuando la verificación de la contraseña sea exitosa; de lo contrario, no habrá señal de alarma.
Retardo(s) de alarma	La señal de alarma no se transmitirá hasta que transcurra el tiempo de retardo de la alarma. El valor oscila entre 1 y 999 segundos.
Contraseña de coacción	Establezca la contraseña de coacción de 6 dígitos. Cuando el usuario ingresa esta contraseña de coacción para verificación, se genera una señal de alarma.

12 Búsqueda de asistencia

Una vez que se verifica la identidad de un usuario, los registros de eventos se guardarán 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 para buscar el registro de acceso/asistencia requerido.

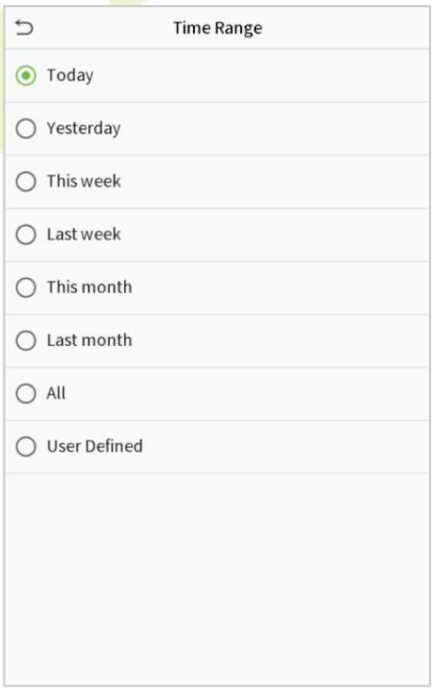


El proceso de búsqueda de fotos de asistencia y lista negra es similar al de búsqueda de registros de acceso. El siguiente es un ejemplo de búsqueda de registros de acceso.

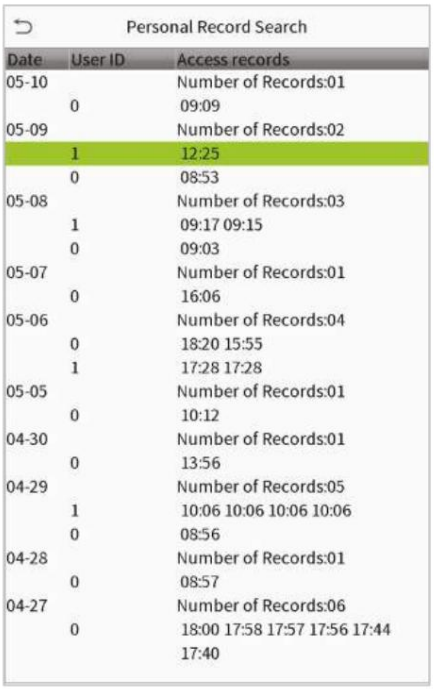
En la interfaz de búsqueda de asistencia, toque Registros de eventos para buscar el registro requerido.

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

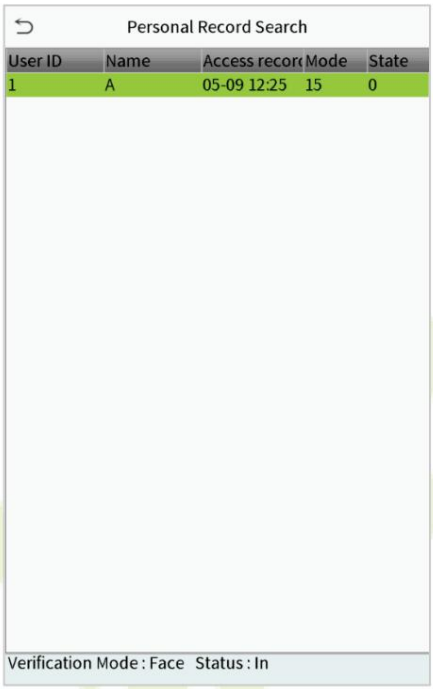
2. Seleccione el rango de tiempo en el que se deben buscar los registros.



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

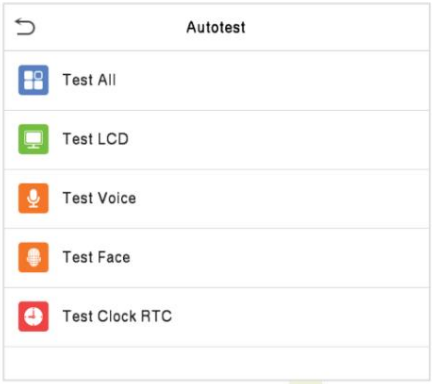


4. La siguiente figura muestra los detalles de la registro seleccionado.



13 Autoprueba

En el menú principal, toque Autoprueba para probar automáticamente si cada módulo funciona correctamente, incluida la pantalla LCD, el audio, la cámara y el reloj en tiempo real.

