

Manual de usuario

Terminal de luz visible de 4 pulgadas

Fecha: julio de 2020

Versión Doc: 1.0

inglés

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



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

www.zkteco.com .

Copyright © 2020 ZKTECO CO., LTD. Reservados todos los derechos.

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

Marca comercial

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

Descargo de responsabilidad

Este manual contiene información sobre el funcionamiento y mantenimiento del equipo ZKTeco. Los derechos de autor de todos los documentos, dibujos, etc. en relación con el equipo suministrado por ZKTeco son propiedad de ZKTeco y son propiedad de ZKTeco. El contenido de este documento 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 el mantenimiento del equipo suministrado. Si alguno de los contenidos del manual parece poco claro o incompleto, comuníquese con ZKTeco antes de iniciar la operación y el mantenimiento de dicho equipo.

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

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

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

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

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

en relación 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 contenida en este documento, que se incorporará en nuevas adiciones / enmiendas al manual. ZKTeco se reserva el derecho de agregar, eliminar, enmendar o modificar la información contenida en el manual de vez en cuando en forma de circulares, cartas, notas, etc. para un mejor funcionamiento y seguridad de la máquina / unidad / equipo. Dichas adiciones o enmiendas están destinadas a mejorar / mejorar el funcionamiento de la máquina / unidad / equipo y tales enmiendas no darán ningún derecho a reclamar compensación o daños bajo ninguna circunstancia.

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

El producto se actualizará 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, comuníquese con nosotros.

Sede de ZKTeco

Dirección Parque Industrial ZKTeco, No. 26, 188 Industrial Road, Tangxia
Town, Dongguan, China.

Teléfono + 86 769 - 82109991

Fax + 86 755 - 89602394

Para consultas relacionadas con el negocio, escribanos a: sales@zkteco.com . Para saber más

sobre nuestras sucursales globales, visite www.zkteco.com .

Sobre la empresa

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

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

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

Acerca del manual

Este manual presenta las operaciones del producto terminal de luz visible de 4 pulgadas.

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

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

Convenciones de documentos

Las convenciones utilizadas en este manual se enumeran a continuación:

Convenciones de la GUI

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

Simbolos






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

Tabla de contenido

1	MEDIDAS DE SEGURIDAD.....	7
2	INSTRUCCIONES DE USO	8
2.1	S TANDING PAG OSICIÓN, PAG OSTURA Y F ACIAL mí XPRESIÓN	8 P ALM R EGISTRACIÓN
2.2	9 F AS R EGISTRACIÓN
2.3	9 S TANDBY I NTERFACE
2.4	10 V IRTUAL K EYBOARD
2.5	13 V ERIFICACIÓN METRO EDO
2.6		
2.6.1	VERIFICACIÓN DE LA PALMA	14
2.6.2	VERIFICACIÓN FACIAL	dieciséis
2.6.3	VERIFICACIÓN DE TARJETA	18
2.6.4	VERIFICACIÓN DE CONTRASEÑA	20
2.6.5	VERIFICACIÓN COMBINADA	22
3	MENÚ PRINCIPAL	24
4	GESTIÓN DE USUARIOS.....	25
4.1	U SER R EGISTRACIÓN	25
4.1.1	ID DE USUARIO Y NOMBRE	25
4.1.2	ROL DEL USUARIO	26
4.1.3	PALMA	26
4.1.4	ROSTRO.....	27
4.1.5	TARJETA.....	28
4.1.6	CONTRASEÑA.....	29
4.1.7	FOTO DE USUARIO	29
4.1.8	PAPEL DE CONTROL DE ACCESO	30
4.2	S BUSCAR U SERS	31
4.3	E DIT U SER	31
4.4	D ELETE U SER	32
5	ROL DEL USUARIO	33
6	AJUSTES DE COMUNICACIÓN	35
6.1	norte ETWORK S AJUSTES	35 S ERIAL C OMM
6.2	37 P CC CONEXIÓN
6.3	37 W IRELESS norte ETWORK
6.4	38 C FUERTE S ERVER S ETTING
6.5	40 W IEGAND S ETUP
6.6	41
6.6.1	ENTRADA WIEGAND	41
6.6.2	SALIDA WIEGAND	43
6.7	N ETWORK D IAGNOSIS	44
7	AJUSTES DEL SISTEMA.....	45
7.1	D COMIDO Y T YO ME	45

7.2	ACCESS LOGS SETTING	46	FAS PAG ARAMETROS
7.3	48	P ALM PAG ARAMETROS
7.4	50	F ACTORIA R ESET
7.5	51	USBU PGRADA
7.6	51	D EVICE T YPE S ETTING
7.7		
8	PERSONALIZAR AJUSTES	53	
8.1	INTERFACE S AJUSTES	53	V OICE S AJUSTES
8.2	54	B ANA S CÓDULOS
8.3	54	P UNCH S TATES O PCIONES
8.4	56	S HORTCUT K EY METRO APLICACIONES
8.5	57	
9	GESTIÓN DE DATOS	59	
9.1	D ELETE D ATA	59	
10	CONTROL DE ACCESO.....	61	
10,1	ACCESS CONTROL O PCIONES	62	
10,2	toneladas YO ME R ULE S ETTING	63	
10,3	H VIERNES		sesenta y cinco
10,4	COMBINADO VERIFICACIÓN	66	
10,5	ANTI-PASSBACK S ETUP	68	
10,6	D URESS O PCIONES	69	
11	ADMINISTRADOR USB	70	
11.1	USBD CARGA PROPIA	70	
11.2	USBU CARGA	71	
12	BÚSQUEDA DE ASISTENCIA	72	
13	AUTO PRUEBA	74	
14	INFORMACIÓN DEL SISTEMA.....	75	
15	CONECTARSE AL SOFTWARE ZKBIOACCESS IVS	76	
15,1	SET EL C OMMUNICACIÓN A DIRECCIÓN	76	
15,2	ADD D EVICE EN EL S OFTWARE	77	
15,3	ADD PAG ERSONNEL EN EL S OFTWARE	78	
APÉNDICE 1		79	
	R EQUIPOS DE L HE C OLLECTION Y R EGISTRACIÓN DE V ISIBLE L IGH T F AS I MAGES	79	R EQUIPOS PARA V ISIBLE L IGH T D IGH T AL
	F AS I Mago D ATA	80	
APÉNDICE 2		81	
	S TATUAJE SOBRE EL R IGH T O PAG RIVACY	81	E CO-AMIGABLE O PERACIÓN
	82	

1 Medidas de seguridad

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

1. **Lea, siga y conserve las instrucciones:** Todas las instrucciones de seguridad y funcionamiento deben estar correctamente leer y seguir antes de poner en servicio el dispositivo.
 2. **No ignore las advertencias:** Respete todas las advertencias de la unidad y las instrucciones de funcionamiento.
 3. **Accesorios** - Utilice solo accesorios recomendados por el fabricante o vendidos por el producto. No se deben utilizar accesorios no recomendados por el fabricante.
 4. **Precauciones para la instalación** - No coloque este dispositivo sobre un soporte o marco inestable. Puede caerse y causar lesiones graves a las personas y daños al dispositivo.
 5. **Servicio** - No intente reparar esta unidad usted mismo. Abrir o quitar las cubiertas puede exponerlo a voltajes peligrosos u otros peligros.
 6. **Daños que requieren servicio** - Desconecte el sistema de la fuente de alimentación principal de CA o CC y consulte al personal de servicio en las siguientes condiciones:
 - Cuando se ve afectado el control del cable o de la conexión.
 - Cuando se derramó el líquido o se cayó un elemento en el sistema.
 - Si se expone al agua y / o inclemencias del tiempo (lluvia, nieve y más). Si el sistema no funciona normalmente según las instrucciones de funcionamiento.
- Simplemente cambie los controles definidos en las instrucciones de funcionamiento. El ajuste inadecuado de otros controles puede resultar en daños e involucrar a un técnico calificado para devolver el dispositivo a la operación normal.
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, descargas eléctricas u otros peligros.
 8. **Verificación de seguridad** - Una vez finalizado el trabajo de servicio o reparación en la unidad, solicite al técnico de servicio que realice comprobaciones de seguridad para garantizar el funcionamiento correcto de la unidad.
 9. **Fuentes de energía** - Utilice el sistema solo desde la fuente de alimentación de la etiqueta. Si no está claro el tipo de fuente de alimentación que debe utilizar, llame a su distribuidor.
 10. **Relámpago** - Se pueden instalar pararrayos externos para proteger contra tormentas eléctricas. Evita que los power-ups destruyan el sistema.

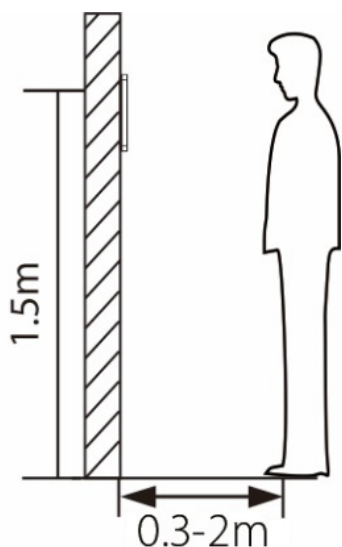
Los dispositivos deben instalarse en áreas con acceso limitado.

2 Instrucciones de uso

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

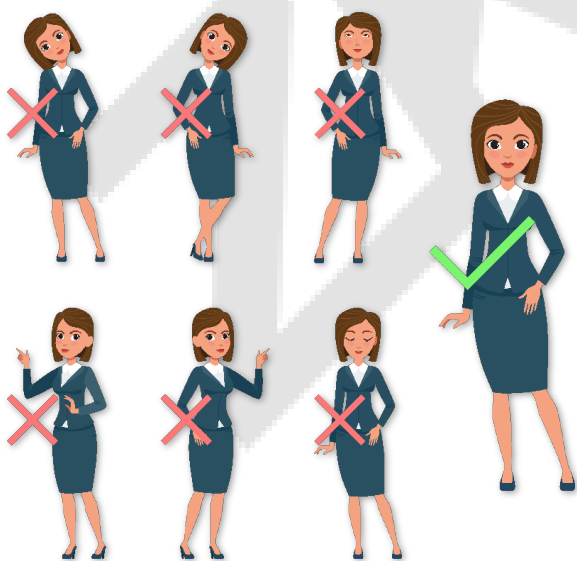
2.1 Posición de pie, postura y expresión facial

- La distancia recomendada



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

- Postura de bipedestación y expresión facial recomendadas



Postura de pie

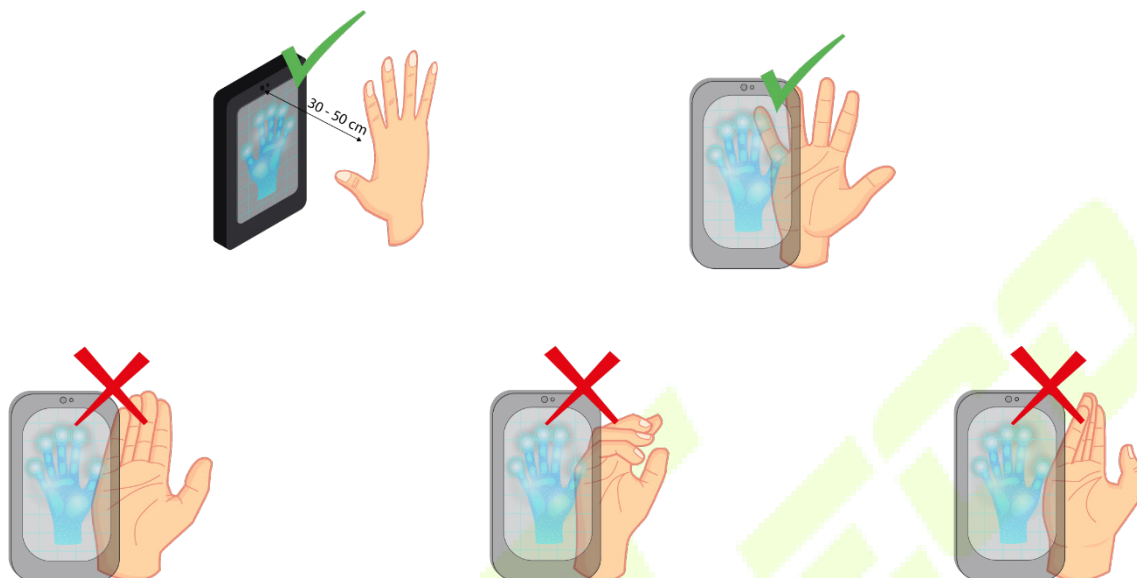


Expresión facial

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

2.2 PalmRegistration

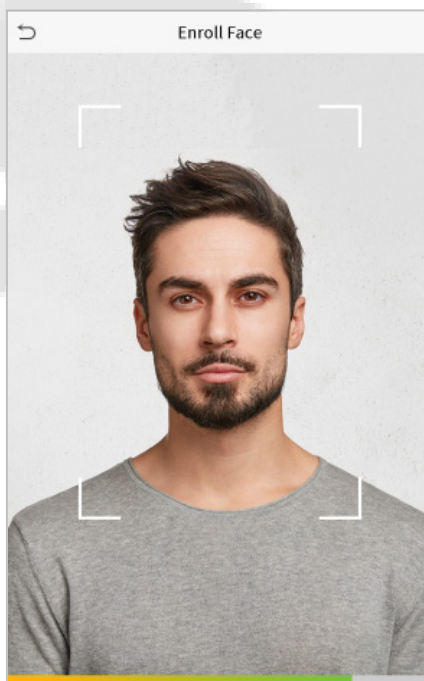
Coloque la palma de la mano en el área de recolección multimodo de la palma de la mano, de modo que la palma quede paralela al dispositivo. Asegúrese de dejar espacio entre los dedos.



