Manual de Usuario

SenseFace 2A

Fecha: Junio 2025
Versión: 1.5

Gracias por elegir nuestro producto. Por favor, lea atentamente las instrucciones antes de utilizarlo. Siga estas instrucciones para asegurarse de que el producto funciona correctamente. Las imágenes mostradas en este manual son sólo para fines ilustrativos. Para más información, visite el sitio www.zkteco.com

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

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

Marca Registrada

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

Exención de Responsabilidad

Este manual contiene información sobre el funcionamiento y el mantenimiento del equipo ZKTeco. El copyright de todos los documentos, dibujos, etc. relacionados con el equipo suministrado por ZKTeco es propiedad de ZKTeco. Su contenido no debe ser utilizado ni compartido por el receptor con terceros sin la autorización expresa y por escrito de ZKTeco.

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

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

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

ZKTeco no ofrece ninguna garantía o representación con respecto a la integridad de cualquier información contenida en este manual o cualquiera de las modificaciones introducidas en el 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 alguna por errores u omisiones en la información o documentos a los que se hace referencia o que están vinculados a este manual. El usuario asume todo el riesgo en cuanto a los resultados y el rendimiento obtenidos de la utilización de la información.

ZKTeco no será responsable en ningún caso ante el usuario ni ante terceros de ningún daño incidental, consecuente, indirecto, especial o ejemplar, incluyendo, sin limitación, la pérdida de negocio, la pérdida de beneficios, la interrupción de negocio, la pérdida de información comercial o cualquier pérdida pecuniaria, que surja de, en conexión con, o en relación con el uso de la información contenida en o referenciada por este manual, incluso si ZKTeco ha sido advertido de la posibilidad de tales daños.

Este manual y la información contenida en el mismo pueden incluir imprecisiones técnicas, de otro tipo o errores tipográficos. ZKTeco modifica periódicamente la información aquí contenida, que se incorporará en nuevas adiciones/enmiendas al manual. ZKTeco se reserva el derecho de añadir, 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 modificaciones están destinadas a mejorar el funcionamiento de la máquina/unidad/equipo y dichas modificaciones no darán derecho a reclamar ninguna compensación o indemnización por daños y perjuicios en ninguna circunstancia.

ZKTeco no será responsable en ningún caso (i) en caso de mal funcionamiento de la máquina/unidad/equipo debido al incumplimiento de las instrucciones contenidas en este manual (II) en caso de funcionamiento de la máquina/unidad/equipo más allá de los límites de la tarifa (III) en caso de funcionamiento de la máquina y el equipo en condiciones diferentes a las prescritas en el manual.

El producto se actualizará de vez en cuando sin previo aviso. Los procedimientos de funcionamiento más recientes y los documentos pertinentes están disponibles en **https://www.zktecolatinoamerica.com**

Sede de ZKTeco

Dirección ZKTeco Industrial Park, No. 26, 188 Industrial Road, Tang Xia Town, Dong guan, China.

Teléfono +86 769 – 82109991

Fax +86 755 - 89602394

Para consultas relacionadas con la empresa, escríbanos a: **sales@zkteco.com.**
Para saber más sobre nuestras sucursales en todo el mundo, visite **www.zkteco.com.**

Acerca de la empresa

ZKTeco es uno de los mayores fabricantes del mundo de lectores RFID y biométricos (huella dactilar, facial y reconocimiento de vena). Su oferta de productos incluye lectores y paneles de control de acceso, cámaras de reconocimiento facial de corto alcance. Cámaras de reconocimiento facial de largo alcance, controladores de acceso de elevadores, torniquetes, controladores de puertas con reconocimiento de placas vehiculares (LPR) y productos de consumo, como cerraduras de puertas con lector facial y de huellas dactilares que funcionan con pilas. Nuestras soluciones de seguridad son multilingües y están localizadas en más de 18 idiomas. En las modernas instalaciones de fabricación de ZKTeco, de 700.000 pies cuadrados y con certificación 1509001, controlamos la fabricación, el diseño de productos, el montaje de componentes y la logística y el envío, todo bajo un mismo techo.

Los fundadores de ZKTeco se han empeñado en la investigación y el desarrollo independientes de procedimientos de verificación biométrica y en la producción del SDK de verificación biométrica, que inicialmente se aplicó ampliamente en los campos de la seguridad de PC y la autenticación de identidad. Con la mejora continua del desarrollo y un montón de aplicaciones de mercado, el equipo ha construido gradualmente una identidad y un ecosistema de seguridad inteligente basados 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 Empresa Nacional de Alta Tecnología durante 6 años consecutivos. Los productos están protegidos por derechos de propiedad intelectual.

Acerca del Manual

Este manual presenta las operaciones del producto SenseFace 2A.
Todas las figuras mostradas son sólo para fines ilustrativos. Las figuras de este manual pueden no coincidir exactamente con los productos reales.

Convenciones del Documento

A continuación, se enumeran las convenciones utilizadas en este manual:
Convenciones GUI

Para el software	
Convención	**Descripción**
Negritas	Usado para identificar interfaz del software como: **OK, Confirmar, Cancelar**
>	Multi.nivel del menú son separados por éstos corchete, Ejemplo: Archivo > Crear > Carpeta.
Para el dispositivo	
Convención	**Descripción**
<>	Nombres de botones o teclas para dispositivos. Por ejemplo, pulse <OK>.
[ ]	Los nombres de ventanas, opciones de menú, tablas de datos y campos aparecen entre corchetes. Por ejemplo, abra la ventana [Nuevo usuario].
/	Los menús de varios niveles se separan mediante barras inclinadas. Por ejemplo, [Archivo / Crear / Carpeta].

Símbolos

Convención	Descripción
	Esto implica sobre el aviso o presta atención en el manual.
	Información general que ayuda a realizar las operaciones más rápidamente.
	Información a considerar.
	Para evitar peligros o errores.
	Declaración o acontecimiento de advertencia de algo o que sirve de ejemplo.

Contenido

1 MEDIDAS DE SEGURIDAD....9
2 SEGURIDAD ELÉCTRICA....10
3 OPERACIÓN SEGURIDAD....11
4 INSTRUCCIONES DE USO....11
4.1 POSICIÓN DE PIE, POSTURA Y EXPRESIÓN FACIAL....11
4.2 REGISTRO DE PLANTILLAS FACIALES....14
4.3 POSICIÓN DE LOS DEDOS....15
4.4 INTERFAZ DE ESPERA....16
4.5 MODO DE VERIFICACIÓN....16
4.5.1 VERIFICACIÓN FACIAL....16
4.5.2 VERIFICACIÓN DE HUELLAS DACTILARES....18
4.5.3 VERIFICACIÓN DE TARJETAS....19
4.5.4 VERIFICACIÓN DE CONTRASEÑA....20
4.5.5 VERIFICACIÓN COMBINADA....21
5 VISIÓN GENERAL....21
5.1 APARIENCIA....21
5.2 DESCRIPCIÓN DE TERMINALES Y CABLE....22
5.2.1 DESCRIPCIÓN DEL TERMINAL....22
5.3 DESCRIPCIÓN DEL CABLEADO....23
5.3.1 CONEXIÓN DE ALIMENTACIÓN....23
5.3.2 CONEXIÓN DE SENSOR DE PUERTA Y PULSADOR DE SALIDA....24
5.3.3 CONEXIÓN DEL RELÉ DE BLOQUEO....24
5.3.4 CONEXIÓN A INTERNET....24
6 INSTALACIÓN....25
6.1 ENTORNO DE INSTALACIÓN....25
6.2 INSTALACIÓN DEL DISPOSITIVO....25
7 MENÚ PRINCIPAL....26
8 GESTIÓN DE USUARIOS....27
8.1 REGISTRO DE NUEVOS USUARIOS....27
8.1.1 REGISTRAR UN ID DE USUARIO Y UN NOMBRE....27
8.1.2 ROL DE USUARIO....28
8.1.3 REGISTRAR HUELLA DACTILAR....28
8.1.4 REGISTRAR CARA....29
8.1.5 TARJETA....29
8.1.6 CONTRASEÑA....30
8.1.7 FOTO DE PERFIL....30
8.1.8 FUNCIÓN DE CONTROL DE ACCESO....31
8.2 TODOS LOS USUARIOS....31

9 ROL DE USUARIO 34
8.2.1 EDITAR USUARIO 31
8.2.2 ELIMINAR USUARIO 32
8.3 ESTILO DE VISUALIZACION 32
10 COMUNICACIÓN 36
10.1 INTERNET 36
10.2 CONEXIÓN PC 37
10.3 CONFIGURACIÓN DE WI-FI 38
10.4 CONFIGURACIÓN DEL SERVIDOR EN LA NUBE 40
10.5 DIAGNÓSTICO DE LA RED 40
11 CONFIGURACIÓN DEL SISTEMA 41
11.1 FECHA Y HORA 41
11.2 CONFIGURACIÓN DE LOS REGISTROS DE ACCESO / ASISTENCIA 42
11.3 PARÁMETROS DE LA CARA 46
11.4 HUELLA DACTILAR 48
11.5 CONFIGURACIÓN DEL TIPO DE DISPOSITIVO 49
11.6 CONFIGURACIÓN DE SEGURIDAD 50
11.7 ACTUALIZACIONES 51
11.8 ACTUALIZAR EL FIRMWARE EN LÍNEA 51
11.9 REESTABLECIMIENTO DE FÁBRICA 52
12 PERSONALIZA LA CONFIGURACIÓN 53
12.1 INTERFAZ DE USUARIO 53
12.2 VOZ 54
12.3 HORARIOS DE TIMBRE 54
12.4 OPCIONES DE PUNZONADO DE ESTADOS 55
12.5 ASIGNACIONES DE TECLAS DE ACCESO DIRECTO 57
13 GESTIÓN DE DATOS 59
14 INTERCOMUNICADOR 61
14.1 CONFIGURACIÓN SIP 61
14.1.1 USO DE LA RED DE ÁREA LOCAL 62
14.1.2 SERVIDOR SIP 63
14.2 CONFIGURACIÓN DEL TIMBRE 67
14.3 CONFIGURACIÓN DEL ONVIF 68
15 CONTROL DE ACCESO 70
15.1 OPCIONES DE CONTROL DE ACCESO 71
15.2 CONFIGURACIÓN DE LAS REGLAS HORARIAS 73
15.3 VACACIONES 74
15.4 VERIFICACIÓN COMBINADA 75
15.5 CONFIGURACIÓN DE LAS OPCIONES DE COACCIÓN 76

16 ADMINISTRADOR DE USB 77
16.1 DESCARGA USB 77
16.2 CARGA USB 78
17 BÚSQUEDA DE ASISTENCIA 79
18 AUTOTEST 81
19 INFORMACIÓN DEL SISTEMA 82
20 CONECTAR AL SOFTWARE ZKBIO CVACCESS 83
20.1 ESTABLECER LA DIRECCIÓN DE COMUNICACIÓN 83
20.2 AÑADIR DISPOSITIVO EN EL SOFTWARE 83
20.3 AÑADIR PERSONAL AL PROGRAMA INFORMÁTICO Y AL REGISTRO EN LÍNEA DE HUELLAS DACTILARES/ROSTRO 84
21 CONECTAR CON EL SOFTWARE ZKBIO TIME 88
21.1 ESTABLEZCA LA DIRECCIÓN DE COMUNICACIÓN 88
21.2 AÑADIR DISPOSITIVO EN EL SOFTWARE 88
21.3 AÑADIR PERSONAL AL SOFTWARE Y AL REGISTRO DE HUELLAS DACTILARES EN LÍNEA 89
22 CONEXIÓN A ZKBIO ZLINK WEB 91
22.1 REGISTRE SU CUENTA 91
22.2 AÑADIR DISPOSITIVO 92
22.2.1 ESTABLECER ORGANIZACIÓN (AGREGAR PERSONA) 93
22.2.2 AÑADIR DISPOSITIVO 95
22.3 FRANJA HORARIA 96
22.3.1 AJUSTAR FRANJA HORARIA 97
22.3.2 PROGRAMAR LA HORA DE ACCESO A LA PUERTA 97
22.3.3 ESTABLECER LA HORA DE ACCESO AL GRUPO 98
22.4 SINCRONIZAR PERSONA A DISPOSITIVO 99
22.5 REGISTRO DE USUARIOS 100
22.5.1 REGISTRAR UN NOMBRE Y UN IDENTIFICADOR DE USUARIO 100
22.5.2 ESTABLECER EL ROL DEL USUARIO 102
22.5.3 REGISTRAR HUELLA DACTILAR 103
22.5.4 PLANTILLA DE REGISTRO FACIAL 104
22.5.5 REGISTRAR CONTRASEÑA 105
22.5.6 REGISTRO DE TARJETA 106
22.6 BÚSQUEDA DE DATOS 108
22.6.1 TABLERO 108
22.6.2 INFORME DEL EVENTO 109
23 CONEXIÓN CON LA APLICACIÓN ZKBIO ZLINK 110
23.1 REGISTRAR CUENTA 110
23.2 AÑADIR PERSONA 111
23.3 AÑADIR DISPOSITIVO 112
23.3.1 AÑADIR SITIO Y ZONA 113
23.3.2 AÑADIR DISPOSITIVO 114

24 CONEXIÓN AL TIMBRE INALÁMBRICO.....117
24.1 CONECTE EL TIMBRE INALÁMBRICO.....117
24.2 DESVINCULAR EL TIMBRE INALÁMBRICO.....117
ANEXO.....118
REQUISITOS DE LA RECOGIDA Y EL REGISTRO EN DIRECTO DE PLANTILLAS FACIALES DE LUZ VISIBLE.....118
REQUISITOS DE LOS DATOS DE LAS PLANTILLAS FACIALES DIGITALES DE LUZ VISIBLE.....119
POLÍTICA DE PRIVACIDAD.....120
OPERACIÓN ECOLÓGICA.....123

1. Medidas de seguridad

Las siguientes instrucciones tienen la intención de garantizar que el usuario pueda usar el producto correctamente para evitar peligros o pérdidas materiales. Las siguientes precauciones son para mantener a los usuarios seguros y evitar cualquier daño. Por favor, lea atentamente antes de la instalación.
El incumplimiento de las instrucciones podría provocar daños en el producto o lesiones físicas (incluso puede causar la muerte).

1. Lea, siga y conserve las instrucciones: todas las instrucciones de seguridad y funcionamiento deben leerse y seguirse correctamente antes de poner el dispositivo en servicio.
2. No ignore las advertencias: cumpla con todas las advertencias de la unidad y de las instrucciones de funcionamiento.
3. Accesorios: use solo accesorios recomendados por el fabricante o productos vendidos. No utilice ningún otro componente que no sea el material sugerido por el fabricante.
4. Precauciones para la instalación: no coloque este dispositivo sobre un soporte o marco inestable. Puede caer 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 de CA o CC de la red y consulte al personal de servicio en las siguientes condiciones: ☐Cuando el cable o el control de conexión estén afectados. ☐ Cuando el líquido se derrame o un artículo caiga en el sistema. ☐Si el sistema está expuesto al agua o a las inclemencias de tiempo (lluvia, nieve y más). ☐Si el sistema no funciona normalmente, bajo las instrucciones de funcionamiento. Basta con cambiar los controles definidos en las instrucciones de funcionamiento. El ajuste incorrecto de los controles puede resultar en daños e involucrar a un técnico calificado para que el dispositivo vuelva a funcionar normalmente. Y no conecte varios dispositivos a un adaptador de corriente, ya que la sobrecarga del adaptador puede causar sobrecalentamiento o peligro de incendio.
7. Piezas de repuesto: cuando se requieren piezas de repuesto, los técnicos de servicio solo deben usar piezas de repuesto proporcionadas por el proveedor. Los sustitutos no autorizados pueden provocar quemaduras, descargas eléctricas u otros peligros.
8. Verificación de seguridad: al finalizar el trabajo de servicio o reparación en la unidad, solicite al técnico de servicio que realice verificaciones de seguridad para garantizar el funcionamiento adecuado del dispositivo.
9. Fuentes de alimentación: opere el sistema solo desde la forma de fuente de energía de la etiqueta. Si no está claro el tipo de fuente de alimentación que debe utilizar, llame a su distribuidor.
10. Rayos: puede instalar pararrayos externos para protegerse contra tormentas eléctricas. Evita que los potenciadores destruyan el sistema. Se recomienda instalar los dispositivos en áreas con acceso limitado.

2. Seguridad eléctrica

☐ Antes de conectar un cable externo al dispositivo, complete la conexión a tierra correctamente y configure la protección contra sobretensiones; de lo contrario, la electricidad estática dañará la placa base. ☐Asegúrese de que se haya desconectado la alimentación antes de cablear, instalar o desmontar el dispositivo. ☐Asegúrese de
que la señal conectada al dispositivo sea una señal de corriente débil (interruptor); de otra manera
Los componentes del dispositivo se dañarán. ☐Asegúrese de que se aplique el voltaje estándar
aplicable en su país o región. Si no está seguro
Acerca del voltaje estándar endosado, consulte a su compañía de energía eléctrica local. La falta de coincidencia de energía puede causar un cortocircuito o daños en el dispositivo. ☐En el caso
de daños en la fuente de alimentación, devuelva el dispositivo al personal técnico profesional o
para su manejo. ☐Para evitar interferencias, mantenga el dispositivo alejado de dispositivos de
alta radiación electromagnética, como generadores (incluidos los generadores eléctricos), radios, televisores (especialmente CRT) monitores o altavoces.

3. Seguridad de la operación

☐ Si el humo, el olor o el ruido salen del dispositivo, apague la alimentación de inmediato y
desconecte el cable de alimentación, y luego comuníquese con el centro de servicio. ☐El transporte y otras causas impredecibles pueden dañar el hardware del dispositivo. Compruebe si
el dispositivo presenta daños intensos antes de la instalación. ☐Si el dispositivo tiene defectos importantes que no puede resolver, póngase en contacto con su distribuidor lo antes posible. ☐El polvo,
la humedad y los cambios bruscos de temperatura pueden afectar a la vida útil del dispositivo. Tú
Se aconseja no guardar el dispositivo en tales condiciones. ☐No guarde el dispositivo en un
lugar que vibre. Manipule el dispositivo con cuidado. No coloque objetos pesados
objetos encima del dispositivo. ☐No aplique colofonia, alcohol, benceno, pesticidas y otras
sustancias volátiles que puedan dañar el dispositivo.
la carcasa del dispositivo. Limpie los accesorios del dispositivo con un paño suave o una pequeña cantidad de agente de limpieza. ☐Si tiene alguna pregunta técnica sobre el uso,
comuníquese con técnicos certificados o experimentados
personal.

Nota:

☐Asegúrese de que la polaridad positiva y la polaridad negativa de la fuente de alimentación de CC de 12 V estén conectadas correctamente. Una conexión inversa puede dañar el dispositivo. No es aconsejable conectar la fuente de alimentación de CA de 24 V al puerto de entrada de CC de 12 V. ☐Asegúrese de conectar los cables siguiendo la polaridad positiva y la polaridad negativa que se
muestran en el

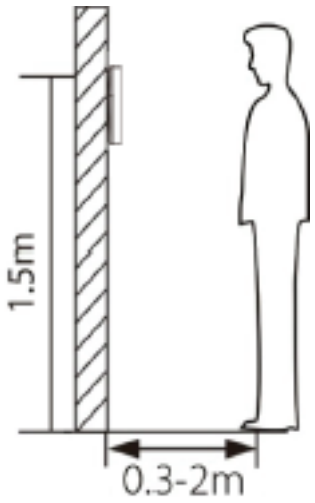
placa de identificación del dispositivo. ☐El servicio de garantía no cubre daños accidentales, daños causados por un mal funcionamiento y daños debidos a la instalación o reparación independiente del producto por parte del usuario

4. Instrucciones de uso

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

4.1 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 m a 1,85 m sea de 0,3 a 2m. Los usuarios pueden avanzar o retroceder ligeramente para mejorar la calidad de las imágenes faciales capturadas.

Postura de pie y expresión facial recomendadas





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

4.2 Registro de plantillas faciales

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



Método correcto de registro y autenticación facial. Recomendación para registrar un rostro

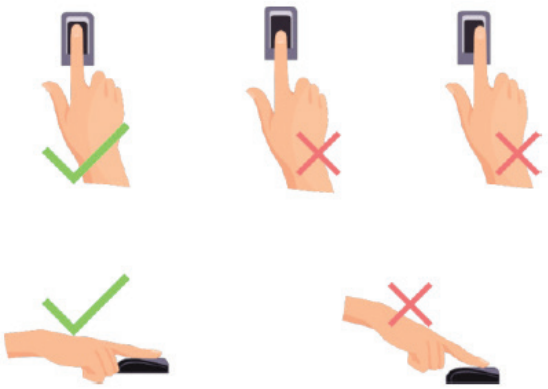
☐Al registrar una plantilla d e rostro, mantenga una distancia de 40 cm a 80 cm entre el dispositivo y la cara.☐Tenga cuidado de no cambiar su expresión facial. (Cara sonriente, cara dibujada, guiño, etc.)☐Si no sigue las instrucciones en pantalla, el registro de la pla ntilla facial puede tardar más o pueden fallar.☐Tenga cuidado de no cubrirse los ojos o las cejas. ☐No use sombreros, mascarillas, gafas de sol ni anteojos.☐Tenga cuidado de no mostrar dos caras en la pantalla. Registre a una persona a la vez.☐Se recomienda que un usuario que use anteojos registre ambos rostros con y sin gafas

☐Recomendación para autenticar una plantilla de rostro

☐Asegúrese de que la cara aparezca dentro de la guía que se muestra en la pantalla del dispositivo. ☐Si se han cambiado las gafas, la autenticación puede fallar. Si la cara sin gafas tiene se ha registrado, autentique la plantilla de la cara sin anteojos más. 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 mascarilla, un parche en el ojo o gafas de sol, Es posible que se produzca un error en la autenticación No cubra la cara, permita que el dispositivo reconozca tanto las cejas como la cara.

4.3 Posicionamiento de los dedos

Dedos recomendados: El dedo índice, medio o anular y evite usar los dedos pulgar o meñique, ya que son difíciles de presionar con precisión en el lector de huellas dactilares.



Nota: Utilice el método correcto al presionar los dedos sobre el lector de huellas dactilares para el registro y la identificación. Nuestra empresa no asumirá ninguna responsabilidad por los problemas de reconocimiento que puedan resultar del uso incorrecto del producto. Nos reservamos el derecho de interpretación y modificación final con respecto a este punto

4.4 Interfaz en espera

El dispositivo utiliza una pantalla a color de 2,4 pulgadas, en la que todas las operaciones se realizan a través del teclado. Después de conectar la fuente de alimentación, se muestra la siguiente interfaz en espera:



Introduzca cualquier número para acceder a la interfaz de entrada del ID de usuario.



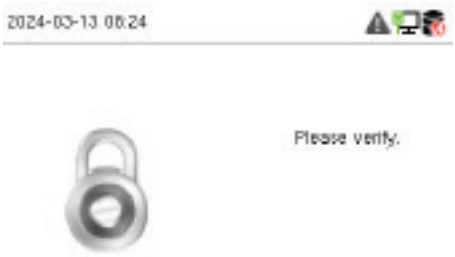


Cuando no haya un superadministrador establecido en el dispositivo, presione M/OK para ir al menú.





Después de agregar un superadministrador en el dispositivo, requiere la verificación del superadministrador antes de abrir el menú funciones.



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

En la interfaz de espera, las opciones de estado de punzonado también se pueden mostrar y utilizar directamente. El atajo las asignaciones de teclas se mostrarán en la pantalla si presiona la tecla de acceso directo correspondiente en el teclado, como se muestra en la imagen a continuación. Para conocer el método de operación específico, consulte “Asignaciones de teclas de acceso directo





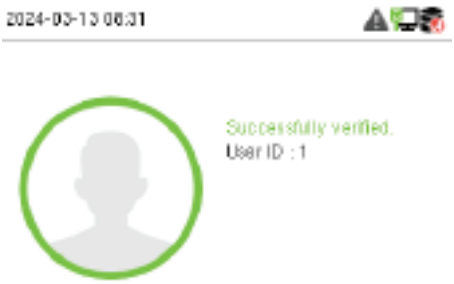
Nota: Las opciones de estado de perforación están habilitadas de forma predeterminada cuando el tipo de dispositivo se establece como un terminal de asistencia.

4.5 Modo de verificación

4.5.1Verificación facial

1: N Verificación facial

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 la solicitud emergente de un resultado de comparación exitoso.



Verificación facial 1:1

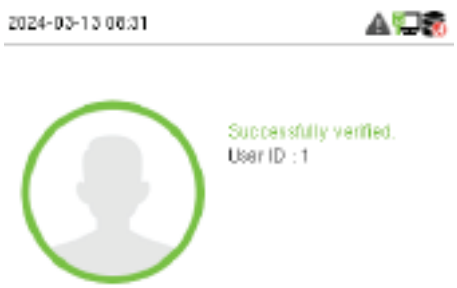
En este modo de verificación, el dispositivo compara el rostro
capturado por la cámara con la plantilla facial relacionada con el ID de usuario ingresado. Ingrese el ID de usuario y presione M/OK para ingresar al modo de verificación facial 1:1.



Si el usuario ha registrado una contraseña, una tarjeta y una huella dactilar además de la cara, y el método de verificación está establecido en Contraseña/Huella dactilar/Tarjeta/Cara, aparecerá la siguiente pantalla. Seleccione Cara para entrar en el modo de verificación facial.



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

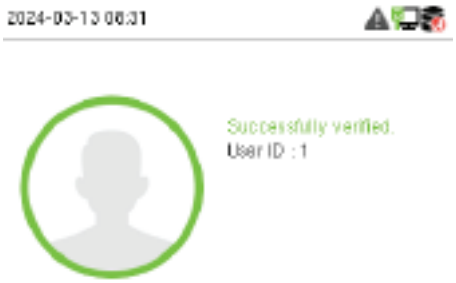


4.5.2 Verificación de huellas dactilares

1: N modo de verificación de huellas dactilares

El dispositivo compara la huella dactilar actual con los datos de huellas dactilares disponibles almacenados en su base de datos. El modo de autenticación de huellas dactilares se activa cuando un usuario coloca su dedo en el escáner de huellas dactilares. Siga la forma recomendada para colocar el dedo en el sensor. Para obtener más información, consulte la
sección Colocación de los dedos

La verificación se ha realizado correctamente:



Se ha producido un error en la verificación:



Modo de verificación de huellas dactilares 1:1

El dispositivo compara la huella digital actual con las huellas dactilares vinculadas a la ID de usuario ingresada a través del teclado virtual. En caso de que los usuarios no puedan obtener acceso utilizando el método de autenticación 1:N, pueden intentar verificar su identidad utilizando el modo de verificación 1:1. Introduzca el ID de usuario y pulse M/OK para entrar en
el modo de verificación de huellas dactilares 1:1.

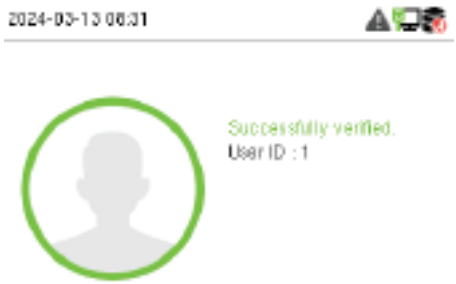


Si un empleado registra una contraseña, una tarjeta y un rostro además de la huella dactilar, aparecerá la siguiente pantalla. Seleccione Huella dactilar para ingresar al modo de verificación de huellas dactilares.



Presione la huella digital para verificar.

La verificación se ha realizado correctamente:

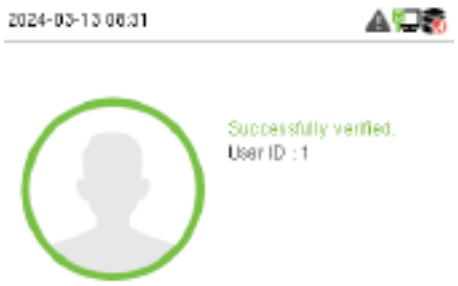


Se ha producido un error en la verificación:



4.5.3 Verificación de la tarjeta

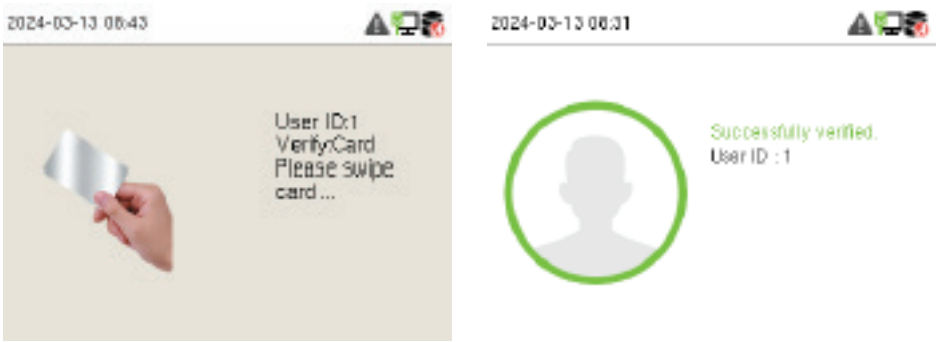
1: N Modo de verificación de tarjeta
El modo de verificación de tarjeta 1: N compara el número de tarjeta en el área de inducción de la tarjeta con todos los datos del número de tarjeta registrados
en el dispositivo. La siguiente pantalla se muestra en la pantalla de verificación de la tarjeta.



Modo de 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 el ID de usuario del empleado registrado en el dispositivo. Introduzca el ID de usuario y pulse M/OK para entrar en el modo de verificación de tarjeta 1:1



Si un empleado registra una huella dactilar, un rostro y una contraseña además de la tarjeta, aparecerá la siguiente pantalla. Seleccione Tarjeta para ingresar al modo de verificación de tarjeta.



4.5.4 Verificación de contraseña

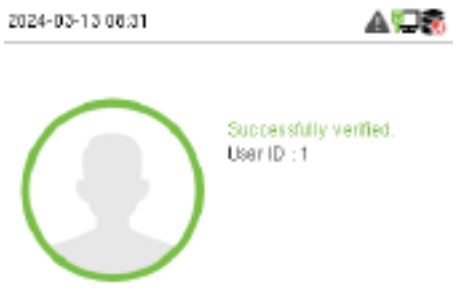
El dispositivo compara la contraseña introducida con la contraseña registrada y el ID de usuario. Introduzca el ID de usuario y pulse M/OK para entrar en el modo de verificación de contraseña 1:1. Luego, ingrese el ID de usuario y presione M / OK.





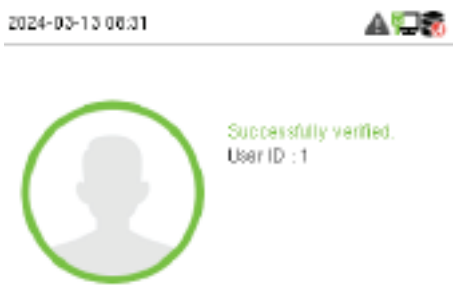
Si un empleado registra una huella dactilar, un rostro y una tarjeta además de la contraseña, aparecerá la siguiente pantalla. Seleccione Contraseña para ingresar al modo de verificación de tarjeta.





A continuación se muestran las pantallas de visualización después de ingresar una contraseña correcta y una contraseña incorrecta, respectivamente

La verificación se ha realizado correctamente:



Se ha producido un error en la verificación:



4.5.5 Verificación combinada

Este dispositivo le permite utilizar diferentes tipos de métodos de verificación para aumentar la seguridad. Hay un total de 21 combinaciones de verificación diferentes que se pueden implementar, como se enumera a continuación:
Definición de símbolo de verificación combinada

Simbólo	Definición	Explicación
/	o	Este método compara la verificación ingresada de una persona con la plantilla de verificación relacionadapreviamente almacenada en ese ID de personal en el dispositivo.
+	y	Este método compara la verificación ingresada de una persona con todas las plantillas de verificación previamente almacenadas en esa ID de personal en el dispositivo.

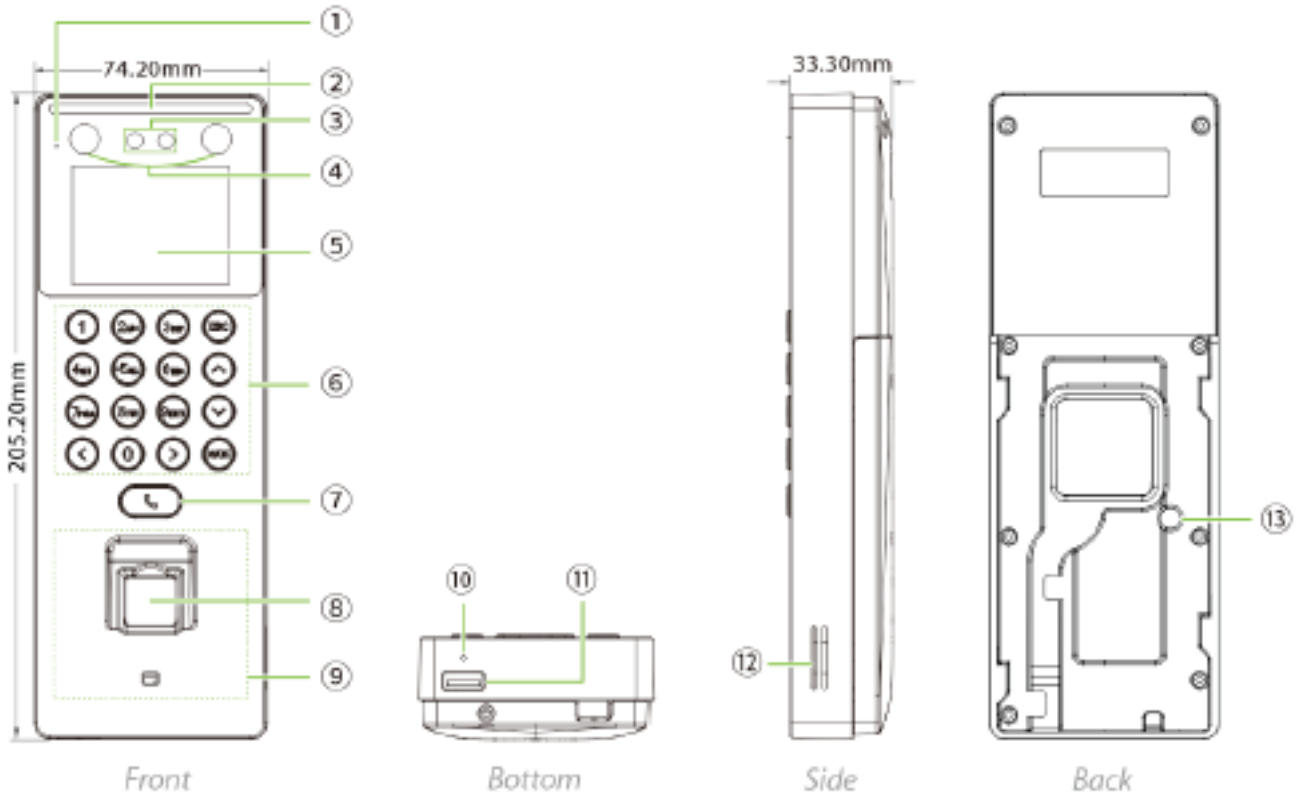


Procedimiento de configuración del modo de verificación combinado:
La verificación combinada requiere que el personal registre todos los diferentes métodos de verificación. De lo contrario, los empleados no podrán verificar con éxito el proceso de verificación combinado. Por ejemplo, si un empleado solo se ha registrado para los datos de contraseña, pero el modo de verificación del dispositivo se establece en "Contraseña + Tarjeta", el empleado no podrá completar con éxito el procedimiento de verificación.