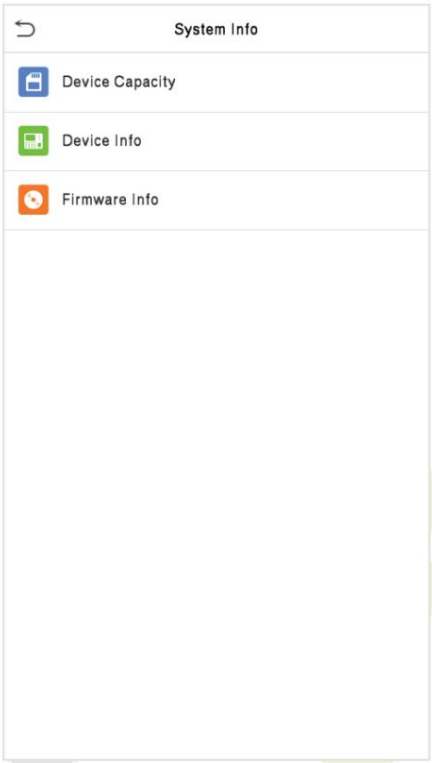


Función descriptiva

Nombre de la función	Descripción
Probar todo	Para probar automáticamente si la pantalla LCD, el audio, la cámara y el RTC son normales.
LCD de prueba	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 si la calidad de la voz es buena.
Cara de prueba	Para probar si la cámara funciona correctamente revisando las fotografías tomadas para ver si son lo suficientemente claras.
Reloj de prueba RTC	Para probar el RTC. El dispositivo comprueba con un cronómetro si el reloj funciona con normalidad y precisión. Toque la pantalla para comenzar a contar y presiónela nuevamente para dejar de contar.

14 Información del sistema

En el menú principal, toque Información del sistema para ver el estado de almacenamiento, la información de la versión del dispositivo y la información del firmware.



Función descriptiva

Nombre de la función	Descripción
Capacidad del dispositivo	Muestra el almacenamiento del usuario, la palma, la tarjeta, la contraseña y el almacenamiento facial del dispositivo actual, administradores, registros, fotos de asistencia y lista de bloqueo, y fotos de perfil.
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la dirección MAC, la información de la versión del algoritmo de la palma y la cara, información de la plataforma y el fabricante. fecha.
Información de firmware	Muestra la versión del firmware y otra información de la versión del dispositivo.

15 Conéctese al software ZKBioSecurity

15.1 Establecer la dirección de comunicación

Lado del dispositivo

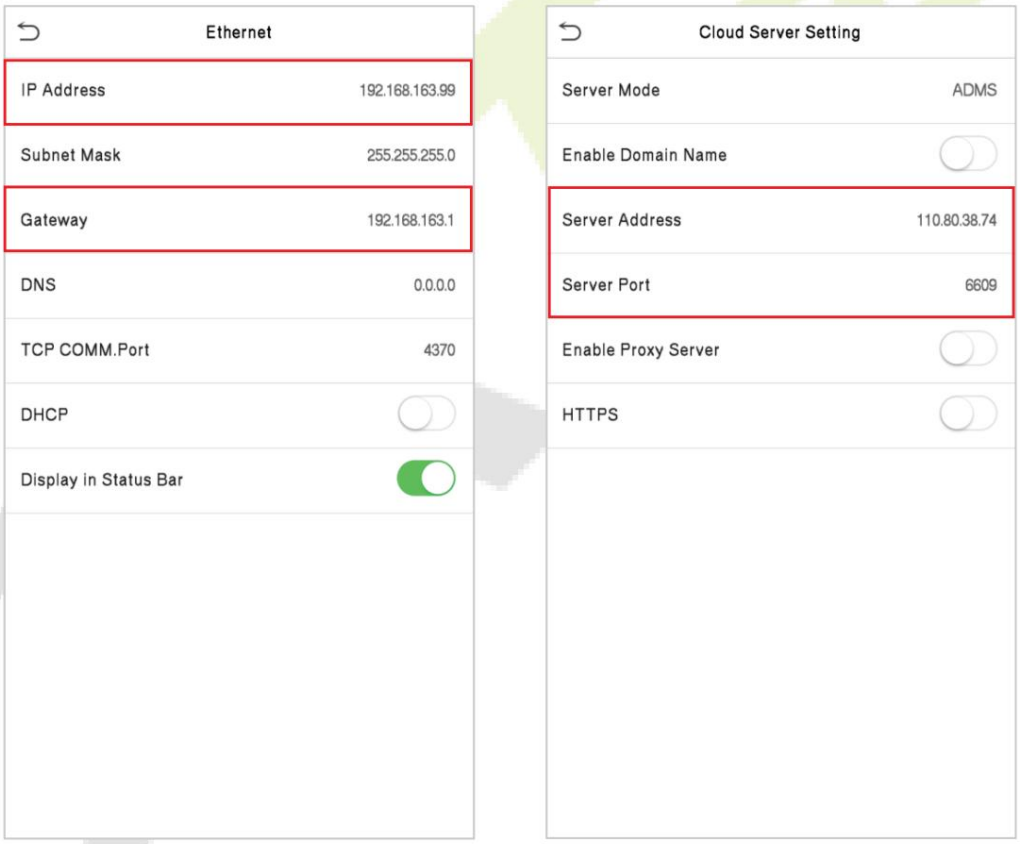
1. Toque COMUNICACIÓN. > Ethernet en el menú principal para configurar la dirección IP y la puerta de enlace del dispositivo.