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

2.3 Registro facial

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

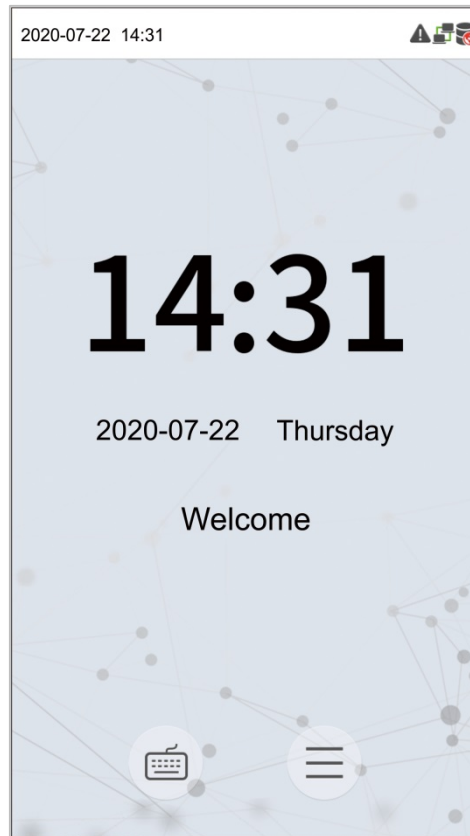




Método correcto de autenticación y registro facial

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

2.4 Interfaz de espera

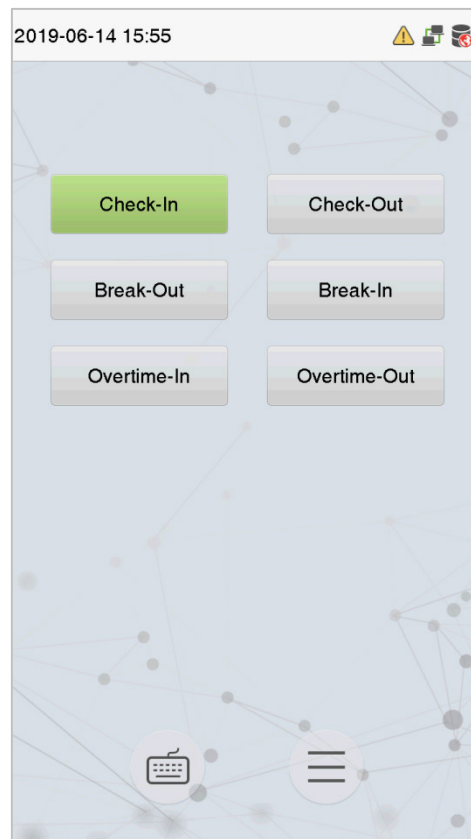
Después de conectar la fuente de alimentación, se muestra la siguiente interfaz de espera:



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

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

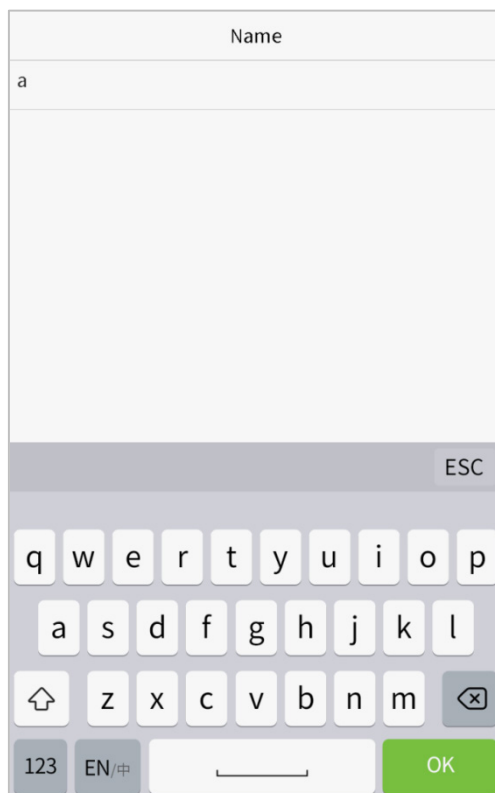
- ★ Las opciones de estado de perforación también se pueden mostrar y utilizar directamente en la interfaz de espera. Hacer clic en cualquier lugar de la pantalla, aparte de los iconos, y aparecen seis teclas de acceso directo en la pantalla, como se muestra en la siguiente figura:



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

NOTA : Las opciones de estado de perforación están desactivadas de forma predeterminada y deben cambiarse a otra opción en el ["8.4 Opciones de los estados de perforación"](#) para obtener las opciones de estado de perforación en la pantalla de espera.

2.5 Teclado virtual



NOTA :

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

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

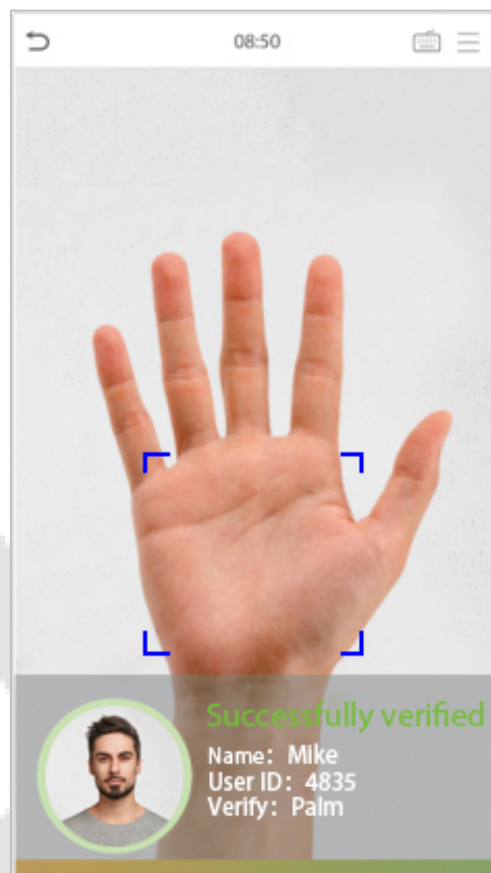
2.6 Modo de verificación

2.6.1 PalmVerification


- **1: N Palm Verificationmode**

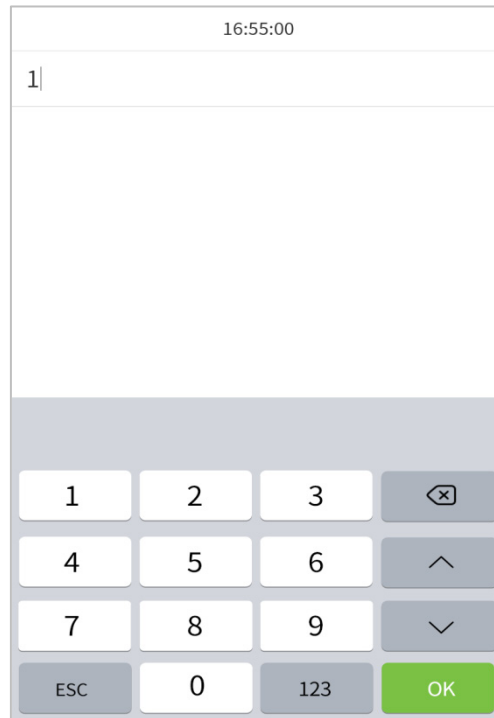
En este modo de verificación, el dispositivo compara la imagen de la palma recopilada por el colector de palma con todos los datos de la palma en el dispositivo.


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



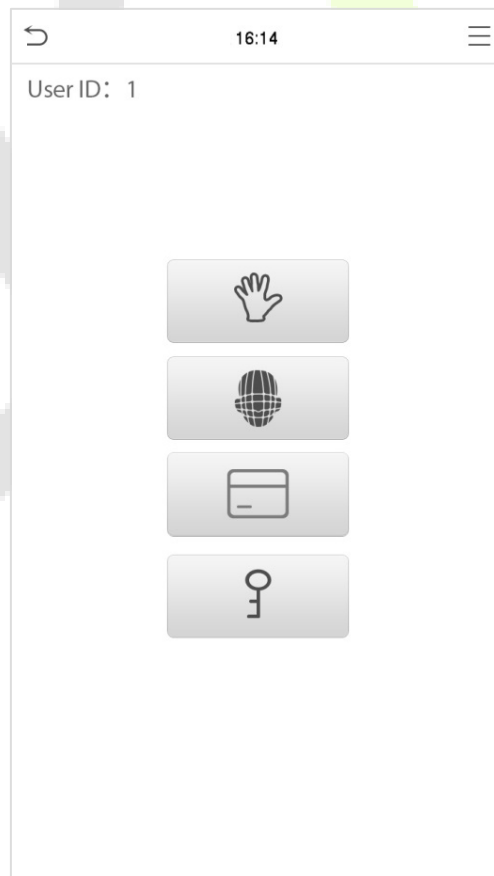
- **Modo de verificación de palma 1: 1**

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



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

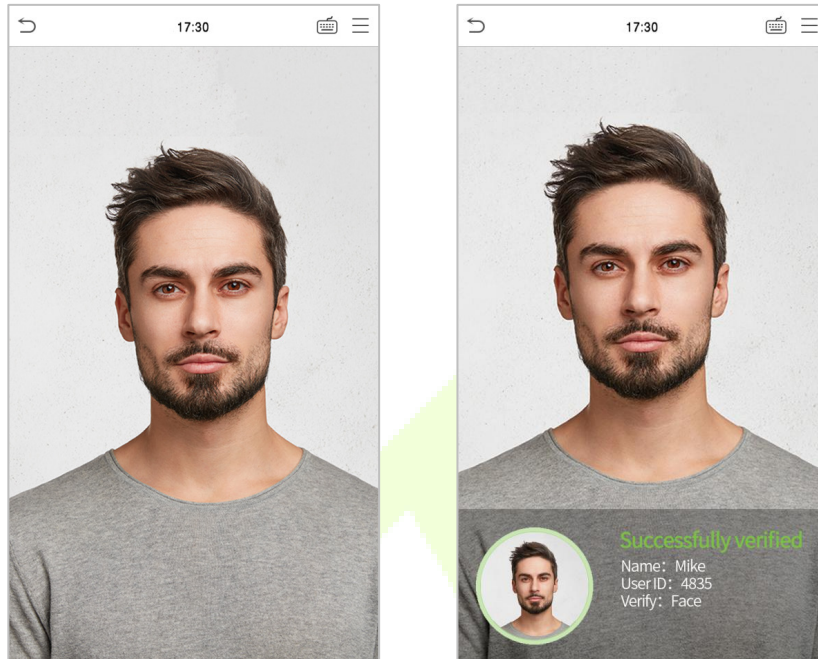
Ingrese al modo de verificación de la palma. Luego coloque su palma para verificación.




2.6.2 Verificación facial

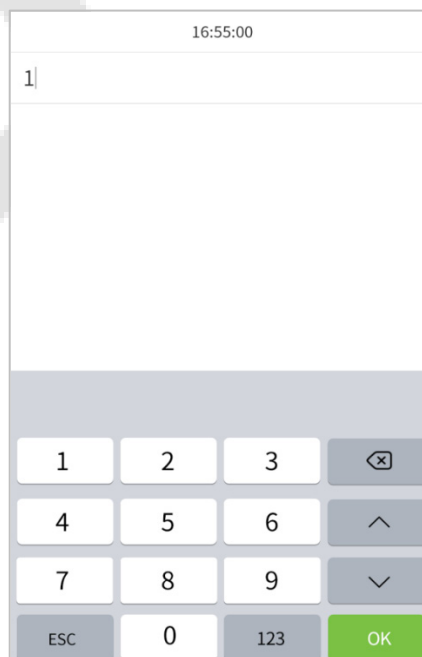
• Verificación facial 1: N


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

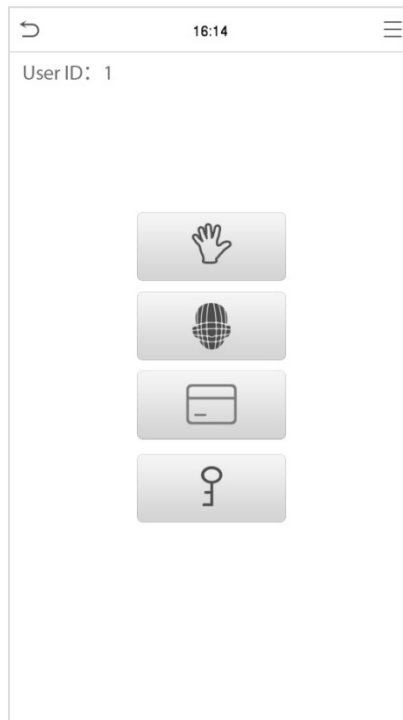


• Verificación facial 1: 1

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



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



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

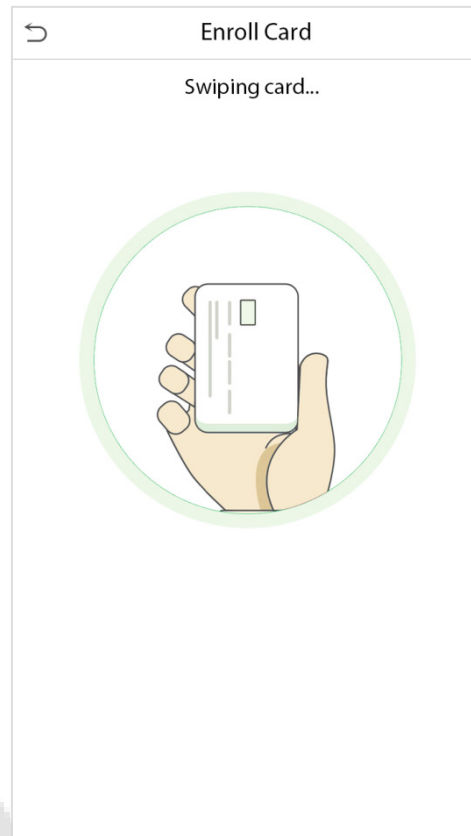


Si falla la verificación, aparecerá el mensaje "¡Por favor, ajuste su posición!".