Motivo:
Esto se debe a que el dispositivo compara la plantilla de contraseña de la persona con la registrada plantilla de verificación (tanto la Tarjeta como la Contraseña) previamente almacenada en ese ID de Personal en el Dispositivo. Pero, dado que el empleado solo ha registrado su contraseña y no su tarjeta, la verificación el proceso no se realizará correctamente y el dispositivo mostrará el mensaje "Error de verificación".

5. Visión general

5.1 Apariencia



No.	Descripción
1	Micrófono
2	Flash
3	Cámara
4	Destello de infrarrojo cercano
5	Pantalla a color de 2,4 pulgadas
6	Teclado numérico
7	Botón de timbre
8	Sensor de huellas dactilares
9	Área de lectura de tarjetas
10	Restablecimiento

11	USB
12	Orador
13	Interruptor antisabotaje

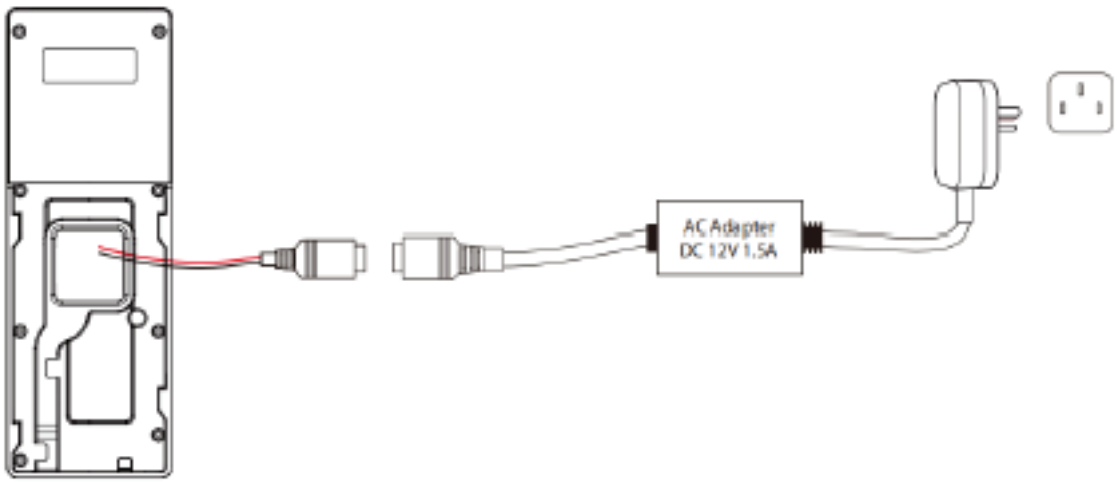
5.2 Descripción del terminal y del cableado

5.2.1Descripción del terminal

<table>
<tr><th>Definición</th><th colspan="2">Definición</th></tr>
<tr><td rowspan="6">
</td><td>NC</td><td rowspan="3">Cerradura</td></tr>
<tr><td>COM</td></tr>
<tr><td>NO</td></tr>
<tr><td>SEN</td><td rowspan="3">Sensor de puerta y botón de salida</td></tr>
<tr><td>GND</td></tr>
<tr><td>BUT</td></tr>
<tr><td>
</td><td colspan="2">Entrada de alimentación de 12 V</td></tr>
<tr><td>
</td><td colspan="2">Interfaz de red</td></tr>
</table>

5.3 Descripción del cableado

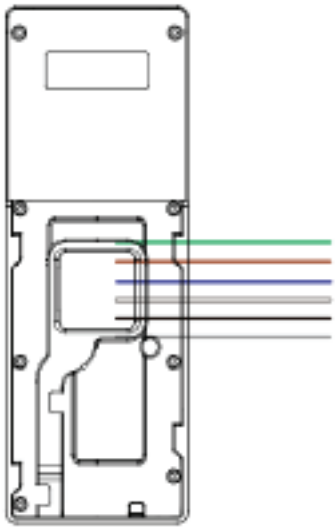
5.3.1Conexión de alimentación

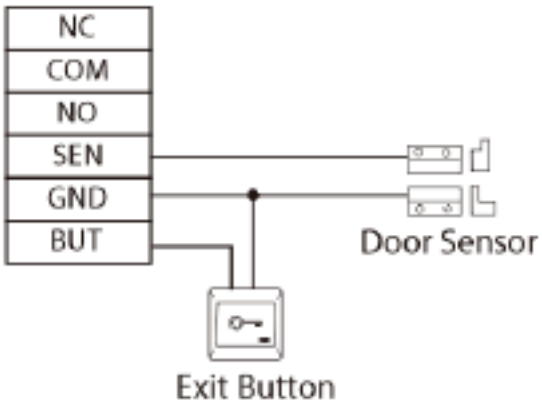


Fuente de alimentación recomendada

- Clasificación de 12 V y 1,5 A.
- Para compartir la energía del dispositivo con otros dispositivos, utilice una fuente de alimentación con clasificaciones de corriente más altas.

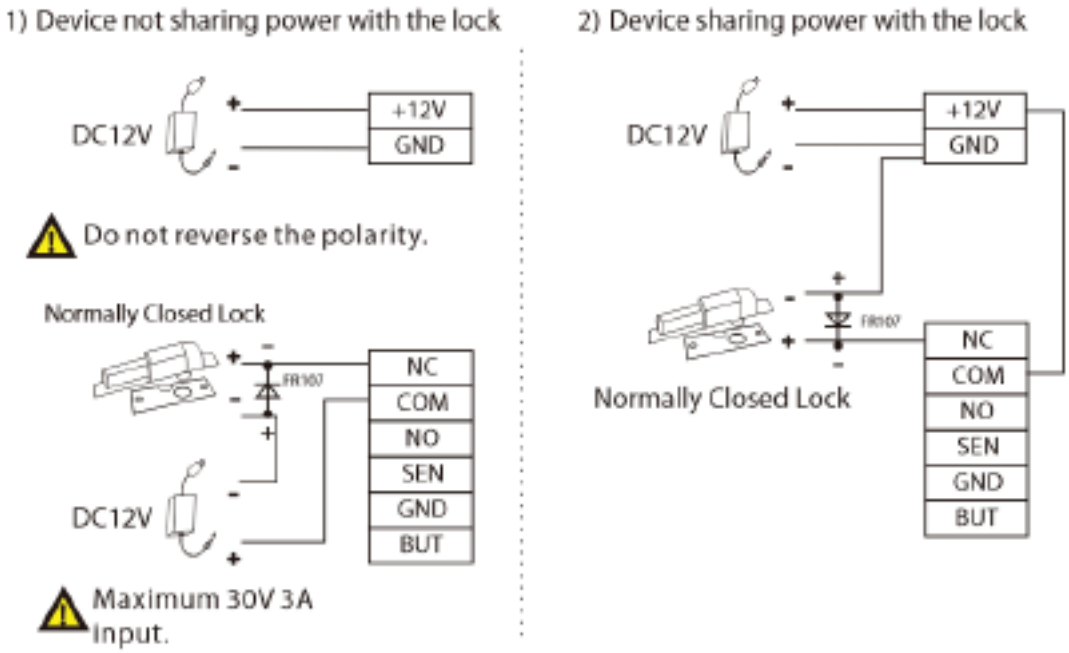
5.3.2 Conexión del sensor de puerta y del botón de salida





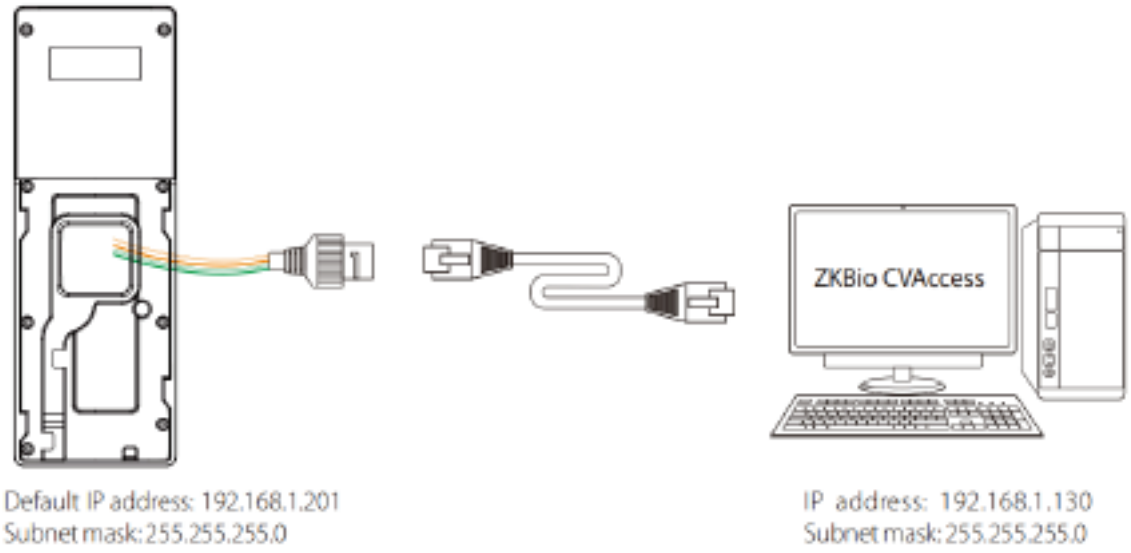
5.3.3 Conexión de relé de bloqueo

El sistema es compatible tanto con la cerradura normalmente abierta como con la cerradura normalmente cerrada. El bloqueo NA (normalmente abierto cuando está alimentado) está conectado con los terminales 'NO1' y 'COM1', y el bloqueo NC (normalmente cerrado cuando está alimentado) está conectado con los terminales 'NC1' y 'COM1'. La energía se puede compartir con la cerradura o se puede usar por separado para la cerradura, como se muestra en el ejemplo con bloqueo NC a continuación:



5.3.4 Conexión Ethernet

Conecte el dispositivo al software de la computadora mediante un cable Ethernet. A continuación se muestra un ejemplo:



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

6. Instalación

6.1 Entorno de instalación

Consulte las siguientes recomendaciones para la instalación.



KEEP DISTANCE



AVOID GLASS REFRACTION



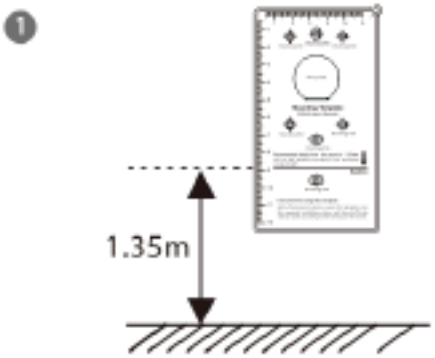
AVOID DIRECT SUNLIGHT AND EXPOSURE



AVOID USE OF ANY HEAT SOURCE NEAR THE DEVICE

6.2 Instalación del dispositivo

1. Pegue la pegatina de la plantilla de montaje a la pared y taladre agujeros de acuerdo con la pegatina de la plantilla de montaje.
2. Fije la placa posterior a la pared con tornillos de montaje en pared.
3. Conecte el dispositivo a la placa posterior.
4. Fije el dispositivo a la placa posterior con un tornillo de seguridad.









7. Menú Principal

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



No.	Descripción
El usuario Mgt.	Para agregar, editar, ver y eliminar información de un usuario.
Rol de usuario	Para establecer el alcance de los permisos del rol personalizado y el inscrito para los usuarios, por ejemplo, los derechos operativos del sistema.
COMM.	Para establecer los parámetros relevantes de red, conexión a PC, Wi-Fi★, servidor en la nube y diagnóstico de red.
Sistema	Para establecer parámetros relacionados con el sistema, incluidos Fecha y hora, Registros de asistencia/acceso, Configuración, Rostro, Huella digital, Configuración de tipo de dispositivo, Configuración de seguridad, Actualización de USB, Actualización de firmware en línea y Restablecimiento a la configuración de fábrica.
Personalizar	Para personalizar la configuración de la interfaz de usuario, la voz, los horarios de campanas, las opciones de estado de perforación y las configuraciones de asignaciones de teclas de acceso directo.
Mgt. de Datos.	Para eliminar los datos.
Intercomunicador	Para establecer los parámetros relevantes del intercomunicador, incluidos los ajustes de SIP, timbre y ONVIF.
Control de acceso	Para establecer los parámetros de la cerradura y el dispositivo de control de acceso correspondiente, incluidas opciones como Regla de tiempo, Configuración de vacaciones, Combinar verificación y Configuración de opciones de coacción.
Administrador de USB	Para cargar o descargar los datos específicos mediante una unidad USB.
Búsqueda de asistencia	Para consultar los registros de eventos especificados, consulte Fotos de asistencia y Fotos de asistencia de lista de bloqueo.
Autotest	Para probar automáticamente si cada módulo funciona correctamente, incluidos el LCDScreen, el audio, el micrófono, el teclado, el sensor de huellas dactilares, la cámara y el reloj en tiempo real.
Información del sistema	Para ver la política de privacidad, la capacidad de datos y la información del dispositivo y firmware del dispositivo actual.

8. Gestión de usuarios

8.1 Registro de nuevos usuarios

Cuando el dispositivo esté en la interfaz inicial, pulse M/OK e introduzca [User Mgt.] > [New User].





8.1.1 Registre un ID de usuario y un nombre

Introduzca el ID de usuario y el nombre.



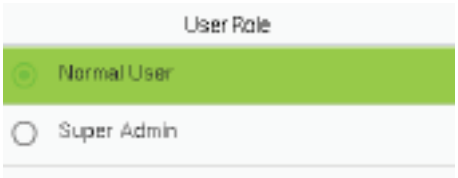
Nota:

1. Un nombre puede tener hasta 36 caracteres.
2. El ID de usuario puede contener de 1 a 14 dígitos de forma predeterminada, admitiendo números y caracteres alfabéticos.
3. Durante el registro inicial, puede modificar su ID, pero no después del registro.
4. Si aparece el mensaje "¡Duplicado!", debe elegir un ID de usuario diferente porque el que ingresó ya existe.

8.1.2 Rol de usuario

En la nueva interfaz de usuario, seleccione Rol de usuario para establecer el rol del suario como Usuario normal o SuperAdmin.

- Superadministrador: El superadministrador posee todos los privilegios de gestión del dispositivo.
- Usuario normal: Si el superadministrador ya está registrado en el dispositivo, los usuarios normales no tiene el privilegio de administrar el sistema y solo puede acceder a verificaciones auténticas.
- Roles definidos por el usuario: Al usuario normal también se le pueden asignar roles personalizados con el rol definido por el usuario. Se puede permitir al usuario acceder a varias opciones de menú según sea necesario.



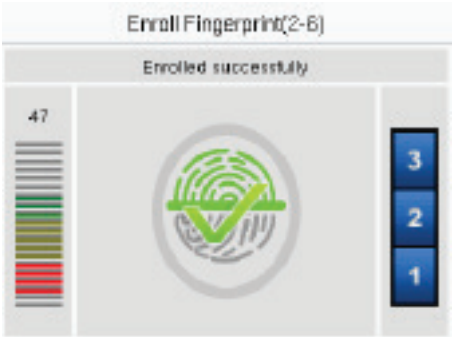
Nota: Si el rol de usuario seleccionado es el Super Admin, entonces el usuario debe pasar la autenticación de identidad para acceder al menú principal. La autenticación se basa en los métodos de autenticación que el superadministrador ha registrado.

8.1.3 Registrar huella dactilar

Seleccione Huella digital en la nueva interfaz de usuario para ingresar a la página de registro de huellas dactilares.

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





8.1.4 Cara de registro

Seleccione Cara en la nueva interfaz de usuario para ingresar a la página de registro de caras.

- Mire hacia la cámara y colóquese de tal manera que la imagen de su cara quepa dentro la caja de guía blanca y permanece quieta durante el registro facial.

- Aparece una barra de progreso mientras se registra la cara y luego se muestra el mensaje "Inscrito correctamente" a medida que se completa la barra de progreso.
- Si la cara ya está registrada, aparece el mensaje "Cara duplicada".

El registro la interfaz es la siguiente:

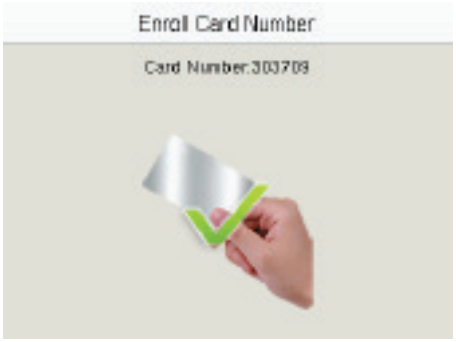


8.1.5 Tarjeta

Seleccione Tarjeta en la nueva interfaz de usuario 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 será si la tarjeta ya ha sido registrada, aparecerá el mensaje "¡Error! Tarjeta ya inscrita". La interfaz de registro aparece de la siguiente manera:





8.1.6 Contraseña

Seleccione Contraseña en la nueva interfaz de usuario 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 presione M/OK.
- Si la contraseña reingresada es diferente de la contraseña ingresada inicialmente, el dispositivo solicita el mensaje "¡La contraseña no coincide!", donde el usuario debe volver a confirmar la contraseña.
- La contraseña puede contener de 6 a 8 dígitos de forma predeterminada.



8.1.7 Foto de perfil

Seleccione Foto de perfil en la nueva interfaz de usuario para ir a la página de registro de foto de perfil.



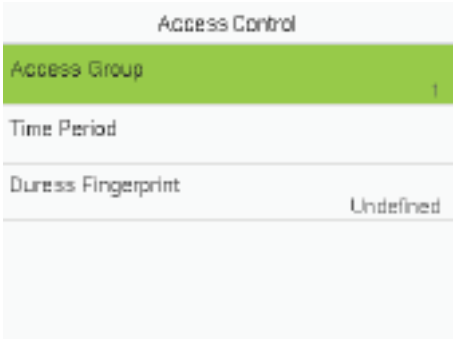
- Toque Foto de perfil, se abrirá la cámara del dispositivo, luego presione M/OK para tomar una foto. La foto capturada se muestra en la esquina superior izquierda de la pantalla.

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

8.1.8 Función de control de acceso

La función de control de acceso establece el privilegio de acceso a la puerta para cada usuario. Incluye el grupo de acceso, el período de tiempo y la huella digital de coacción.

- Introduzca [Rol de control de acceso] > [Grupo de acceso] para asignar los usuarios registrados a diferentes grupos para una mejor gestión. Los nuevos usuarios pertenecen al Grupo 1 de forma predeterminada y se pueden reasignar a otros grupos. El dispositivo admite hasta 99 grupos de control de acceso.
- Toque Período de tiempo para seleccionar el tiempo de uso.
- El usuario puede especificar una o más huellas dactilares que se hayan registrado como huellas dactilares coaccionadas. Cuando presione el dedo correspondiente a la huella digital de coacción en el sensor y pase la verificación, el sistema generará inmediatamente una alarma de coacción.



8.2 Todos los usuarios

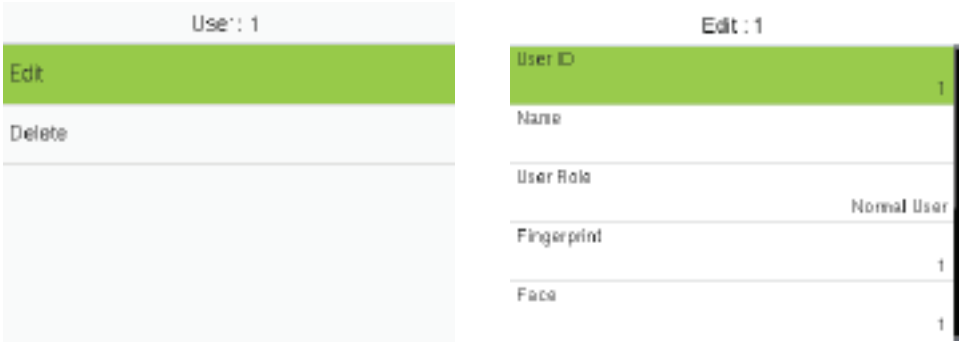
Cuando el dispositivo esté en la interfaz inicial, presione M/OK e ingrese [User Mgt.] >[Todos los usuarios].

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



8.2.1 Editar usuario

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



Nota: El proceso de edición de la información del usuario es el mismo que el de agregar un nuevo usuario, excepto que el ID de usuario no se puede modificar mientras se edita un
usuario. El proceso en detalle se refiere al "Registro de Usuario".

8.2.2 Eliminar usuario

En la interfaz Todos los usuarios, toque el usuario requerido de la lista y toque Eliminar para eliminar el usuario o la información específica del usuario del dispositivo. En la interfaz Eliminar, toque la operación requerida y luego presione M/OK para confirmar la eliminación.

Operaciones de eliminación:

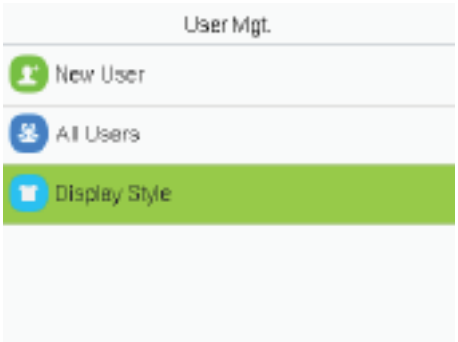
- Eliminar usuario: Elimina toda la información del usuario (elimina el usuario seleccionado en su totalidad) del dispositivo.
- Solo eliminar rol de usuario: Elimina los privilegios de administrador del usuario y convierte al usuario en un usuario normal.
- Eliminar solo huella digital: Elimina la información de la huella digital del usuario seleccionado.
- Eliminar solo rostro: Elimina la información facial del usuario seleccionado.
- Eliminar solo contraseña: Elimina la información de la contraseña del usuario seleccionado.
- Eliminar solo número de tarjeta: Elimina la información de la tarjeta del usuario seleccionado.
- Eliminar solo foto de perfil: Elimina la foto de perfil del usuario seleccionado.





8.3 Estilo de visualización

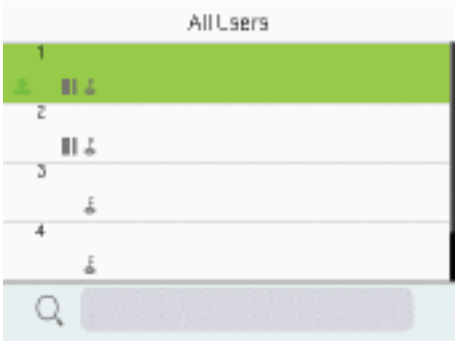
Cuando el dispositivo esté en la interfaz inicial, pulse M/OK e introduzca [User Mgt.] > [Estilo de visualización].



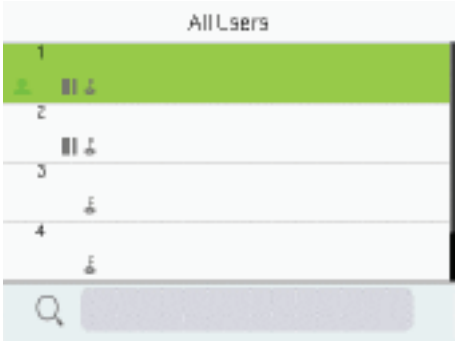


Todos los estilos de visualización se muestran a continuación:

Línea múltiple:



Línea Mixta:



9. Rol de usuario

Rol de usuario le permite asignar permisos específicos a ciertos usuarios en función de sus requisitos.

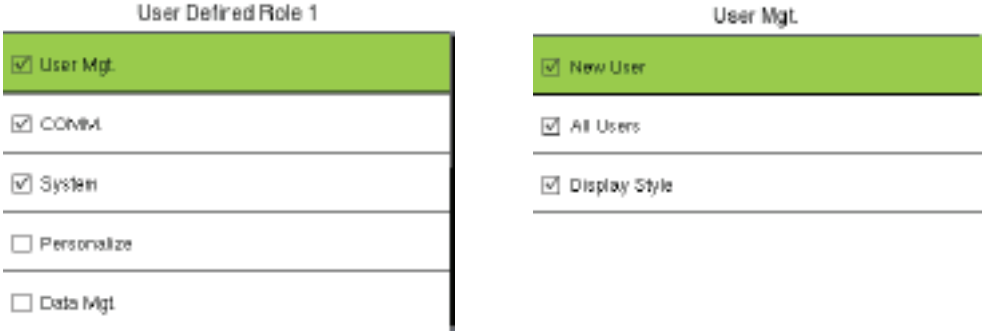
- Cuando el dispositivo esté en la interfaz inicial, presione M/OK e ingrese [Rol de usuario] > [Rol definido por el usuario] para establecer los permisos definidos por el usuario.
- El alcance de permisos del rol personalizado se puede configurar en 3 roles, es decir, el funcionamiento personalizado alcance de las funciones del menú del usuario.



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



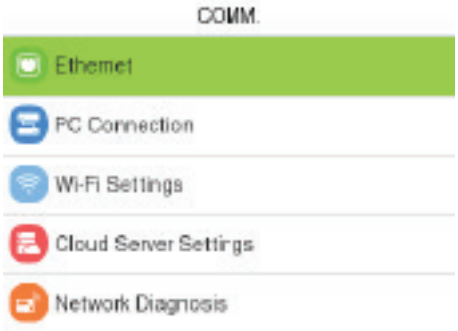
- A continuación, seleccionando en Definir rol de usuario, seleccione los privilegios necesarios para el nuevo rol y, a continuación presione la tecla M/OK.
- Primero toque el nombre de la función del menú principal requerida, luego presione M/OK y seleccione su sub-menú de la lista.



Nota: Si el rol de usuario está habilitado para el dispositivo, ingrese [Administrador de usuario] > [Nuevo usuario] > [Rol de usuario] para asignar los roles creados a los usuarios requeridos. Pero si no hay un superadministrador registrado en el dispositivo, el dispositivo solicitará "¡Inscriba primero al superadministrador!" al habilitar la función de rol de usuario.

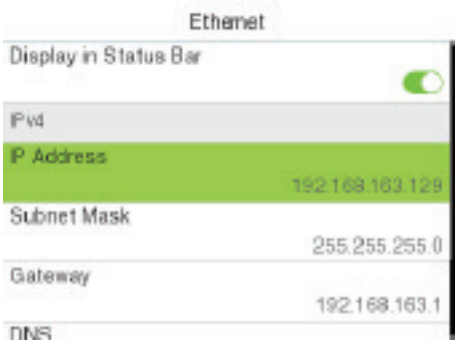
10. Comunicación

La configuración de comunicación se utiliza para establecer los parámetros de la red, la conexión a la PC, Wi-Fi★, el servidor en la nube y el diagnóstico de red. Cuando el dispositivo esté en la interfaz inicial, presione M / OK y seleccione COMM.



10.1 Ethernet

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



Nombre de la función	Descripción
Visualización en la barra de estado	Alternar para establecer si se muestra el icono de red en la barra de estado.
Dirección IP	La dirección IP predeterminada es 192.168.1.201. Se puede modificar según la disponibilidad de la red.
Máscara de subred	La máscara de subred predeterminada es 255.255.255.0. Se puede modificar según la disponibilidad de la red.

Entrada	La dirección de puerta de enlace predeterminada es 0.0.0.0. Se puede modificar según la disponibilidad de la red.
DNS	La dirección DNS predeterminada es 0.0.0.0. Se puede modificar según la disponibilidad de la red.
DHCP	El protocolo de configuración dinámica de host asigna dinámicamente las direcciones IP de los clientes a través del servidor.

10.2 Conexión a PC

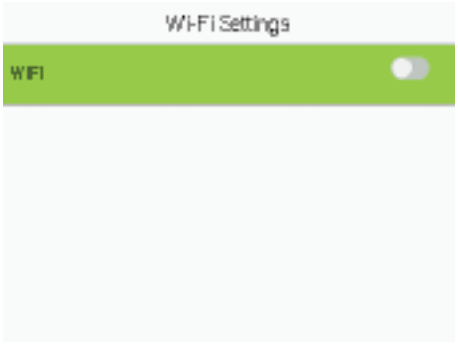
Comm Key facilita mejorar la seguridad de los datos mediante la configuración de la comunicación entre el dispositivo y la PC. Una vez que se establece la tecla de comunicación, se requiere una contraseña para conectar el dispositivo al software de la PC. Seleccione Conexión de PC en la interfaz de configuración de COMM. para configurar los ajustes de comunicación.



Nombre de la función	Descripción
Tecla de comunicación	La contraseña predeterminada es 0 y se puede cambiar. La tecla de comunicación puede contener de 1 a 6 dígitos
ID de dispositivo	Es el número de identificación del dispositivo, que oscila entre 1 y 254.
Puerto TCP COMM	El valor predeterminado de fábrica es 4370. Establezca el valor según los requisitos.
HTTPS	Para aumentar la seguridad del acceso al software, los usuarios pueden habilitar el protocolo HTTPS para crear una transmisión de red segura y encriptada y garantizar la seguridad de los datos enviados a través de la autenticación de identidad y la comunicación encriptada. Esta función está habilitada de forma predeterminada. Esta función se puede habilitar o deshabilitar a través de la interfaz del menú, y al cambiar el estado de HTTPS, el dispositivo mostrará un mensaje de seguridad y se reiniciará después de la confirmación.

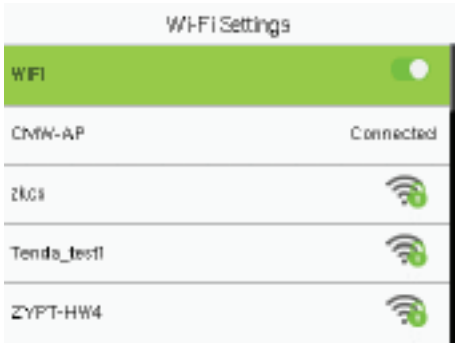
10.3 Configuración de Wi-Fi★

El dispositivo proporciona un módulo Wi-Fi, que puede estar integrado dentro del módulo del dispositivo o puede 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. Wi-Fi está habilitado de forma predeterminada en el dispositivo. Si no necesita usar la red Wi-Fi, puede alternar el Wi-Fi para desactivar el botón. Seleccione Configuración de Wi-Fien la interfaz de Configuración de COMM. para configurar los ajustes de Wi-Fi.



Búsqueda en la red Wi-Fi

- El Wi-Fi está activado por defecto en el dispositivo. Activa o desactiva el Wi-Fi pulsando el botón.
- Una vez que se enciende el Wi-Fi, el dispositivo buscará el Wi-Fi disponible dentro del alcance de la red.
- Toque el nombre de Wi-Fi requerido de la lista disponible e ingrese la contraseña correcta en el contraseña y, a continuación, pulse M/OK.



WIFI habilitado: Toque la red requerida de la lista de redes buscadas.



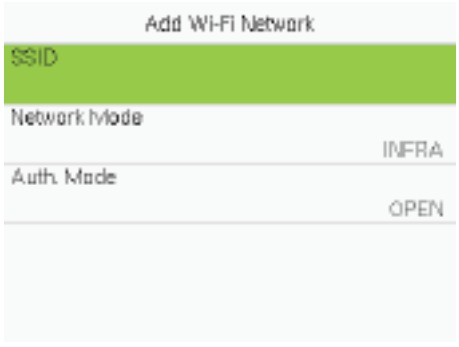
Toque el campo de contraseña para ingresar el contraseña y presione M / OK .

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

Agregar red Wi-Fi manualmente
El Wi-Fi también se puede agregar manualmente si el Wi-Fi requerido no se muestra en la lista.



Toque Agregar red Wi-Fi para agregar el Wi-Fi manualmente.



En esta interfaz, introduzca los parámetros de la red Wi-Fi. (La red agregada debeexistir).

Nota: Después de agregar con éxito el Wi-Fi manualmente, siga el mismo proceso para buscar el nombre de Wi-Fi agregado.

Configuración avanzada

En la interfaz de configuración de Wi-Fi, toque Avanzado para establecer los parámetros relevantes según sea necesario.

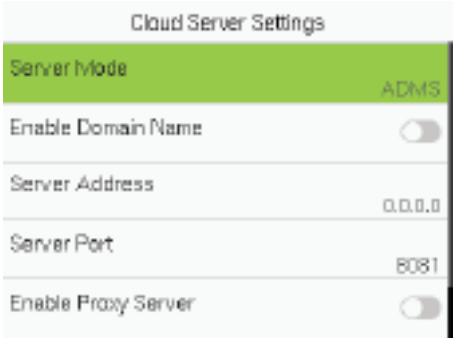




Nombre de la función	Descripción
DHCP	El protocolo de configuración dinámica de host (DHCP) asigna dinámicamente direcciones IP a los clientes de red. Si el DHCP está habilitado, la IP no se puede configurar manualmente.
Dirección IP	La dirección IP de la red Wi-Fi, el valor predeterminado es 0.0.0.0.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

10.4 Configuración del servidor en la nube

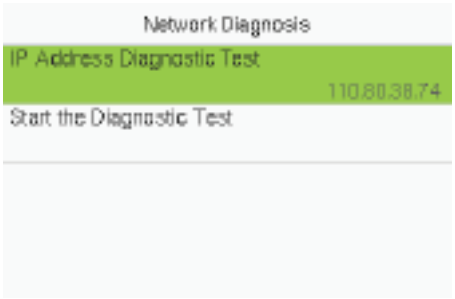
Seleccione Configuración del servidor en la nube en la interfaz Configuración de COMM. para conectarse con el servidor ADMS.



Nombre de la función		Descripción
Habilitar nombre de dominio	Dirección del servidor	Una vez que este modo está activado, el modo de nombre de dominio "http://...", como http://www.XYZ.com, mientras que "XYZ" denota el nombre de dominio.
Deshabilitar nombre de dominio	Dirección del servidor	La dirección IP del servidor ADMS
	Puerto del servidor	Puerto utilizado por el servidor ADMS.
Habilitar servidor proxy		La dirección IP y el número de puerto del servidor proxy se establecen manualmente cuando el proxy está habilitado.