   (NOTA: La dirección IP debe poder comunicarse con el servidor ZKBioSecurity, preferiblemente en el mismo segmento de red que la dirección del servidor)

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

   Dirección del servidor: Establezca la dirección IP del servidor de ZKBioSecurity.

   Puerto del servidor: configure el puerto del servidor a partir de ZKBioSecurity (el valor predeterminado es 6609).



Lado del software

Inicie sesión en el software ZKBioSecurity, haga clic en Sistema > Comunicación > Monitor de comunicación para configurar el

Puerto de servicio ADMS, como se muestra en la siguiente figura:

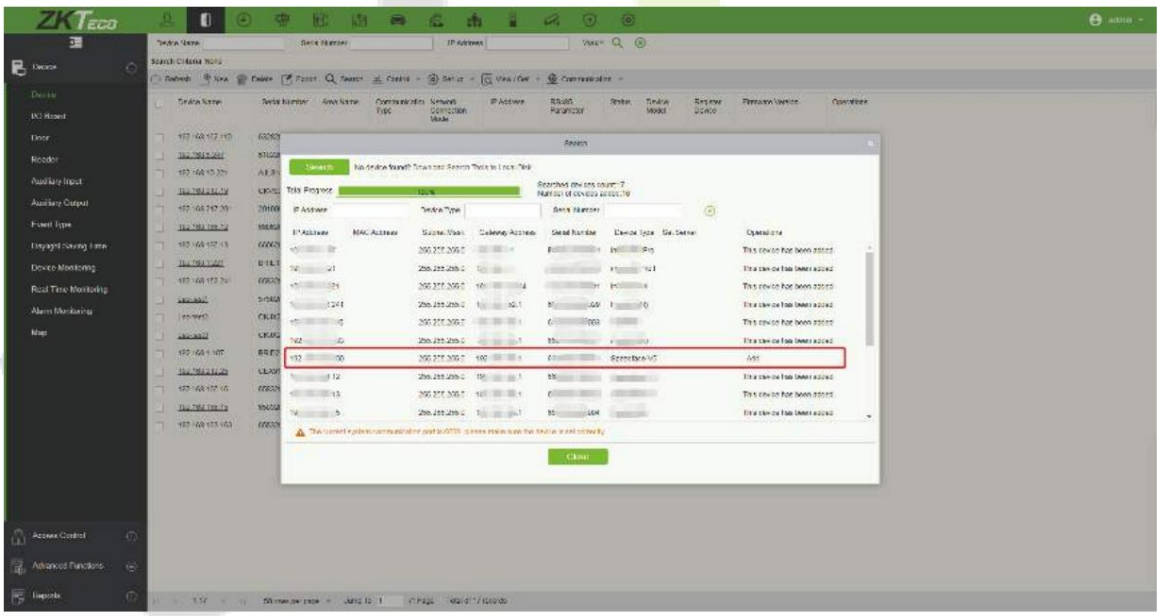
15.2 Agregar dispositivo en el software

Agregue el dispositivo buscando. El proceso es el siguiente:

1Haga clic en Acceso > Dispositivo > Buscar para abrir la interfaz de búsqueda en el software.

2Haga clic en Buscar y aparecerá el mensaje [Buscando……].