2.6.3 Verificación de tarjeta

- **Verificación de tarjeta 1: N**


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



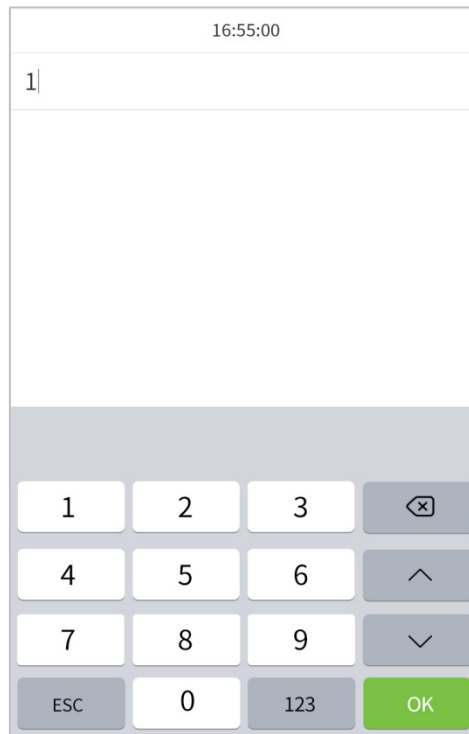
- **Verificación de tarjeta 1: 1**


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

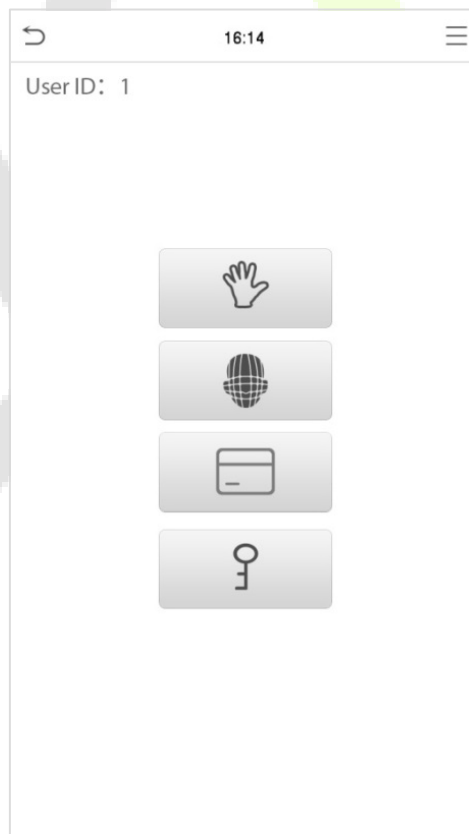


Prensa  en la interfaz principal para abrir el modo de verificación de tarjeta 1: 1.

Ingrese el ID de usuario y haga clic en [**OK**].




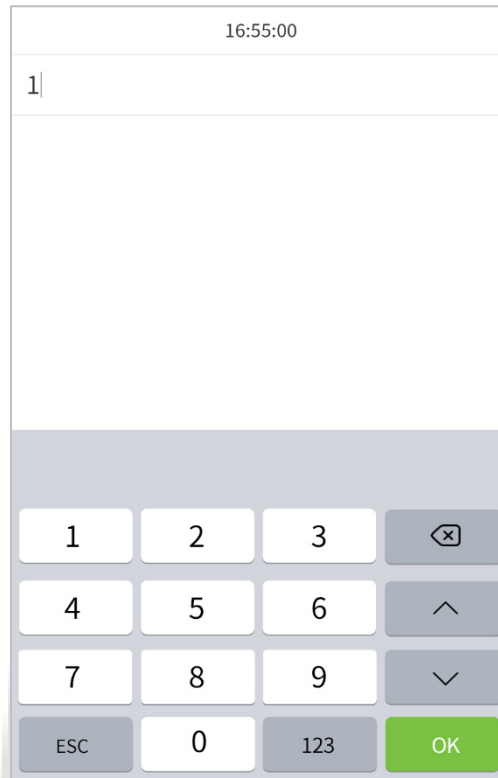
Si el usuario ha registrado la palma, el rostro y la contraseña además de su tarjeta, y el método de verificación está configurado como verificación de palma / rostro / tarjeta / contraseña, aparecerá la siguiente pantalla. Selecciona el  icono para entrar en el modo de verificación de la tarjeta.




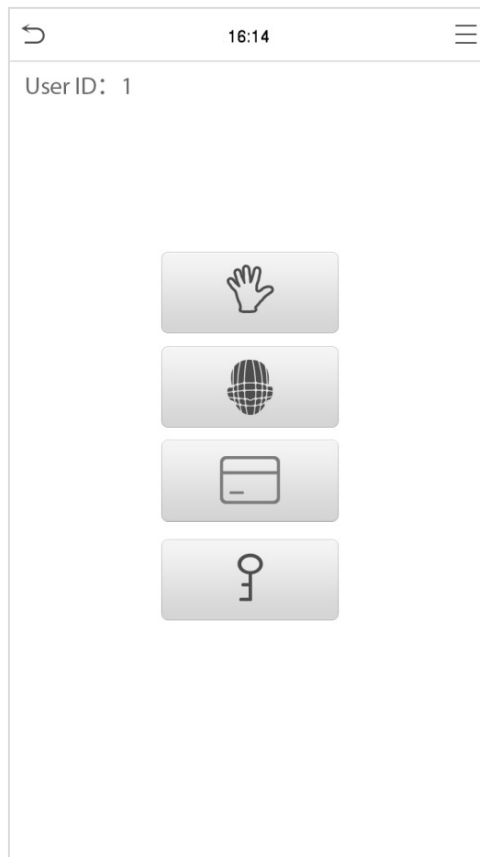
2.6.4 Verificación de contraseña

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

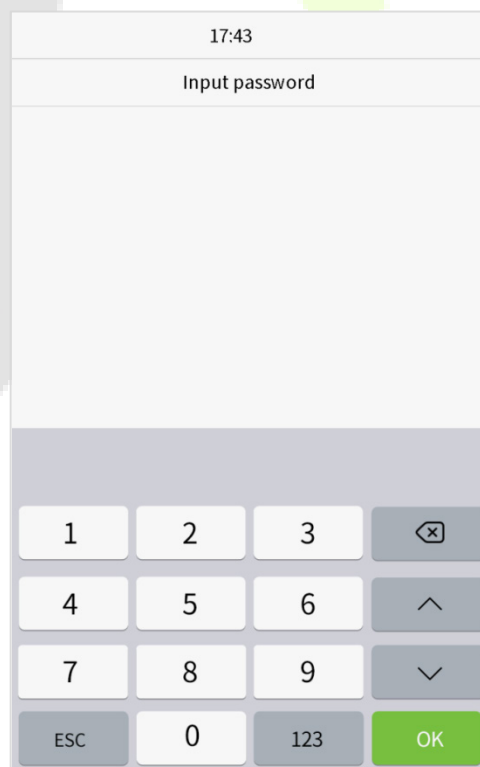
Haga clic en el  en la pantalla principal para ingresar al modo de verificación de contraseña 1: 1. Luego, ingrese el usuario ID y presione [**OK**].



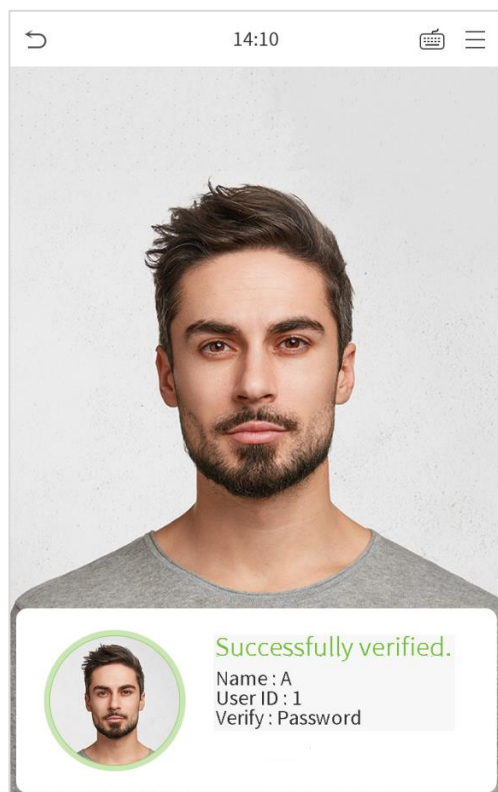
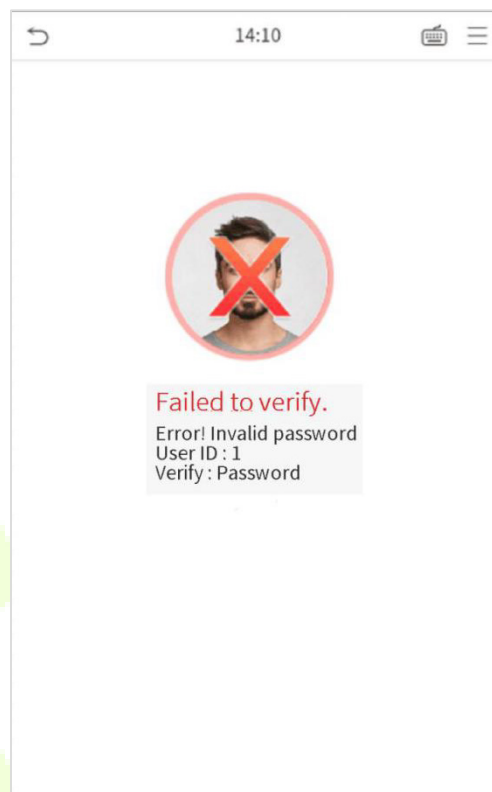
Si el usuario ha registrado la palma, el rostro y la tarjeta además de la contraseña, y el método de verificación está configurado como verificación de palma / rostro / tarjeta / contraseña, aparecerá la siguiente pantalla. Selecciona el  icono para entrar modo de verificación de contraseña.



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:**Error de verificación:****2.6.5 Verificación combinada**

Para aumentar la seguridad, este dispositivo ofrece la opción de utilizar múltiples formas de métodos de verificación. Se pueden utilizar un total de 12 combinaciones de verificación diferentes, como se muestra a continuación:

Definición de símbolo de verificación combinada

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


←	Verification Mode	↕
<input checked="" type="radio"/>	Password/Card/Face/Palm	
<input type="radio"/>	User ID only	
<input type="radio"/>	Password	
<input type="radio"/>	Card only	
<input type="radio"/>	Password+Card	
<input type="radio"/>	Password/Card	
<input type="radio"/>	Face only	
<input type="radio"/>	Face+Password	
<input type="radio"/>	Face+Card	
<input type="radio"/>	Palm	

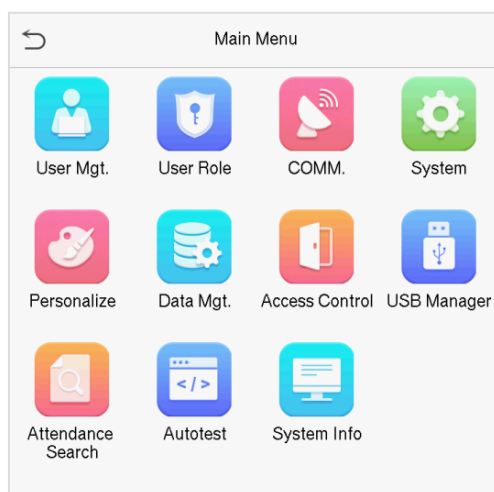
←	Verification Mode	↕
<input checked="" type="radio"/>	Password	
<input type="radio"/>	Card only	
<input type="radio"/>	Password+Card	
<input type="radio"/>	Password/Card	
<input type="radio"/>	Face only	
<input type="radio"/>	Face+Password	
<input type="radio"/>	Face+Card	
<input type="radio"/>	Palm	
<input type="radio"/>	Palm+Card	
<input type="radio"/>	Palm+Face	

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, 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 escaneado de la persona con la plantilla de verificación registrada (tanto el Rostro como la Contraseña) almacenada previamente con esa ID de personal en el Dispositivo.
- Pero como el empleado ha registrado solo el rostro pero no la contraseña, la verificación no se completará y el dispositivo muestra "Verificación fallida".

3 Menú principal

Prensa  en la interfaz de espera para ingresar al **Menú principal**, Se mostrará la siguiente pantalla:




Función descriptiva

Menú	Descripciones
Administrador de usuarios	Agregar, editar, ver y eliminar información básica de un usuario.
Rol del usuario	Para establecer el alcance del permiso del rol personalizado y el registrador para los usuarios, es decir, los derechos para operar el sistema.
COMM.	Para configurar los parámetros relevantes de Red, Comunicaciones Serie, Conexión de PC, Red Inalámbrica, Servidor en la Nube, Wiegand y Diagnóstico de Red.
Sistema	Para configurar los parámetros relacionados con el sistema, incluyendo Fecha y hora, Configuración de registros de acceso, Palm, Parámetros faciales, Restablecimiento de fábrica, Actualización de USB y Configuración de tipo de dispositivo.
Personalizar	Esto incluye la interfaz de usuario, voz, horarios de timbre, opciones de estado de perforación y configuraciones de asignaciones de teclas de acceso directo.
DataMgt.	Para eliminar todos los datos relevantes en el dispositivo.
Control de acceso	Para configurar los parámetros de la cerradura y el dispositivo de control de acceso relevante, incluidas opciones como Regla de tiempo, Configuración de vacaciones, Verificación combinada, Configuración de anti-retorno y Configuración de opciones de coacción.
USBManager	Touploador descargar los datos específicos mediante aUSBdrive.
Asistencia Buscar	Para consultar los registros de eventos especificados, verifique las fotos de asistencia y las fotos de asistencia de la lista de bloqueo.
Auto prueba	Para probar automáticamente si cada módulo funciona correctamente, incluida la pantalla LCD, el audio, el micrófono, la cámara y el reloj en tiempo real.
Información del sistema	Para ver la capacidad de datos y la información del dispositivo y firmware del dispositivo actual.

4 Gestión de usuarios

4.1 registro de usuario

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

User Mgt.	
	New User
	All Users
	Display Style

4.1.1 ID de usuario y nombre

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

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

Notas:

- 1) Un nombre puede tener hasta 17 caracteres.
- 2) El ID de usuario puede contener de 1 a 9 dígitos de forma predeterminada.
- 3) Durante el registro inicial, puede modificar su ID, que no se puede modificar después del registro.
- 4) Si un mensaje " **¡Duplicado!** " aparece, debe elegir otro ID, ya que el ID de usuario ingresado ya existe.

4.1.2 Rol del usuario

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

Administración.