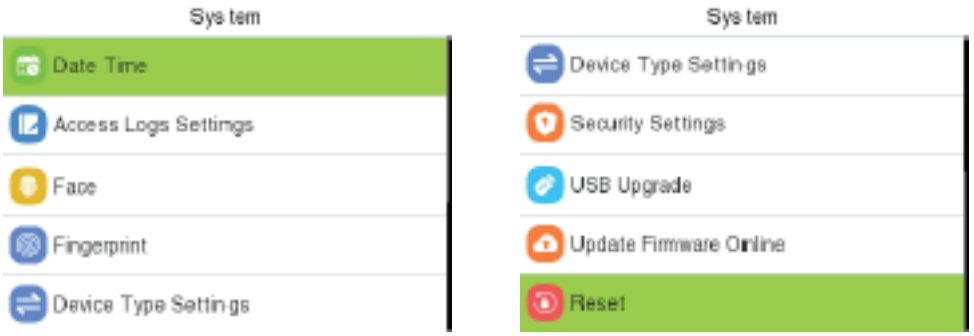
10.5 Diagnóstico de la red

Ayuda a establecer los parámetros de diagnóstico de la red. Seleccione Diagnóstico de red en la interfaz de configuración de COMM. Ingrese la dirección IP que debe diagnosticarse y toque Iniciar la prueba de diagnóstico para verificar si la red puede conectarse al dispositivo.

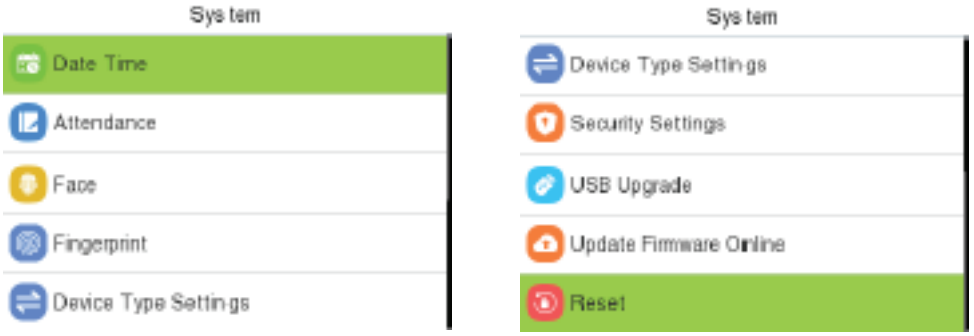


11. Configuración del sistema

Ayuda a establecer los parámetros del sistema relacionados para optimizar la accesibilidad del dispositivo. Cuando el dispositivo esté en la interfaz inicial, presione M/OK y seleccione System Access Control Terminal:

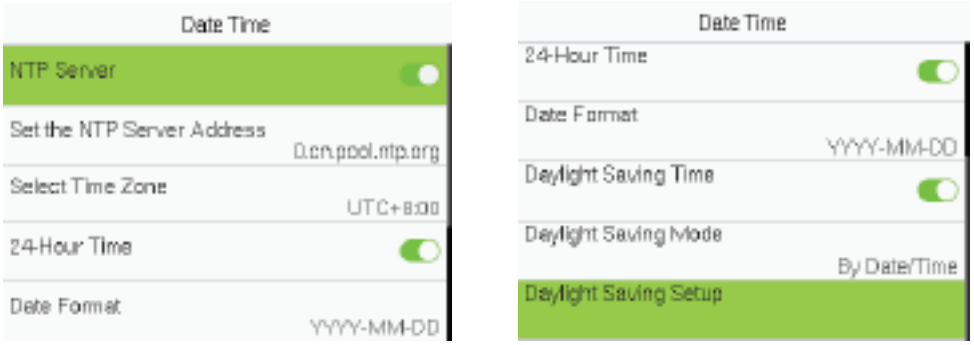


Terminal de Asistencia Horaria:



11.1 Fecha y hora

Seleccione Fecha y hora en la interfaz del sistema para establecer la fecha y la hora.

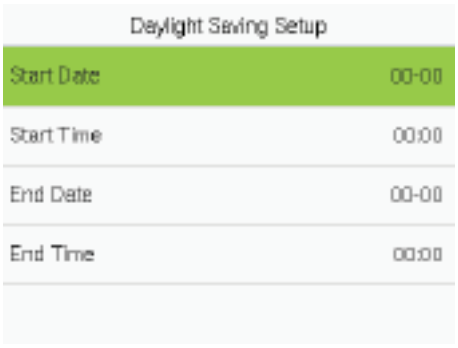


- Toque Servidor NTP para habilitar la sincronización automática de la hora en función de la dirección de servicio que ingrese.
- Toque Fecha y hora manual para configurar manualmente la fecha y la hora y luego toque Confirmar y guardar.

- Toque Seleccionar zona horaria para seleccionar manualmente la zona horaria donde se encuentra el dispositivo.
- Habilite o deshabilite este formato tocando Hora de 24 horas. Si está habilitado, toque Formato de fecha para configurar a fecha.
- Toque Horario de verano para activar o desactivar la función. Si está habilitado, toca Horario de verano para seleccionar un modo de horario de verano y, a continuación, toque Configuración de horario de verano para establecer el tiempo de conmutación.



Modo Semana



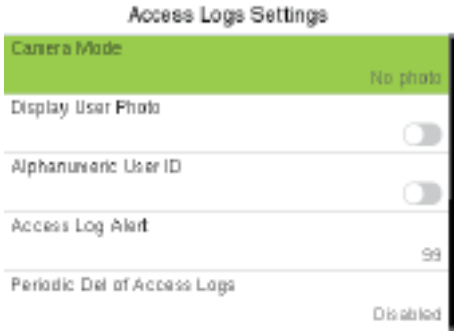
Modo de Fecha

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

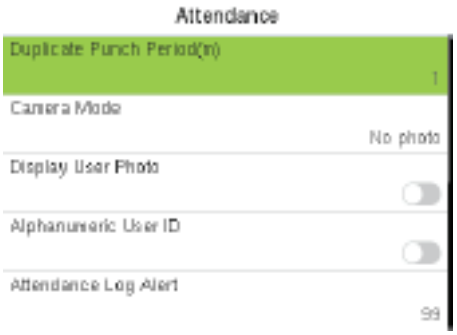
Nota: Por ejemplo, si un usuario establece la hora del dispositivo desde las 18:35 del 15 de marzo de 2020 hasta las 18:30 del 1 de enero de 2021. Después de restaurar la configuración de fábrica, la hora del dispositivo seguirá siendo a las 18:30 del 1 de enero de 2021.

11.2 Configuración de registros de acceso / Asistencia

Seleccione Configuración de registros de acceso / Asistencia en la interfaz del sistema.
Terminal de control de acceso:



Terminal de Asistencia Horaria:



Nombre de la función	Descripción
Modo de cámara	Esta función está desactivada de forma predeterminada. Cuando se habilita, un elemento de seguridad aparecerá un mensaje y el sonido del obturador en la cámara se encenderá obligatoriamente. Hay 5 modos: • Sin foto: No se toma ninguna foto durante la verificación del usuario. • Tomar foto, no guardar: la foto se toma pero no se guarda durante verificación. • Tomar foto y guardar: Todas las fotos tomadas durante la verificación son guardado. • Ahorre en una verificación exitosa: se toman fotos y se guardan para cada una Verificación exitosa. • Guardar en verificación fallida: la foto se toma y se guarda solo para cada verificación fallida.
ID de usuario alfanumérico	Habilite/deshabilite el alfanumérico como ID de usuario.
Alerta de registro de acceso	Cuando el espacio de registro del acceso de asistencia alcanza el valor umbral máximo, el dispositivo muestra automáticamente la advertencia de espacio de memoria. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999
Del periódico de los registros de acceso	Cuando los registros de acceso alcanzan su capacidad máxima, el dispositivo elimina automáticamente un conjunto de registros de acceso antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999

Del periódico de la foto de T&A	Cuando las fotos de asistencia alcanzan su capacidad máxima, el dispositivo elimina automáticamente un conjunto de fotos de asistencia antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99
Del periódico de la foto de la lista de bloqueo	Cuando las fotos de la lista de bloques alcanzan su capacidad máxima, el dispositivo elimina automáticamente un conjunto de fotos antiguas de la lista de bloques. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99
Tiempo de espera de autenticación	La cantidad de tiempo que se tarda en mostrar un mensaje de verificación correcto. Valor válido: de 1 a 9 segundos.

Descripción de la función del terminal de asistencia temporal:

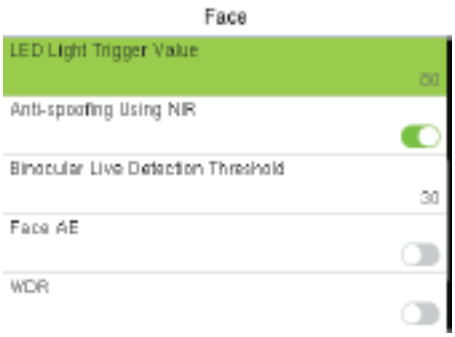
Nombre de la función	Descripción
Duplicado Período de punzonado (m)	Dentro de un período de tiempo establecido (unidad: minutos), el registro de asistencia duplicado no se reservará (el valor oscila entre 1 y 999999 minutos).
Modo de cámara	Esta función está desactivada de forma predeterminada. Cuando se habilita, un elemento de seguridad aparecerá un mensaje y el sonido del obturador en la cámara se encenderá obligatoriamente. Hay 5 modos: • Sin foto: No se toma ninguna foto durante la verificación del usuario. • Tomar foto, no guardar: la foto se toma pero no se guarda durante verificación. • Tomar foto y guardar: Todas las fotos tomadas durante la verificación son guardado. • Ahorre en una verificación exitosa: se toman fotos y se guardan para cada una • Verificación exitosa. Guardar en verificación fallida: la foto se toma y se guarda solo para cada verificación fallida.
Mostrar foto de usuario	Si se mostrará la foto del usuario cuando el usuario pase la verificación.
ID de usuario alfanumérico	Habilite/deshabilite el alfanumérico como ID de usuario.

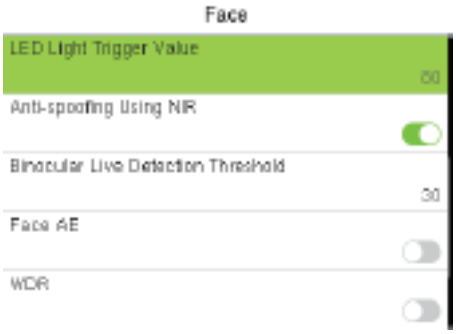
Alerta de registro de asistencia	Cuando el espacio de registro de la asistencia alcanza el valor de umbral máximo, el dispositivo muestra automáticamente la advertencia de espacio de memoria. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999.
Del periódico de los datos de T&A	Cuando los registros de asistencia alcanzan su capacidad máxima de almacenamiento, el dispositivo elimina automáticamente un conjunto de registros de asistencia antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 999.
Del periódico de la foto de T&A	Cuando las fotos de asistencia alcanzan su capacidad máxima, el dispositivo elimina automáticamente un conjunto de fotos de asistencia antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Tiempo de espera de autenticación	La cantidad de tiempo que se tarda en mostrar un mensaje de verificación correcto. Valor válido: de 1 a 9 segundos.
Intervalo(s) de reconocimiento	Después de hacer clic (seleccionar) en el intervalo de identificación, por ejemplo, si el intervalo de comparación se establece en 5 segundos, el reconocimiento facial verificará la cara cada 5 segundos. Valor válido: de 0 a 9 segundos. 0significa identificación continua, 1 a 9 significa identificación a intervalos.

11.3 Parámetros faciales

Seleccione Cara en la interfaz del sistema para ir a la configuración de parámetros de la plantilla de cara.







Nombre de la función	Descripción
Valor de umbral 1:N	En el modo de verificación 1:N, la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas sea mayor que el valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será la tasa de errores de juicio y mayor la tasa de rechazo, y viceversa. Se recomienda establecer el valor predeterminado de 47.
Valor umbral 1:1	En el modo de verificación 1:1, la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y las plantillas faciales del usuario inscritas en el dispositivo sea mayor que el valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será la tasa de errores de juicio y mayor la tasa de rechazo, y viceversa. Se recomienda establecer el valor predeterminado de 63.
Umbral de inscripción facial	Durante la inscripción facial, se utiliza la comparación 1:N para determinar si el usuario ya se ha registrado antes. Cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas es mayor que el umbral establecido, indica que la cara ya ha sido registrada.

Calidad de imagen	Es la calidad de la imagen para el registro facial y la comparación. Cuanto mayor sea el valor, más clara será la imagen necesaria.
Distancia de reconocimiento facial	Cuanto más lejos está el individuo, más pequeña es la cara y menor es el número de píxeles de la cara obtenidos por el algoritmo. Por lo tanto, el ajuste de este parámetro puede ajustar la distancia de comparación más lejana de las caras.
Valor de disparo de luz LED	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, la luz LED se encenderá o apagará con más frecuencia.
Anti-spoofing usando NIR	Uso de imágenes de espectros de infrarrojo cercano para identificar y prevenir ataques de fotos y videos falsos.
Detección binocular en vivo Umbral	Es conveniente juzgar si las imágenes espectrales del infrarrojo cercano son fotos y videos falsos. Cuanto mayor sea el valor, mejor será el rendimiento anti-spoofing de las imágenes espectrales del infrarrojo cercano.
Cara AE	Cuando la cara está frente a la cámara en el modo Face AE, el brillo del área de la cara aumenta, mientras que otras áreas se vuelven más oscuras.
Modo antiparpadeo	El amplio rango dinámico (WDR) equilibra la luz y amplía la visibilidad de la imagen para los vídeos de vigilancia en escenas de iluminación de alto contraste y mejora la identificación de objetos en entornos brillantes y oscuros.
WDR	Se utiliza cuando WDR está desactivado. Ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea a la misma frecuencia que la luz.
Algoritmo de cara	Tiene información relacionada con el algoritmo facial y pausa la actualización de la plantilla facial.

11.4 Huellas

Seleccione Huella digital en la interfaz del sistema para ir a la configuración de parámetros de huella digital.

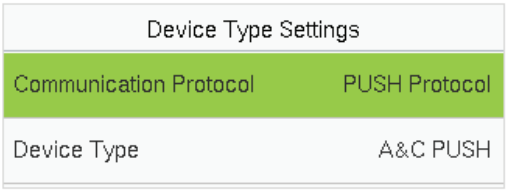


Nombre de la función	Descripción
Umbral 1:1	Bajo el método de verificación 1:1, la verificación solo será exitosa cuando la similitud entre los datos de huellas dactilares adquiridos y la plantilla de huellas dactilares asociada con el ID de usuario ingresado inscrito en el dispositivo sea mayor que el valor establecido.
Umbral 1:N	Bajo el método de verificación 1:N, la verificación solo será exitosa cuando la similitud entre los datos de huellas dactilares adquiridos y las plantillas de huellas dactilares inscritas en el dispositivo sea mayor que el valor establecido.
Sensibilidad del sensor FP	Para establecer la sensibilidad de la adquisición de huellas dactilares. Se recomienda utilizar el nivel predeterminado "Medio". Cuando el ambiente es seco, lo que resulta en una detección lenta de huellas dactilares, puede establecer el nivel en "Alto" para aumentar la sensibilidad; cuando el ambiente es húmedo, lo que dificulta la identificación de la huella dactilar, puede establecer el nivel en "Bajo"
Intentos de reintento 1:	En la verificación 1:1, los usuarios pueden olvidar la huella dactilar registrada o presionar el dedo incorrectamente. Para reducir el proceso de volver a introducir el ID de usuario, se permite el reintento.
Algoritmo de huellas dactilares	Se utiliza para cambiar la versión del algoritmo de huellas dactilares. El valor predeterminado es Finger VX13.0, puede cambiar a Finger VX10.0.

Imagen de huella dactilar	Para establecer si se muestra la imagen de la huella digital en la pantalla durante la inscripción o verificación de la huella dactilar. Hay cuatro opciones disponibles:Mostrar para inscribir: para mostrar la imagen de la huella digital en la pantalla solo durante la inscripción. Mostrar coincidencia: para mostrar la imagen de la huella dactilar en la pantalla solo durante la verificación. Mostrar siempre: para mostrar la imagen de la huella dactilar en la pantalla durante la inscripción y la verificación. Ninguno: no para mostrar la imagen de la huella dactilar.

11.5 Configuración del tipo de dispositivo

Seleccione Configuración de tipo de dispositivo en la interfaz del sistema para configurar los ajustes de tipo de dispositivo.

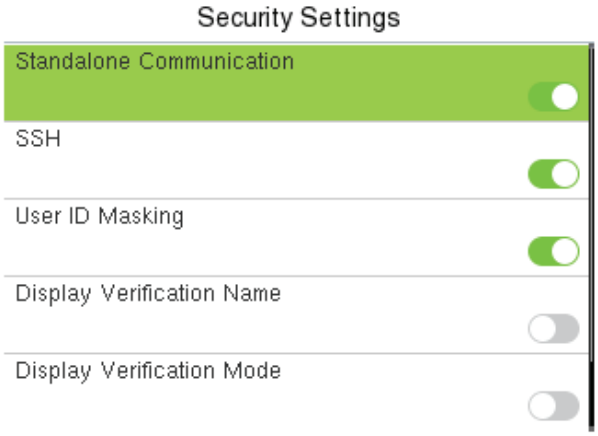


Nombre de la función	Descripción
Protocolo de comunicación	Establezca el protocolo de comunicación del dispositivo. (El mejor protocolo es adecuado para ZKBio Zlink, consulte 22 Conexión a ZKBio Zlink Web).
Tipo de dispositivo	Configure el dispositivo como terminal de control de acceso o terminal de asistencia.

Nota: Después de cambiar el tipo de dispositivo, el dispositivo eliminará todos los datos y se reiniciará, y algunas funciones se ajustarán en consecuencia.

11.6 Configuración de seguridad

Seleccione Configuración de seguridad en la interfaz del sistema para ir a la configuración de seguridad.



Nombre de la función	Descripción
Comunicación independiente	Para evitar no poder usarlo cuando el dispositivo está fuera de línea, puede descargar el software C/S (como ZKAccess 3.5) en su computadora con anticipación para usarlo sin conexión
SSH	SSH se utiliza para ingresar al fondo del dispositivo para su mantenimiento.
Enmascaramiento de ID de usuario	Cuando está habilitado, y luego el usuario se compara y verifica con éxito, el ID de usuario en el resultado de verificación mostrado se reemplazará por un * para lograr una protección segura de los datos privados confidenciales.
Mostrar nombre de verificación	Establezca si desea mostrar el nombre de usuario en la interfaz de resultados de verificación.
Modo de verificación de pantalla	Establezca si desea mostrar el modo de verificación en la interfaz
Guardar foto como plantilla	Después de deshabilitar esta función, es necesario volver a registrar la cara después de una actualización del algoritmo.

11.7 Actualización USB

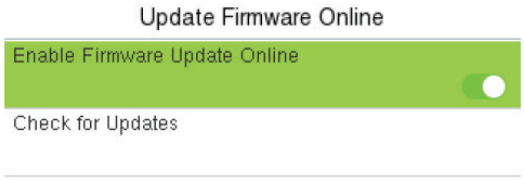
El programa de firmware del dispositivo se puede actualizar con el archivo de actualización en una unidad USB. Antes de realizar esta operación, asegúrese de que la unidad USB contenga el archivo de actualización correcto y esté insertada correctamente en el dispositivo. Si no hay ningún disco USB insertado, el sistema muestra el siguiente mensaje después de tocar Actualización USB en la interfaz del sistema. Seleccione Actualización USB en la interfaz del sistema.



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

11.8 Actualizar firmware en línea

Seleccione Actualizar firmware en línea en la interfaz del sistema.



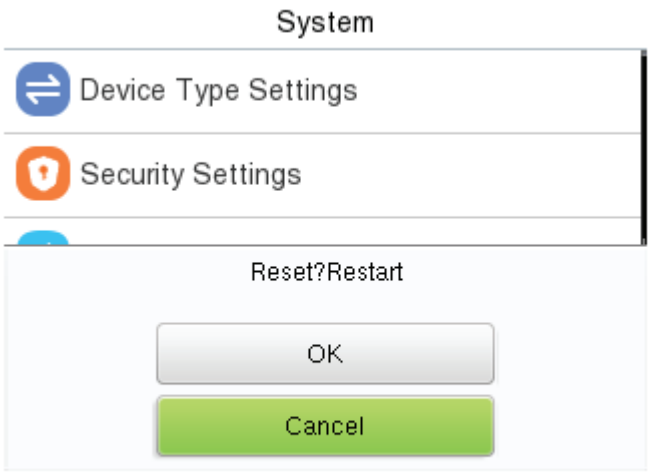
La función de actualización de firmware en línea está habilitada de forma predeterminada. Toque Buscar actualizaciones, puede tener los siguientes 3 escenarios:

- Si la consulta falla, la interfaz preguntará "Error de consulta".
- Si la versión de firmware del dispositivo es la más reciente, solicitará que la versión de firmware actual ya es la última.

Si la versión de firmware del dispositivo no es la más reciente, se mostrará el número de versión y el registro de cambios de la última versión. Los usuarios pueden elegir si desean actualizar a la última versión del firmware.

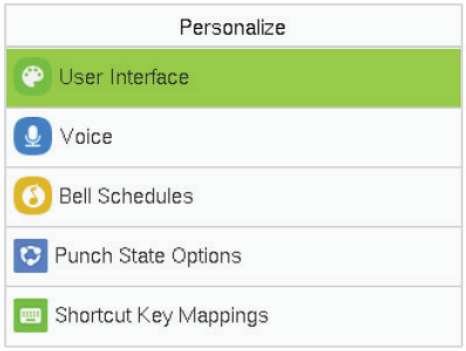
11.9 Restablecimiento de fábrica

La función de restablecimiento de fábrica restaura la configuración del dispositivo, como la configuración de comunicación y la configuración del sistema, a la configuración predeterminada de fábrica (esta función no borra los datos de usuario registrados). Seleccione Restablecer en la interfaz del sistema y, a continuación, toque Aceptar para restaurar la configuración predeterminada de fábrica.



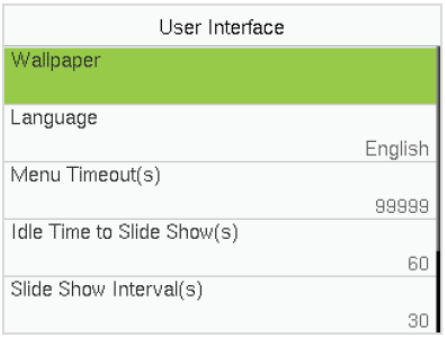
12. Personalizar la configuración

Cuando el dispositivo esté en la interfaz inicial, presione M/OK y seleccione Personalizar para personalizar la configuración de la interfaz, la voz, la campana, las opciones de estado de perforación y las asignaciones de teclas de acceso directo.



12.1 Interfaz de usuario

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



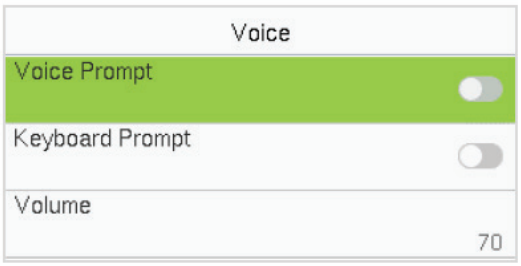


Nombre de la función	Descripción
Wallpaper	Ayuda a seleccionar el fondo de pantalla de la pantalla principal según las preferencias del usuario.
Idioma	Es útil seleccionar el idioma del dispositivo.
Tiempo de espera del menú (s)	Cuando no hay ninguna operación y el tiempo supera el valor establecido, el dispositivo vuelve automáticamente a la interfaz inicial. La función se puede desactivar o establecer el valor requerido entre 60 y 99999 segundos.
Tiempo de inactividad para presentaciones de diapositivas	Cuando no hay ninguna operación y el tiempo supera el valor establecido, se muestra una presentación de diapositivas. La función se puede desactivar, o puede establecer el valor entre 3 y 999 segundos.

Intervalo (s) de presentación de diapositivas	Es el intervalo de tiempo para cambiar entre diferentes imágenes de presentación de diapositivas. La función se puede desactivar, o puede establecer el intervalo entre 3 y 999 segundos.
Tiempo de inactividad para dormir (m)	Si el modo de suspensión está activado y cuando no hay operación en el dispositivo, el dispositivo entrará en modo de espera. Esta función se puede desactivar o establecer un valor en un plazo de 1 a 999 minutos.
Estilo de pantalla principal	El estilo de la pantalla principal se puede seleccionar según las preferencias del usuario.

12. 2 Voz

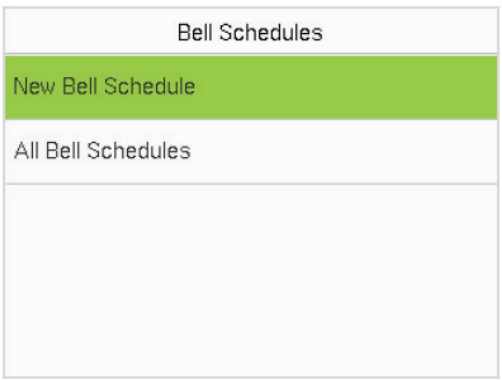
Seleccione Voz en la interfaz Personalizar para configurar los ajustes de voz.



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

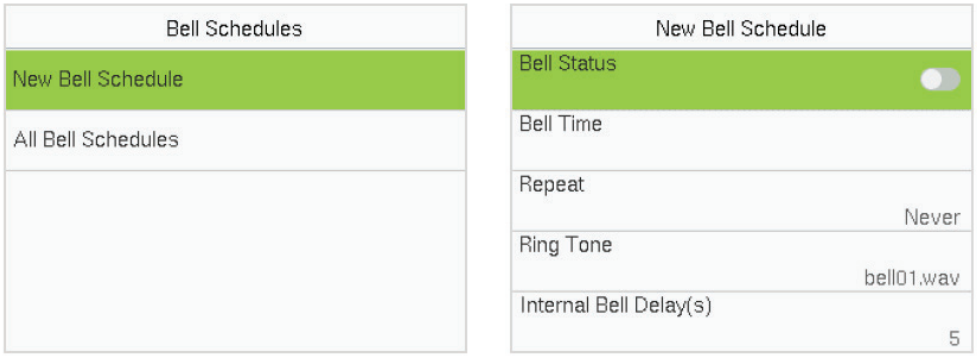
12. 3 Horarios de campanas

Seleccione «Horarios de timbre» en la interfaz «Personalizar» para configurar los ajustes del timbre.



- Nuevo horario de campanas:

Toca «Nuevo horario de timbre» en la interfaz del horario de timbre para añadir un nuevo horario de timbre.



Nombre de la función	Descripción
Estado de la campana	Alternar para habilitar o deshabilitar el estado de la campana.
Hora de la campana	Una vez que se establece el tiempo requerido, el dispositivo se activa automáticamente para hacer sonar la campana durante ese tiempo.
Repetir	Establezca el número necesario de recuentos para repetir la campana programada.
Tono	Selecciona un tono de llamada.
Retardo(s) de campana interno	Establezca el tiempo de reproducción de la campana interna. Rango de valores válidos de 1 a 999 segundos.

- Todos los horarios de las campanas:

Una vez que la campana esté programada, en la interfaz Horarios de campana, toque Todos los horarios de campana para ver la campana recién programada.

- Edite la campana programada:

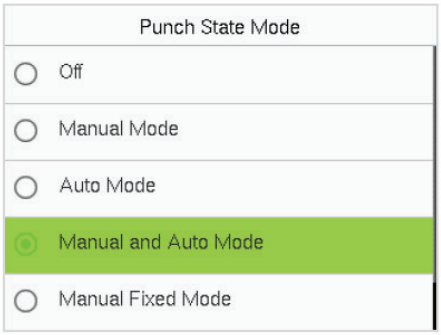
En la interfaz Todos los horarios de campanas, toque el horario de campanas requerido y toque Editar para editar el horario de campanas seleccionado. El método de edición es el mismo que las operaciones de agregar un nuevo horario de campana.

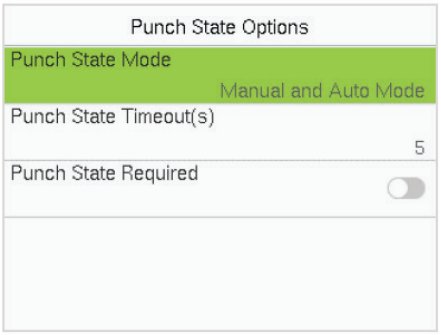
- Eliminar un horario de campana:

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

12. 4 Opciones de estados de punzón

Seleccione Opciones de estados de punzonado en la interfaz Personalizar para configurar los ajustes de estado de punzonado.

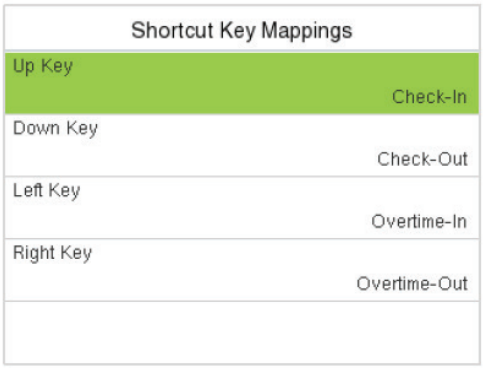




Nombre de la función	Descripción
Modo de estado de punzonado	Desactivado: Desactiva la función de estado de perforación. Por lo tanto, la clave de estado de punch establecida en el menú Asignaciones de teclas de método abreviado dejará de ser válida. Modo manual: Cambie la tecla de estado de punzonado manualmente, y la tecla de estado de punzonado desaparecerá después del tiempo de espera del estado de perforación. Modo automático: La tecla de estado de punzonado cambiará automáticamente a un estado de punzonado específico de acuerdo con el programa de tiempo predefinido que se puede configurar en las asignaciones de teclas de acceso directo. Modo manual y automático: La interfaz principal mostrará la tecla de estado de punzonado de cambio automático. Sin embargo, los usuarios aún podrán seleccionar la alternativa que es el estado de asistencia manual. Después de que se agote el tiempo de espera, el cambio manual a la tecla de estado de punzonado se convertirá en la tecla de estado de punzonado de cambio automático. Modo fijo manual: Después de que la tecla de estado de punzón se establezca manualmente en un estado de punzón particular, la función permanecerá sin cambios hasta que se vuelva a cambiar manualmente. Modo fijo: Solo se mostrará la tecla de estado de punzonado fijada manualmente. Los usuarios no pueden cambiar el estado tocando ninguna otra tecla.
Tiempo de espera del estado de punzonado	Es el tiempo durante el cual se muestra el estado de perforación. El valor oscila entre 5 y 999 segundos.
Estado de punzón requerido	Seleccione si es necesario seleccionar un estado de asistencia después de la verificación. ON: El estado de asistencia debe seleccionarse después de la verificación. OFF: No es necesario seleccionar el estado de asistencia después de la verificación. Derechos

12. 5 Mapeo de teclas de acceso directo

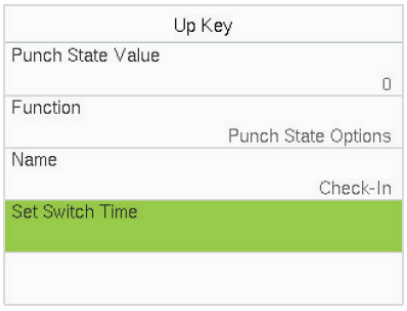
Los usuarios pueden definir teclas de acceso directo para el estado de asistencia y las teclas funcionales que se definirán en la interfaz principal. Por lo tanto, en la interfaz principal, cuando se tocan las teclas de acceso directo, se mostrará directamente el estado de asistencia correspondiente o la interfaz de función. Seleccione Asignaciones de teclas de método abreviado en la interfaz Personalizar para establecer las teclas de método abreviado necesarias.

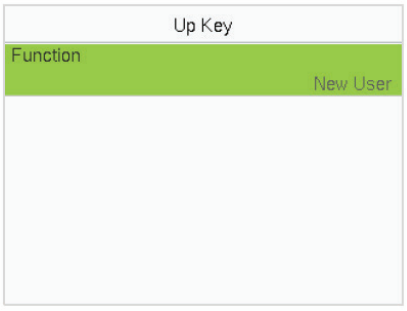


- En la interfaz Asignación de teclas de acceso rápido, pulse la tecla de acceso rápido deseada para configurar los ajustes de la tecla de acceso rápido.

- En la interfaz de teclas de acceso directo (por ejemplo, «tecla arriba»), pulse la función para configurar el proceso funcional de la tecla de acceso directo como tecla de estado de pulsación 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 tal y como se muestra en la imagen siguiente.

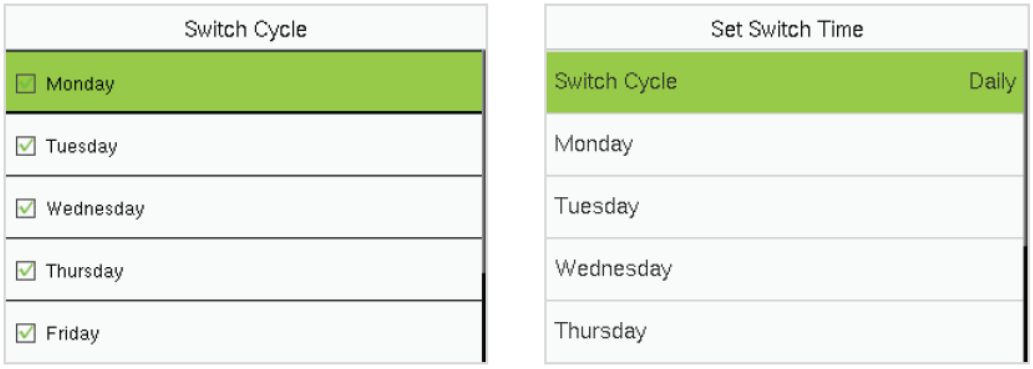




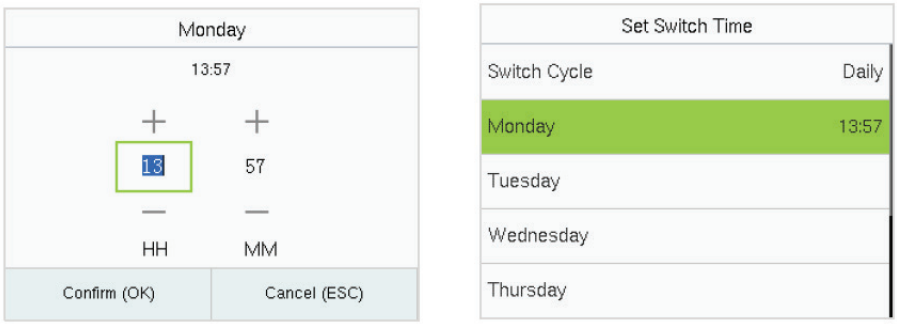
- Si la tecla de acceso directo se configura como una tecla de estado de fichaje (como fichar la entrada, fichar la salida, etc.), es necesario establecer el valor del estado de fichaje (valor válido de 0 a 250) y el nombre.