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

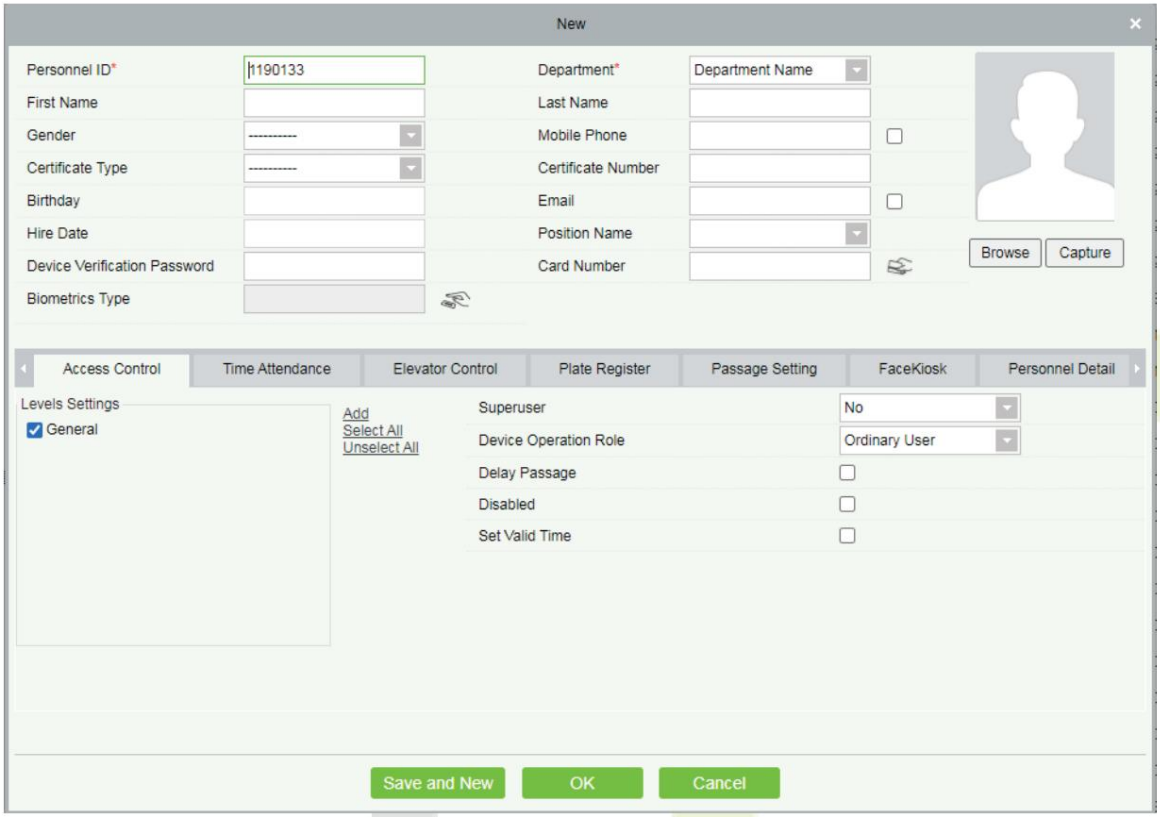


4Haga clic en [Agregar] en la columna de operación y aparecerá una nueva ventana. Seleccione Tipo de icono, Área y Agregar a

Nivele desde cada menú desplegable y haga clic en [Aceptar] para agregar el dispositivo.

15.3 Agregar personal en el software

1. Haga clic en Personal > Persona > Nuevo:



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

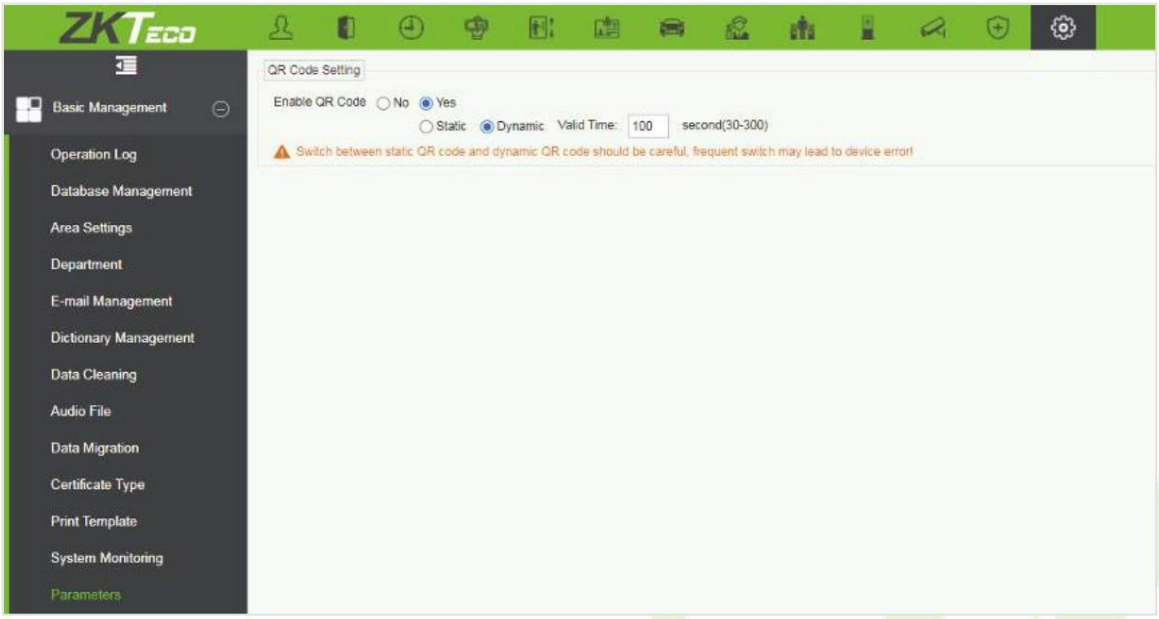
3. Haga clic en Acceso > Dispositivo > Control > Sincronizar todos los datos con los dispositivos para sincronizar todos los datos con el dispositivo, incluidos los nuevos usuarios.