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

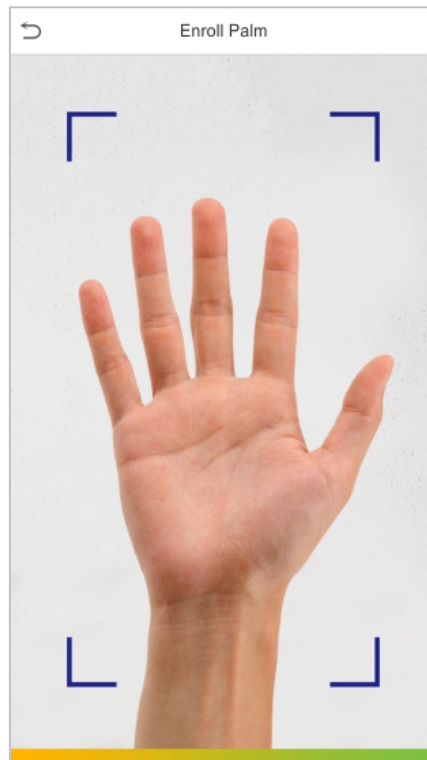


Nota: Si el rol de usuario seleccionado es el superadministrador, el usuario debe pasar la autenticación de identidad para acceder al menú principal. La autenticación se basa en los métodos de autenticación que ha registrado el superadministrador. Por favor refiérase a [2.6 Modo de verificación](#).

4.1.3 Palma

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

- Seleccione la palma que desea inscribir.
- Coloque la palma de la mano dentro de la caja guía y manténgala quieta mientras se registra. Aparece una barra de progreso mientras se registra la palma y un **"Inscrito correctamente"** se muestra a medida que se completa la barra de progreso.
- Si la palma ya está registrada, la **"Palma duplicada"** aparece el mensaje. La interfaz de registro es la siguiente:



4.1.4 Rostro

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

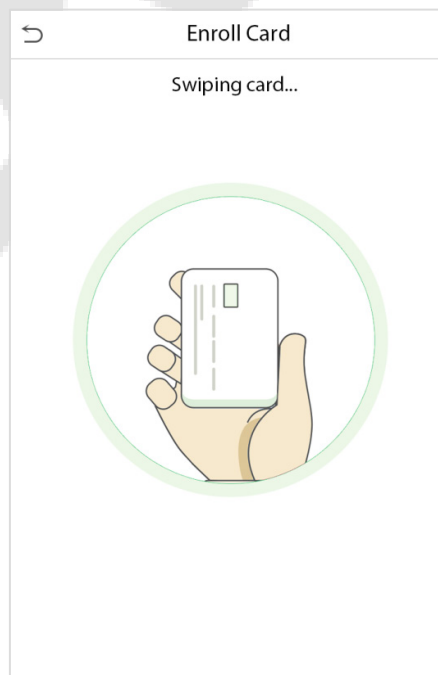
- Mire hacia la cámara y coloque su rostro dentro de la caja guía blanca y permanezca quieto durante el registro facial.
- Aparece una barra de progreso mientras se registra la cara y un **"Inscrito correctamente"** se muestra a medida que se completa la barra de progreso.
- Si la cara ya está registrada,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



4.1.5 Tarjeta

Grifo **Tarjeta** en el **Nuevo Usuario** interfaz para ingresar a la página de registro de la tarjeta.

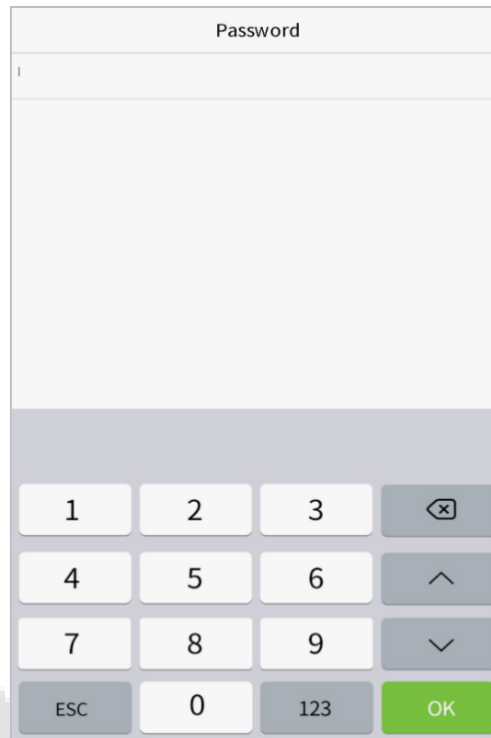
- En la interfaz de la tarjeta, deslice la tarjeta debajo del área de lectura de la tarjeta. El registro de la tarjeta se realizará correctamente.
- Si la tarjeta ya está registrada, entonces el “**Tarjeta duplicada**” Aparece el mensaje. La interfaz de registro es la siguiente:



4.1.6 Contraseña

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

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

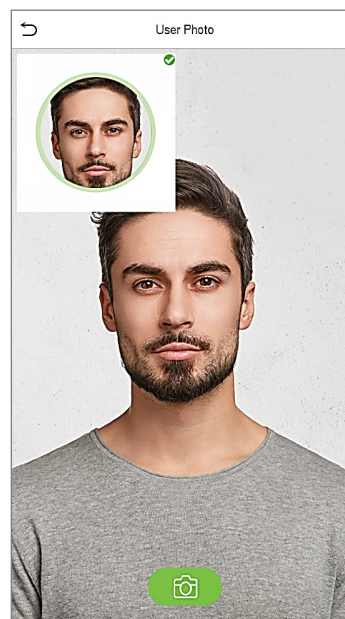


Nota: La contraseña puede contener de 1 a 8 dígitos de forma predeterminada.

4.1.7 Foto de usuario

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

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



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

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

4.1.8 Rol de control de acceso

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

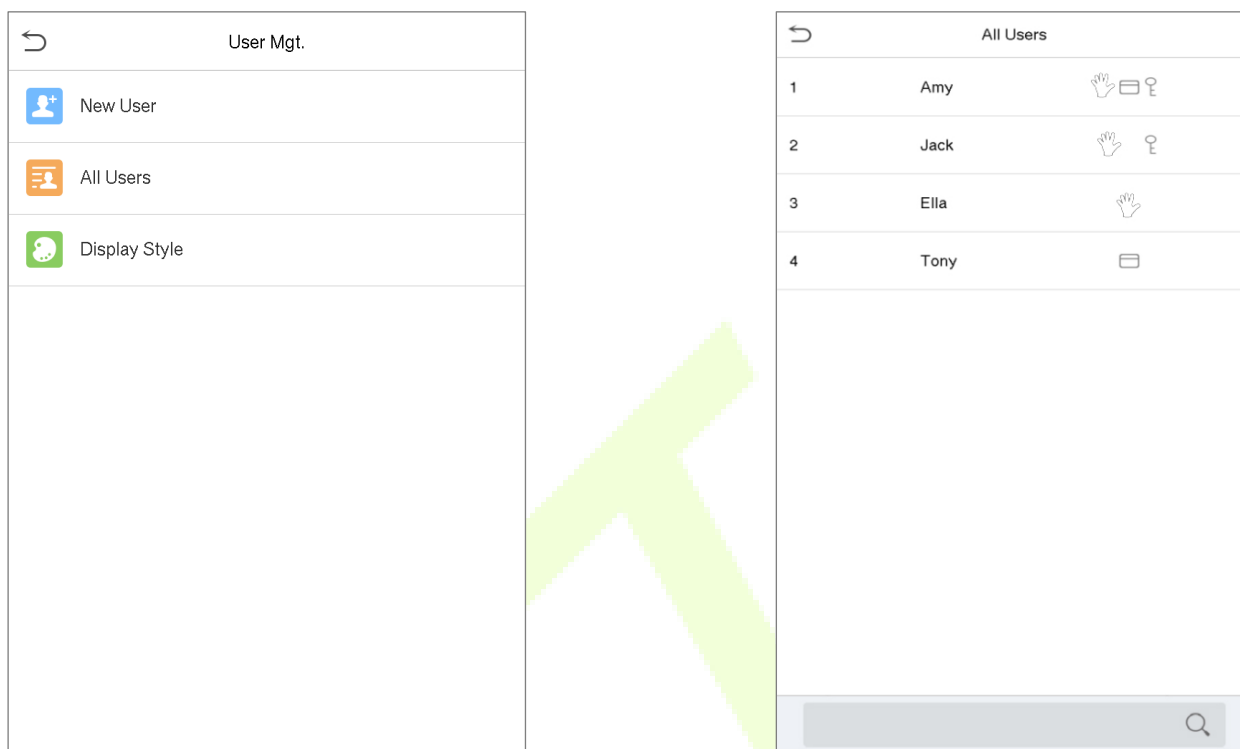
- Grifo **Función de control de acceso > Grupo de acceso**, asignar a los usuarios registrados a diferentes grupos para una mejor gestión. Los nuevos usuarios pertenecen al Grupo 1 de forma predeterminada y se pueden reasignar a otros grupos. El dispositivo admite hasta 99 grupos de control de acceso.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

Access Control	
Access Group	1
Time Period	

4.2 Buscar usuarios

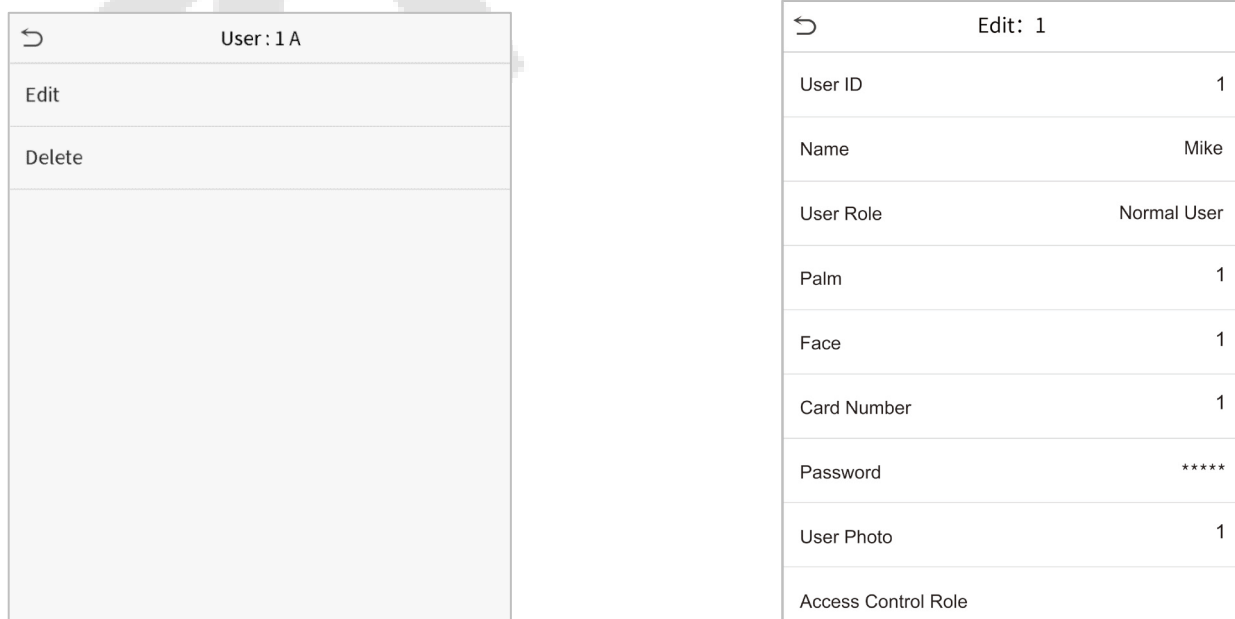
Sobre el **Menú principal**, grifo **Gestión de usuarios**, y luego toque **Todos los usuarios** para buscar un usuario.

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



4.3 editar usuario

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



NOTA : El proceso de editar la información del usuario es el mismo que el de agregar un nuevo usuario, excepto que el ID de usuario no se puede modificar al editar un usuario. El proceso en detalle se refiere a "[4 Gestión de usuarios](#)".

4.4 Borrar usuario

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

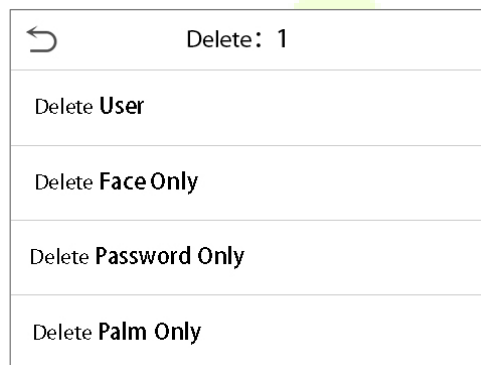
Eliminar operaciones

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

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

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

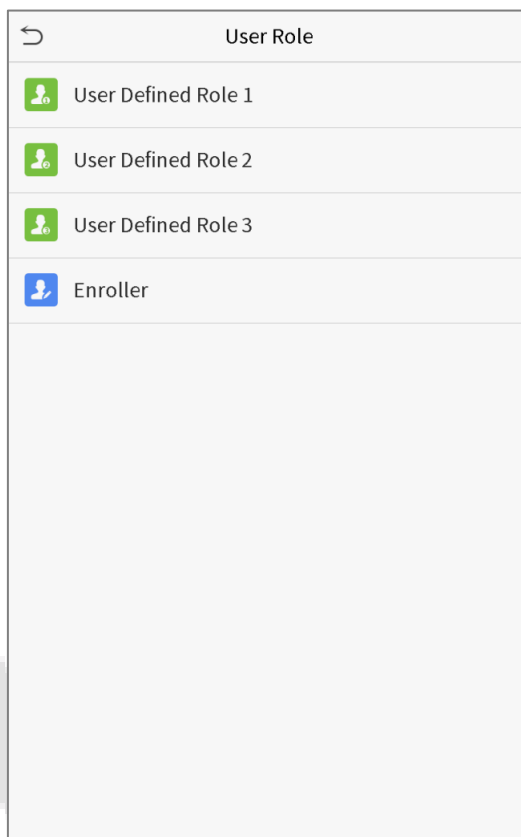
Eliminar PalmOnly: Elimina la información de la palma del usuario seleccionado.