Establecer la hora del interruptor

- El tiempo de cambio se configura de acuerdo con las opciones de estado de fichaje.
- Cuando el modo de estado de fichaje está configurado en modo automático, se debe configurar el tiempo de cambio.
- En la interfaz de teclas de acceso directo, pulse «Configurar tiempo de cambio» para configurar el tiempo de cambio.
- En la interfaz «Ciclo de cambio», seleccione el ciclo de cambio (lunes, martes, etc.) como se muestra en la imagen siguiente.



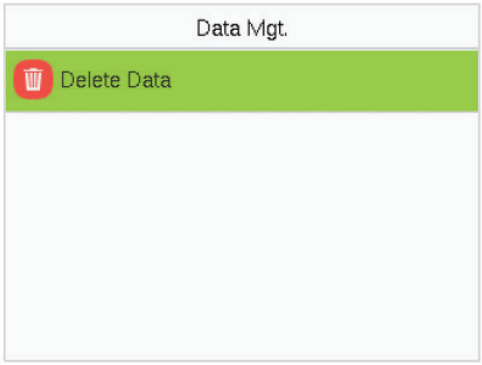
- Una vez seleccionado el ciclo de interruptor, configure la hora del interruptor para cada día y toque OK para confirmar, como se muestra en la imagen a continuación.



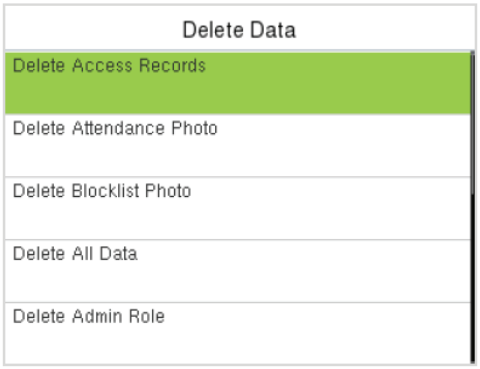
Nota: Cuando la función se establece en Indefinido, el dispositivo no habilitará la tecla de estado de perforación.

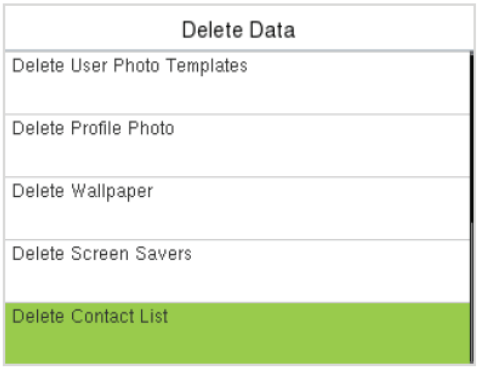
13 Gestión de datos

Cuando el dispositivo esté en la interfaz inicial, presione M/OK y seleccione Data Mgt. para administrar los datos relevantes en el dispositivo.



Seleccione Eliminar datos en la interfaz de Data Mgt. para eliminar los datos necesarios.

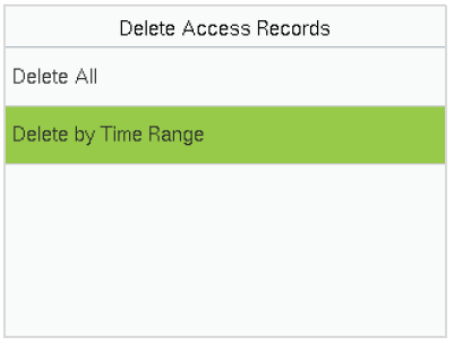


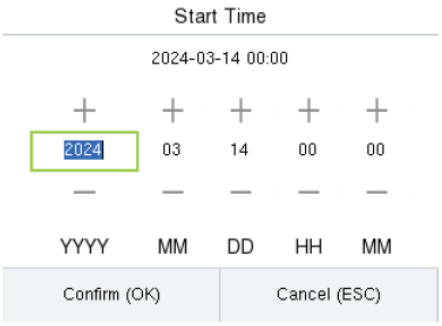


Nombre de la función	Descripción
Eliminar registros de acceso / Datos de asistencia	Para eliminar los registros de acceso y los datos de asistencia de forma condicional.
Eliminar foto de asistencia	Para eliminar las fotos de asistencia del personal designado.
Eliminar foto de la lista de bloqueo	Para eliminar las fotos tomadas durante las verificaciones fallidas
Eliminar todos los datos	Eliminar la información y los registros de acceso y datos de asistencia de todos los usuarios registrados.
Eliminar rol de administrador	Para eliminar todos los privilegios de administrador.
Eliminar control de acceso	Para eliminar todos los datos de acceso.
Eliminar plantillas de fotos de usuario	Para eliminar plantillas de fotos de usuario en el dispositivo. Al eliminar fotos de plantilla, hay un recordatorio de riesgo: "Se requiere volver a registrar la cara después de una actualización del algoritmo".

Eliminar foto de perfil	Para eliminar todas las fotos de perfil en el dispositivo.
Eliminar fondo de pantalla	Para eliminar todos los fondos de pantalla del dispositivo.
Eliminar protectores de pantalla	Para eliminar todos los protectores de pantalla del dispositivo.
Eliminar lista de contactos	Para eliminar toda la lista de contactos del videoportero en el dispositivo.

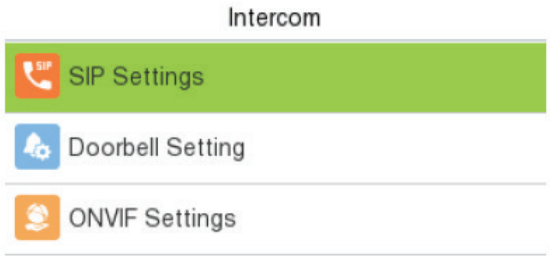
El usuario puede seleccionar Eliminar todo o Eliminar por rango de tiempo al eliminar los registros de acceso / datos de asistencia, para Eliminar por rango de tiempo, debe establecer un rango de tiempo específico para eliminar todos los datos dentro de un período específico.





14 Intercomunicador

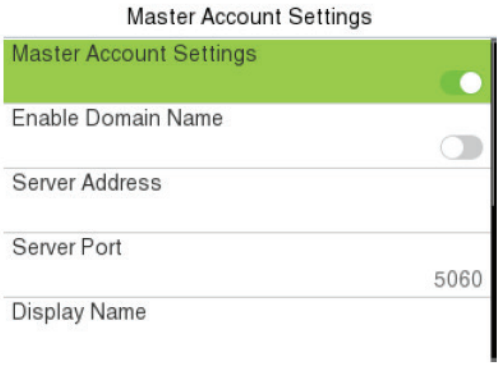
Cuando el dispositivo esté en la interfaz inicial, presione M / OK y seleccione Intercomunicador para establecer los parámetros relevantes del intercomunicador, incluidos los ajustes de SIP, timbre y ONVIF.



14.1 Configuración SIP

Seleccione Configuración SIP en la interfaz de intercomunicador para configurar los ajustes. Nota: Esta función debe utilizarse con la estación interior.





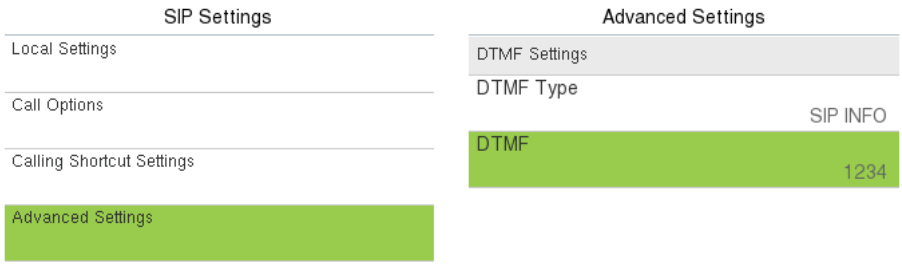
Nombre de la función		Descripción
Configuración local	Servidor SIP	Seleccione si desea habilitar el servidor SIP. Cuando está habilitado, se debe establecer la cuenta de servidor.
	Configuración de la cuenta maestra	Seleccione si desea habilitar la configuración de la cuenta maestra. Después de habilitar, es necesario establecer la dirección del servidor, el puerto del servidor, el nombre para mostrar, el nombre de usuario, el ID de verificación, la contraseña y el protocolo de transporte. (Nota: Al desactivar esta función, se desactivará la función de servidor SIP). **Habilitar nombre de dominio:** seleccione si desea habilitar el modo de nombre de dominio. **Dirección del servidor:** Introduzca la dirección del servidor. **Puerto del servidor:** Introduzca el puerto del servidor. **Nombre para mostrar:** Introduzca el nombre para mostrar del servidor. **Nombre de usuario:** Introduzca el nombre de usuario del servidor. **ID de verificación:** Introduzca el ID de verificación del servidor. **Contraseña:** Introduzca la contraseña del servidor. Protocolo de transporte: Establezca el protocolo de transporte entre el dispositivo y la estación interior.
	Configuración de la cuenta de respaldo	Seleccione si desea habilitar la configuración de la cuenta de respaldo.
	Puerto del dispositivo	Cuando utilice una red de área local para el intercomunicador, introduzca el número de puerto del dispositivo.
	Información local	Configure la información específica de ubicación del dispositivo, incluyendo el bloque, la unidad, el piso y el número de puerta.
	Protocolo de transporte	Configure el protocolo de transporte entre el dispositivo y la estación interior.
Configuración local	Retraso de llamada(s)	Establezca el tiempo de llamada, valor válido entre 30 y 60 segundos.
	Retraso de conversación(es)	Configure el tiempo del intercomunicador, valor válido entre 60 y 120 segundos.
	Configuración del volumen de llamada	Ajuste el volumen de la llamada, con valores válidos entre 0 y 100.
	Tipo de llamada	Configure el tipo de llamada como Solo voz o Voz + Vídeo.
	Configuración de respuesta automática	Seleccione si desea habilitar la función de respuesta automática. Cuando está habilitada, el dispositivo responderá automáticamente si la estación interior llama.
	Tiempo de retraso de respuesta automática	El dispositivo responderá automáticamente tras el tiempo de retardo establecido si llama la estación interior, valor válido de 0 a 10 segundos.

Lista de contactos	Cuando el servidor SIP está deshabilitado, aquí se puede agregar el número de dispositivo y la dirección de llamada de las estaciones interiores.	
Calling Shortcut Settings	Modo de llamada	Se puede configurar como Modo Estándar o Modo de Llamada Directa. En el modo Estándar, hay 3 teclas de acceso directo que se pueden definir en el dispositivo: Centro de Gestión, ROOM1 y ROOM2. Puede configurar una tecla de acceso directo para llamar a la estación interior rápidamente sin ingresar la dirección IP o el número de la estación interior cada vez. En el modo de llamada directa, el usuario puede llamar a varias estaciones interiores al mismo tiempo.
Ajustes Avanzados	Tipo DTMF	Establezca el tipo de DTMF como AUTO, SIP INFO o RFC2833.
	DTMF	El valor debe establecerse igual que el valor de DTMF en la estación interior.

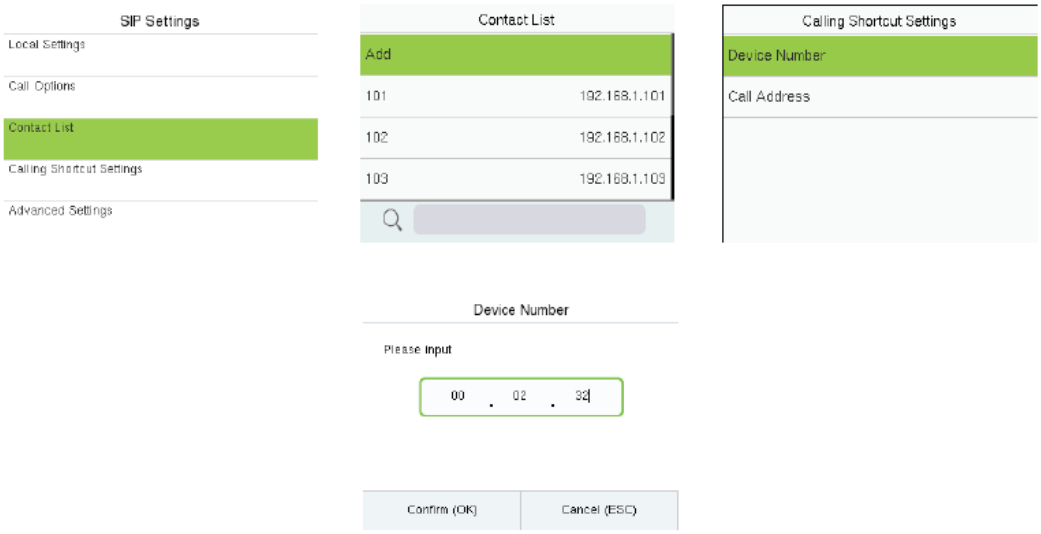
El dispositivo y la estación interior para lograr el videoportero hay dos modos, respectivamente, el servidor LAN y SIP.

14.1 Uso de la red de área local

1.Configure la estación interior en el mismo segmento de red que el dispositivo.
2.En la interfaz de configuración SIP, ingrese [Configuración avanzada] > [DTMF] para establecer el valor igual al valor de DTMF en la estación interior.

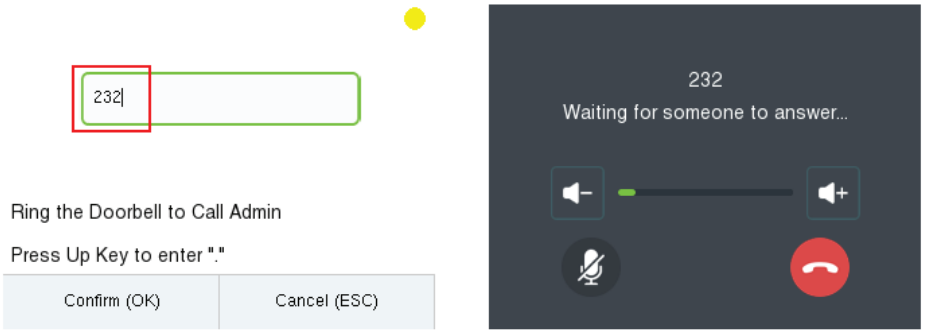


3.En la interfaz de configuración SIP, ingrese [Lista de contactos]> [Agregar] para agregar la estación interior conectada. Nota: La lista de contactos solo está disponible cuando el servidor SIP está deshabilitado.



Número de dispositivo: Personalice el número de la estación interior, puede ingresar este número en el dispositivo para llamar rápidamente a la estación interior para el videoportero. (Por ejemplo, 232 corresponde a 00.02.32 en la configuración Número de dispositivo).
Dirección de llamada: Es la dirección IP de la estación interior.

4. Para habilitar la función de videoportero, pulse el botón del timbre del dispositivo e introduzca la dirección IP o el número de la estación interior en la interfaz proporcionada.



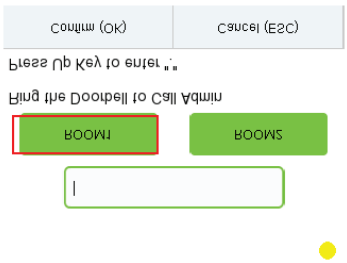
Personalizar las teclas de acceso directo de llamada

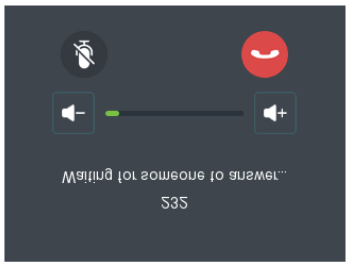
1.En la interfaz de configuración de SIP, toque Configuración de acceso directo de llamada para definir las teclas de acceso directo.



Nombre: Personaliza el nombre de las teclas de método abreviado.
Número de dispositivo: Es el número de dispositivo que se establece en el menú de la lista de contactos.
Dirección IP: Una vez que se establece el número de dispositivo, se mostrará automáticamente.

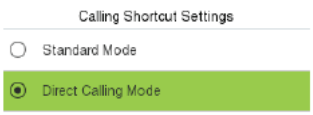
2.Luego puede presionar el botón del timbre en el dispositivo y seleccione las teclas de acceso directode llamada para llamar la estación interior.

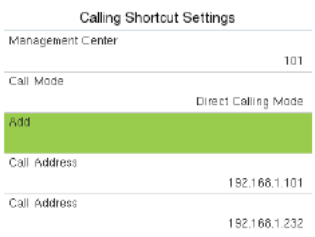


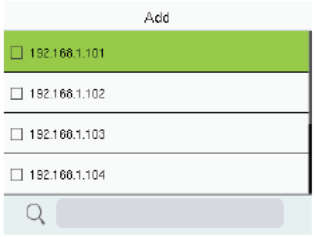


Llamadas directas

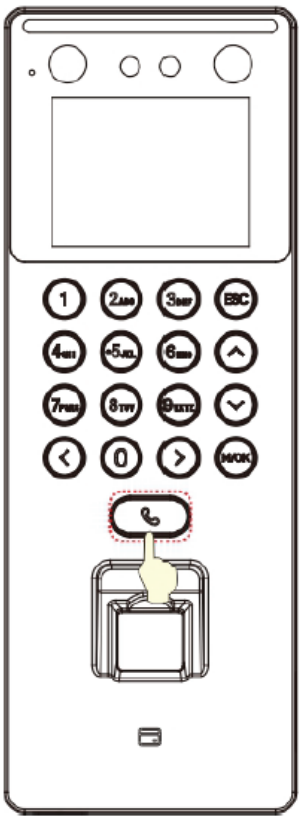
1. En la interfaz de configuración SIP, ingrese [Configuración de acceso directo de llamadas] > [Modo de llamada] > [Modo de llamada directa] > [Agregar]. Seleccione las direcciones IP de las estaciones interiores a las que desea llamar, luego las estaciones interiores se mostrarán en la lista.

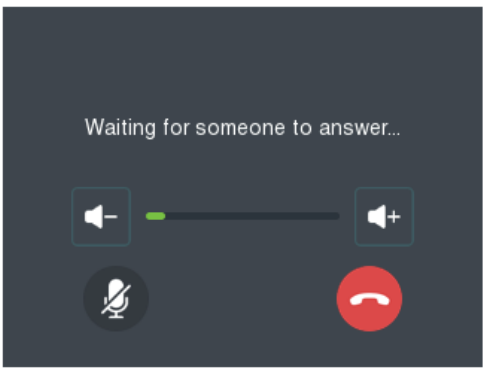






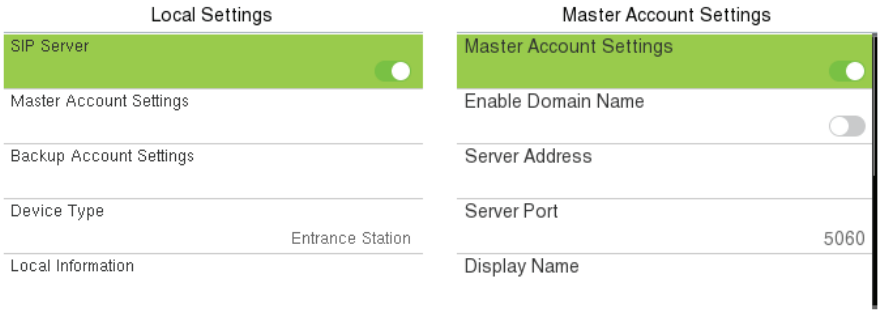
2. A continuación, puede pulsar el botón del timbre  del dispositivo para llamar a las estaciones interiores al mismo tiempo.



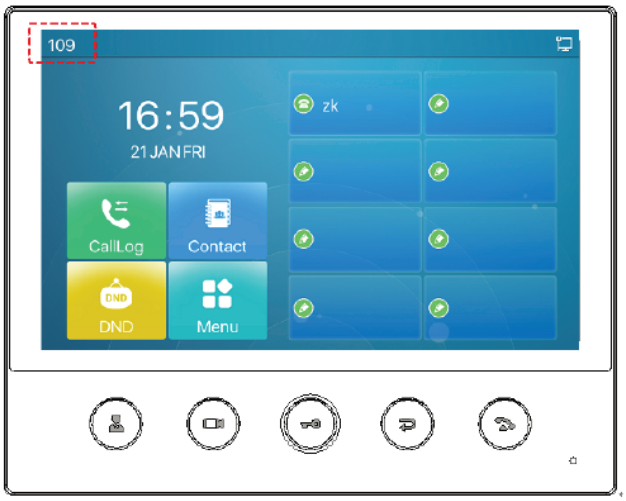


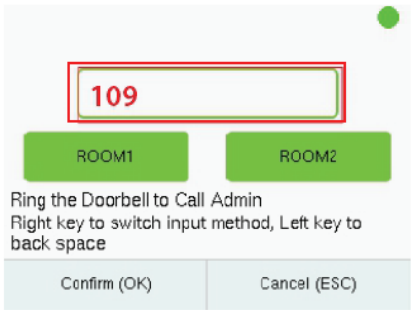
14.1.2 Servidor SIP

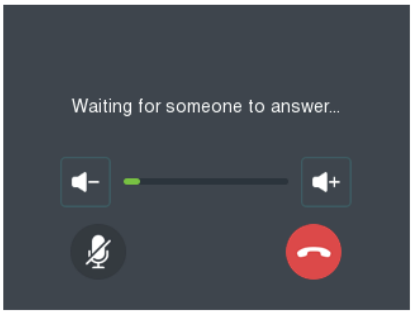
1.En la interfaz de configuración SIP, ingrese [Configuración local]> [Servidor SIP] para habilitarlo e ingrese [Configuración de la cuenta maestra] para establecer los parámetros relacionados con el servidor, como se muestra a continuación:



2. Después de configurar correctamente el SIP, el punto amarillo en la esquina superior derecha de la página de llamada se volverá verde, lo que indica que el dispositivo está conectado al servidor. A continuación, puede iniciar una llamada al nombre de la cuenta de la estación interior. Nota: Los clientes crean su propio servidor SIP.



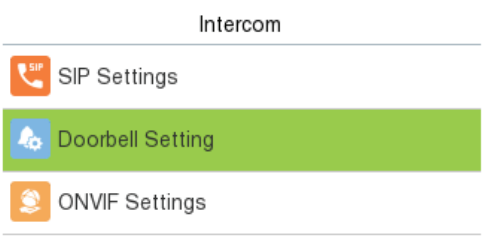


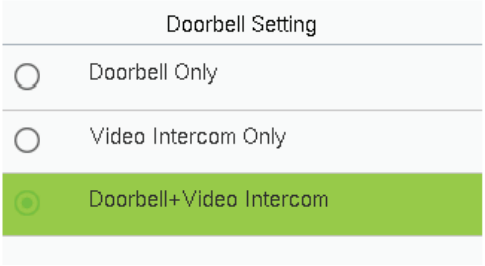


Para obtener detalles sobre el funcionamiento y el uso de la estación interior, consulte el Manual del usuario de la estación interior.

14.2 Configuración del timbre

Seleccione Configuración del timbre en la interfaz del intercomunicador para configurar el timbre.



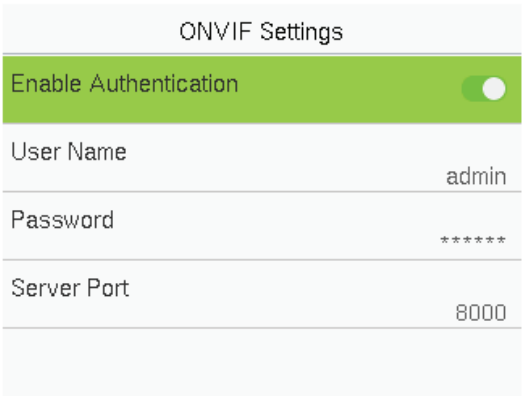


Nombre de la función	Descripción
Configuración del timbre	Solo timbre: cuando el usuario hace clic en el botón del timbre, solo suena el timbre. Solo videoportero: Cuando el usuario hace clic en el botón del timbre, solo el dispositivo realiza una llamada. Timbre+Video Intercomunicador: Cuando el usuario hace clic en el botón del timbre, suena el timbre y el dispositivo realiza una llamada al mismo tiempo.

14.3 Configuración de ONVIF

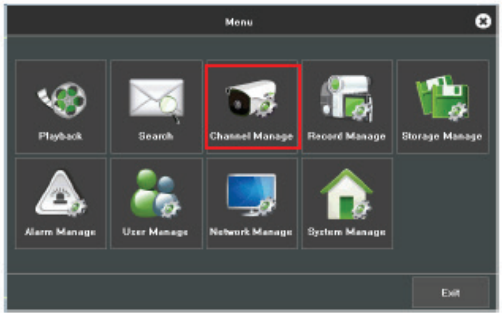
Nota: Esta función debe utilizarse con la grabadora de vídeo en red (NVR).

1.Configure el dispositivo en el mismo segmento de red que el NVR.
2.Seleccione Configuración de ONVIF en la interfaz del sistema.

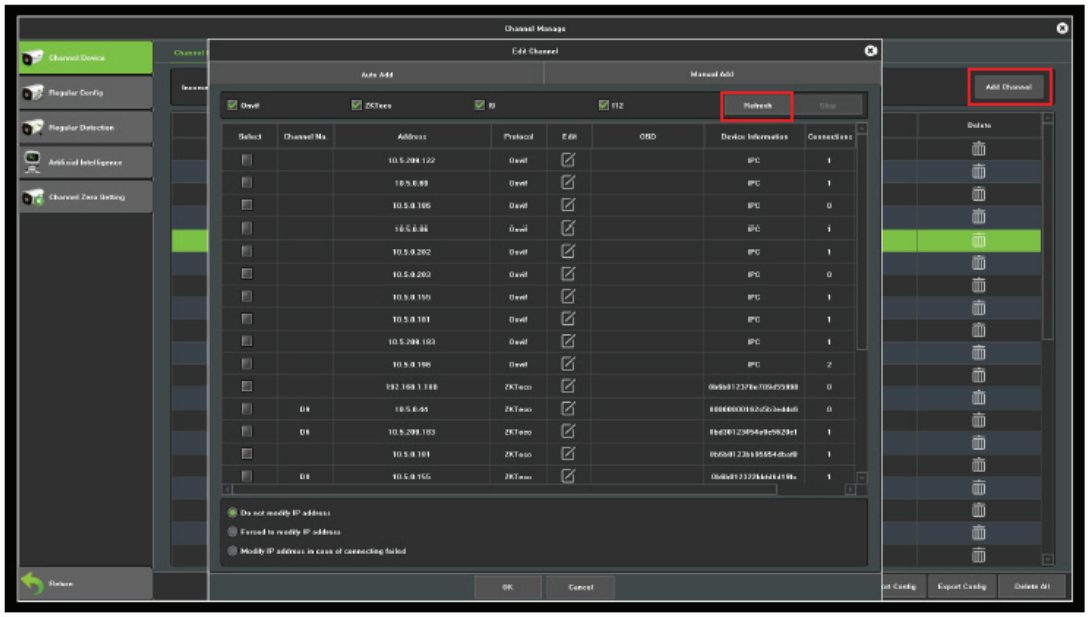


Nombre de la función	Descripción
Habilitar autenticación	Habilite/deshabilite la función de autenticación. Cuando está deshabilitado, no es necesario ingresar el nombre de usuario y la contraseña al agregar el dispositivo al NVR.
Nombre de usuario	Establezca el nombre de usuario. El valor predeterminado es admin.
Contraseña	Establezca la contraseña. El valor predeterminado es admin.
Puerto del servidor	El valor predeterminado es 8000 y no se puede modificar.

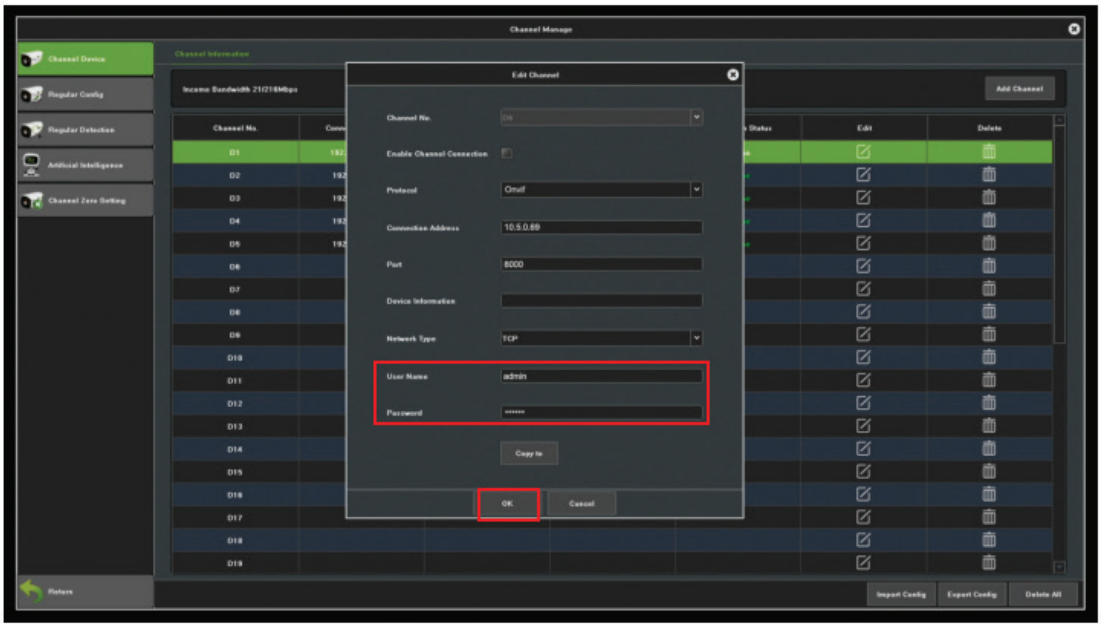
3. En el sistema NVR, haga clic en [Inicio] > [Menú], luego aparecerá el menú principal.



4. Haga clic en [Administrar canal> [Agregar canal] > [Actualizar] para buscar el dispositivo.

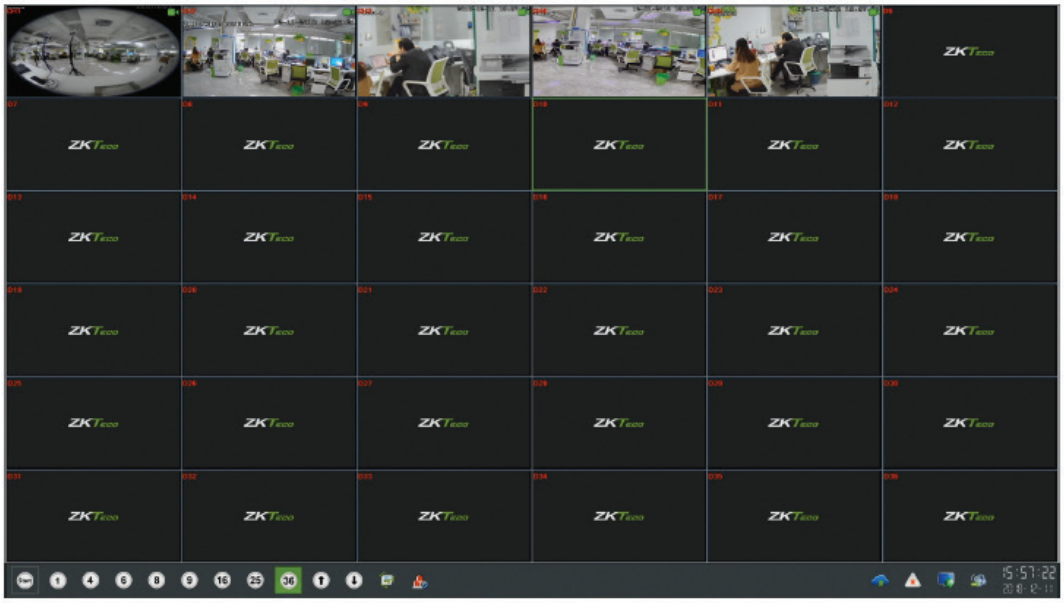


5.Seleccione la casilla de verificación del dispositivo que desea agregar y edite los parámetros en el campo de texto correspondiente, luego haga clic en Aceptar para agregarlo a la lista de conexiones.



Nota: El nombre de usuario y la contraseña se establecen en la configuración de ONVIF del dispositivo.

6. Después de agregar con éxito, la imagen de video obtenida del dispositivo se puede ver en tiempo real.

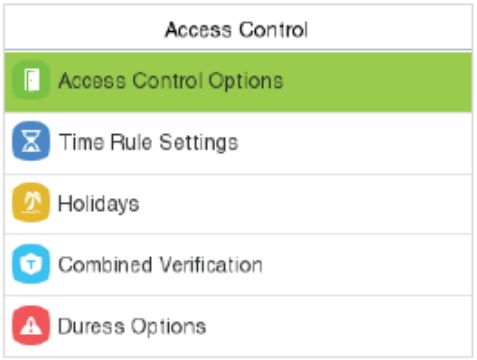


Para obtener más detalles, consulte el Manual del usuario de NVR.

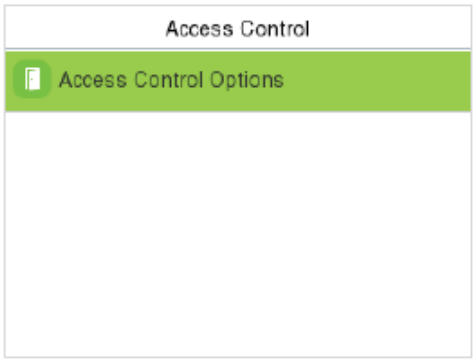
15 Control de acceso

Cuando el dispositivo esté en la interfaz inicial, presione M/OK y seleccione Control de acceso para configurar el horario de apertura de la puerta, el control de cerraduras y para configurar otros ajustes de parámetros relacionados con el control de acceso.