15.4 Credencial móvil

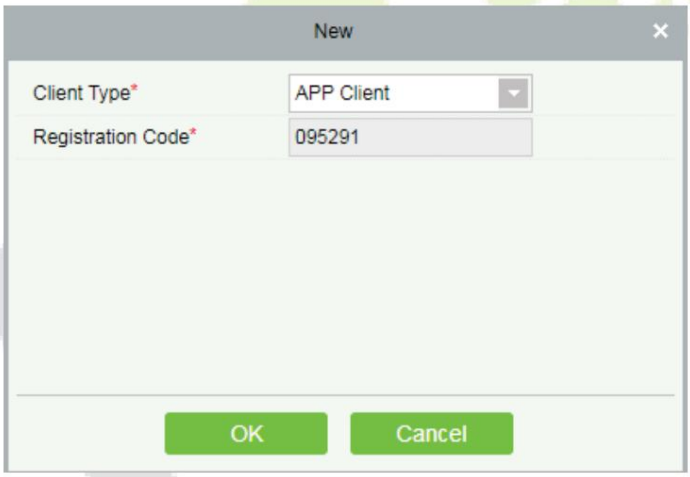
Después de descargar e instalar la aplicación, el usuario debe configurar el servidor antes de iniciar sesión. Los pasos se detallan a continuación:

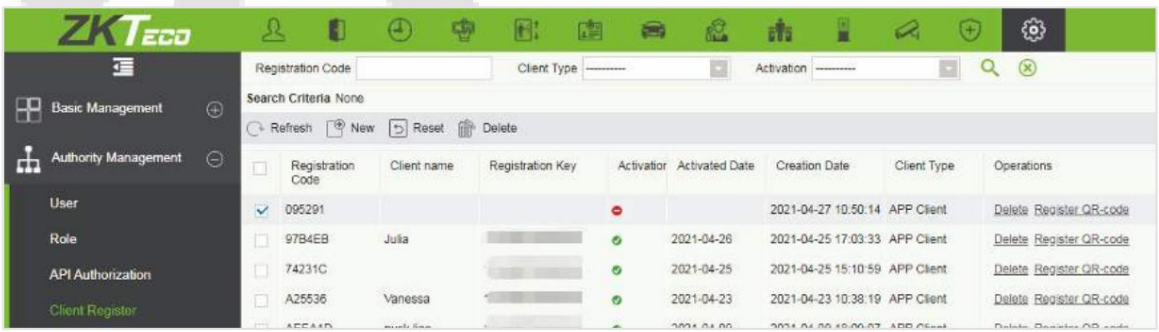
1. En [Sistema] > [Administración básica] > [Parámetros], configure Habilitar código QR en "Sí" y seleccione el estado del código QR según la situación real. El valor predeterminado es Dinámico, el tiempo válido del QR.

   Se puede configurar el código.



2. En el servidor, elija [Sistema] > [Administración de autoridades] > [Registro de cliente] para agregar un cliente de aplicación registrado.

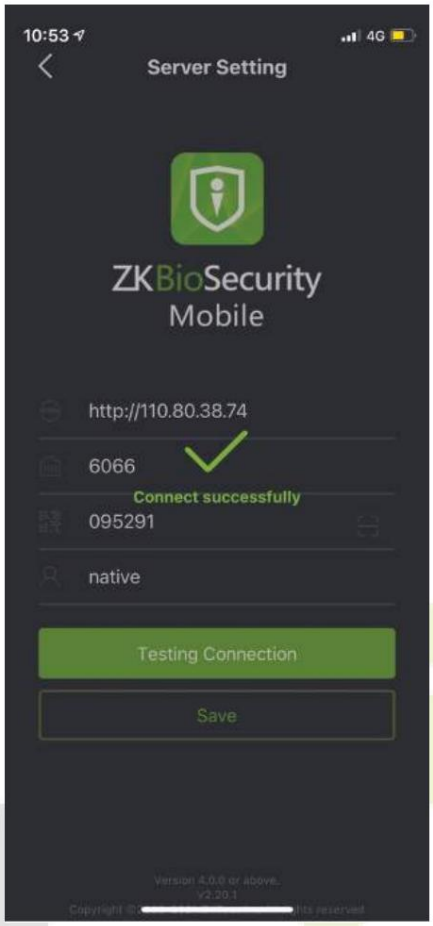




3. Abra la aplicación en el teléfono inteligente. En la pantalla de inicio de sesión, toque [Configuración del servidor] y escriba la IP Dirección o el Nombre de Dominio del Servidor, y su Número de Puerto.