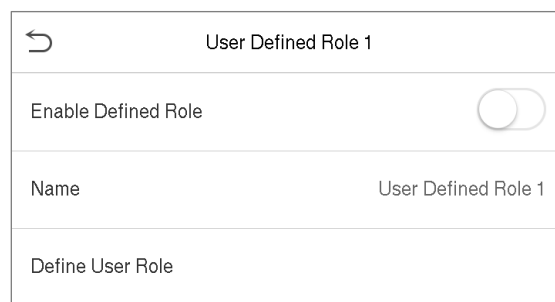
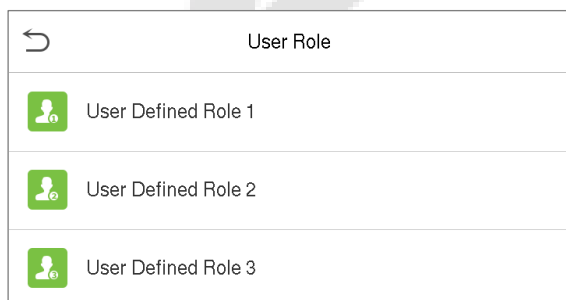
5 Rol del usuario

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

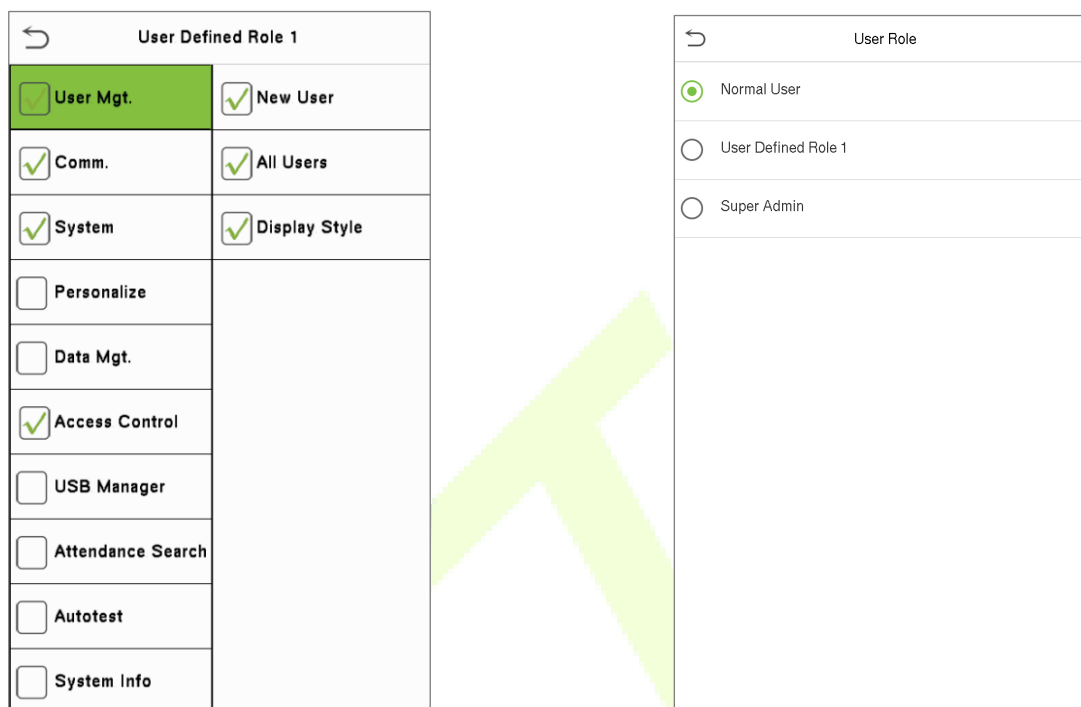
- Sobre el **Principal** menú, toque **Rol del usuario**, y luego toque en el **Rol definido por el usuario** para establecer los permisos definidos por el usuario.
- El alcance del permiso del rol personalizado se puede configurar hasta 3 roles, es decir, el alcance operativo personalizado de las funciones del menú del usuario.



- Sobre el **Rol definido por el usuario** interfaz, alternar **Habilitar rol definido** para habilitar o deshabilitar el rol definido por el usuario.
- Toque en **Nombre** e ingrese el nombre personalizado del rol.



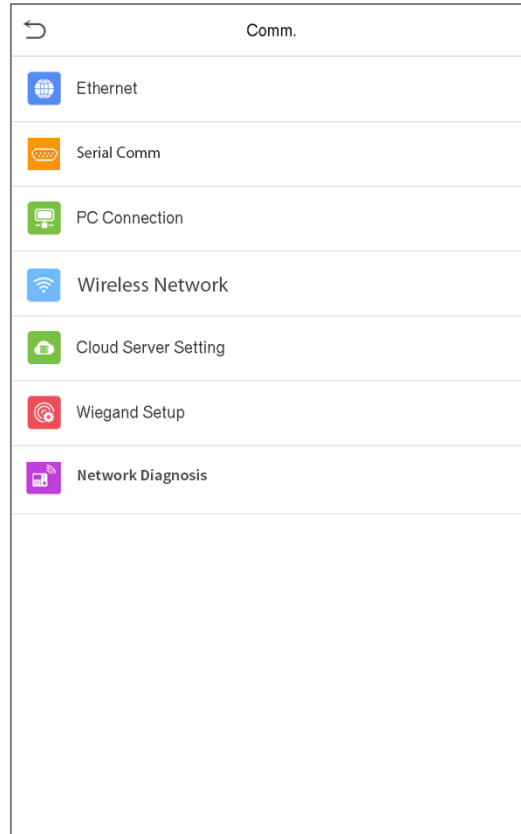
- Luego, toca **Definir rol de usuario** y seleccione los privilegios necesarios para asignar a la nueva función, y luego toque el **Regreso** botón.
- Durante la asignación de privilegios, los nombres de las funciones del menú principal se mostrarán a la izquierda y sus submenús se enumerarán a la derecha.
- Primero toque en el requerido **Menú principal** nombre de la función y, a continuación, seleccione los submenús necesarios de la lista.



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

6 Configuración de comunicación

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



6.1 Configuración de la red

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

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

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

Función descriptiva

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

6.2 Comunicaciones en serie

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

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

Serial Comm	
Serial Port	RS485(PC)
Baudrate	115200

Serial Port	
<input checked="" type="radio"/>	no using
<input type="radio"/>	RS485(PC)
<input type="radio"/>	Master Unit

Función descriptiva

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

6.3 Conexión a PC

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

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

PC Connection	
Comm Key	0
Device ID	1

Función descriptiva

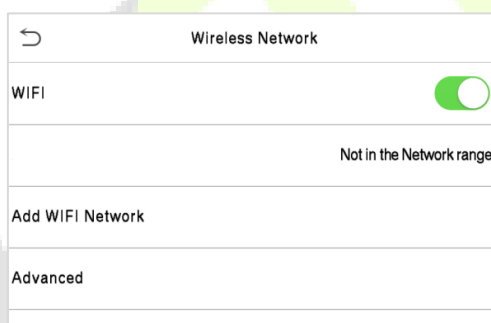
Nombre de la función	Descripciones
CommKey	La contraseña predeterminada es 0, que se puede cambiar. La clave de comunicación puede contener de 1 a 6 dígitos.
ID del dispositivo	Número de identificación del dispositivo, que oscila entre 1 y 254. Si el método de comunicación es RS232 / RS485, debe ingresar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

6.4 Red inalámbrica


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

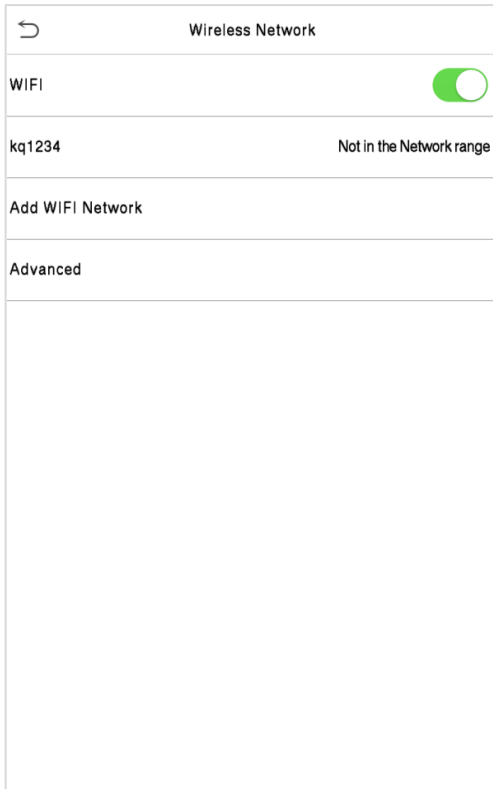
El módulo Wi-Fi permite la transmisión de datos a través de Wi-Fi (Wireless Fidelity) y establece un entorno de red inalámbrica. El Wi-Fi está habilitado de forma predeterminada en el dispositivo. Si no necesita usar la red Wi-Fi, puede alternar el botón Wi-Fi para deshabilitar.

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

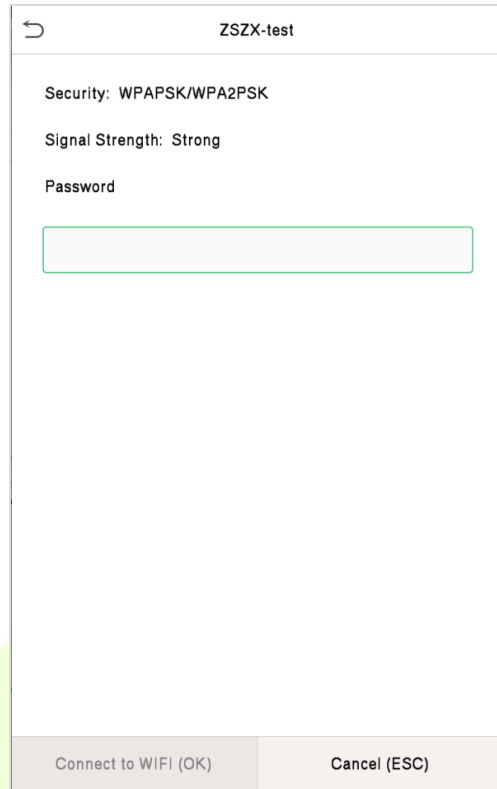


Buscar en la red wifi

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



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



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

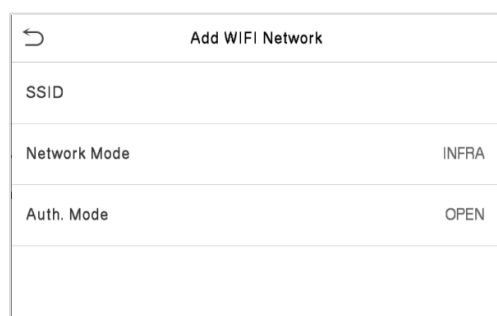
- Cuando el WIFI se conecta correctamente, la interfaz inicial mostrará el Wi-Fi  logo.

Agregar red WIFI manualmente

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



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



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

NOTA : Af

nombre. Clic

siga el mismo proceso para buscar la red WIFI FI agregada.

Configuración avanzada

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

Wireless Network	
WIFI	<input checked="" type="checkbox"/>
	Not in the Network range
Add WIFI Network	
Advanced	

Ethernet	
DHCP	<input checked="" type="checkbox"/>
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0

Función descriptiva

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

6.5 Configuración del servidor en la nube

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

Cloud Server Setting	
Server Mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	0.0.0.0
Server Port	8081
Enable Proxy Server	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>

Función descriptiva

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

6.6 Configuración de Wiegand

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

Wiegand Setup	
Wiegand Input	
Wiegand Output	

6.6.1 Entrada Wiegand

Wiegand Options	
Wiegand Format	
Wiegand Bits	26
Pulse Width(us)	100
Pulse Interval(us)	1000
ID Type	User ID

Función descriptiva

Nombre de la función	Descripciones
Formato Wiegand	Los valores oscilan entre 26 bits, 34 bits, 36 bits, 37 bits y 50 bits. Número de bits
Pedazos de Wiegand	de datos Wiegand.
PulseWidth (nosotros)	El valor del ancho de pulso enviado por Wiegand es 100 microsegundos por defecto, que se puede ajustar dentro del rango de 20 a 400 microsegundos.
Legumbres Intervalo (nosotros)	El valor predeterminado es 1000 microsegundos, que se puede ajustar dentro del rango de 200 a 20000 microsegundos.
tipo de identificación	Seleccione entre ID de usuario y número de tarjeta.