Terminal de control de acceso:



Terminal de Asistencia Horaria:



Para obtener acceso, el usuario registrado debe cumplir las siguientes condiciones:

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

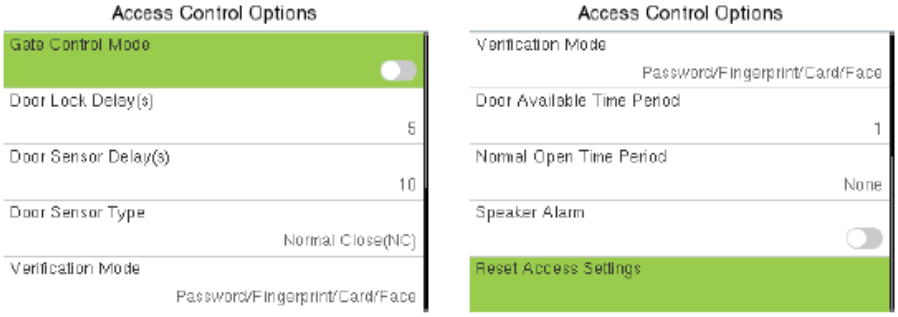
2. El grupo del usuario correspondiente ya debe estar configurado en la combinación de desbloqueo de la puerta (y si hay otros grupos, al estar configurados en el mismo combo de acceso, también se requiere la verificación de los miembros de ese grupo para desbloquear la puerta).

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

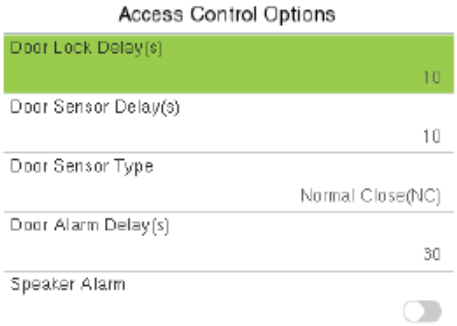
15.1 Opciones de control de acceso

Seleccione Opciones de control de acceso en la interfaz de control de acceso para establecer los parámetros del bloqueo de control del terminal y el equipo relacionado.

Terminal de control de acceso:



Terminal de Asistencia Horaria:



Nombre de la función	Descripción
Modo de control de puerta	Permite alternar entre los modos ON (activado) y OFF (desactivado) para entrar o salir del modo de control de puerta. Cuando se establece en ON, la interfaz elimina las opciones Retardo de bloqueo de puerta, Retardo del sensor de puerta y Tipo de sensor de puerta.
Retardo (s) de bloqueo de puerta	La cantidad de tiempo que el dispositivo controla la cerradura eléctrica para estar en estado de desbloqueo. Valor válido: 1~99 segundos.
Retardo (s) del sensor de puerta	Si la puerta no está cerrada y se deja abierta durante un tiempo determinado (retardo del sensor de puerta), se activará una alarma. El valor válido de Retardo del sensor de puerta oscila entre 1 y 255 segundos.

Tipo de sensor de puerta	Hay tres tipos de sensores: Ninguno, Normal abierto y Normal cerrado.Ninguno: Significa que el sensor de la puerta no está en uso. Normalmente abierta: Significa que la puerta siempre se deja abierta cuando la energía eléctrica está encendida. Normalmente cerrada: Significa que la puerta siempre se deja cerrada cuando la energía eléctrica está encendida.
Modo de verificación	El modo de verificación compatible incluye contraseña/huella dactilar/tarjeta/rostro, solo huella dactilar, solo ID de usuario, contraseña, solo tarjeta, etc.
Período de tiempo disponible de la puerta	Establece el tiempo de la puerta para que la puerta sea accesible solo durante ese período.
Período de tiempo de apertura normal	Es el período de tiempo programado para el modo "Abierto normal", de modo que la puerta siempre está abierta durante este período
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 cancela la alarma del local.
Restablecer configuración de acceso	Los parámetros de restablecimiento del control de acceso incluyen el retardo del bloqueo de la puerta, el retardo del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el periodo de tiempo de disponibilidad de la puerta, el periodo de tiempo de apertura normal y la alarma. Sin embargo, se excluyen los datos de control de acceso borrados en Gestión de datos.

Descripción de la función del terminal de asistencia temporal:

Nombre de la función	Descripción
Retardo (s) de bloqueo de puerta	La cantidad de tiempo que el dispositivo controla la cerradura eléctrica para estar en estado de desbloqueo. Valor válido: de 0 a 10 segundos.
Retardo (s) del sensor de puerta	Si la puerta no está cerrada y se deja abierta durante un tiempo determinado (retardo del sensor de puerta), se activará una alarma. El valor válido de Retardo del sensor de puerta oscila entre 1 y 255 segundos.

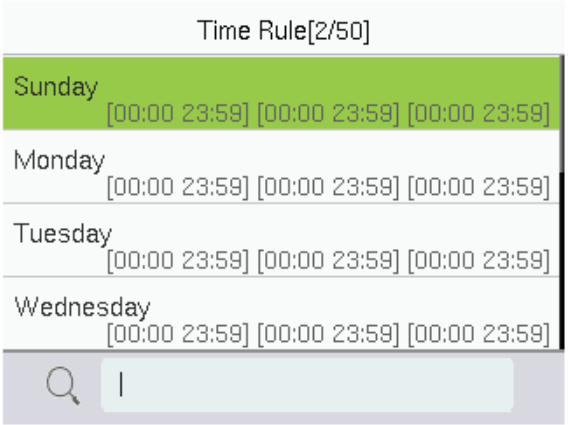
Tipo de sensor de puerta	Hay tres tipos de sensores: Ninguno, Normal abierto y Normal cerrado.Ninguno: Significa que el sensor de la puerta no está en uso. Normalmente abierta (NO): Significa que la puerta siempre se deja abierta cuando hay energía eléctrica. Normalmente cerrada (NC): Significa que la puerta siempre se deja cerrada cuando hay energía eléctrica.
Retardo(s) de alarma de puerta	Cuando el estado del sensor de la puerta es inconsistente con el del tipo del sensor de la puerta, la alarma se activará después de un período de tiempo; este período de tiempo es el retardo de la alarma de la puerta (el valor oscila entre 1 y 999 segundos).
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 cancela la alarma del local.

15.2 Configuración de la regla de tiempo

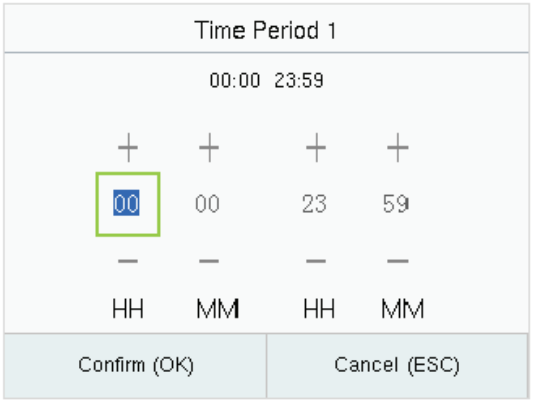
Seleccione Configuración de regla de tiempo en la interfaz de control de acceso para configurar los ajustes de tiempo.

- Todo el sistema puede definir hasta 50 períodos de tiempo.
- Cada período de tiempo representa 10 zonas horarias, es decir, 1 semana y 3 días festivos, y cada zona horaria es un período estándar de 24 horas por día y el usuario solo puede verificar dentro del período de tiempo válido.
- Se puede establecer un máximo de 3 períodos de tiempo para cada zona horaria. La relación entre estos puntos es "O". Por lo tanto, cuando el tiempo de verificación cae en cualquiera de estos períodos de tiempo, la verificación es válida.
- El formato de zona horaria de cada período de tiempo es HH MM-HH MM, que tiene una precisión de minutos según el reloj de 24 horas.

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



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



Especifique la hora de inicio y finalización y, a continuación, presione M/OK.

Nota:

1. La puerta es inaccesible durante todo el día cuando la Hora de Finalización ocurre antes de la Hora de Inicio (por ejemplo, 23:57 a 23:56).

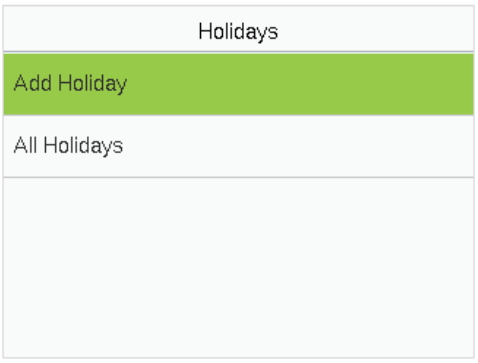
2. Es el intervalo de tiempo para el acceso válido cuando la hora de finalización es posterior a la hora de inicio (por ejemplo, de 08:00 a 23:59).

3.La puerta es accesible durante todo el día cuando la hora de finalización se produce después de la hora de inicio (de modo que la hora de inicio es a las 00:00 y la hora de finalización es a las 23:59).

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

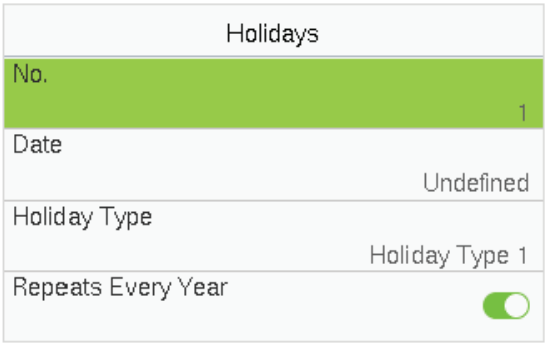
15.3 Días festivos

Cuando hay un día festivo, es posible que necesite un horario de acceso diferente; Sin embargo, alterar el tiempo de acceso de todos uno por uno lleva mucho tiempo. De este modo, se puede establecer un horario de acceso a las vacaciones que se aplique a todos los trabajadores, y el usuario podrá abrir la puerta durante las vacaciones. Seleccione Días festivos en la interfaz de control de acceso para establecer el acceso a los días festivos.



Añadir un nuevo día festivo:

Toque Agregar día festivo en la interfaz de días festivos y establezca los parámetros de días festivos.



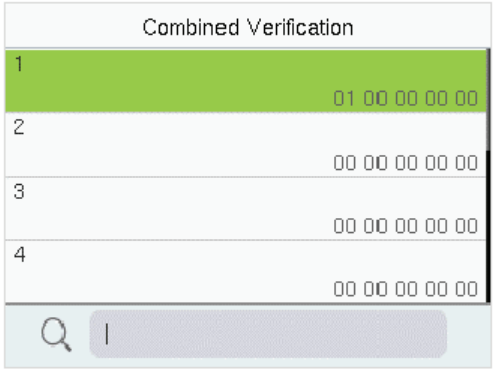
Editar un día festivo:
En la interfaz Días festivos, seleccione un elemento festivo para modificarlo. Pulse Editar para modificar los parámetros de vacaciones.

Eliminar un día festivo:
En la interfaz de días festivos, seleccione un elemento festivo para eliminarlo y toque Eliminar. Pulse M/OK para confirmar la eliminación. Después de la eliminación, este día festivo no se muestra en la interfaz Todos los días festivos.

15.4 Verificación combinada

Los grupos de acceso se organizan en diferentes combinaciones de desbloqueo de puertas para lograr múltiples verificaciones y reforzar la seguridad.

En una combinación de desbloqueo de puertas, el rango del número combinado N es $0 \leq N \leq 5$ y el número de miembros N puede pertenecer a un grupo de acceso o a cinco grupos de acceso diferentes. Seleccione Verificación combinada en la interfaz de control de acceso para configurar la opción de verificación combinada.



En la interfaz de verificación combinada, pulse la combinación de desbloqueo de la puerta que desea configurar y pulse las teclas arriba y abajo para introducir el número de la combinación. A continuación, pulse M/OK.
Por ejemplo:

Si la combinación de desbloqueo de puerta 1 se configura como (01 03 05 06 08). Esto indica que la combinación de desbloqueo 1 consta de 5 personas y que las 5 personas pertenecen a 5 grupos, a saber, el grupo AC 1, el grupo AC 3, el grupo AC 5, el grupo AC 6 y el grupo AC 8, respectivamente.

Si la combinación de desbloqueo de la puerta 2 se establece como (02 02 04 04 07). Esto indica que la combinación de desbloqueo 2 consta de 5 personas; las dos primeras pertenecen al grupo AC 2, las dos siguientes pertenecen al grupo AC

Grupo 4, y la última persona es del Grupo AC 7.

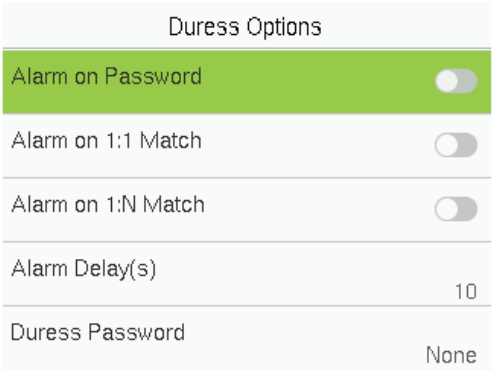
Si la combinación de desbloqueo de la puerta 3 se establece como (09 09 09 09 09), esto indica que hay 5 personas en esta combinación, todas ellas pertenecientes al grupo AC 9.

Si la combinación para desbloquear la puerta 4 se establece como (03 05 08 00 00), esto indica que la combinación para desbloquear 4 está formada solo por tres personas. La primera persona pertenece al grupo AC 3, la segunda al grupo AC 5 y la tercera al grupo AC 8.

Nota: Para eliminar la combinación de desbloqueo de puertas, establezca todas las combinaciones de desbloqueo de puertas en 0.

15.5 Configuración de opciones de coacción

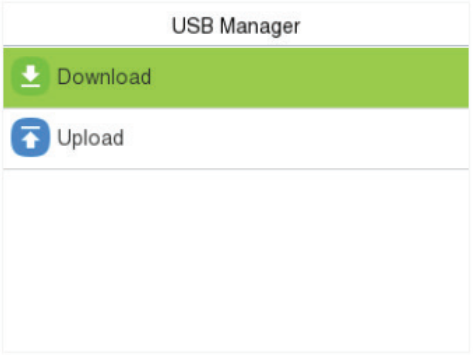
Una vez que un usuario activa la función de verificación de coacción con uno o varios métodos de autenticación específicos, y cuando está bajo coerción y se autentica mediante la verificación de coacción, el dispositivo desbloquea la puerta como de costumbre. Al mismo tiempo, se envía una señal para activar también la alarma.
En la interfaz de control de acceso, seleccione Opciones de coacción para configurar los ajustes de coacción.



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

16 Administrador USB

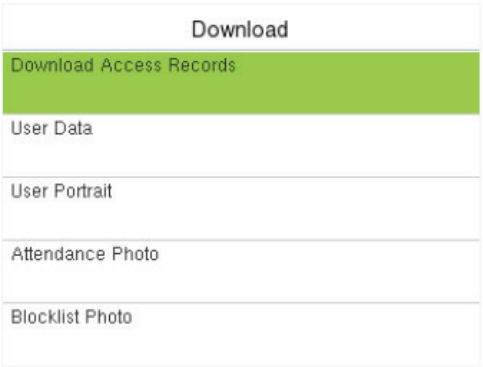
Puede importar información de usuario, datos de acceso y otros datos desde una unidad USB a la computadora u otros dispositivos. Antes de cargar/descargar datos desde/hacia el disco USB, inserte primero el disco USB en la ranura USB. Seleccione Administrador USB en la interfaz del menú principal.



Nota: Solo se admite el formato FAT32 cuando se descargan datos mediante un disco USB.

16.1 Descarga USB

En la interfaz del Administrador USB, toque Descargar.

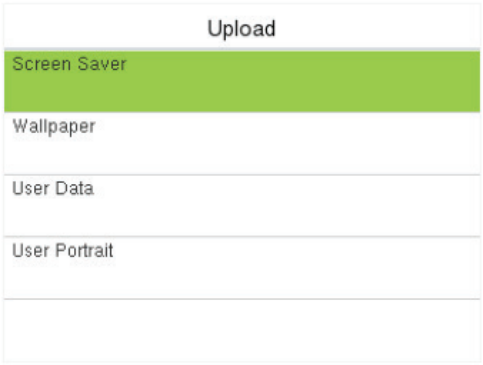


Menú	Descripción
Acceso a la descarga Archivo	Para descargar el registro de acceso en el período de tiempo especificado en un disco USB.
Datos del usuario	Para descargar toda la información del usuario del dispositivo en un disco USB.
Retrato de usuario	Para descargar todas las imágenes de usuario del dispositivo en un disco USB.

Foto de asistencia	Para descargar todas las fotos de asistencia del dispositivo a un disco USB.
Foto de la lista de bloqueo	Para descargar todas las fotos incluidas en la lista de bloqueo (fotos tomadas después de verificaciones fallidas) desde el dispositivo a un disco USB.

16.2 Carga USB

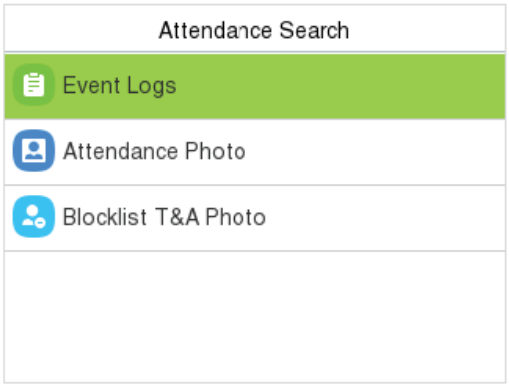
En la interfaz del Administrador USB, toque Cargar.



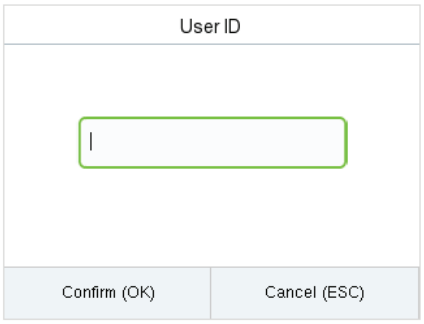
Menú	Descripción
Guardar pantalla	Para cargar todos los protectores de pantalla desde un disco USB al dispositivo. Puede elegir Cargar la foto seleccionada o Cargar todas las fotos . Las imágenes se mostrarán en la interfaz principal del dispositivo después de la carga.
Papel tapiz	Para cargar todos los fondos de pantalla desde un disco USB en el 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 en el dispositivo.
Retrato de usuario	Para cargar todos los retratos de usuario desde un disco USB en el dispositivo.

17 Búsqueda de asistencia

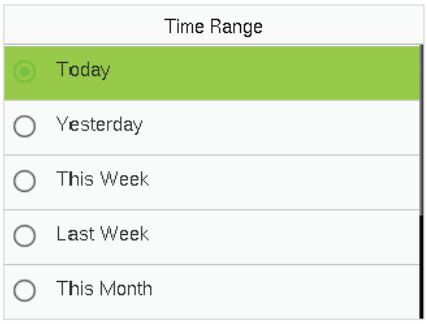
Una vez verificada la identidad de un usuario, el registro de acceso se guarda en el dispositivo. Esta función permite a los usuarios comprobar sus registros de eventos. Cuando el dispositivo esté en la interfaz inicial, presione M/OK y seleccione Búsqueda de asistencia para buscar los registros de eventos requeridos.



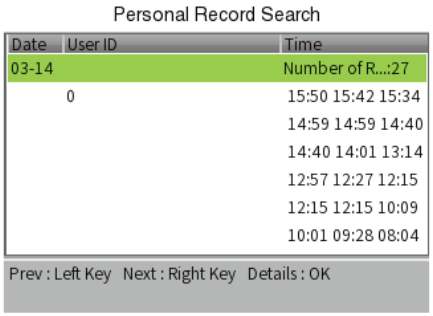
El proceso de búsqueda de fotos de asistencia y de listas de bloqueo es similar al de búsqueda de registros de eventos. A continuación se muestra un ejemplo de búsqueda de registro de asistencia. En la interfaz de búsqueda de asistencia, seleccione Registros de eventos para buscar el registro requerido.



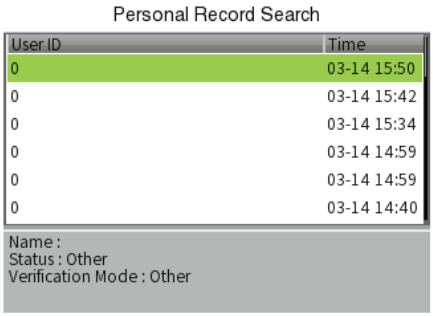
1.Introduzca el ID de usuario que desea buscar y pulse M/OK. Si desea buscar registros de todos los usuarios, presione M / OK sin ingresar ningún ID de usuario.



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



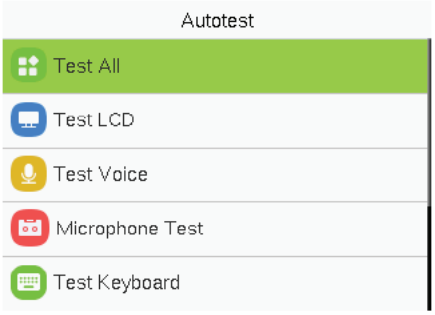
3. Una vez que se complete la búsqueda de registros. Toque el registro resaltado en verde para ver sus detalles.



4.La figura muestra los detalles del registro seleccionado.

18 Autotest

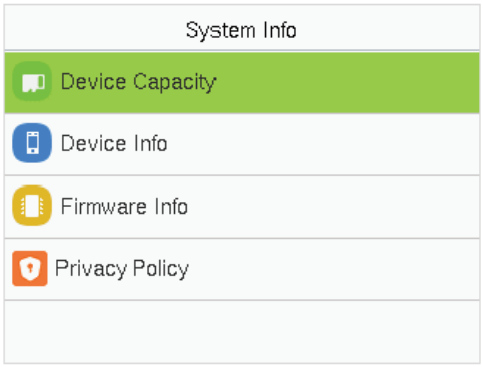
Cuando el dispositivo esté en la interfaz inicial, presione M / OK y seleccione Autotest, permite que el sistema pruebe automáticamente si las funciones de varios módulos funcionan normalmente, incluidos la pantalla LCD, la voz, el micrófono, el teclado, la huella dactilar, la cámara y el reloj en tiempo real (RTC).



Nombre de la función	Descripción
Probar todo	Para probar automáticamente si la pantalla LCD, la voz, el micrófono, el teclado, la huella dactilar, la cámara y el reloj en tiempo real (RTC) son normales.
Prueba 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 colores normalmente.
Voz de prueba	Para probar automáticamente si los archivos de audio almacenados en el dispositivo están completos y la calidad de la voz es buena.
Teclado de prueba	El terminal comprueba si todas las teclas del teclado funcionan normalmente. Presione cualquier tecla en la interfaz del teclado de prueba para verificar si la tecla presionada coincide con la tecla que se muestra en la pantalla. Las teclas se muestran en gris oscuro antes y se vuelven verdes después de presionarlas. Presione ESC para salir de la prueba.
Prueba de leva	Para comprobar si la cámara funciona correctamente. (Igual que “cara de prueba”)
Reloj de prueba RTC	Para probar el RTC. El dispositivo comprueba si el reloj funciona de forma normal y precisa con un cronómetro. Presione M / OK para comenzar a contar y presione nuevamente para detener el conteo.

19 Información del sistema

Cuando el dispositivo esté en la interfaz inicial, presione M / OK y seleccione Información del sistema para ver el estado de almacenamiento, la información de la versión del dispositivo, la información de firmware y la política de privacidad.



Nombre de la función	Descripción
Capacidad del dispositivo	Muestra el almacenamiento de usuario del dispositivo actual, el rostro, la huella dactilar, el almacenamiento de tarjetas y contra-señas, los administradores, los registros, la asistencia, la lista de bloqueo y las fotos de perfil.
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la direc-ción MAC, el algoritmo de huellas dactilares, el algoritmo facial, la información de la plataforma, la versión de MCU y el fabricante.
Información de firmware	Muestra la versión del firmware y otra información de la versión del dispositivo.
Política de privacidad	Muestra la política de privacidad del dispositivo.

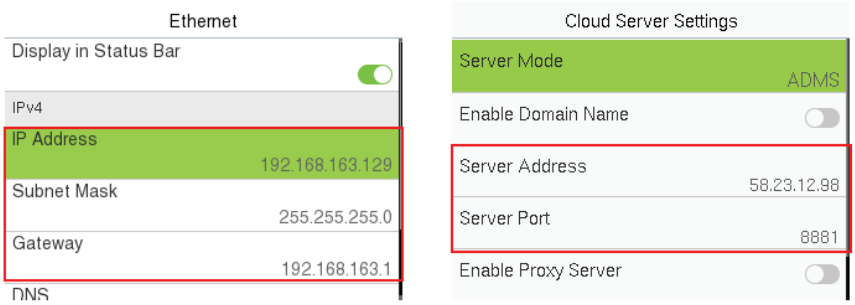
20. Conéctese al software ZKBio CVAccess

20.1 Establecer la dirección de comunicación

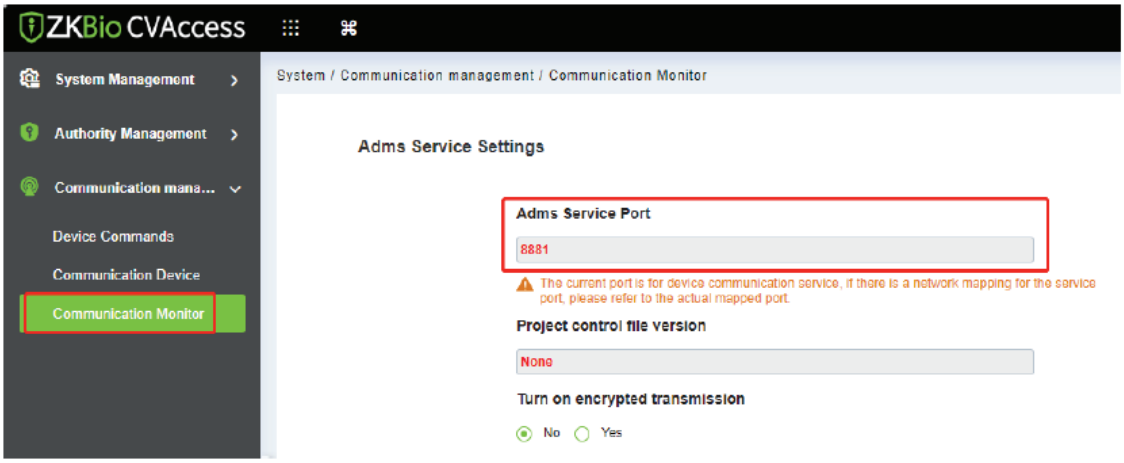
Cuando el dispositivo esté en la interfaz inicial, presione M / OK y seleccione Información del sistema para ver el estado de almacenamiento, la información de la versión del dispositivo, la información de firmware y la política de privacidad.

Lado del dispositivo

1. Presione M/OK e ingrese COMM. > Ethernet para configurar la dirección IP y la puerta de enlace del dispositivo. (Nota: La dirección IP debe poder comunicarse con el servidor CVAccessserver de ZKBio)
2. Presione M/OK e ingrese COMM. > Configuración del servidor en la nube para establecer la dirección del servidor y el puerto del servidor. Dirección del servidor: Establezca la dirección IP como del servidor ZKBio CVAccess. Puerto del servidor: Establezca el puerto del servidor a partir de ZKBio CVAccess.



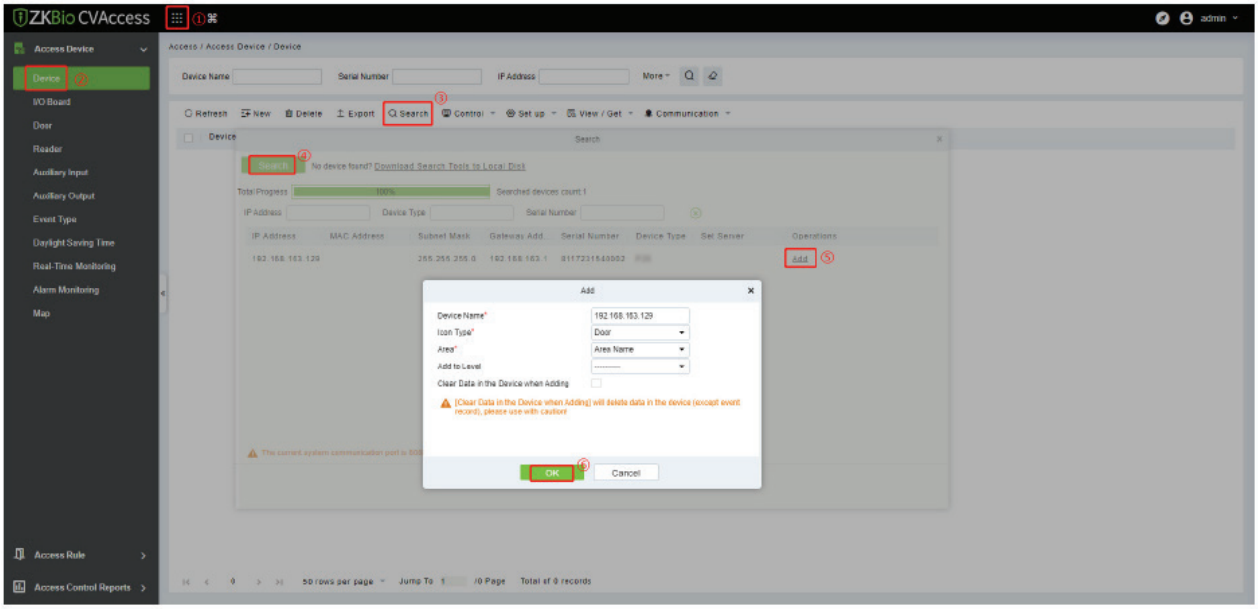
Lado del software
Inicie sesión en el software ZKBio CVAccess, haga clic en Sistema > Gestión de comunicaciones > CommunicationMonitor para configurar el puerto del servicio ADMS, tal y como se muestra en la siguiente imagen:



20.2 Agregar dispositivo en el software

Agregue el dispositivo mediante la búsqueda. El proceso es el siguiente:
1. Haga clic en Acceder > dispositivo > Buscar > Buscar, para abrir la interfaz de búsqueda en el software.

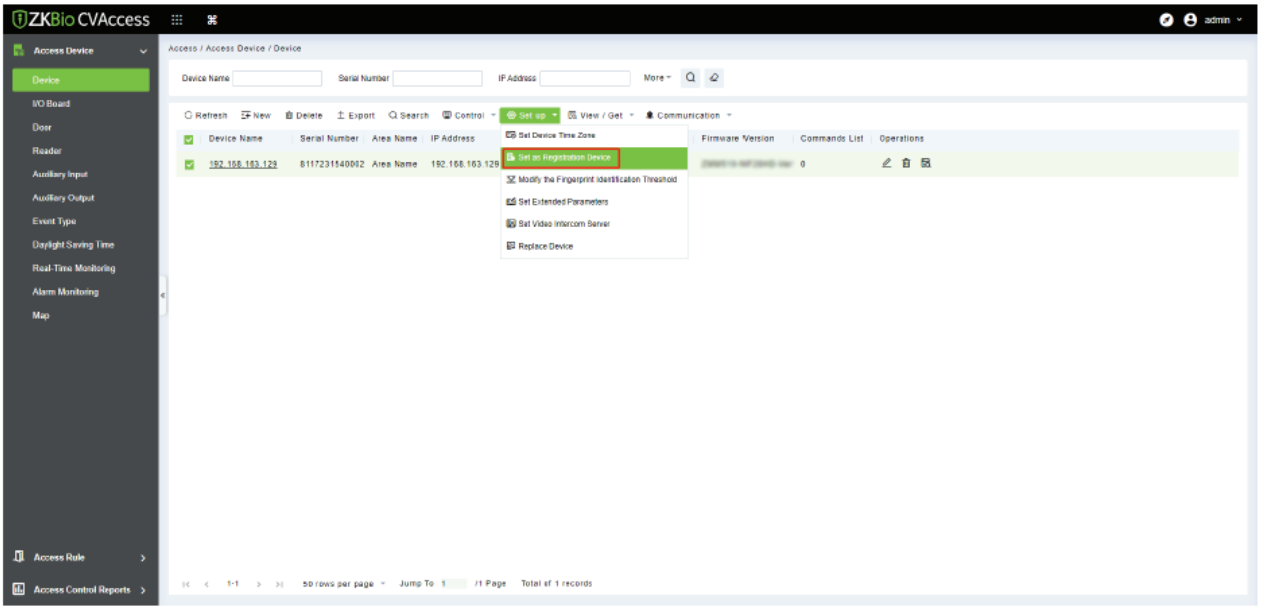
2. Haga clic en Buscar y aparecerá [Buscando.....].
3. Después de buscar, se mostrará la lista y el número total de controladores de acceso.



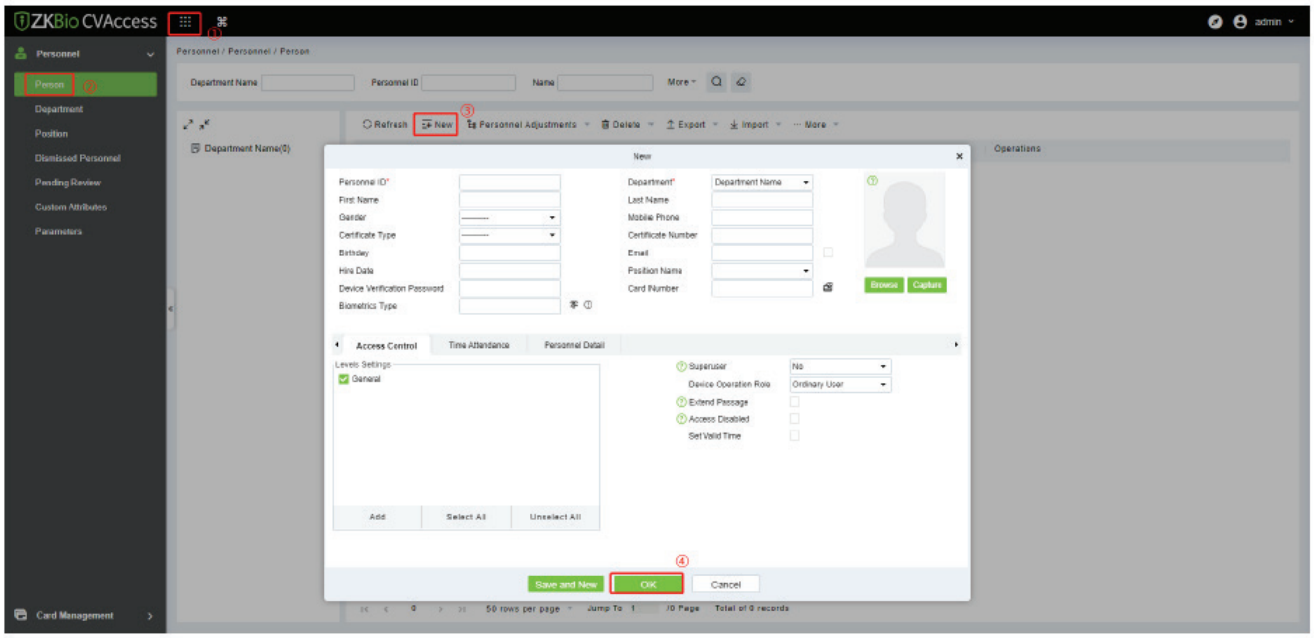
4. Haga clic en [Agregar] en la columna de operación, aparecerá una nueva ventana. Seleccione Tipo de icono, Área y Agregar a nivel en cada menú desplegable y haga clic en [Aceptar] para agregar el dispositivo.
5. Una vez que la adición se haya realizado correctamente, el dispositivo se mostrará en la lista de dispositivos.