4. Toque el ícono Código QR para escanear el código QR del nuevo cliente de la aplicación. Una vez identificado el cliente correctamente, configure el nombre del cliente y toque [Prueba de conexión].

5. Una vez que la red se haya conectado correctamente, toque [Guardar].

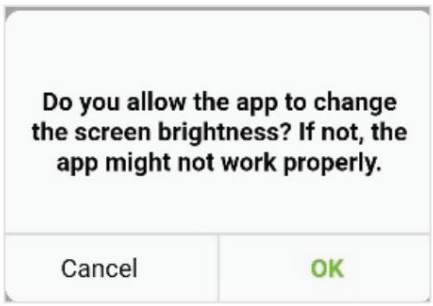


La función de credencial móvil solo es válida cuando inicia sesión como empleado; toque Empleado para cambiar a la pantalla de inicio de sesión de empleado. Ingrese el ID de empleado y la contraseña (predeterminado: 123456) para iniciar sesión.

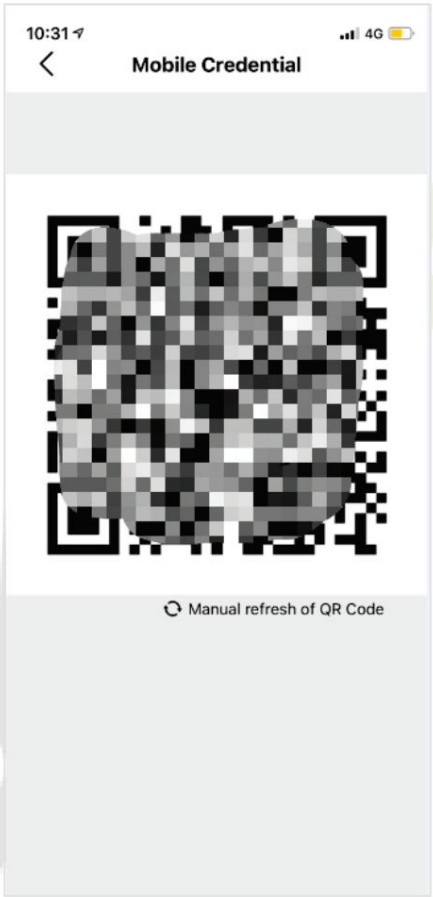
6. Toque [Credencial móvil] en la aplicación y aparecerá un código QR que incluye la identificación del empleado y Información del número de tarjeta (el código QR estático solo incluye el número de tarjeta).

El código QR puede reemplazar una tarjeta física en un dispositivo específico para lograr una autenticación sin contacto para abrir la puerta.

Al utilizar esta función por primera vez, la aplicación le pedirá que autorice la modificación de la configuración de brillo de la pantalla, como se muestra en la figura:



El código QR se actualiza automáticamente cada 30 segundos y también admite la actualización manual.



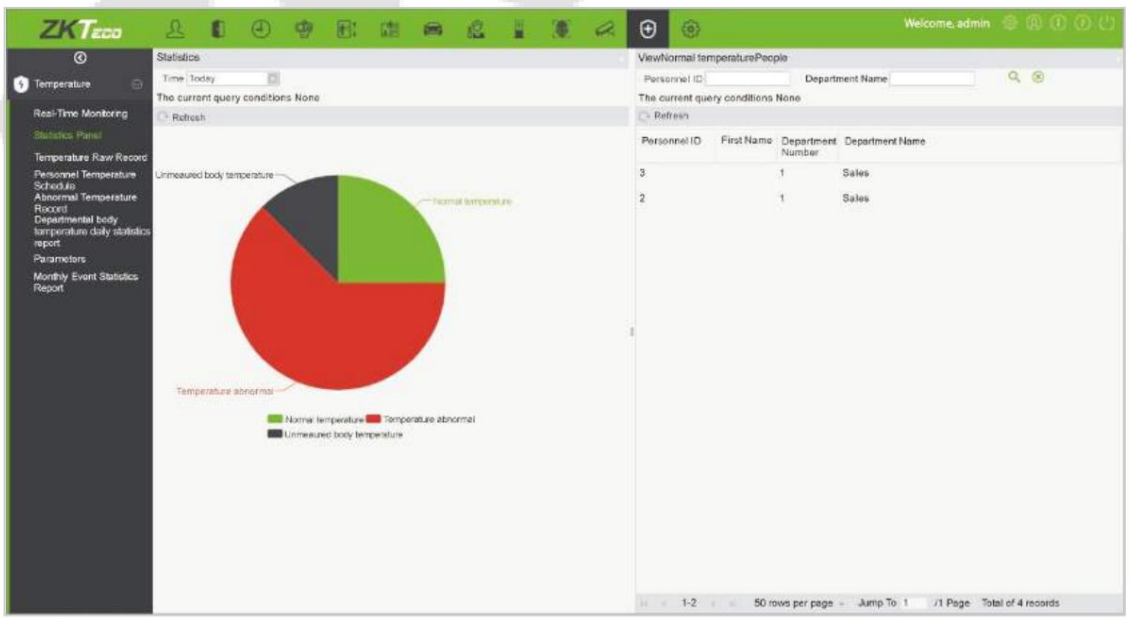
NOTA: Para otras operaciones específicas, consulte el Manual del usuario de la aplicación móvil ZKBioSecurity.