Varias descripciones del formato CommonWiegand:

Formato Wiegand	Descripción
Wiegand26	<p>ECCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 26 bits de código binario. El 1^{er} bit es el bit de paridad par del 2^o Dakota del Norte a 13^{er} bits, mientras que los 26^{er} bit es el bit de paridad impar del 14^{er} hasta 25^{er} bits. El 2^o Dakota del Norte hasta 25^{er} bits son los números de las tarjetas.</p>
Wiegand26a	<p>ESSSSSSSSCCCCCCCCCCCCCCCCCO</p> <p>Consta de 26 bits de código binario. El 1^{er} bit es el bit de paridad par del 2^o Dakota del Norte a 13^{er} bits, mientras que los 26^{er} bit es el bit de paridad impar del 14^{er} hasta 25^{er} bits. El 2^o Dakota del Norte al 9^{er} bits son los códigos de sitio, mientras que los 10^{er} hasta 25^{er} bits son los números de las tarjetas.</p>
Wiegand34	<p>ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 34 bits de código binario. El 1^{er} bit es el bit de paridad par del 2^o Dakota del Norte hasta 17^{er} bits, mientras que el 34^{er} bit es el bit de paridad impar de los 18^{er} hasta 33^{er} bits. El 2^o Dakota del Norte hasta 25^{er} bits son los números de las tarjetas.</p>
Wiegand34a	<p>ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 34 bits de código binario. El 1^{er} bit es el bit de paridad par del 2^o Dakota del Norte hasta 17^{er} bits, mientras que el 34^{er} bit es el bit de paridad impar de los 18^{er} hasta 33^{er} bits. El 2^o Dakota del Norte al 9^{er} bits son los códigos de sitio, mientras que los 10^{er} hasta 25^{er} bits son los números de las tarjetas.</p>
Wiegand36	<p>OFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME</p> <p>Consta de 36 bits de código binario. El 1^{er} bit es el bit de paridad impar del 2^o Dakota del Norte hasta 18^{er} bits, mientras que los 36^{er} bit es el bit de paridad par del 19^{er} hasta 35^{er} bits. El 2^o Dakota del Norte hasta 17^{er} bits son los códigos de dispositivo. El 18^{er} hasta 33^{er} bits son los números de la tarjeta, y los 34^{er} hasta 35^{er} bits son los códigos del fabricante.</p>

Wiegand36a	<p>EEEEEEEEEEEEEEEEFFFFCCCCCCCCCCCCCCCC</p> <p>Consta de 36 bits de código binario. El 1^{er} bit es el bit de paridad par del 2^o Dakota del Norte hasta 18th bits, mientras que los 36th bit es el bit de paridad impar del 19th hasta 35th bits. El 2^o Dakota del Norte hasta 19th bits son los códigos de dispositivo, y los 20th hasta 35th los bits son los números de las tarjetas.</p>
Wiegand37	<p>OMMMMSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE</p> <p>Consta de 37 bits de código binario. El 1^{er} bit es el bit de paridad impar del 2^o Dakota del Norte hasta 18th bits, mientras que el 37th bit es el bit de paridad par del 19th hasta 36th bits. El 2^o Dakota del Norte para 4th los bits son los códigos del fabricante. El 5th hasta 16th bits son los códigos de sitio, y los 21^{er} hasta 36th los bits son los números de las tarjetas.</p>
Wiegand37a	<p>EMMMFFFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCCO</p> <p>Consta de 37 bits de código binario. El 1^{er} bit es el bit de paridad par del 2^o Dakota del Norte hasta 18th bits, mientras que el 37th bit es el bit de paridad impar del 19th hasta 36th bits. El 2^o Dakota del Norte para 4th los bits son los códigos del fabricante. El 5th hasta 14th los bits son los códigos de dispositivo, y 15th hasta 20th bits son los códigos de sitio, y los 21^{er} hasta 36th los bits son los números de las tarjetas.</p>
Wiegand50	<p>ESSSSSSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Consta de 50 bits de código binario. El 1^{er} bit es el bit de paridad par del 2^o Dakota del Norte hasta 25th bits, mientras que los 50th bit es el bit de paridad impar del 26th hasta 49th bits. El 2^o Dakota del Norte hasta 17th bits son los códigos de sitio, y los 18th hasta 49th los bits son los números de las tarjetas.</p>
<p>"C" denota el número de tarjeta; "MI" denota el bit de paridad par; "O" denota el bit de paridad impar; "F" denota el código de la instalación; "METRO" denota el código del fabricante; "PAG" denota el bit de paridad; y "S" denota el código del sitio.</p>	

6.6.2 Salida Wiegand

Wiegand Options	
Wiegand Format	
Wiegand output bits	26
Failed ID	Disabled
Site Code	Disabled
Pulse Width(us)	100
Pulse Interval(us)	1000
ID Type	User ID

Función descriptiva

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

6,7 Diagnóstico de red

Para configurar los parámetros de diagnóstico de la red.

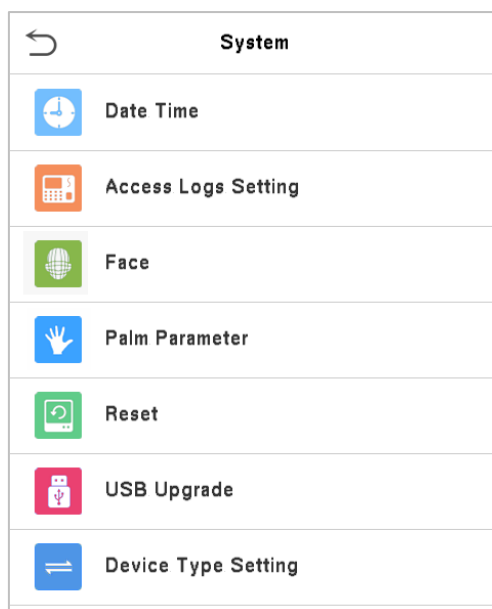
Grifo **Diagnóstico de red** sobre el **Comm**. Interfaz de configuración para configurar el diagnóstico de la dirección IP e iniciar los parámetros de diagnóstico.

Network Diagnosis	
IP address diagnostic test	0.0.0.0
Start the diagnostic test	

7 Ajustes del sistema

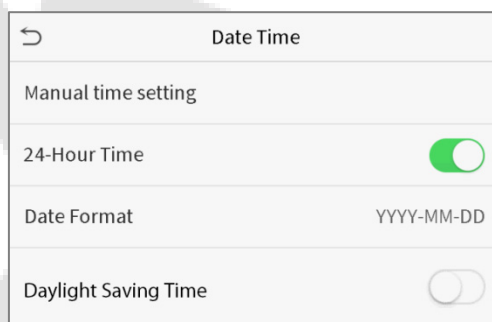
Configure los parámetros del sistema relacionados para optimizar el rendimiento del dispositivo.

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



7.1 Fecha y hora

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



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

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

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

Modo de semana**Modo de fecha**

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

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

7.2 Configuración de registros de acceso

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

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

Función descriptiva

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

7.3 Parámetros faciales

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

←	Face	↕
	1:N Match Threshold	74
	1:1 Match Threshold	63
	Face Enrollment Threshold	70
	Face Pitch Angle	35
	Face Rotation Angle	25
	Image Quality	40
	Minimum Face Size	80
	LED Light Triggered Threshold	80
	Motion Detection Sensitivity	4
	Live Detection	<input type="checkbox"/>

←	Face	↕
	Face Pitch Angle	35
	Face Rotation Angle	25
	Image Quality	40
	Minimum Face Size	80
	LED Light Triggered Threshold	80
	Motion Detection Sensitivity	4
	Live Detection	<input type="checkbox"/>
	Live Detection Threshold	70
	Anti-counterfeiting with NIR	<input checked="" type="checkbox"/>
	Face Algorithm	

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

Función descriptiva

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

Luz LED activada Umbral	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, con mayor frecuencia se encenderá la luz LED.
Detección de movimiento Sensibilidad	Sirve para establecer el valor de la cantidad de cambio en el campo de visión de una cámara, lo que se conoce como detección de movimiento potencial que activa el terminal desde el modo de espera a la interfaz de comparación. Cuanto mayor sea el valor, más sensible será el sistema, es decir, si se establece un valor mayor, la interfaz de comparación es mucho más fácil y la detección de movimiento se activa con frecuencia.
Detección en vivo	Detectar el intento de falsificación utilizando imágenes de luz visible para determinar si la muestra de fuente biométrica proporcionada es realmente una persona (un ser humano vivo) o una representación falsa.
Detección en vivo Umbral	Facilita juzgar si la imagen visible capturada es realmente una persona (un ser humano vivo). Cuanto mayor sea el valor, mejor será el rendimiento anti-spoofing con luz visible.
Lucha contra la falsificación con NIR	Uso de imágenes de espectros de infrarrojo cercano para identificar y prevenir ataques de fotos y videos falsos.
Algoritmo facial	Información relacionada con el algoritmo facial y actualización de la plantilla facial de pausa.
Notas	Un ajuste inadecuado de los parámetros de exposición y calidad puede afectar gravemente al rendimiento del dispositivo. Ajuste el parámetro de exposición solo bajo la guía del personal de servicio posventa de nuestra empresa.

7.4 Parámetros de la palma

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

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

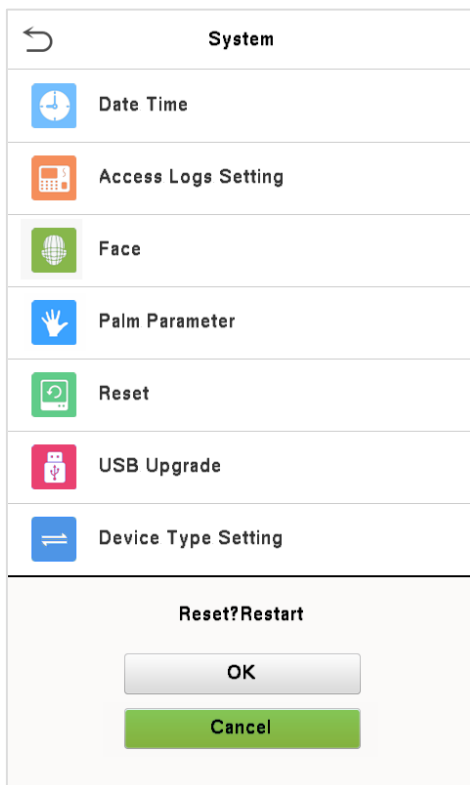
Función descriptiva

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

7.5 Restablecimiento de fábrica

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

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

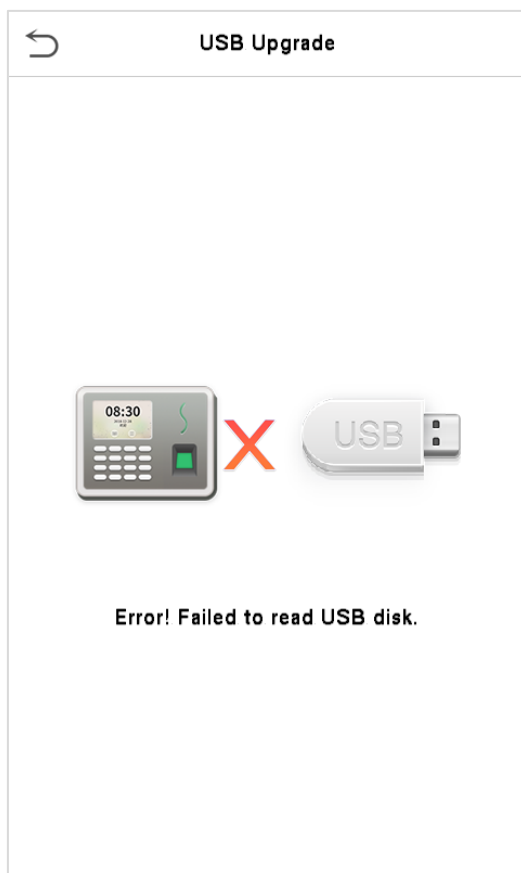


7.6 Actualización USB

Grifo **Actualización USB** en la interfaz del sistema.

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

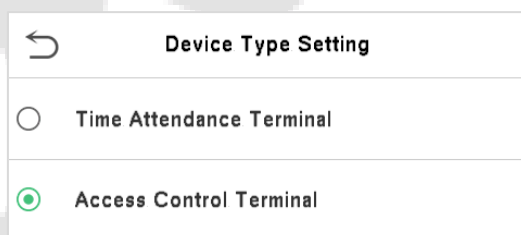
Si no hay ningún disco USB insertado, el sistema muestra el siguiente mensaje después de tocar **Actualización USB** en la interfaz del sistema.



Nota: Si necesita un archivo de actualización, comuníquese con nuestro soporte técnico. La actualización del firmware no se reinicia en circunstancias normales.

7.7 Configuración del tipo de dispositivo

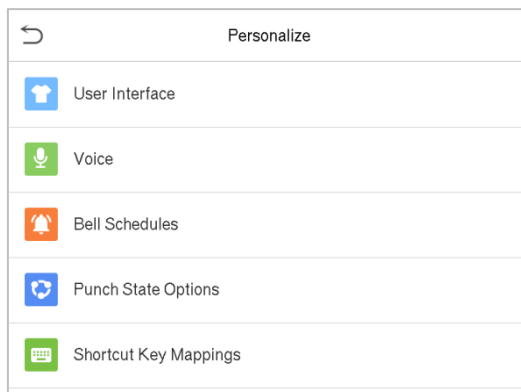
Grifo **Configuración del tipo de dispositivo** en la interfaz del sistema.



Nombre de la función	Descripción
Terminal de asistencia de tiempo	Configure el dispositivo como terminal de control de presencia.
Terminal de control de acceso	Configure el dispositivo como terminal de control de acceso.

8 Personalizar la configuración

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



8.1 Configuración de la interfaz

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

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

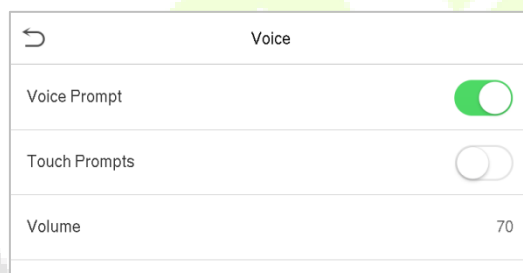
Función descriptiva

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

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

8.2 Configuración de voz

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



Función descriptiva

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

8.3 Horarios de campana

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



Nuevo horario de timbre

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

New Bell Schedule	
Bell Status	<input type="checkbox"/>
Bell Time	
Repeat	Never
Ring Tone	bell01.wav
Internal bell delay(s)	5

Función descriptiva

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

Todos los horarios de campana

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

Editar la campana programada

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

Eliminar una campana

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

8.4 Opciones de estados de perforación

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

Punch State Options	
Punch State Mode	Off

Punch State Mode	
<input checked="" type="radio"/>	Off
<input type="radio"/>	Manual Mode
<input type="radio"/>	Auto Mode
<input type="radio"/>	Manual and Auto Mode
<input type="radio"/>	Manual Fixed Mode
<input type="radio"/>	Fixed Mode

Función descriptiva

Nombre de la función	Descripción
Perforar StateMode	<p>Apagado: Desactive la función de estado de perforación. Por lo tanto, la clave de estado de perforación establecida en Asignaciones de teclas de método abreviado el menú dejará de ser válido.</p> <p>Modo manual: Cambie la tecla de estado de perforación manualmente y la tecla de estado de perforación desaparecerá después Tiempo de espera del estado de perforación.</p> <p>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.</p> <p>Modo manual y automático: La interfaz principal mostrará la tecla de estado de perforación de cambio automático. Sin embargo, los usuarios aún podrán seleccionar una alternativa que sea el estado de asistencia manual. Después del tiempo de espera, la tecla de estado de perforación de conmutación manual se convertirá en la tecla de estado de perforación de conmutación automática.</p> <p>Modo fijo manual: Después de que la tecla de estado de perforación se establezca manualmente en un estado de perforación particular, la función permanecerá sin cambios hasta que se cambie manualmente nuevamente.</p> <p>Modo fijo: Solo se mostrará la clave de estado de perforación fijada manualmente. Los usuarios no pueden cambiar el estado presionando otras teclas.</p>

8.5 Asignaciones de teclas de método abreviado

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

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

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

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

F1	
Punch State Value	0
Function	Punch State Options
Name	
Set Switch Time	

F1	
Function	New User

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

Establecer la hora del cambio

- El tiempo de conmutación se establece de acuerdo con las opciones de estado de perforación.
- Cuando el **punch statemode** se establece en **Modo automático**, debe establecerse el tiempo de conmutación.
- Sobre el **Tecla de acceso directo** interfaz, toque **Establecer hora de cambio** para configurar la hora del cambio.