20.3 Agregar personal en el software y registro de huellas dactilares/facial en línea

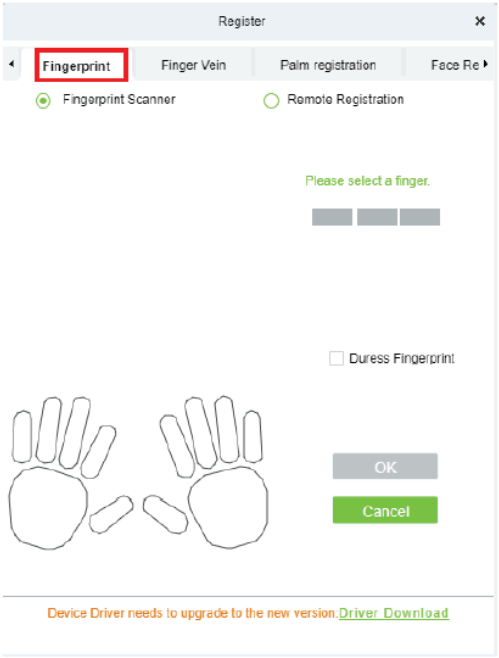
1. En la lista de dispositivos, seleccione el dispositivo y haga clic en Configurar > Establecer como dispositivo de registro.



2. Haga clic en Personal > Persona > Nuevo:



3. Rellene todos los campos obligatorios del usuario y haga clic y seleccione Huella digital para acceder a la interfaz de registro de huellas digitales en línea.



4. Haga clic en Descargar controlador para instalar primero el controlador.
5. Seleccione Registro remoto, luego seleccione la dirección IP del dispositivo y el dedo que desea registrar, haga clic en Confirmar

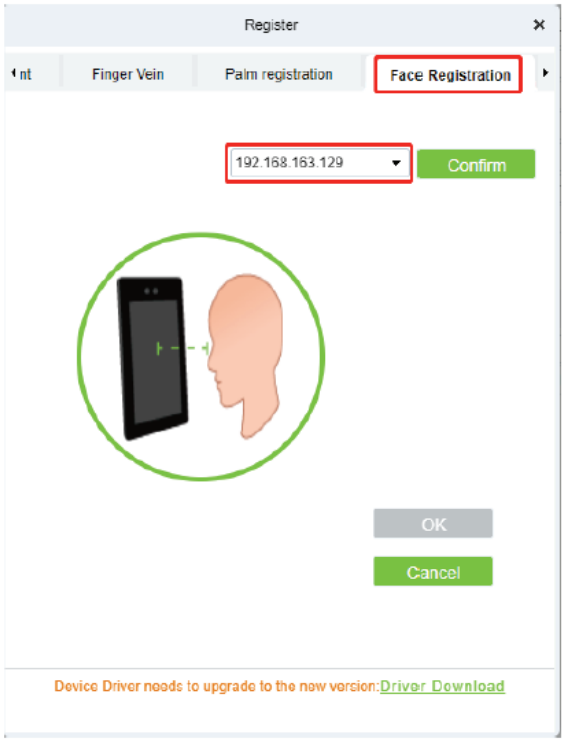


6. Después de que el dispositivo indique "Presione su dedo", presione su dedo sobre el sensor de huellas dactilares del dispositivo tres veces. Si la huella dactilar se registra correctamente, el dispositivo indicará "Registrado correctamente".

7. Si desea registrar una huella dactilar de coacción, puede hacer clic en Huella dactilar de coacción antes de registrar la huella dactilar.

- Huella dactilar de coacción: En cualquier caso, se genera una alarma de coacción cuando una huella dactilar coincide con la huella dactilar de coacción.

8. Haga clic en Registro facial para ingresar a la interfaz de registro facial en línea. Seleccione la dirección IP del dispositivo y haga clic en Confirmar.

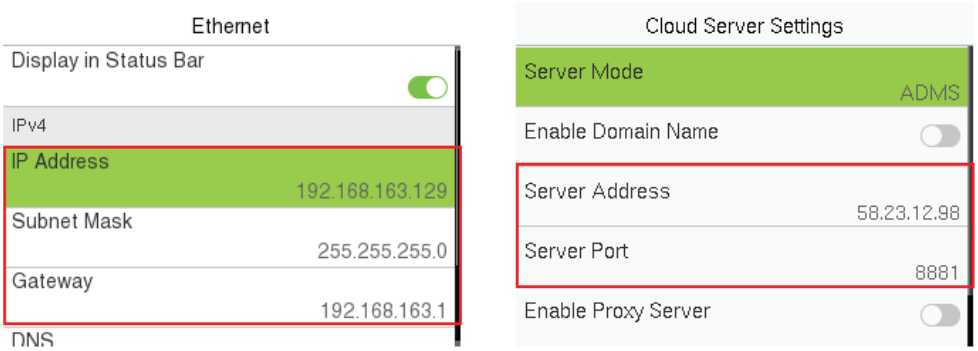


9. Después de que el dispositivo indique "Comenzar el registro facial", mire hacia la cámara y mantenga la cara en el centro de la pantalla y permanezca quieta durante el registro facial. Si la cara se registra correctamente, el dispositivo solicitará "Registrado correctamente".
10. Haga clic en Aceptar para guardar el usuario.
11. Haga clic en Acceder > dispositivo > Control > sincronizar todos los datos con los dispositivos para sincronizar todos los datos con el dispositivo, incluidos los nuevos usuarios. Nota: Para otras operaciones específicas, consulte el Manual del usuario de ZKBio CVAccess.

21 Conéctese al software ZKBio Time

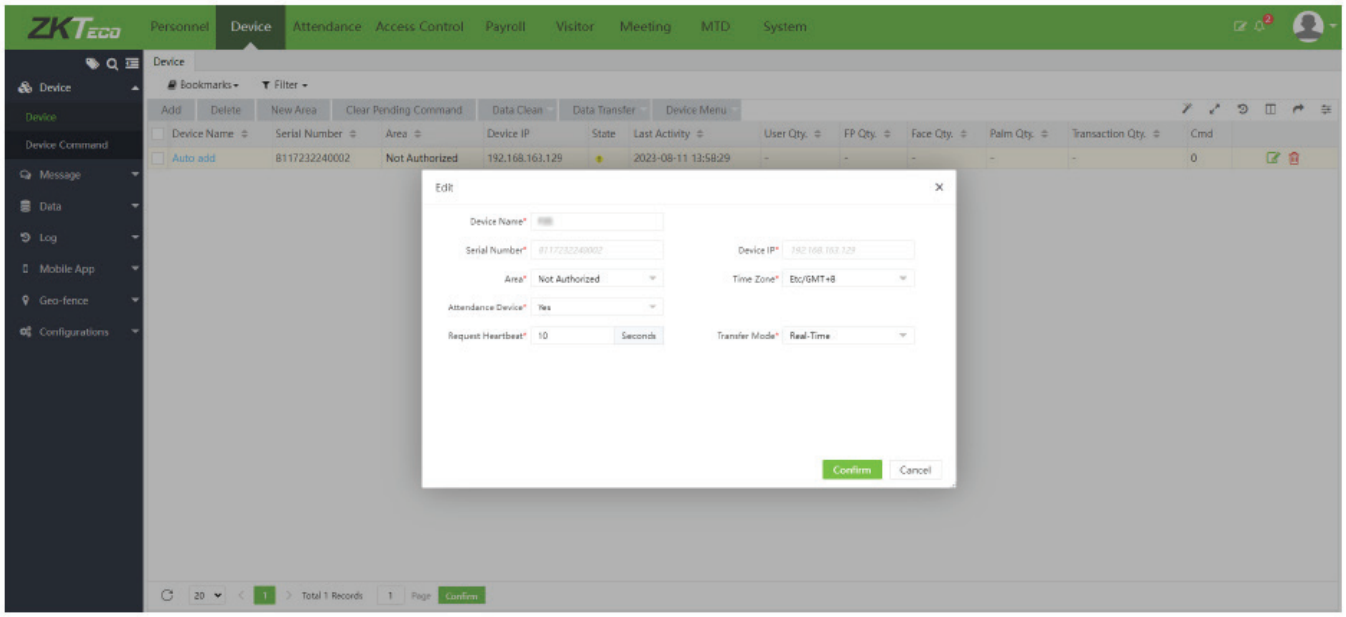
21.1 Establecer la dirección de comunicación

1. Presione M/OK e ingrese COMM. > Ethernet para configurar la dirección IP y la puerta de enlace del dispositivo. (Nota: La dirección IP debe poder comunicarse con el servidor ZKBio Time, preferiblemente en el mismo segmento de red que la dirección del servidor)
2. Presione M/OK e ingrese COMM. > Configuración del servidor en la nube para establecer la dirección del servidor y el puerto del servidor.
Dirección del servidor: Establezca la dirección IP como del servidor de tiempo de ZKBio.
Puerto del servidor: Establezca el puerto del servidor como del servidor de tiempo de ZKBio.



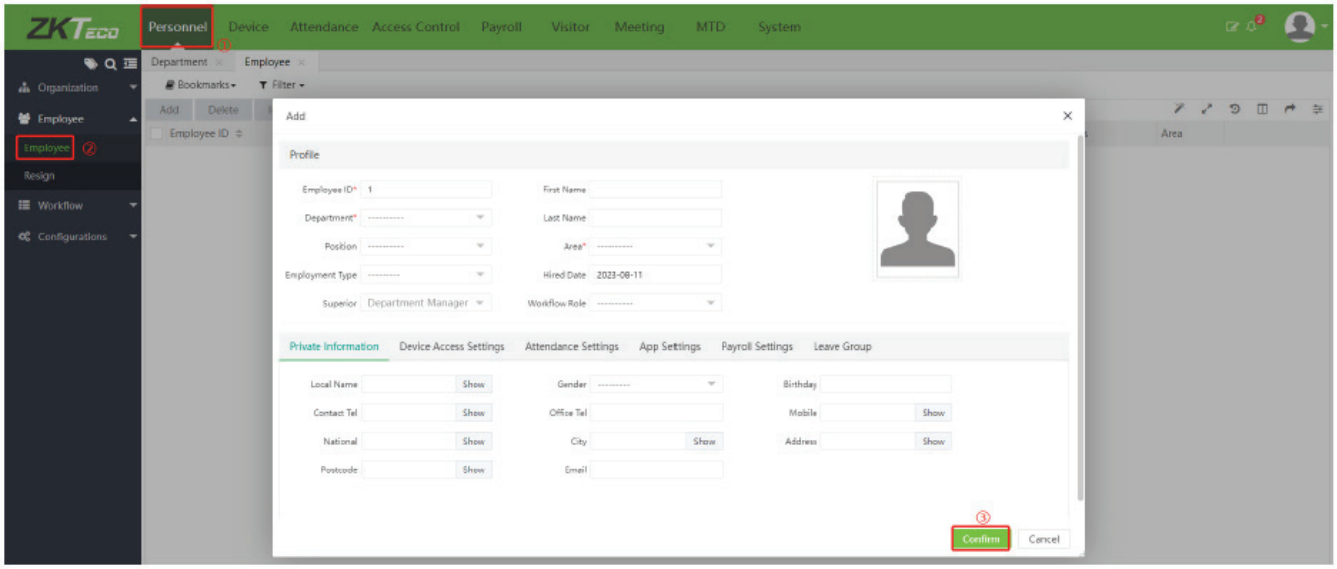
21.2 Agregar dispositivo en el software

Después de la configuración en el dispositivo, el dispositivo se agregará automáticamente al software. Abra el software ZKBio Time, luego seleccione [Módulo de dispositivo] > [Dispositivo] > [Dispositivo], haga clic en el dispositivo en la lista, cambie el nombre y el área del dispositivo.Nota: Los dispositivos agregados automáticamente deben asignarse a áreas personalizadas para comunicarse con el software.

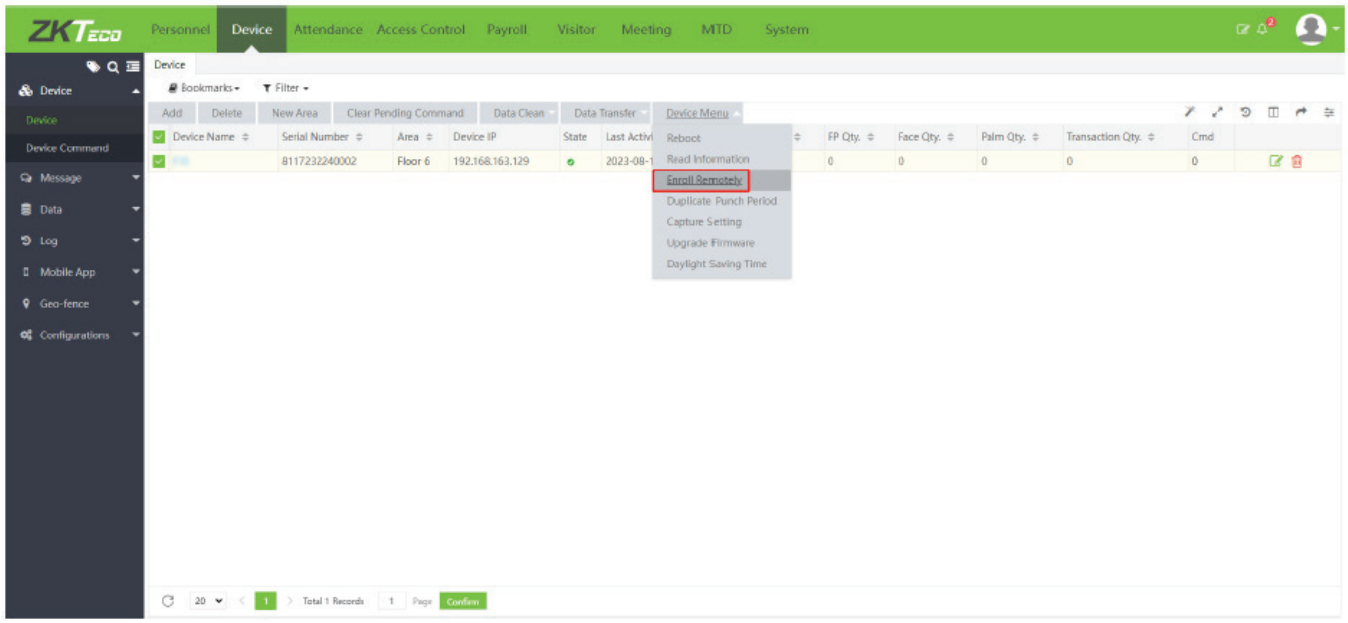


21.3 Agregar personal en el software y el registro de huellas dactilares en línea

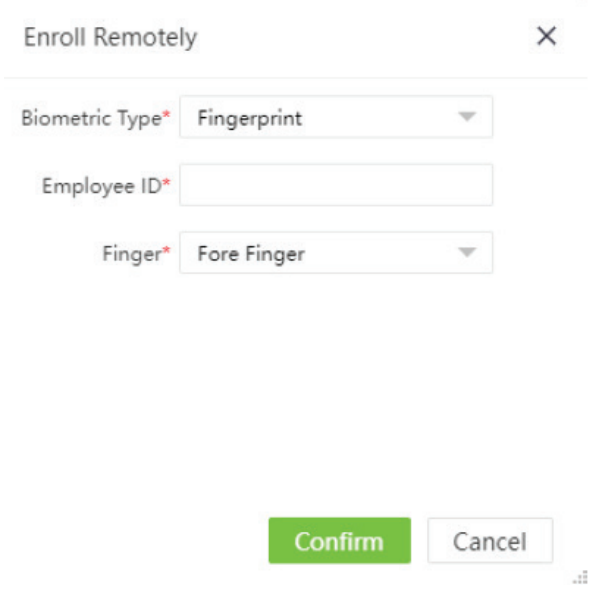
1. Haga clic en Personal > Empleado > agregar:



2. Rellene todos los campos obligatorios y haga clic en [Confirmar] para registrar un nuevo usuario.
3. Haga clic en Dispositivo > dispositivo, seleccione el dispositivo y haga clic en Menú de dispositivo > Inscribir de forma remota.



4. Ingrese la ID de empleado y seleccione el dedo que desea registrar y presione su dedo en el sensor de huellas dactilares del dispositivo tres veces. Si la huella digital se registra correctamente, el dispositivo indicará "Inscrito correctamente"



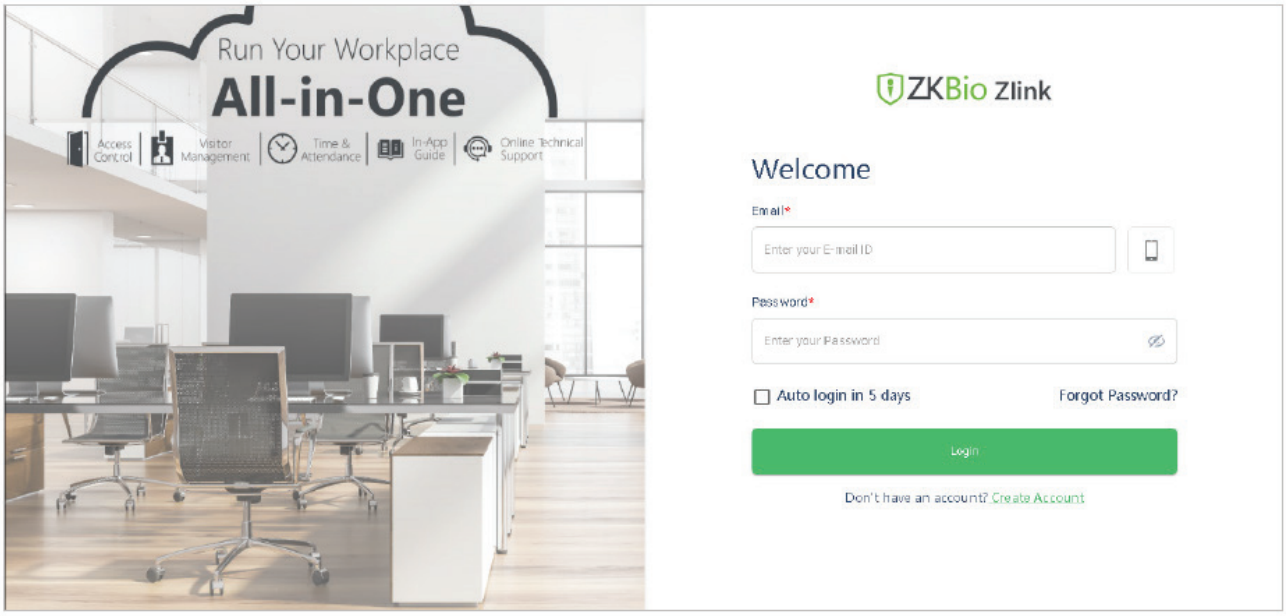
5. Haga clic en Dispositivo > Transferencia de datos > dispositivo > Sincronizar datos con el dispositivo para sincronizar todos los datos con el dispositivo, incluidos los nuevos usuarios. Nota: Para otras operaciones específicas, consulte el Manual del usuario de ZKBio Time.

22 Conexión a ZKBio Zlink Web

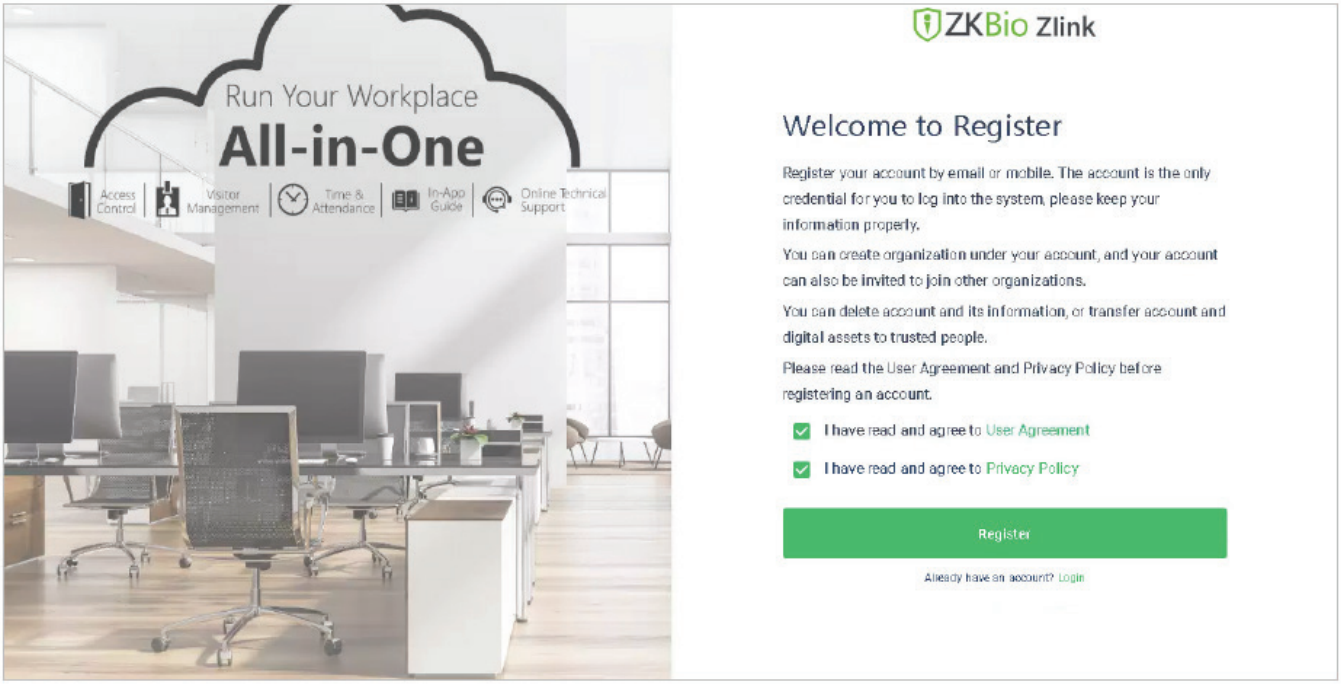
Cambie el protocolo de comunicación del dispositivo al protocolo BEST, luego el dispositivo puede ser administrado por ZKBioZlink, consulte 11.5 Configuración del tipo de dispositivo.Los usuarios pueden usar la cuenta creada para acceder a ZKBio Zlink Web para conectar dispositivos, agregar nuevo personal, registrar el método de verificación del personal registrado, sincronizar personal con dispositivos y consultar registros.

22.1 Registrar cuenta

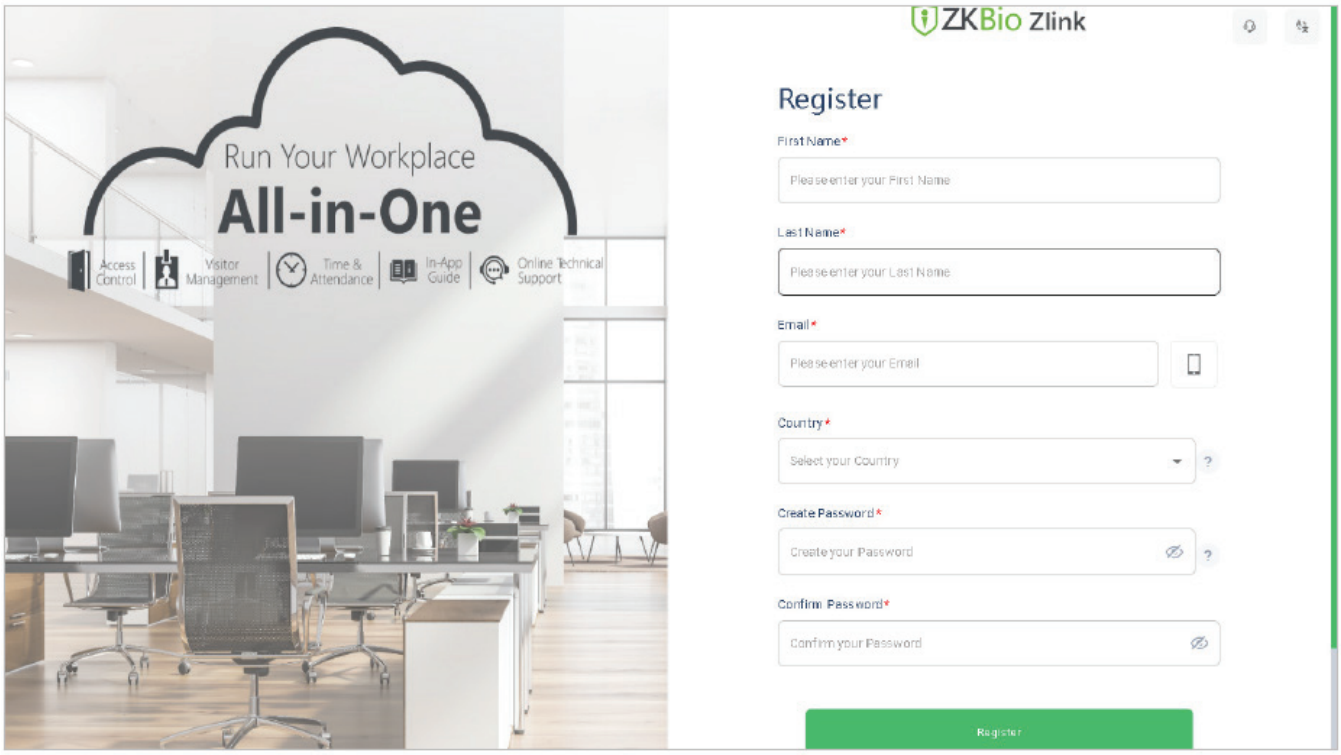
1.Acceda al sitio web de ZKBio Zlink (http://zlink.minervaiot.com).
2. Si no tiene una cuenta, haga clic en Crear cuenta para agregar una nueva cuenta.



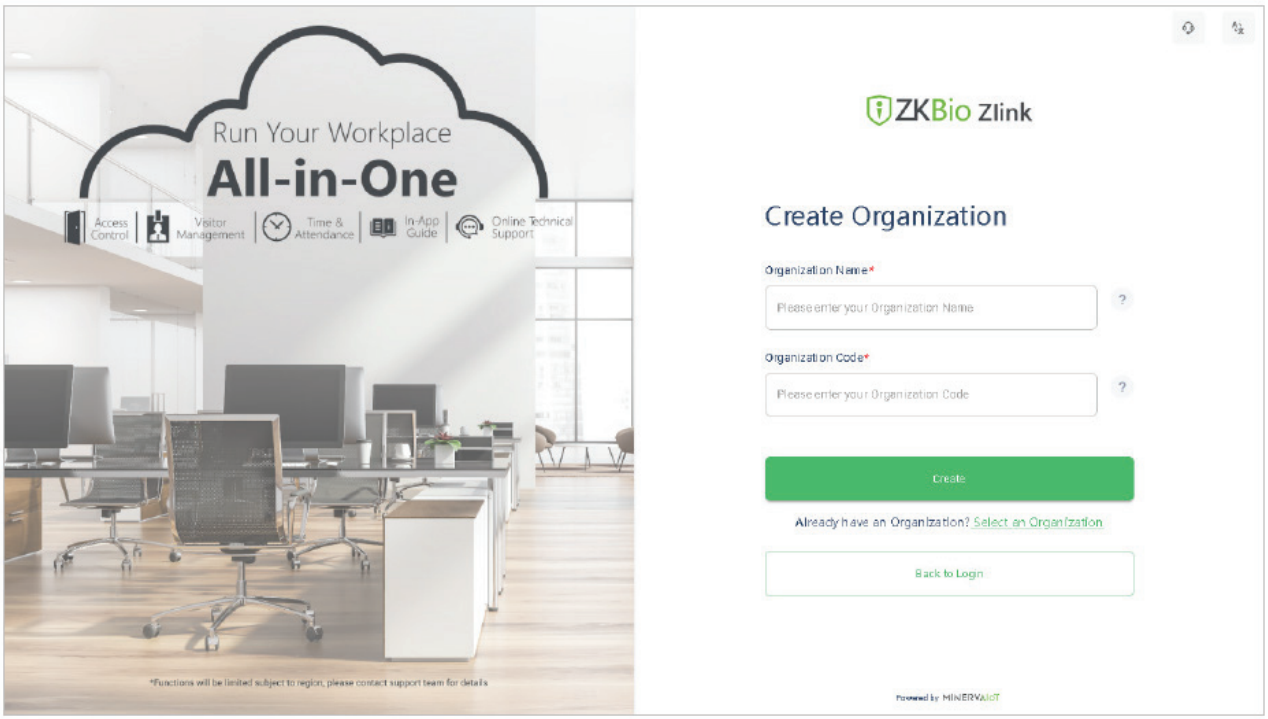
3.Lea y acepte el Acuerdo de usuario y la Política de privacidad, luego haga clic en Registrarse.



4.Ingrese la información del usuario y establezca la contraseña, luego haga clic en Registrarse.



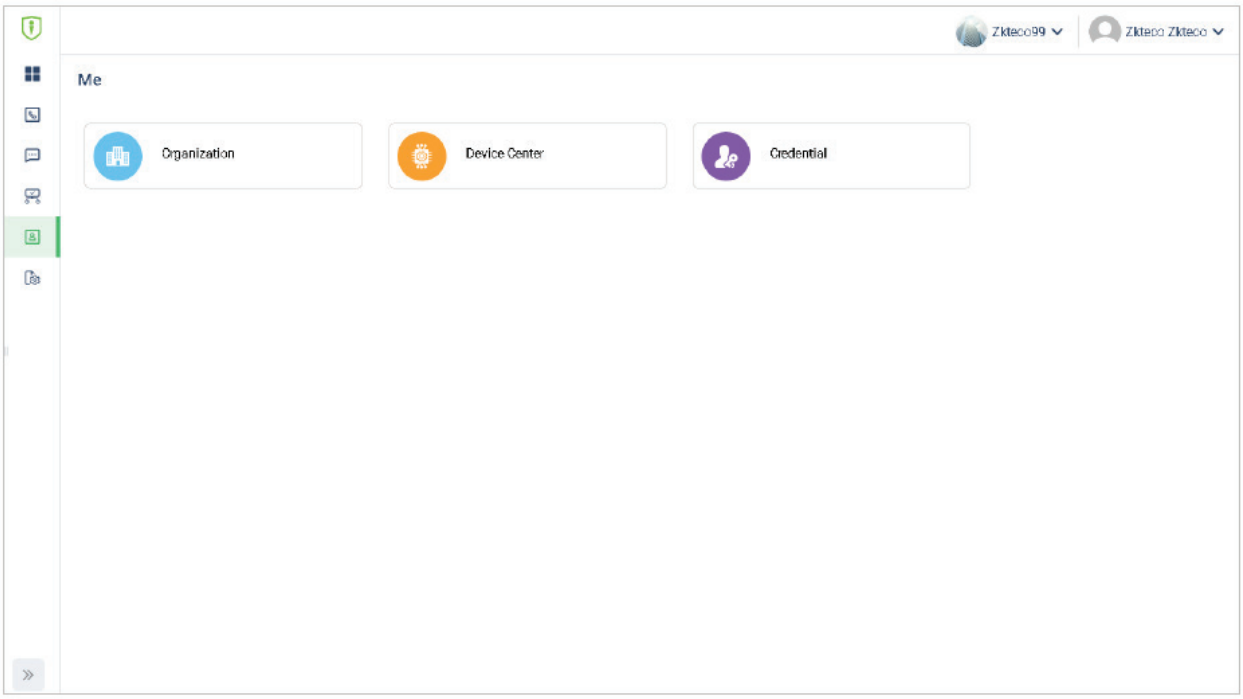
5.Establezca el nombre y el código de la organización, haga clic en Crear y, a continuación, complete el registro. Si tiene una organización, haga clic en Seleccionar una organización.