15.5 Monitoreo en tiempo real en el software ZKBioSecurity

1. Haga clic en Prevención > Epidemia > Detección de temperatura > Monitoreo en tiempo real para ver todos los eventos del personal presentes en Temperatura anormal, Sin máscaras y Registros normales.

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

2. Haga clic en Epidemia > 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, se puede ver información detallada del personal a la derecha haciendo clic en la categoría particular en el gráfico circular.



NOTA: Para otras operaciones específicas, consulte el Manual del usuario de ZKBioSecurity.

Apéndice 1

Requisitos de Colección en Vivo y Registro de Visible

Imágenes de Cara Clara

1Se recomienda realizar el registro en un ambiente interior con una iluminación adecuada.

fuente sin subexposición o sobreexposición.

2No dispare hacia fuentes de luz exteriores como puertas o ventanas u otras fuentes de luz intensas.

3) Se recomienda usar prendas de colores oscuros que sean diferentes al color de fondo.

registro.

4) Por favor, muestre su cara y frente, y no se cubra la cara ni las cejas con el cabello.

5Se recomienda mostrar una expresión facial sencilla. Sonreír es aceptable, pero no cierres tu

ojos o incline la cabeza en cualquier orientación. Se requieren dos imágenes para personas con anteojos, una imagen con anteojos y otra sin anteojos.

6No use accesorios como bufandas o máscaras que puedan cubrir su boca o barbilla.

7Mire hacia el dispositivo de captura y ubique su rostro en el área de captura de imágenes como

se muestra en la Imagen 1.

8No incluya más de una cara en el área de captura.

9Se recomienda 50 cm - 80 cm para capturar una distancia ajustable según la altura del cuerpo.

Imagen 1 Área de captura de rostro

Requisitos para datos de imágenes faciales digitales en luz visible

La fotografía digital debe tener bordes rectos, color y estar medio retratada con una sola persona, y la persona debe estar inexplorada y vestida de manera informal. Las personas que usan anteojos deben quedarse poniéndoselos para tomar fotografías.

Distancia ocular

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

Expresión facial

Se recomienda una cara neutra o una sonrisa con los ojos naturalmente abiertos.

Gesto y Ángel

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

Accesorios

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

cara

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

Formato de imagen

Debe estar en BMP, JPG o JPEG.

Requisito de datos

Deberá cumplir con los siguientes requisitos:

1Fondo blanco con vestimenta de color oscuro.

2Modo de color verdadero de 24 bits.

3) Imagen comprimida en formato JPG con un tamaño no superior a 20 kb.

4La resolución debe estar entre 358 x 441 y 1080 x 1920.

5La escala vertical de la cabeza y el cuerpo debe estar en una proporción de 2:1.

6La fotografía debe incluir los hombros de la persona capturada al mismo nivel horizontal.

7Los ojos de la persona capturada deben estar abiertos y con el iris claramente visible.

8Se prefiere una cara o sonrisa neutral, no se prefiere mostrar los dientes.

9) La persona capturada debe ser claramente visible, de color natural, sin sombras intensas, puntos de luz o reflejos en la cara o el fondo. El nivel de contraste y luminosidad debe ser el adecuado.

Apéndice 2

política de privacidad

Aviso:

Para ayudarlo a utilizar mejor los productos y servicios de ZKTeco (en adelante, "nosotros", "nuestro" o "nos"), un proveedor de servicios inteligentes, recopilamos constantemente su información personal. Dado que entendemos la importancia de su información personal, tomamos su privacidad con sinceridad y hemos formulado esta política de privacidad para proteger su información personal. Hemos enumerado las políticas de privacidad a continuación para comprender con precisión las medidas de protección de datos y privacidad relacionadas con nuestros productos y servicios inteligentes

Antes de utilizar nuestros productos y servicios, lea atentamente y comprenda todas las reglas y disposiciones de esta Política de Privacidad. Si no está de acuerdo con el acuerdo correspondiente o cualquiera de sus términos, debe dejar de utilizar nuestros productos y servicios.