- Sobre el **Ciclo de cambio** interfaz, seleccione el ciclo de conmutación (lunes, martes, etc.) como se muestra en la imagen siguiente.

F1		Switch Cycle		Set Switch Time	
Punch State Value	0	<input checked="" type="checkbox"/> Monday		Switch Cycle	Monday Tuesday Wednes...
Function	Punch State Options	<input checked="" type="checkbox"/> Tuesday		Monday	
Name		<input checked="" type="checkbox"/> Wednesday		Tuesday	
Set Switch Time		<input checked="" type="checkbox"/> Thursday		Wednesday	
		<input checked="" type="checkbox"/> Friday		Thursday	
		<input type="checkbox"/> Saturday		Friday	
		<input type="checkbox"/> Sunday			

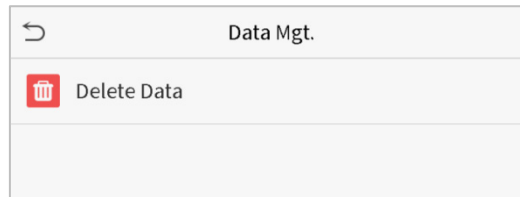
- Una vez que se selecciona el ciclo de cambio, configure el tiempo de cambio para cada día y toque **OK** para confirmar, como se muestra en la imagen de abajo.

Monday		Set Switch Time	
08:00		Switch Cycle	Monday Tuesday Wednes...
<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <input type="text" value="08"/> ↑ <input type="text" value="08"/> ↓ HH </div> <div style="text-align: center;"> <input type="text" value="00"/> ↑ <input type="text" value="00"/> ↓ MM </div> </div>		Monday	08:00
		Tuesday	
		Wednesday	
		Thursday	
		Friday	
Confirm (OK)	Cancel (ESC)		

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

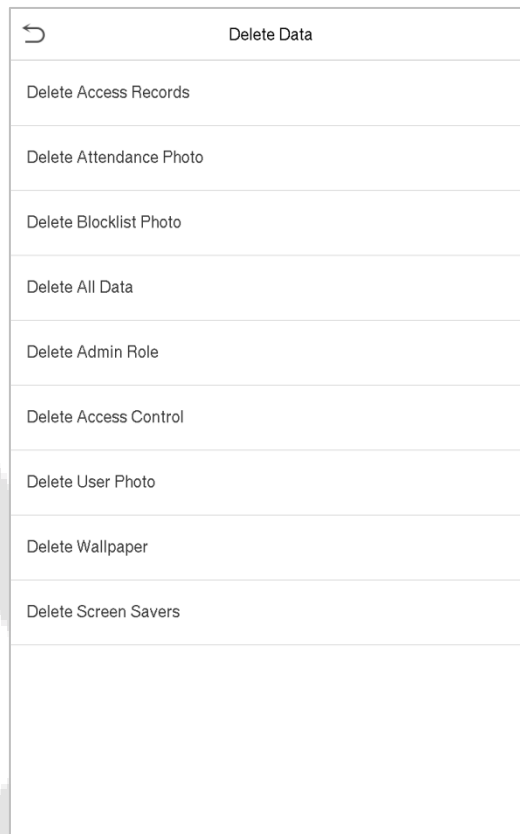
9 Gestión de datos

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



9.1 Borrar datos

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



Función descriptiva

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

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

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

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

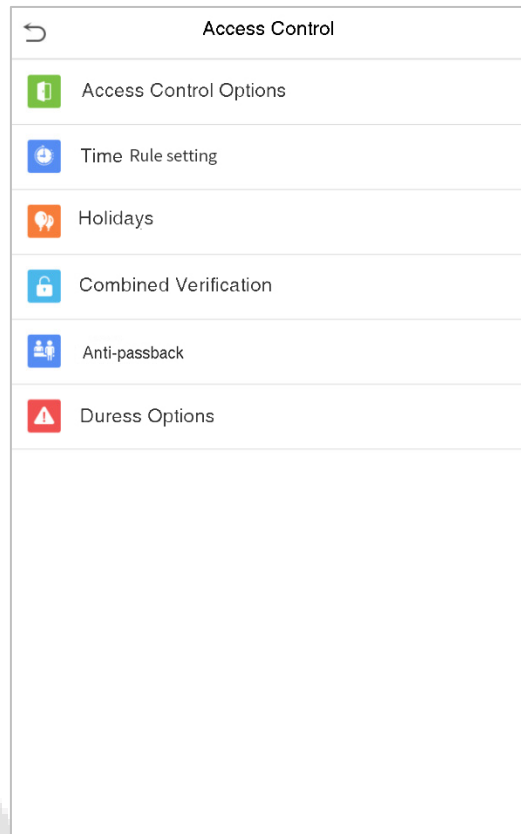
Seleccione Eliminar por rango de tiempo.

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

Establezca el rango de tiempo y haga clic en **está bien**.

10 Control de acceso

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

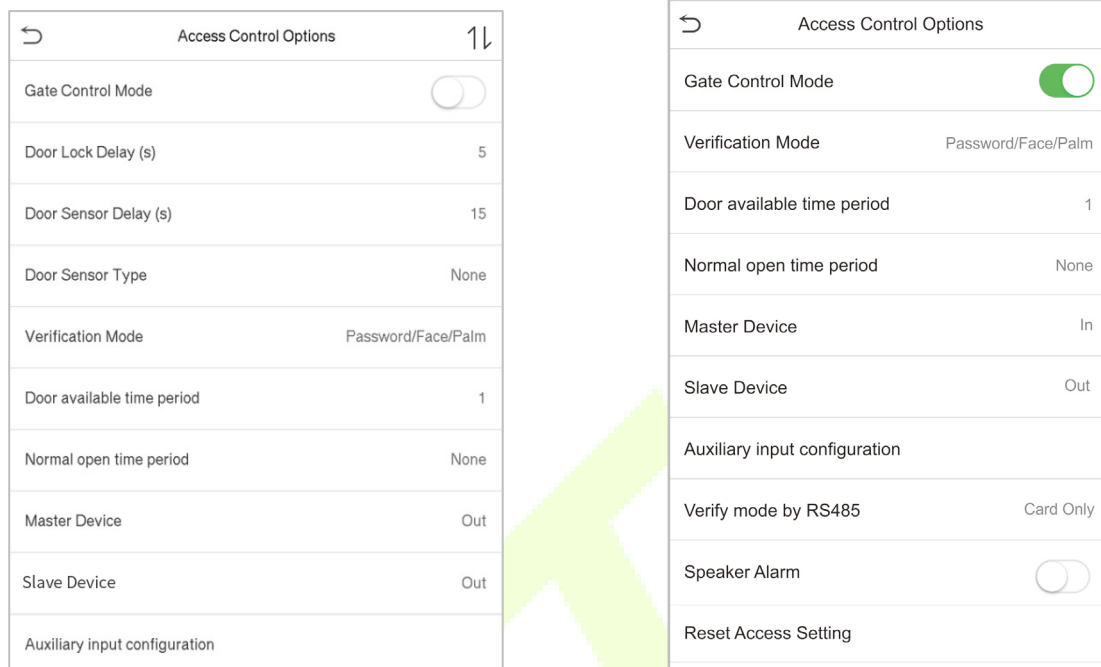


Para acceder, el usuario registrado debe cumplir las siguientes condiciones:

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

10.1 Opciones de control de acceso

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



Función descriptiva

Nombre de la función	Descripción
Modo de control de puerta	Cambie entre el interruptor de ENCENDIDO o APAGADO para entrar en el modo de control de puerta o no. Cuando se establece en EN , en esta interfaz eliminará las opciones de tipo de sensor de puerta, relé de bloqueo de puerta y sensor de puerta.
Retraso de bloqueo de puerta (s)	El tiempo que el dispositivo controla que la cerradura eléctrica esté en estado de desbloqueo. Valor válido: 1 ~ 10 segundos; 0 segundos representa la desactivación de la función.
Retraso del sensor de puerta	Si la puerta no está bloqueada y se deja abierta durante un tiempo determinado (retardo del sensor de puerta), se activará una alarma. El valor válido del retardo del sensor de puerta varía de 1 a 255 segundos.
Tipo de sensor de puerta	Hay tres tipos de sensores: Ninguno , normalmente abierto y Normal Cerrado . Ninguno : Significa que el sensor de la puerta no está en uso. Abierto normal : Significa que la puerta siempre se deja abierta cuando la energía eléctrica está encendida. Normal Cerrado : Significa que la puerta siempre se deja cerrada cuando la energía eléctrica está encendida.

VerificationMode	El modo de verificación admitido incluye contraseña / rostro, solo ID de usuario, contraseña, solo rostro y rostro + contraseña.
Puerta disponible tiempo período	Para establecer un período de tiempo para la puerta, de modo que la puerta esté disponible solo durante ese período.
Tiempo abierto normal Período	Período de tiempo programado para el modo de "apertura normal", de modo que la puerta siempre se deje abierta durante este período.
Dispositivo maestro	Al configurar el maestro, el estado del maestro se puede configurar para salir al entrar. Fuera: El registro verificado en el host es el registro de salida. En: El registro verificado en el anfitrión es el registro de entrada.
Dispositivo esclavo	Al configurar el esclavo, el estado del esclavo se puede configurar para salir al entrar. Fuera: El registro verificado en el host es el registro de salida. En: El registro verificado en el anfitrión es el registro de entrada.
Entrada auxiliar configuración	Establece el período de tiempo de desbloqueo de la puerta y el tipo de salida auxiliar del dispositivo terminal auxiliar. Los tipos de salidas auxiliares incluyen Ninguno, Puerta del gatillo abierta, Alarma del gatillo, Puerta del gatillo abierta y Alarma.
Verificar modo por RS485	El modo de verificación se usa cuando el dispositivo se usa como host o esclavo. El modo de verificación admitido incluye solo tarjeta, tarjeta + contraseña.
Alarma de altavoz	Transmite una alarma sonora o una alarma de desmontaje desde el local. Cuando la puerta está cerrada o la verificación es exitosa, el sistema cancelará la alarma del local.
Restablecer configuración de acceso	Los parámetros de restablecimiento del control de acceso incluyen el retardo de la cerradura de la puerta, el retardo del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el período de tiempo disponible de la puerta, el período de tiempo de apertura normal, el dispositivo maestro y la alarma. Sin embargo, los datos de control de acceso borrados en Data Mgt. está excluido.

10,2 Configuración de la regla de tiempo

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

- Todo el sistema puede definir hasta 50 períodos de tiempo. Cada período de tiempo representa **10** Zonas horarias, es decir **1** semana y **3** días festivos, y cada zona horaria es un período estándar de 24 horas por día y el usuario solo puede verificar dentro del período de tiempo válido.
- Se puede establecer un máximo de 3 períodos de tiempo para cada zona horaria. La relación entre estos períodos de tiempo es "**0**". Por lo tanto, cuando el tiempo de verificación cae en cualquiera de estos períodos de tiempo, la verificación es válida.

Time Period 1

00:00 23:59

↑	↑	↑	↑
00	00	23	59
↓	↓	↓	↓
HH	MM	HH	MM

Confirm (OK) Cancel (ESC)

Especifique la hora de inicio y finalización y luego toque **está bien**.

NOTA :

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

10,3 Vacaciones

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

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

Holidays	
Add Holiday	
All Holidays	

- **Agregar un nuevo feriado**

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

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

- **Editar un día festivo**

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

- **Eliminar un feriado**

Sobre el **Vacaciones** interfaz, seleccione un elemento de vacaciones para eliminar y toque **Borrar**. Prensas **OK** para confirmar la eliminación. Después de la eliminación, este día festivo ya no se muestra en **Todos los días festivos** interfaz.

10,4 Verificación combinada

Los grupos de acceso se organizan en diferentes combinaciones de desbloqueo de puertas para lograr múltiples verificaciones y fortalecer la seguridad. En una combinación de desbloqueo de puerta, el rango del número combinado N es: $0 \leq N \leq 5$, y el número de miembros N pueden pertenecer todos a un grupo de acceso o pueden pertenecer a cinco grupos de acceso diferentes.

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

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

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

Por ejemplo:

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

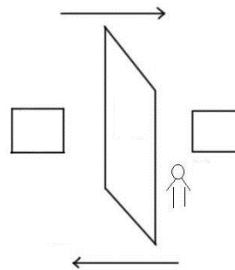
Eliminar una combinación de desbloqueo de puertas

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

10,5 Configuración anti-passback

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

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



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

Anti-passback Setup	Anti-passback Direction
Anti-passback Direction: No Anti-passback	<input checked="" type="radio"/> No Anti-passback <input type="radio"/> Out Anti-passback <input type="radio"/> In Anti-passback <input type="radio"/> In/Out Anti-passback

Función descriptiva

Nombre de la función	Descripción
Anti-passback dirección	<p>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.</p> <p>Fuera Anti-passback: Después de que un usuario se retira, solo si el último registro es un registro de entrada, el usuario puede volver a retirar; de lo contrario, se activará la alarma. Sin embargo, el usuario puede realizar el check-in libremente.</p> <p>En Anti-passback: Después de que un usuario se registra, solo si el último registro es un registro de salida, el usuario puede registrarse nuevamente; de lo contrario, se activará la alarma. Sin embargo, el usuario puede realizar el check-out libremente.</p> <p>Antirretorno de entrada / salida: Después de que un usuario se registra de entrada / salida, solo si el último registro es un registro de salida, el usuario puede registrarse nuevamente; o si se trata de un registro de entrada, el usuario puede volver a realizar la salida; de lo contrario, se disparará la alarma.</p>

10,6 Opciones de coacción

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

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

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

Función descriptiva

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

11 USBManager

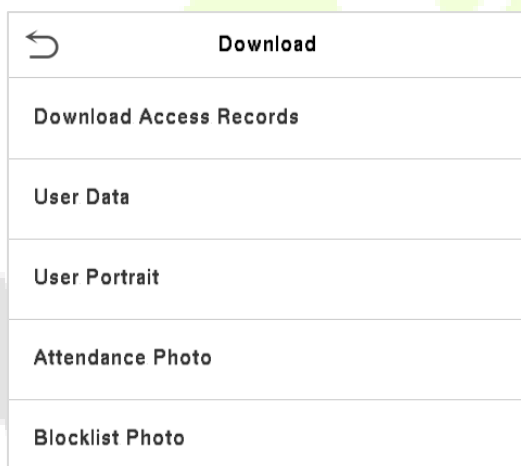
Puede importar la información del usuario y los datos de asistencia en la máquina al software de asistencia correspondiente para su procesamiento mediante un disco USB, o importar la información del usuario a otros dispositivos para realizar una copia de seguridad.