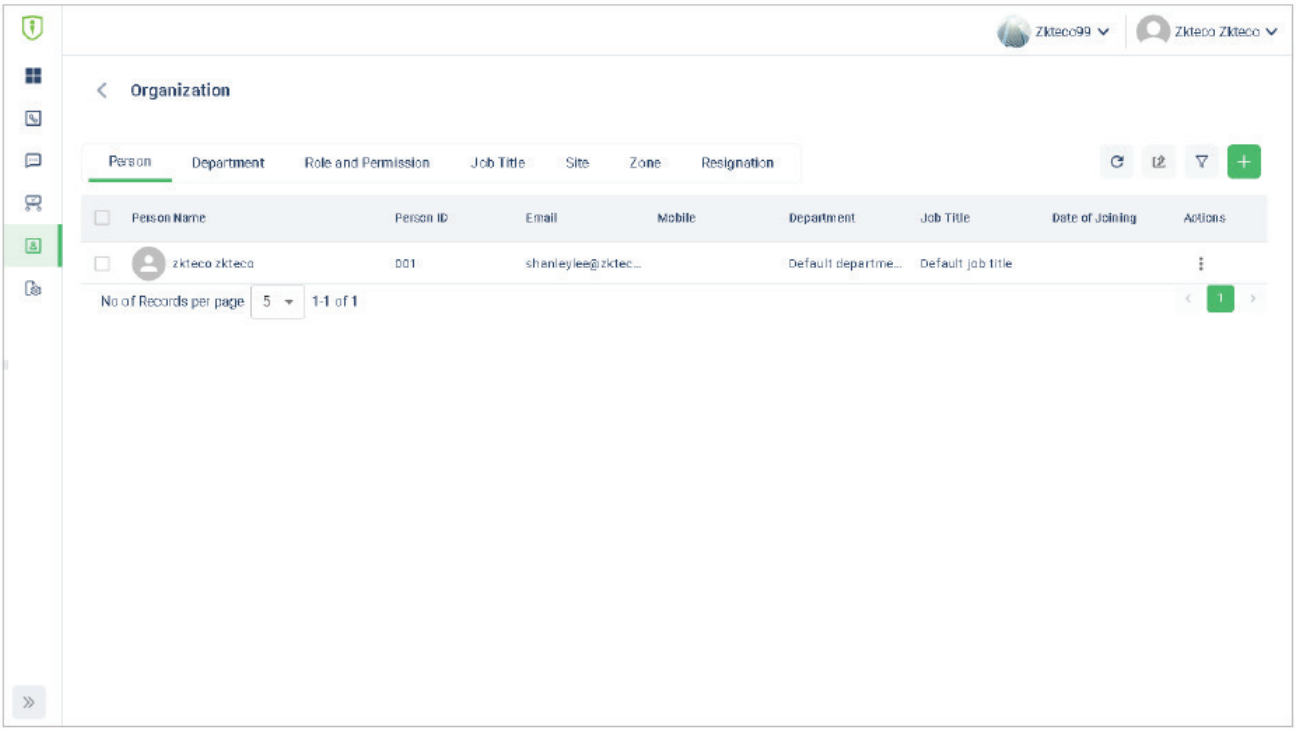
22.2 Agregar dispositivo

22.2.1 Establecer organización (agregar persona)

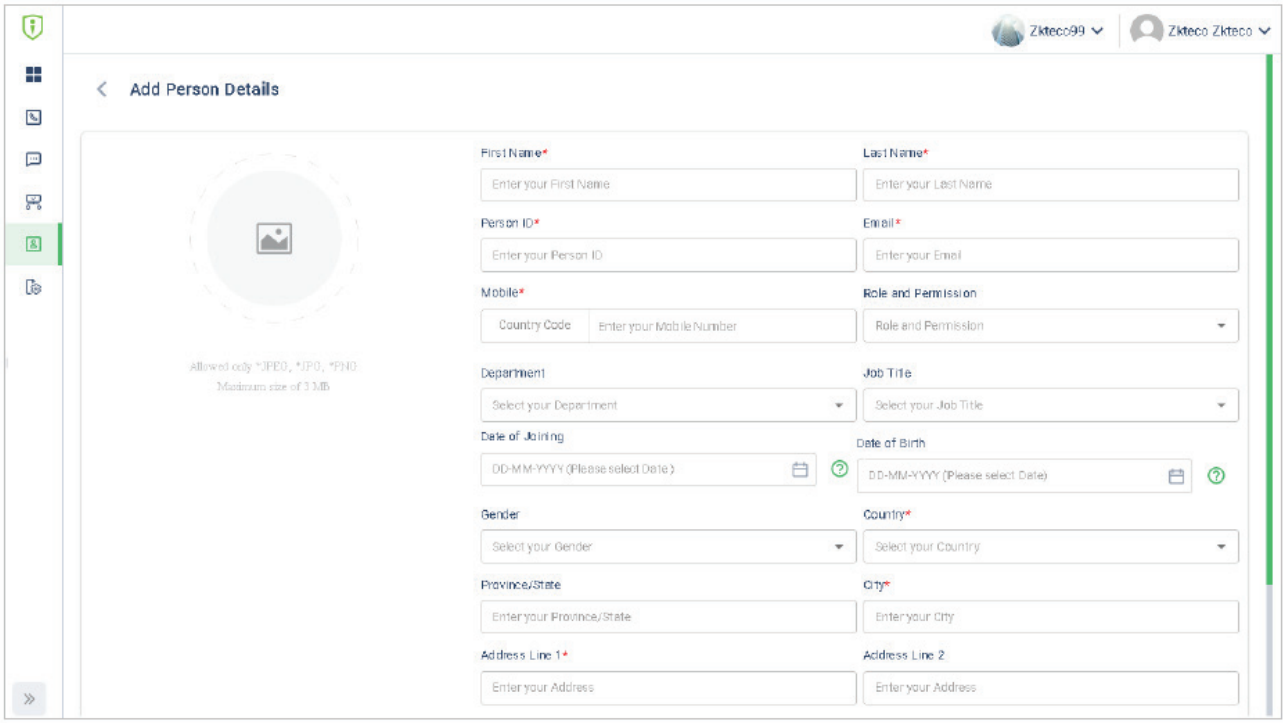
1.Haga clic en Yo > organización en el menú principal.



2.Haga clic en el icono Agregar para agregar una nueva persona (repita agregando el departamento, el rol y el permiso, Título del trabajo, lista de sitios y lista de zonas).

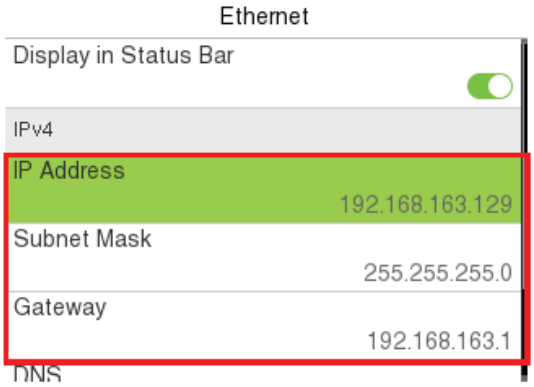


3.Introduzca los datos de la persona y haga clic en Guardar (repita agregando el departamento, el rol y el permiso, el cargo, la lista de sitios y la lista de zonas).

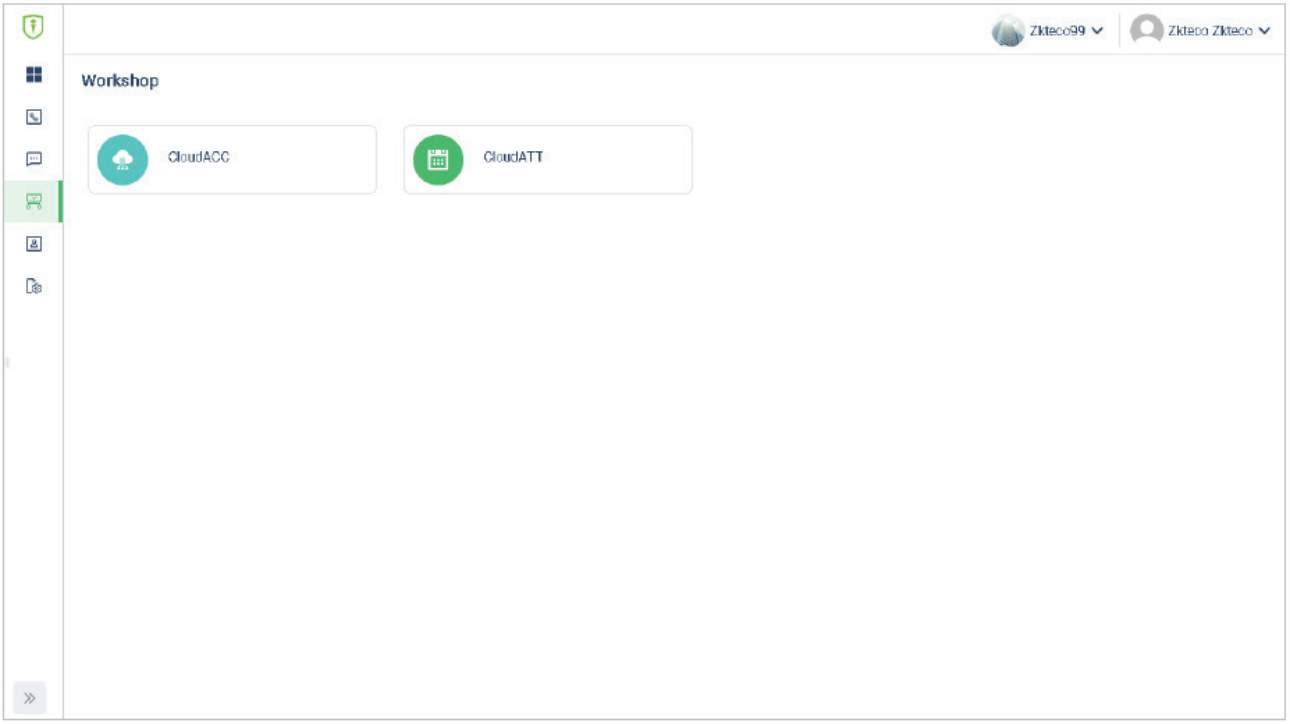


22.2.2 Agregar dispositivo

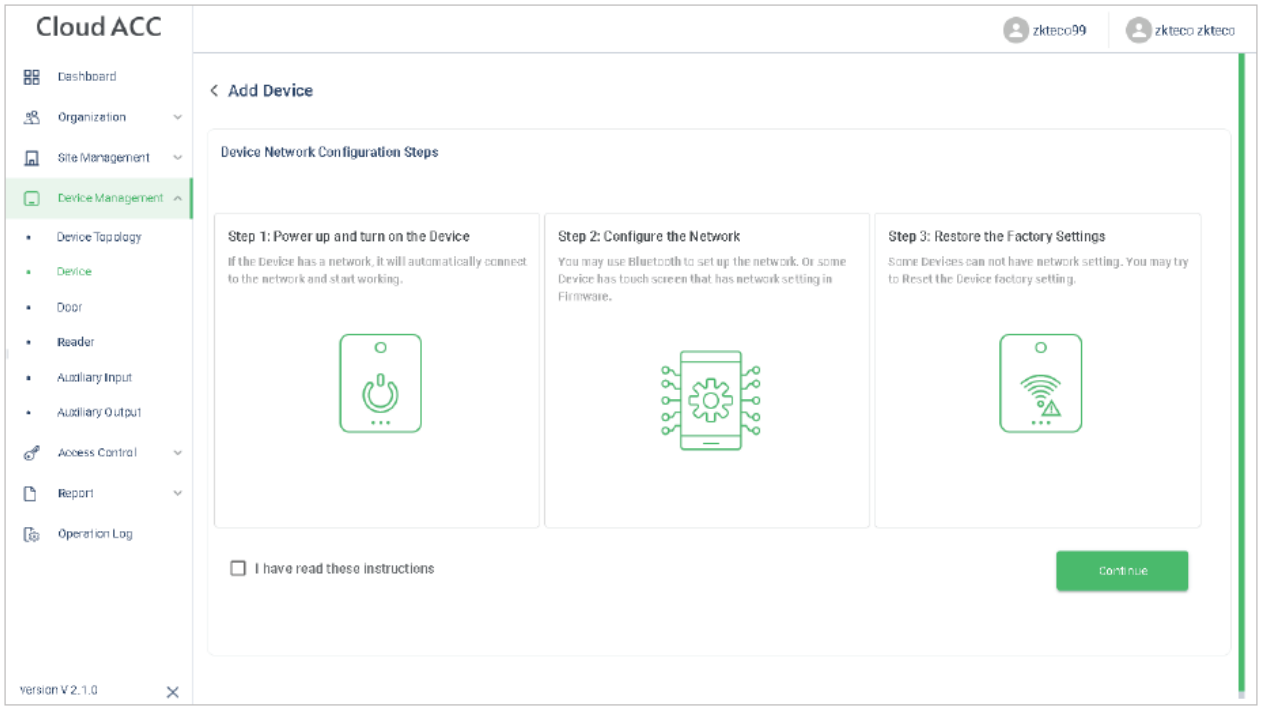
1.Presione M/OK e ingrese COMM. > Ethernet en el dispositivo para configurar la dirección IP y la puerta de enlace del dispositivo.



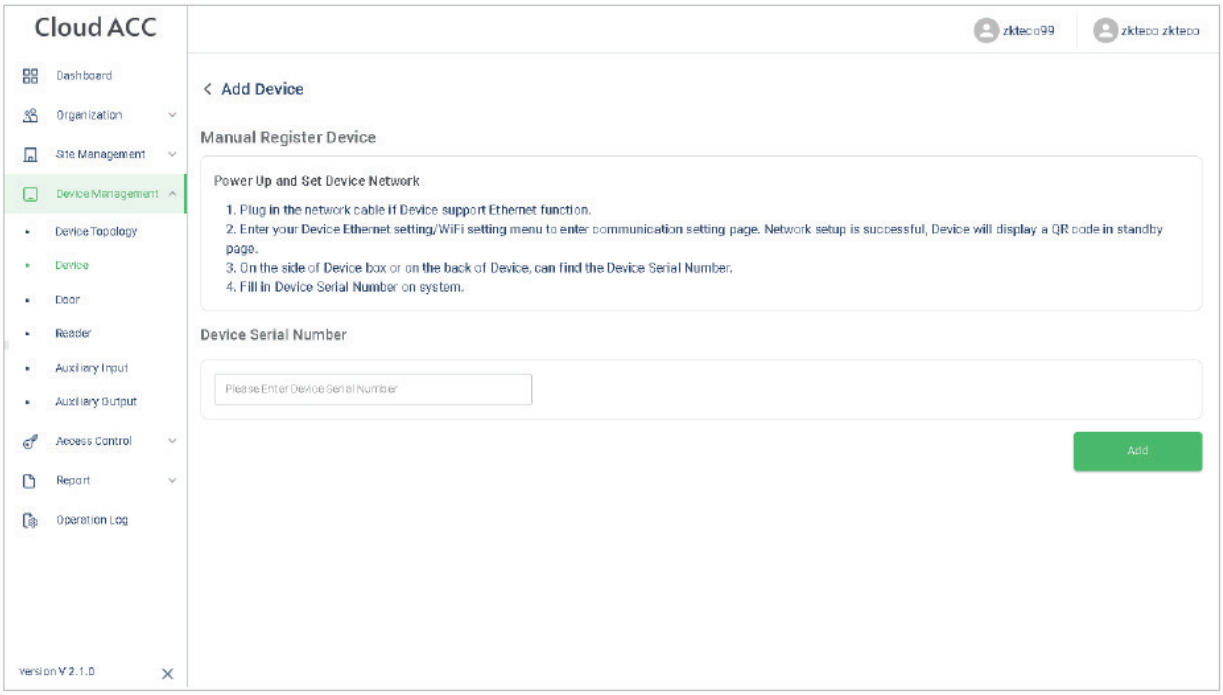
2.Haga clic en Workshop > CloudACC en el menú principal para ingresar a la interfaz de ZKBio Cloud Access.



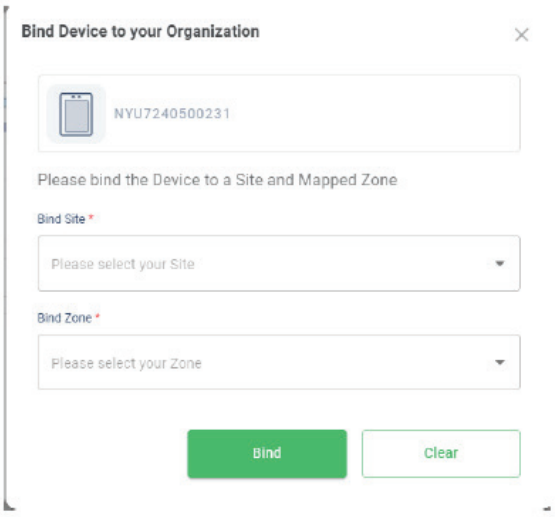
3.Haga clic en Administración de dispositivos > dispositivo para ingresar a la interfaz del dispositivo en ZKBio Cloud Access.
4.Haga clic en el botón +Agregar dispositivo para agregar un nuevo dispositivo.
5.Lea y verifique las instrucciones, luego haga clic en Continuar.



6.Ingrese el número de serie del dispositivo, luego haga clic en Agregar. (Presione M/OK e ingrese Información del sistema > DeviceInfo en el dispositivo para ver el número de serie)



7.Elija un sitio y una zona, luego haga clic en Vincular para finalizar.

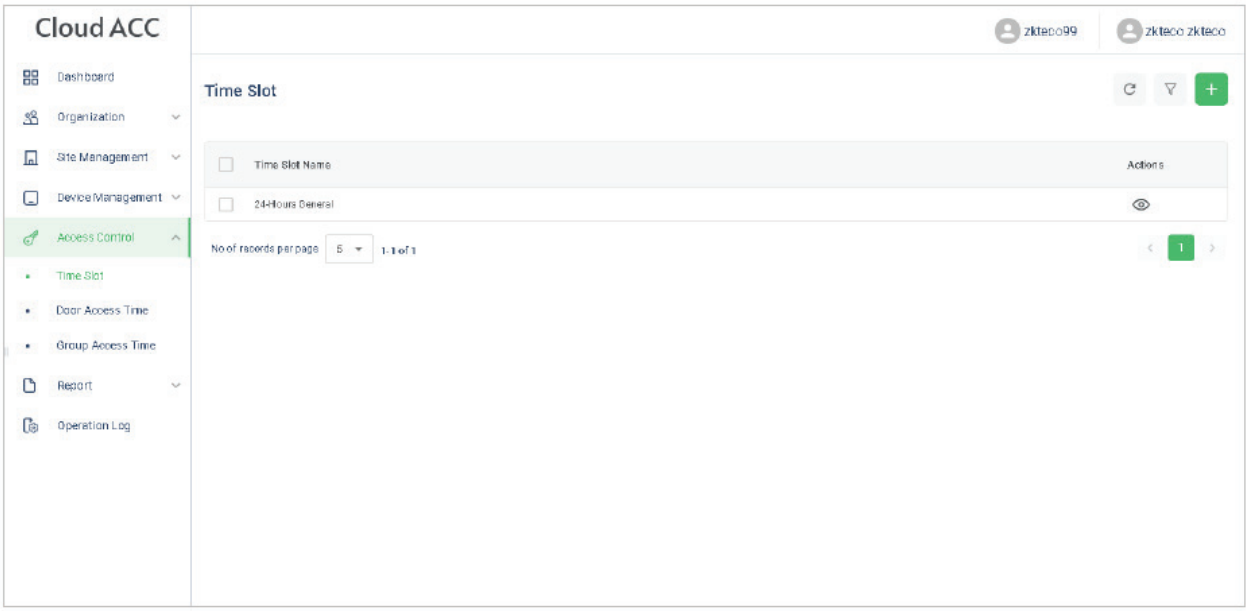


22.3 Franja horaria

La franja horaria se utiliza para establecer el período de tiempo de acceso para personas o puertas.

22.3.1 Establecer franja horaria

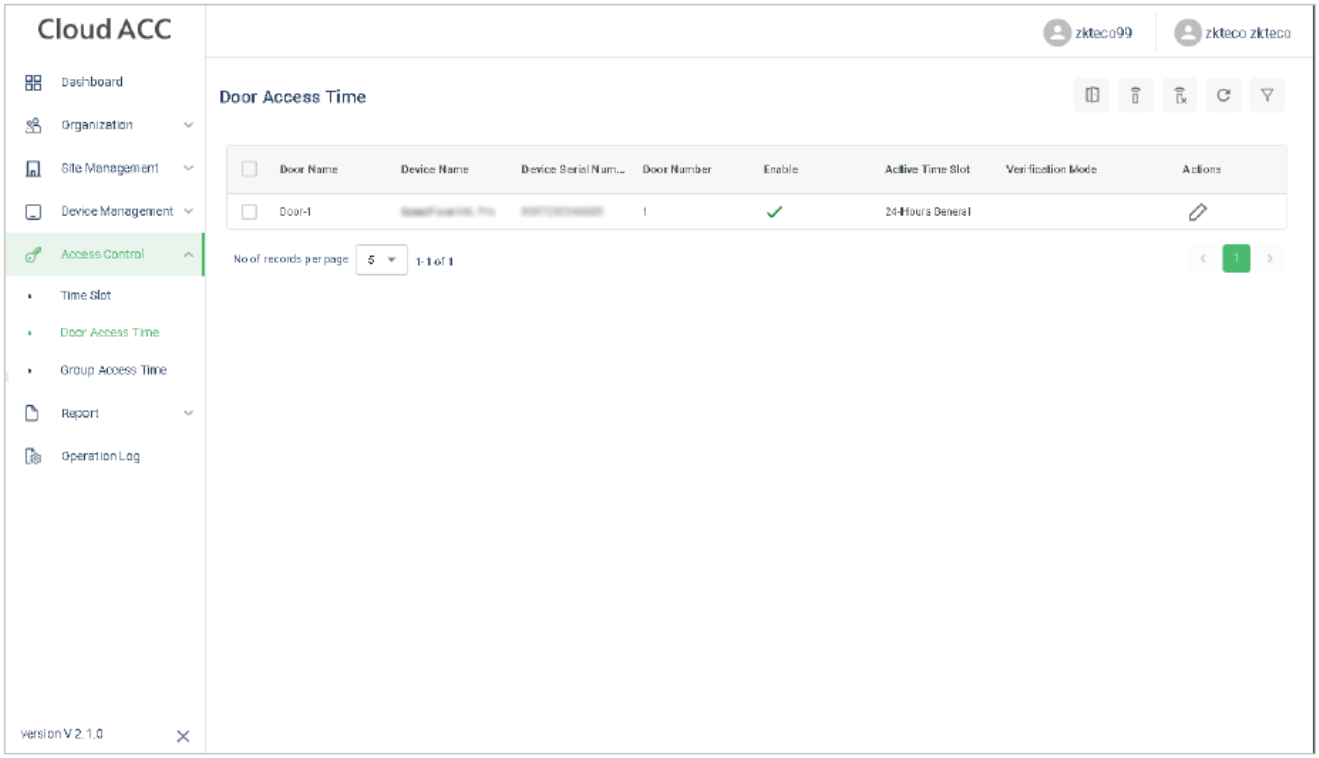
En la interfaz de acceso a la nube de ZKBio, haga clic en Control de acceso > franjas horarias para establecer la franja horaria.



Haga clic en +Añadir franjas horarias para añadir una nueva franja horaria, o haga clic para modificar una franja horaria existente.

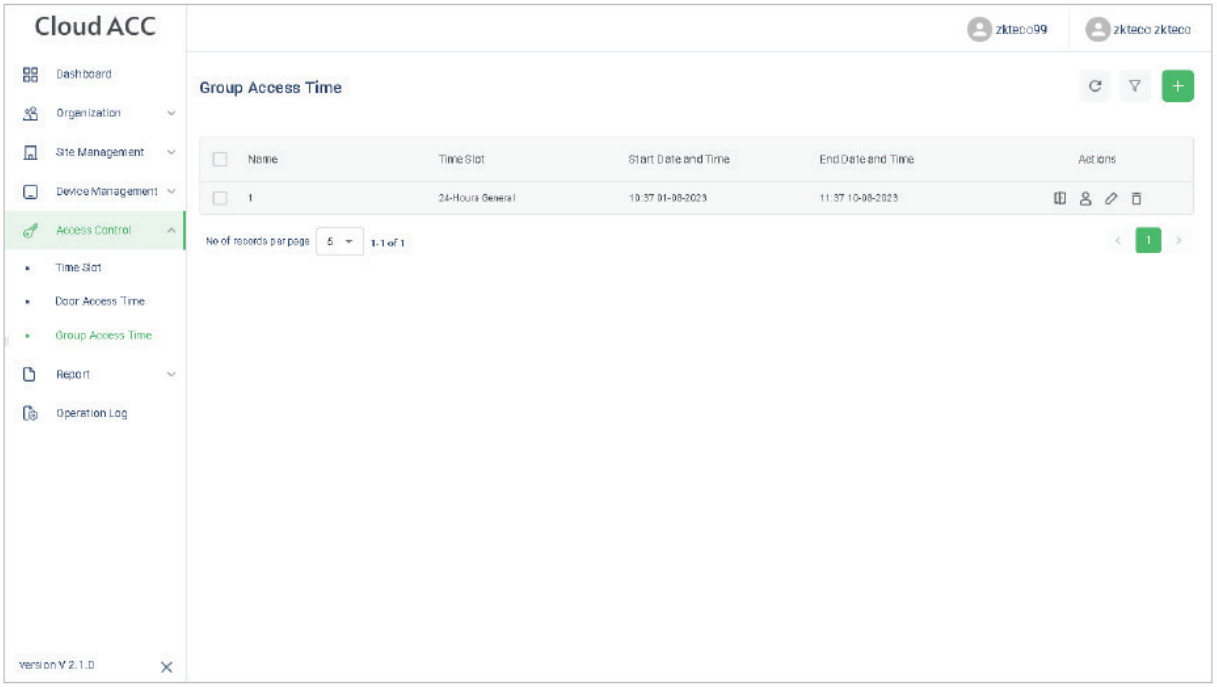
22.3.2 Establecer el tiempo de acceso a la puerta

En la interfaz de ZKBio Cloud Access, haga clic en Control de acceso > Tiempo de acceso a la puerta y haga clic para asignar un intervalo de tiempo a esta puerta.



22.3.3 Establecer el tiempo de acceso al grupo

Puede configurar un grupo para controlar el tiempo de acceso de la persona y la puerta al mismo tiempo. En la interfaz de acceso a la nube de ZKBio, haga clic en Control de acceso > Tiempo de acceso grupal.

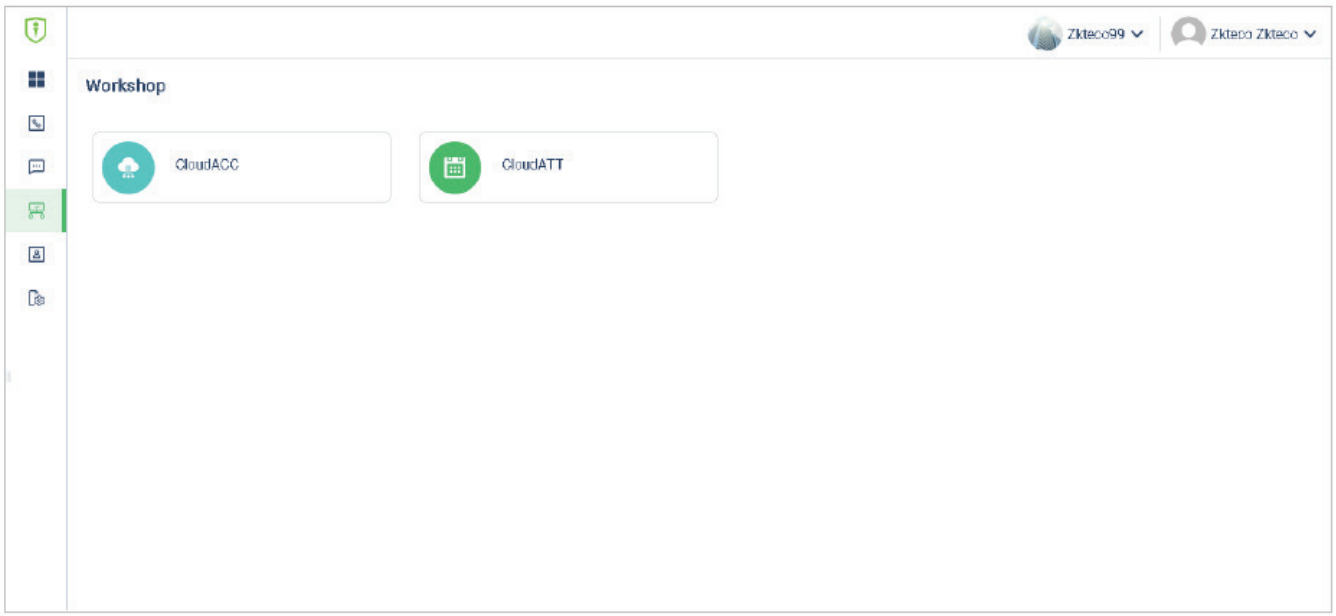


Haga clic en + Agregar tiempo de acceso grupal para agregar un nuevo grupo.
Clic para asignar puertas a este grupo.

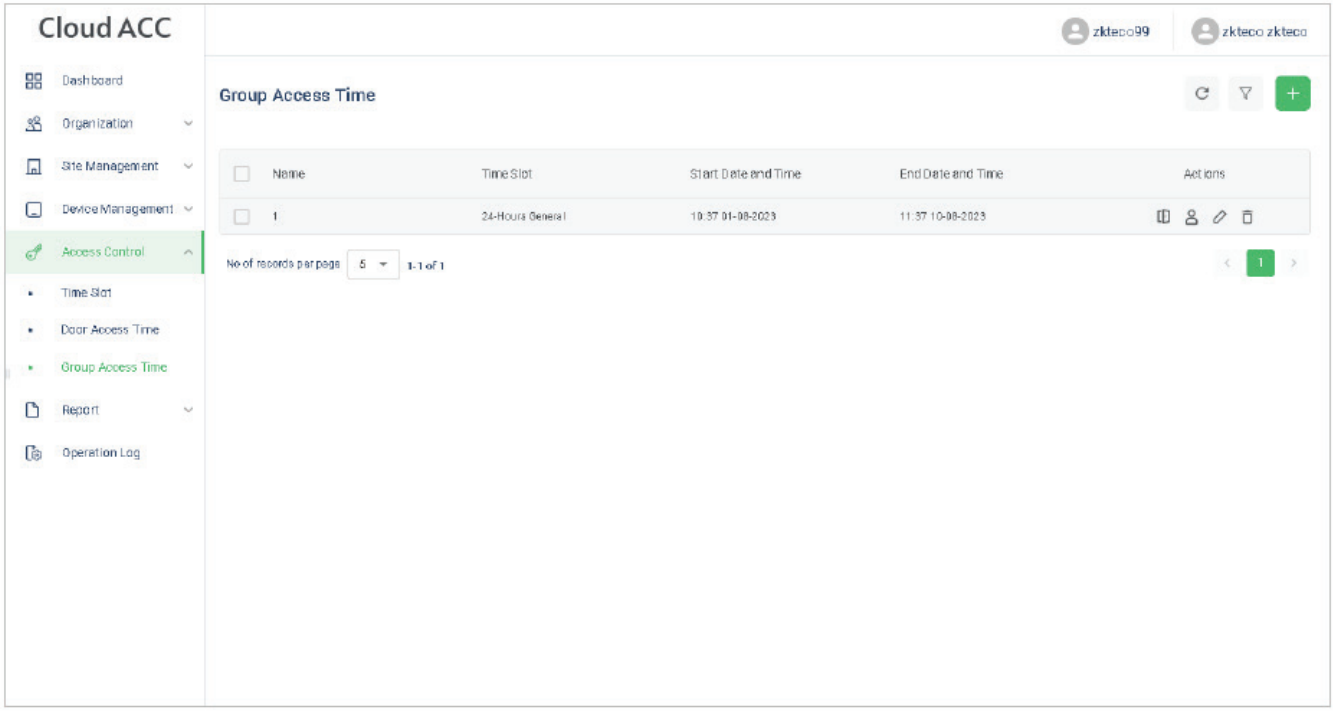
Clic para asignar una persona a este grupo.
Clic para asignar un intervalo de tiempo a este grupo.
Clic para eliminar este grupo.

22.4 Sincronizar persona con dispositivo

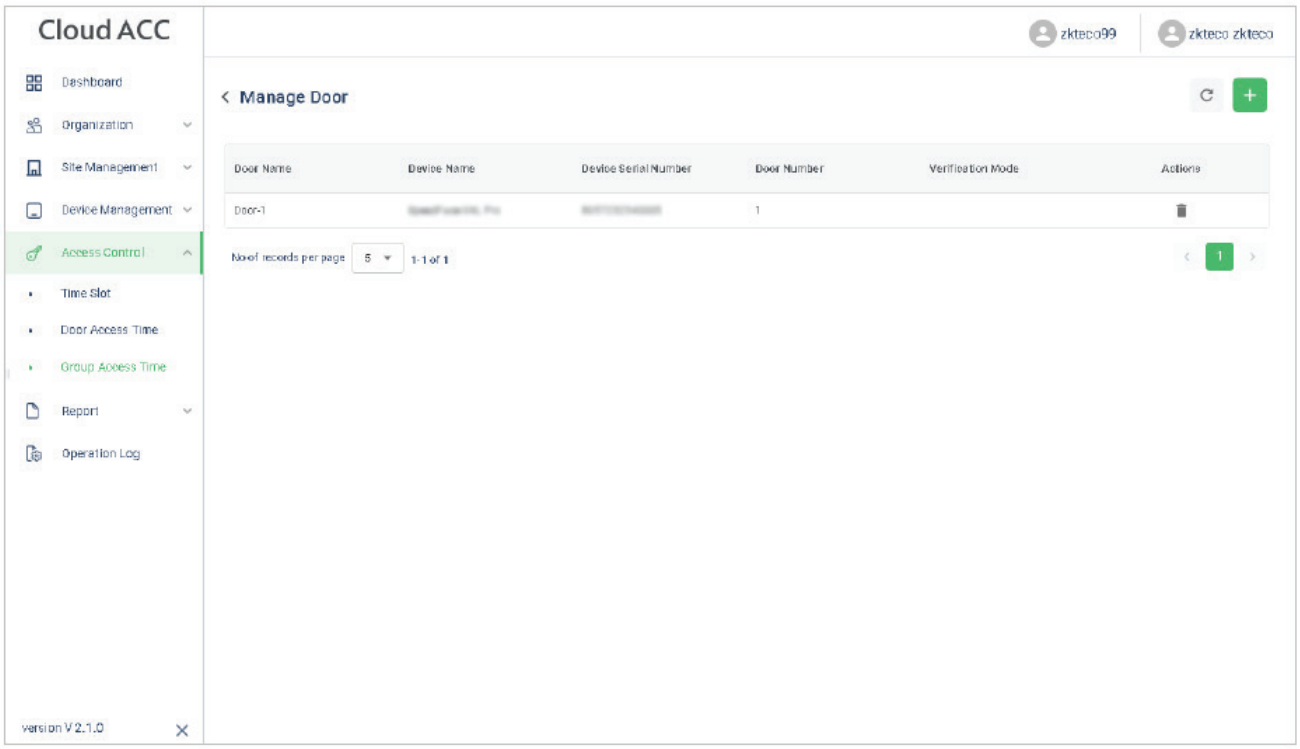
1.Haga clic en Workshop > CloudACC en el menú principal para ingresar a la interfaz de ZKBio CloudAccess.



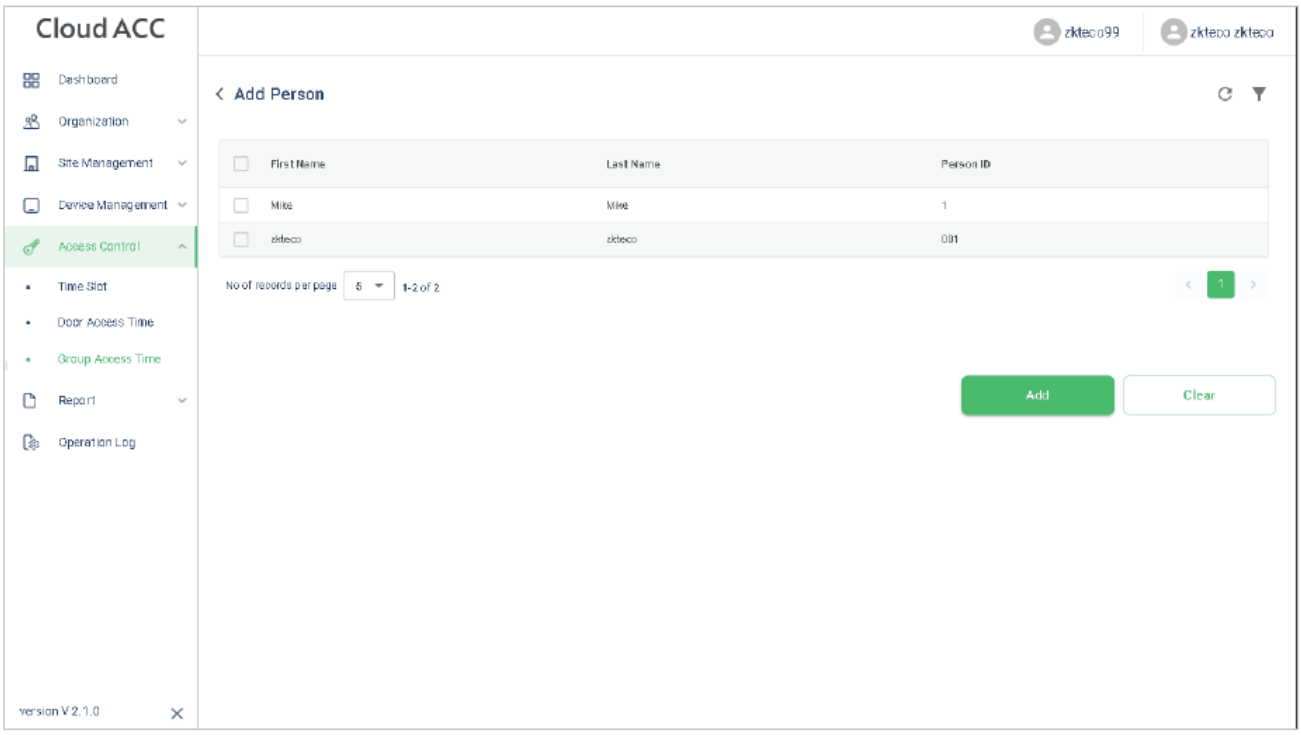
2.Haga clic en Control de acceso > Tiempo de acceso grupal.