I. Información recopilada

Para garantizar el funcionamiento normal del producto y ayudar a mejorar el servicio, recopilaremos la información proporcionada voluntariamente por usted o proporcionada según su autorización durante el registro y el uso o generada como resultado de su uso de los servicios.

1. Información de registro de usuario: en su primer registro, la plantilla de función (plantilla de huella digital/plantilla de rostro/plantilla de palma) se guardará en el dispositivo de acuerdo con el tipo de dispositivo que haya seleccionado para verificar la similitud única entre usted y la identificación de usuario que se han registrado. Opcionalmente puede ingresar su Nombre y Código. La información anterior es necesaria para que pueda utilizar nuestros productos. Si no proporciona dicha información, no podrá utilizar algunas funciones del producto con regularidad.

2. Información del producto: De acuerdo con el modelo del producto y el permiso otorgado al instalar y utilizar nuestros servicios, la información relacionada del producto en el que se utilizan nuestros servicios se recopilará cuando el producto esté conectado al software, incluido el modelo del producto. , Número de versión del firmware, Número de serie del producto e Información sobre la capacidad del producto.
Cuando conecte su producto al software, lea atentamente la política de privacidad del software específico.

II. Seguridad y gestión del producto

1. Cuando utilice nuestros productos por primera vez, deberá configurar el privilegio de Administrador antes de realizar operaciones específicas. De lo contrario, se le recordará con frecuencia que establezca el privilegio de Administrador cuando ingrese a la interfaz del menú principal. Si todavía no configuras el

Privilegio de administrador después de recibir el aviso del sistema, debe tener en cuenta el posible riesgo de seguridad (por ejemplo, los datos pueden modificarse manualmente).

2. Todas las funciones de visualización de información biométrica están deshabilitadas en nuestros productos de forma predeterminada. Puede elegir Menú > Configuración del sistema para configurar si desea mostrar la información biométrica. Si habilita estas funciones, asumimos que conoce los riesgos de seguridad de la privacidad personal especificados en la política de privacidad.

3. De forma predeterminada, solo se muestra su ID de usuario. Puede configurar si desea mostrar otra información de verificación del usuario (como nombre, departamento, foto, etc.) bajo el privilegio de administrador. Si elige mostrar dicha información, asumimos que conoce los posibles riesgos de seguridad (por ejemplo, su foto se mostrará en la interfaz del dispositivo).

4. La función de la cámara está desactivada en nuestros productos de forma predeterminada. Si desea habilitar esta función para tomar fotografías de usted mismo para registrar la asistencia o tomar fotografías de extraños para el control de acceso, el producto habilitará el tono de aviso de la cámara. Una vez que habilite esta función, asumimos que conoce los posibles riesgos de seguridad.

5. Todos los datos recopilados por nuestros productos se cifran mediante el algoritmo AES 256. Todos los datos cargados por el Administrador a nuestros productos se cifran automáticamente utilizando el algoritmo AES 256 y se almacenan de forma segura. Si el Administrador descarga datos de nuestros productos, asumimos que necesita procesar los datos y que conoce el riesgo potencial de seguridad. En tal caso, usted asumirá la responsabilidad del almacenamiento de los datos. Deberá saber que algunos datos no se pueden descargar por razones de seguridad.

6. Toda la información personal de nuestros productos puede ser consultada, modificada o eliminada. si no
Si ya no utiliza nuestros productos, borre sus datos personales.

III. Otros

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

Operación ecológica

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

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

Sustancias peligrosas o tóxicas y sus cantidades.

Componente Nombre	Sustancia/elemento peligroso/tóxico					
	Dirigir (Pb)	Mercurio (Hg)	Cadmio (Cd)	hexavalente Cromo (Cr6+)	polibromado Bifenilos (NACIONES UNIDAS)	polibromado Éteres de difenilo (PBDE)
Resistencia de chip	×	•	•	•	•	•
Condensador de chip	×	•	•	•	•	•
Inductor de chip	×	•	•	•	•	•
Diodo	×	•	•	•	•	•
ESD componente	×	•	•	•	•	•
Zumbador	×	•	•	•	•	•
Adaptador	×	•	•	•	•	•
Tornillos	•	•	•	×	•	•

• 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 están fabricados 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. 32, Vía Industrial,

Ciudad de Tangxia, Dongguan, China.

Teléfono: +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com