Antes de cargar / descargar datos desde / hacia el disco USB, inserte primero el disco USB en la ranura USB. Grifo **USBManager** en la interfaz del menú principal.



11,1 Descarga USB

Sobre el **USBManager** interfaz, toque **Descargar**.



Nombre de la función	Descripción
Descargar acceso Registro	Para descargar el registro de acceso en un periodo de tiempo especificado en un disco USB.
Datos del usuario	Para descargar toda la información del usuario del dispositivo en un disco USB. Para descargar
Retrato de usuario	todos los retratos de usuario del dispositivo a un disco USB.
Asistencia Foto	Para descargar todas las fotos de asistencia desde el dispositivo a un disco USB.
Foto de lista de bloqueo	Para descargar todas las fotos de la lista de bloqueo (fotos tomadas después de verificaciones fallidas) desde el dispositivo al disco USB.

11,2 Carga USB

Sobre el **USBManager** interfaz, toque **Descargar**.

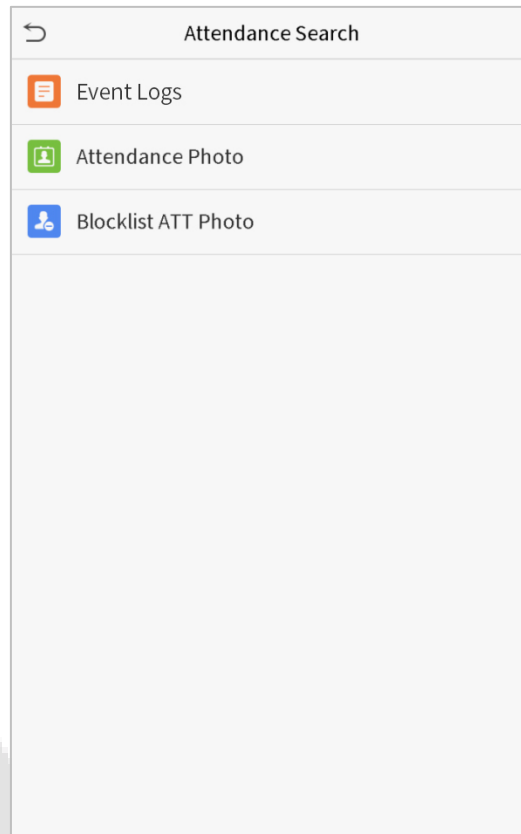
←	Upload
	Screen Saver
	Wallpaper
	User Data
	User Portrait

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

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.

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



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

Sobre el **Búsqueda de asistencia** interfaz, toque **Registros de eventos** para buscar el registro requerido.

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

User ID

Please Input(query all data without input)

1	2	3	
4	5	6	
7	8	9	
ESC	0	123	OK

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

Time Range

- Today
- Yesterday
- This week
- Last week
- This month
- Last month
- All
- User Defined

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

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

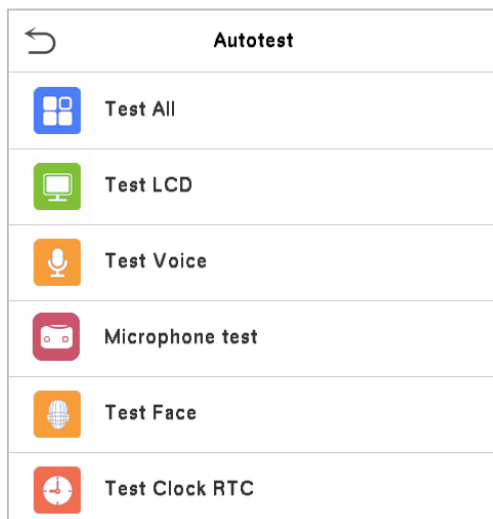
4. La siguiente figura muestra los detalles del registro seleccionado.

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

Verification Mode : Face Status : In

13 Auto prueba

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

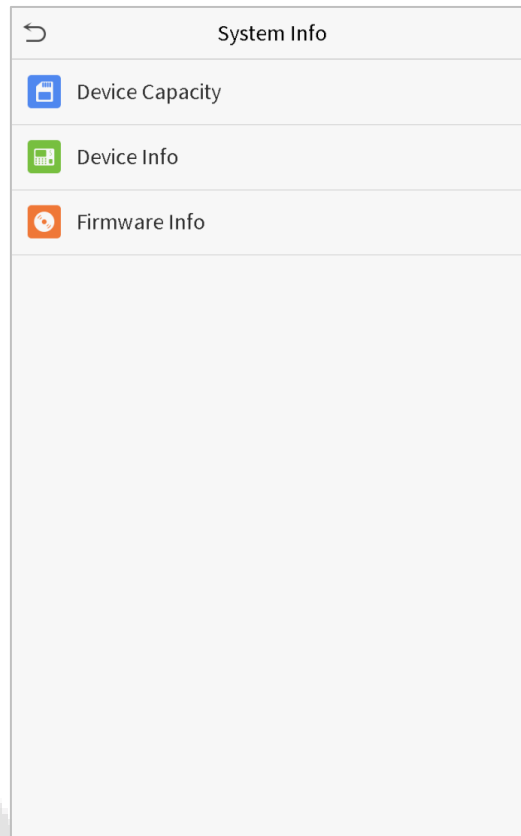


Función descriptiva

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

14 Información del sistema

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



Función descriptiva

Nombre de la función	Descripción
Capacidad del dispositivo	Muestra el almacenamiento de usuario del dispositivo actual, la palma, la contraseña, el almacenamiento de caras y tarjetas, los administradores, los registros de acceso, las fotos de listas de asistencia y de bloqueo y las fotos de los usuarios.
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la dirección MAC, el algoritmo de la palma y la cara, la información de la versión, la información de la plataforma y el fabricante y la fecha de fabricación.
Información de firmware	Muestra la versión de firmware y otra información de la versión del dispositivo.

15 Conéctese al software ZKBioAccess IVS

15.1 Establecer la dirección de comunicación

- Lado del dispositivo

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

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

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

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

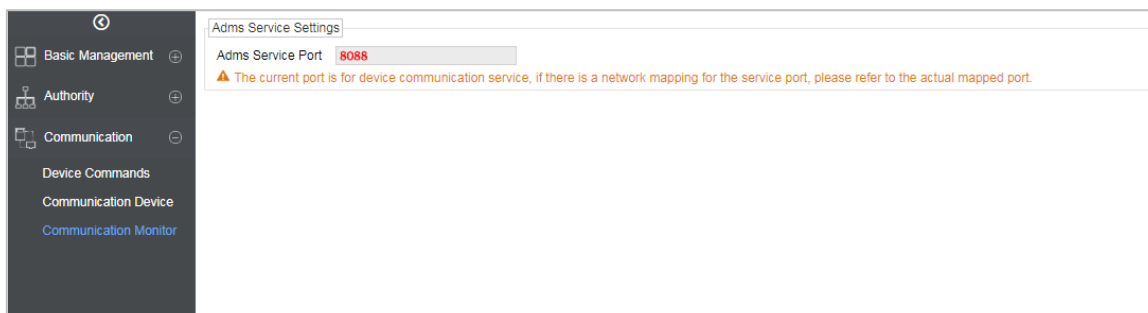
Puerto de servicio: Configure el puerto del servidor como ZKBioAccess IVS (el valor predeterminado es 8088).

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

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

- **Lado del software**

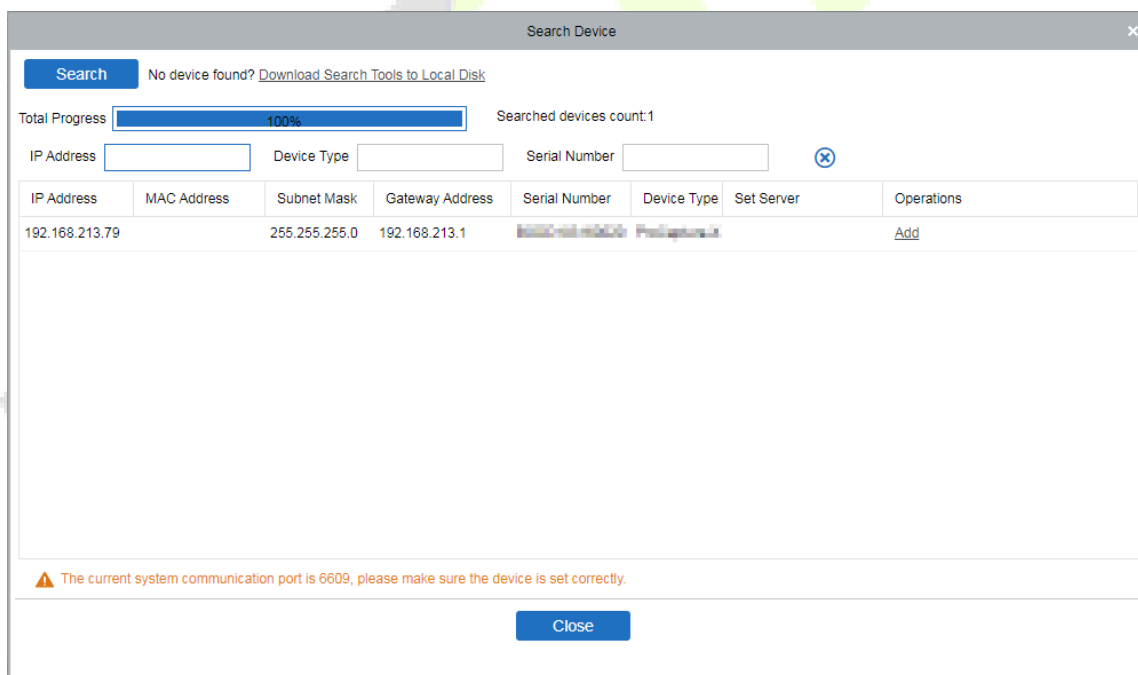
Inicie sesión en el software ZKBioAccess IVS, haga clic en **Sistema> Comunicación> Monitor de comunicación** para configurar el puerto de servicio ADMS, como se muestra en la siguiente figura:



15,2 Agregar dispositivo en el software

Agregue el dispositivo buscando. El proceso es el siguiente:

- 1) Hacer clic **Control de acceso> Dispositivo> Dispositivo de búsqueda**, para abrir la interfaz de búsqueda en el software.
- 2) Hacer clic **Buscar**, y le indicará [**buscando**].
- 3) Después de la búsqueda, se mostrará la lista y el número total de controladores de acceso.



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

15,3 Agregar personal al software

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

2. Complete todos los campos obligatorios y haga clic en [**OK**] para registrar un nuevo usuario.
3. Hacer clic **Acceda > Dispositivo > Control de dispositivo > Sincronizar todos los datos con los dispositivos** para sincronizar todos los datos al dispositivo, incluidos los nuevos usuarios.

Apéndice 1

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

visible

- 1) Se recomienda realizar el registro en un entorno interior con una luz adecuada fuente sin subexposición o sobreexposición.
- 2) No coloque el dispositivo hacia fuentes de luz exteriores como puertas o ventanas u otra luz fuerte fuentes.
- 3) Se recomienda la ropa de color oscuro, diferente del color de fondo para el registro.
- 4) Exponga la cara y la frente correctamente y no se cubra la cara y las cejas con su pelo.
- 5) Se recomienda mostrar una expresión facial sencilla. (Una sonrisa es aceptable, pero no cierre la ojos o inclinar la cabeza hacia cualquier orientación).
- 6) Se requieren dos imágenes para una persona con anteojos, una imagen con anteojos y la otra sin los anteojos.
- 7) No use accesorios como bufandas o mascarillas que puedan cubrir su boca o barbilla.
- 8) Mire a la derecha hacia el dispositivo de captura y ubique su rostro en el área de captura de imágenes como como se muestra en la imagen de abajo.
- 9) No incluya más de una cara en el área de captura.
- 10) Se recomienda una distancia de 50 cm a 80 cm para capturar la imagen. (la distancia es ajustable, sujeta a la altura del cuerpo).



Requisitos para datos de imagen facial digital con luz visible

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

- **Distancia del ojo**

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

- **Expresión facial**

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

- **Gesto y ángel**

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

- **Accesorios**

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

- **Rostro**

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

- **Formato de imagen**

Debe estar en BMP, JPG o JPEG.

- **Requisito de datos**

Debe cumplir con los siguientes requisitos:

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

Apéndice 2

Declaración sobre el derecho a la privacidad

Queridos clientes:

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

Declaramos que:

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

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

Nota:

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

1. No habrá arresto, detención, registro o infracción ilegal de personas;
2. La dignidad personal está relacionada con la libertad personal y no debe ser violada;
3. No se puede violar la casa de un ciudadano;
4. El derecho a la comunicación de un ciudadano y la confidencialidad de esa comunicación están protegidos por la ley.

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

Operación ecológica



El "período 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 de funcionamiento ecológico de la batería es de 5 años.

Sustancias peligrosas o tóxicas y sus cantidades

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

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

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

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

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

Town, Dongguan, China.

Teléfono: +86769 - 82109991 Fax

: +86 755 - 89602394

www.zkteco.com