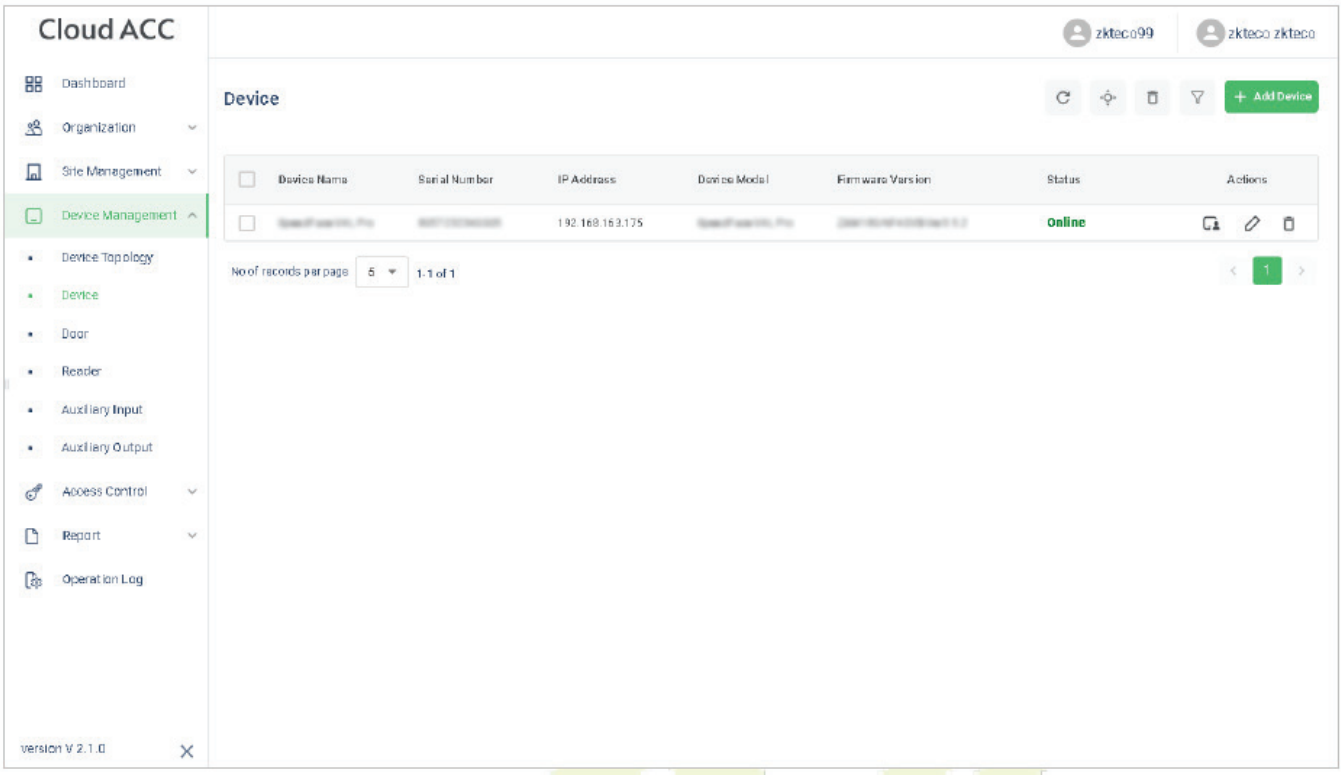
3.Clic > para elegir un dispositivo.



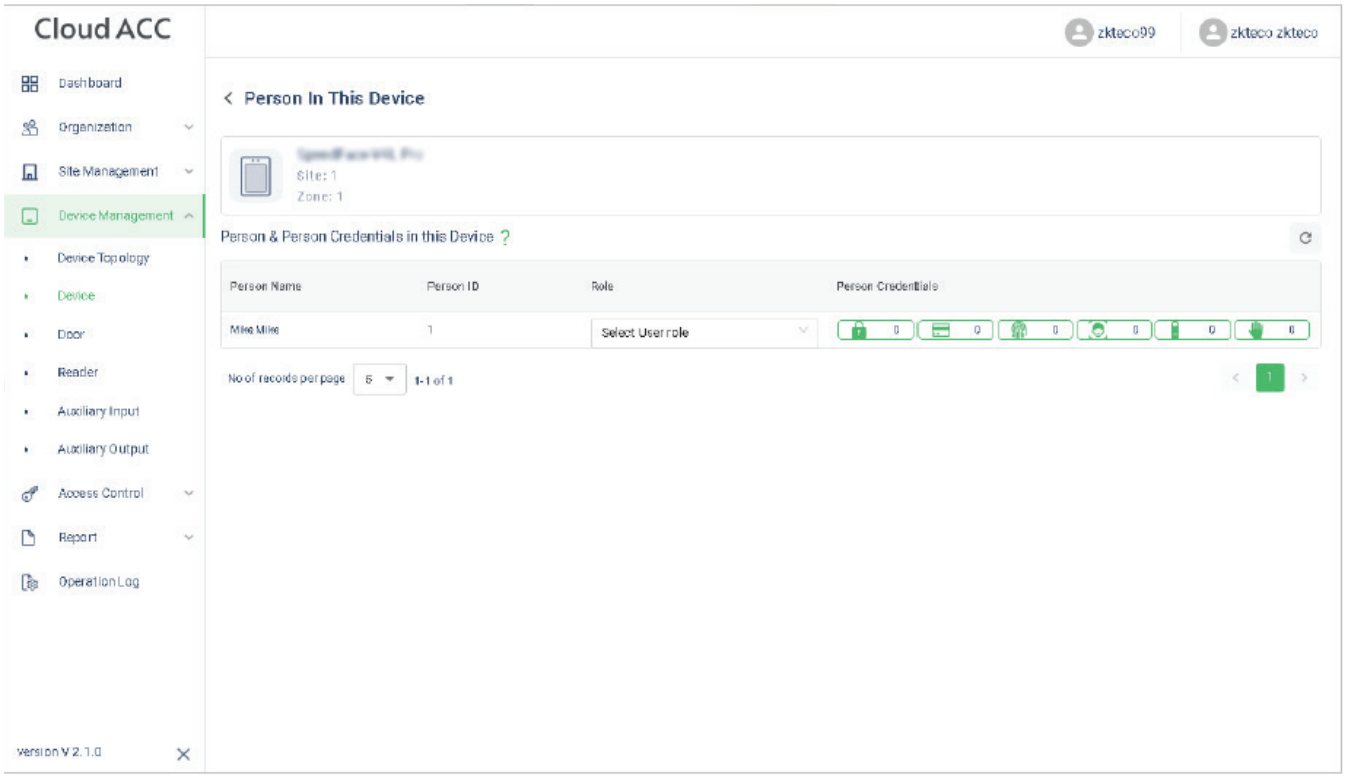
4.Clic > para asignar una persona a este dispositivo.



5.Haga clic en Administración de dispositivos > dispositivo para ingresar a la interfaz del dispositivo.



6.Elija un dispositivo y haga clic en Personas en el icono  Dispositivo para ver la lista de personas.



22.5 Registro de usuario

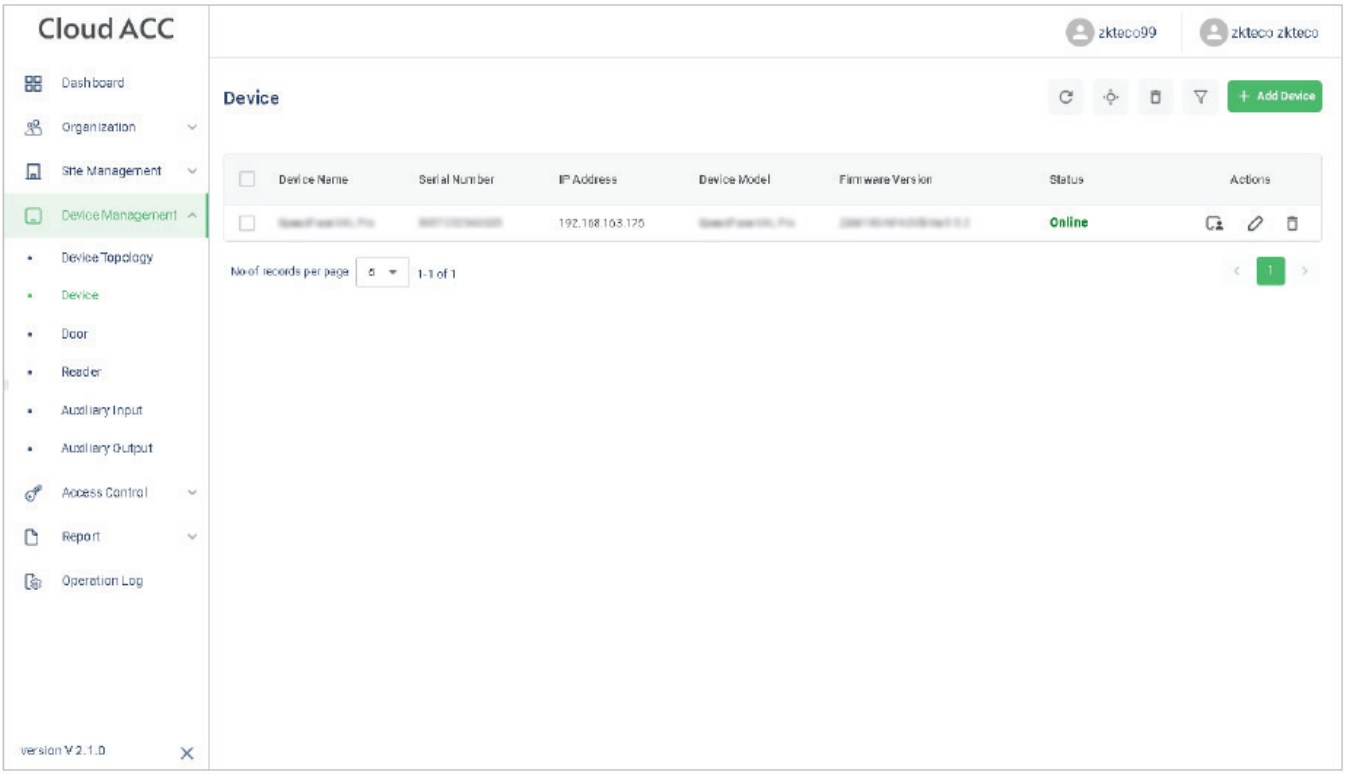
22.5.1 Registre un ID de usuario y un nombre

Consulte 22.2.1 Organización de conjuntos.

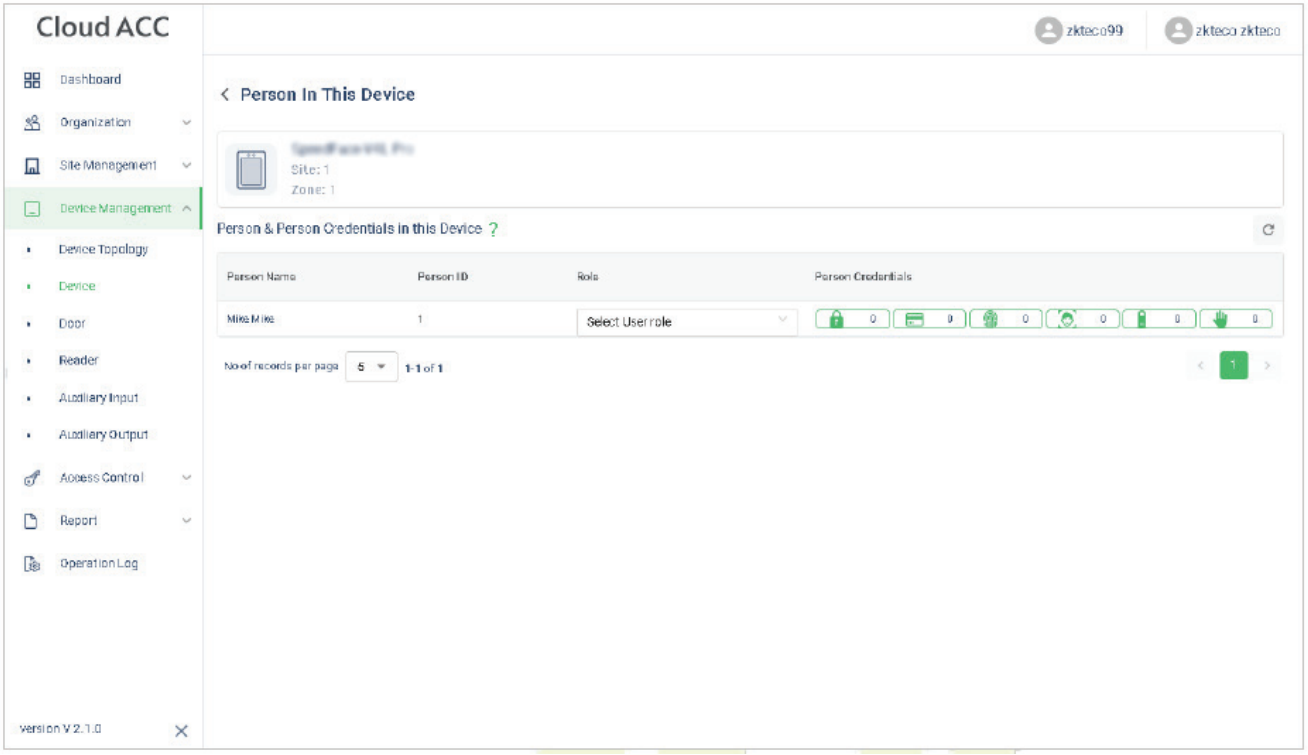
22.5.1 Registre un ID de usuario y un nombre

Hay dos tipos de cuentas de usuario: el usuario normal y el superadministrador. Si ya hay un administrador registrado, los usuarios normales no tienen derechos para administrar el sistema y solo pueden acceder a las verificaciones de autenticación. El administrador posee todos los privilegios de administración.

1.Haga clic en Administración de dispositivos > dispositivo en la interfaz de acceso a la nube de ZKBio para ingresar a la interfaz del dispositivo.
2. Seleccione un dispositivo y haga clic en «Personas» en el icono del dispositivo para ver la lista de personas.

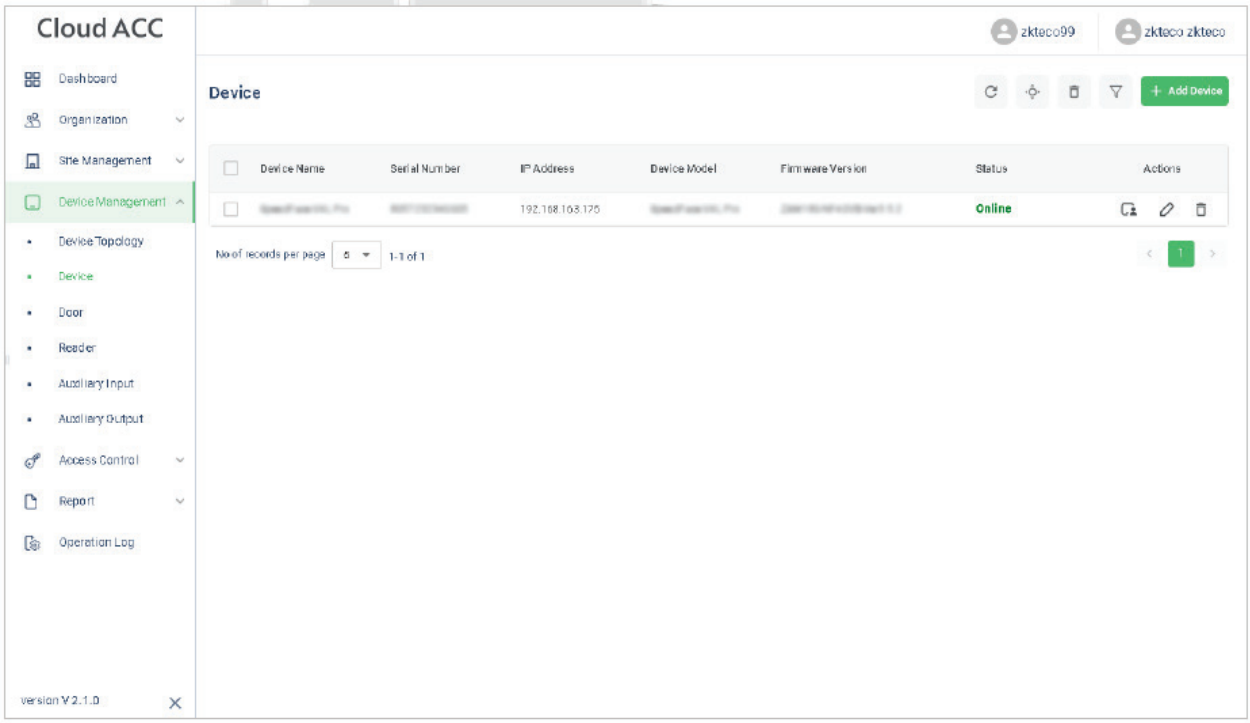


3.Elija el rol Seleccionar usuario.

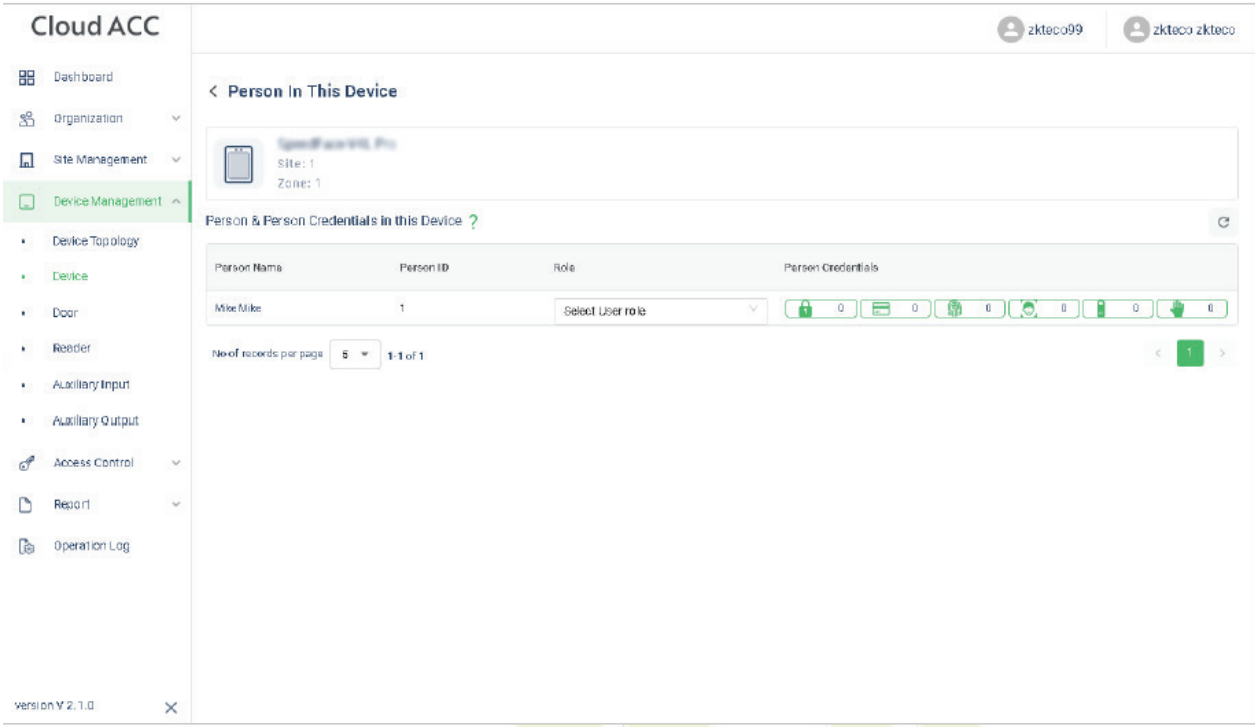


22.5.3 Registrar huella dactilar

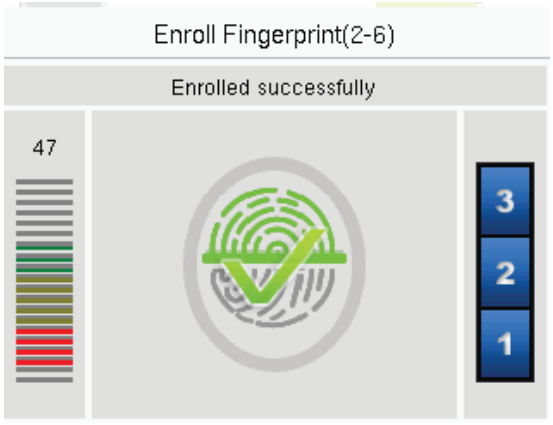
1.Haga clic en Administración de dispositivos > dispositivo en la interfaz de acceso a la nube de ZKBio para ingresar a la interfaz del dispositivo.
2.Elija un dispositivo y haga clic en Personas en el icono Dispositivo para ver la lista de personas.



3.Haga clic en para elegir un dedo, haz clic en Enviar y, a continuación, registra la huella digital en el dispositivo.

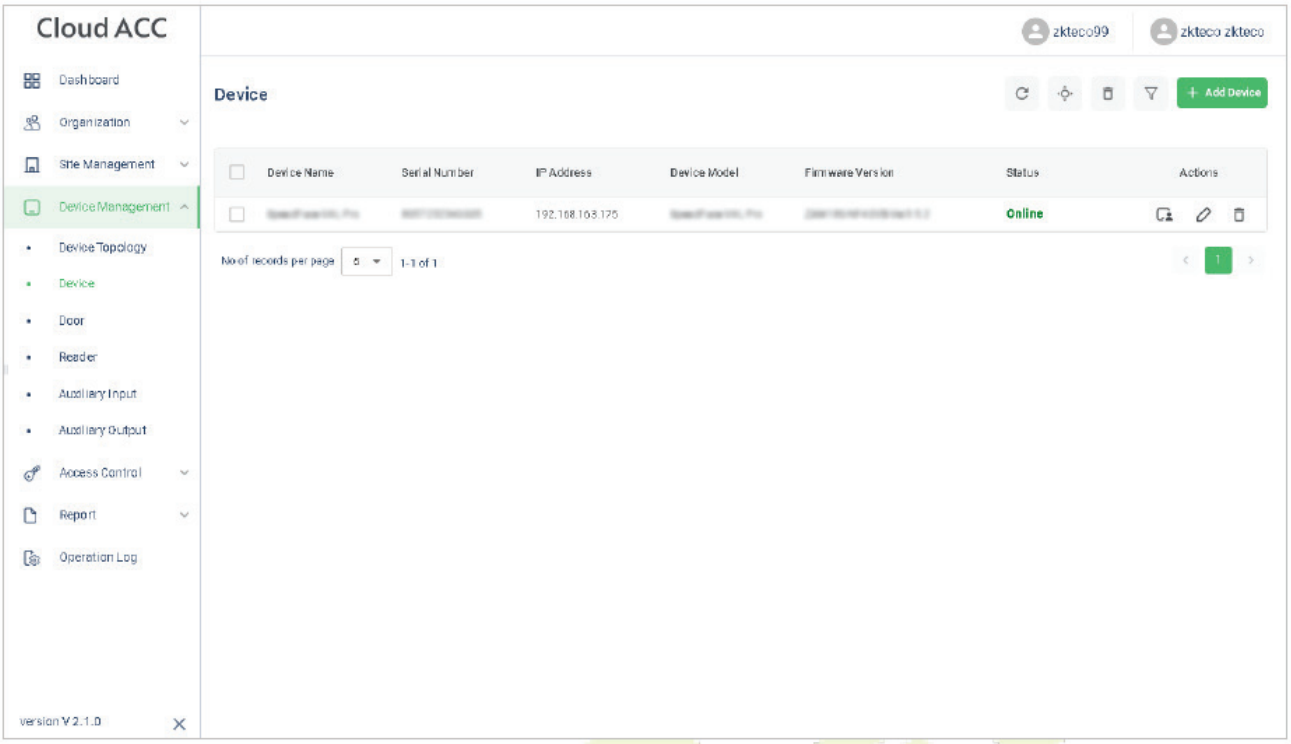


4.Presione el mismo dedo en el dispositivo tres veces. El verde indica que la huella digital se registró correctamente.

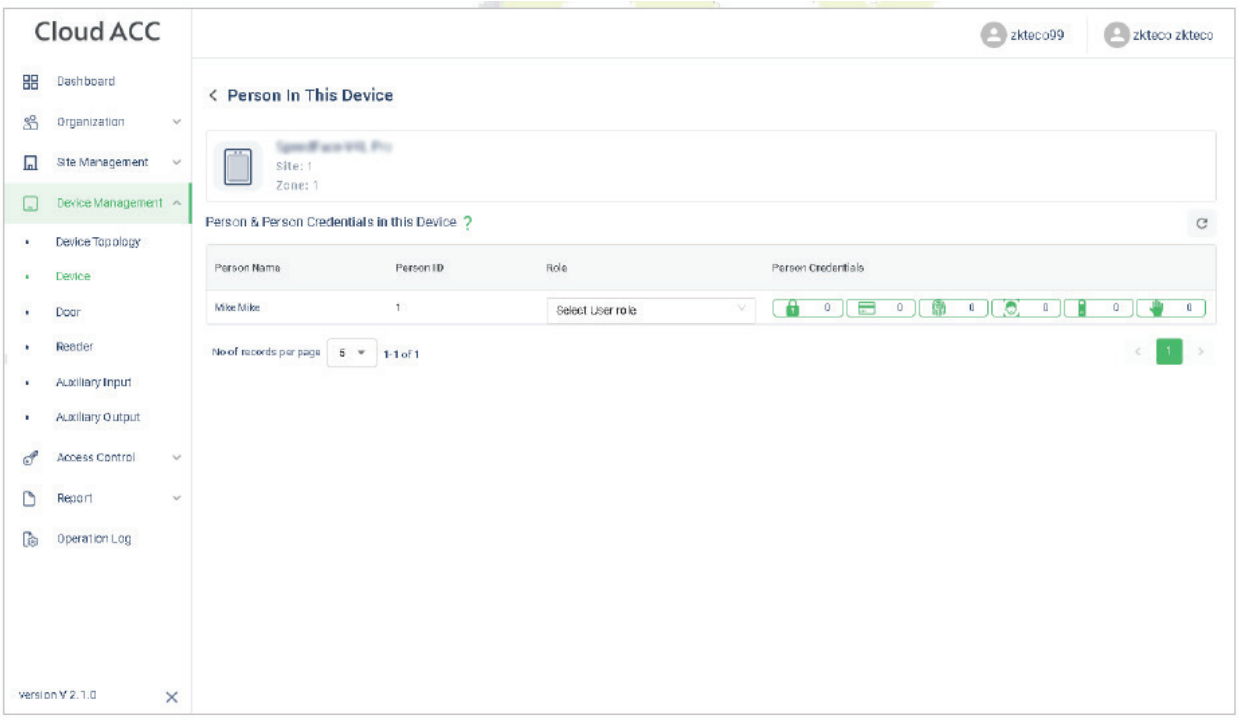


22.5.4 Plantilla de cara de registro

1.Haga clic en Administración de dispositivos > dispositivo en la interfaz de acceso a la nube de ZKBio para ingresar a la interfaz del dispositivo.
2.Elija un dispositivo y haga clic en Personas en el icono Dispositivo para ver la lista de personas.

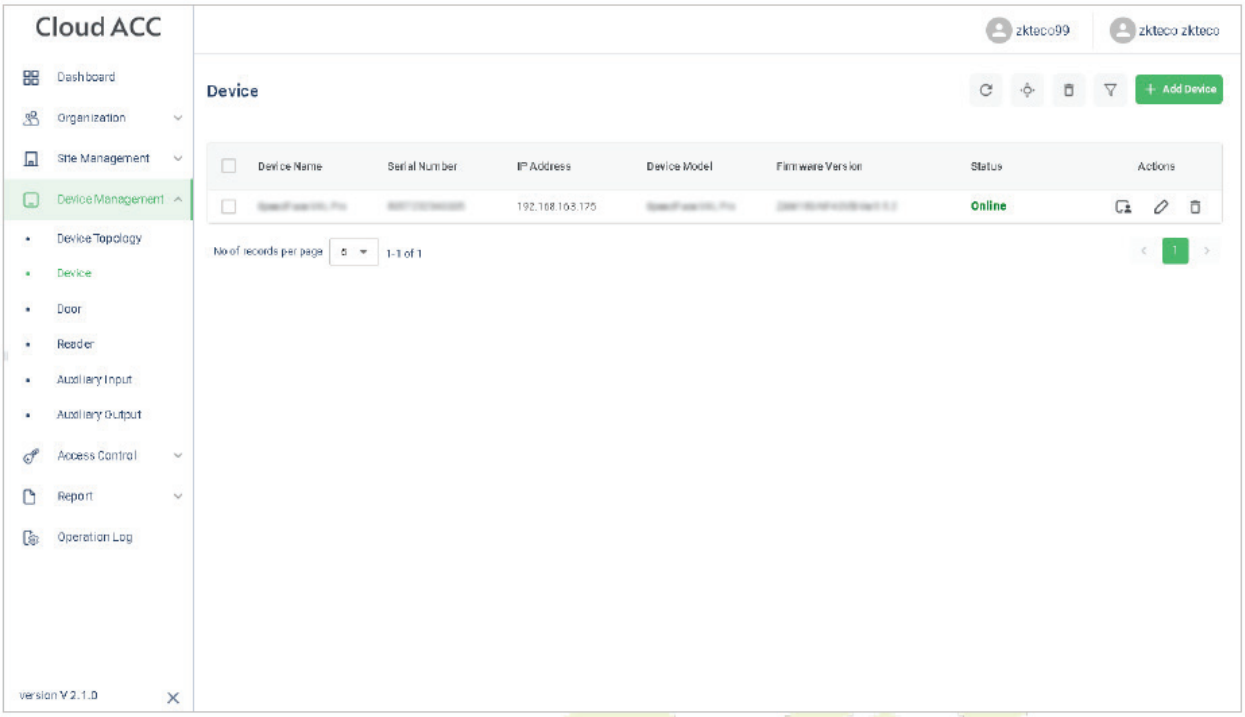


3.Haga clic en  para registrar la plantilla de cara en el dispositivo.

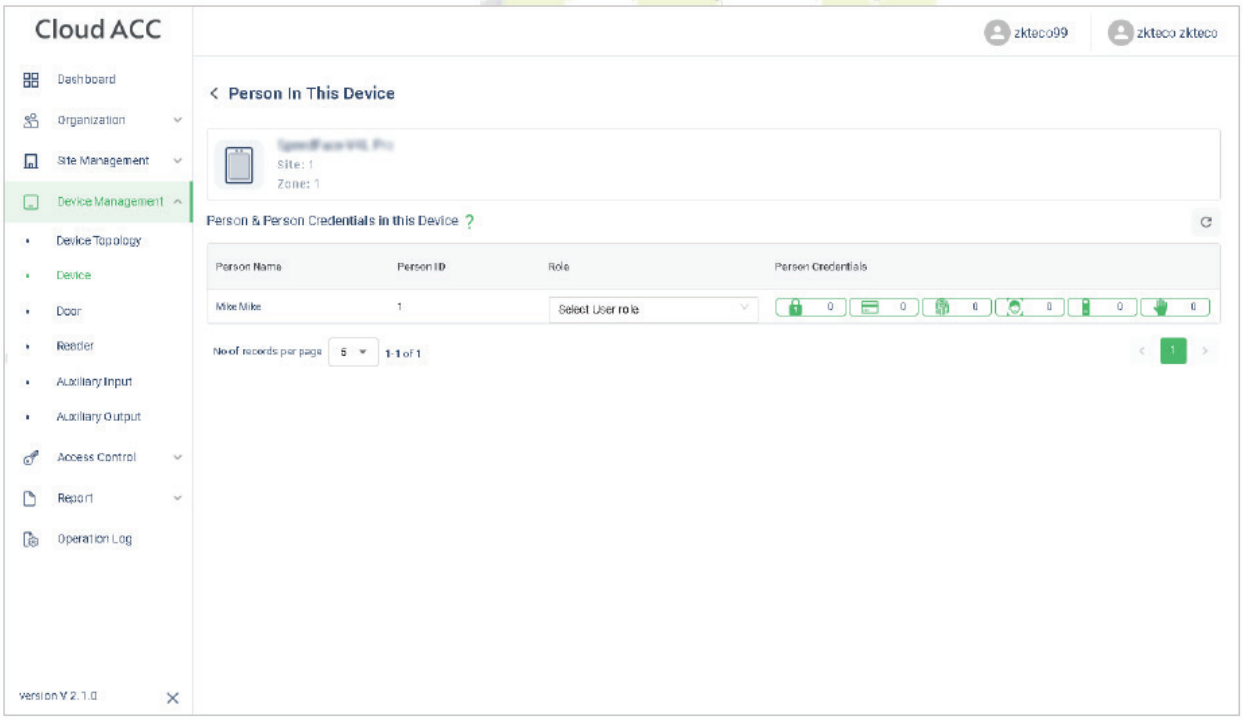


22.5.5 Contraseña de registro

1.Haga clic en Administración de dispositivos > dispositivo en la interfaz de acceso a la nube de ZKBio para ingresar a la interfaz del dispositivo.
2.Elija un dispositivo y haga clic en Personas en el icono Dispositivo para ver la lista de personas.



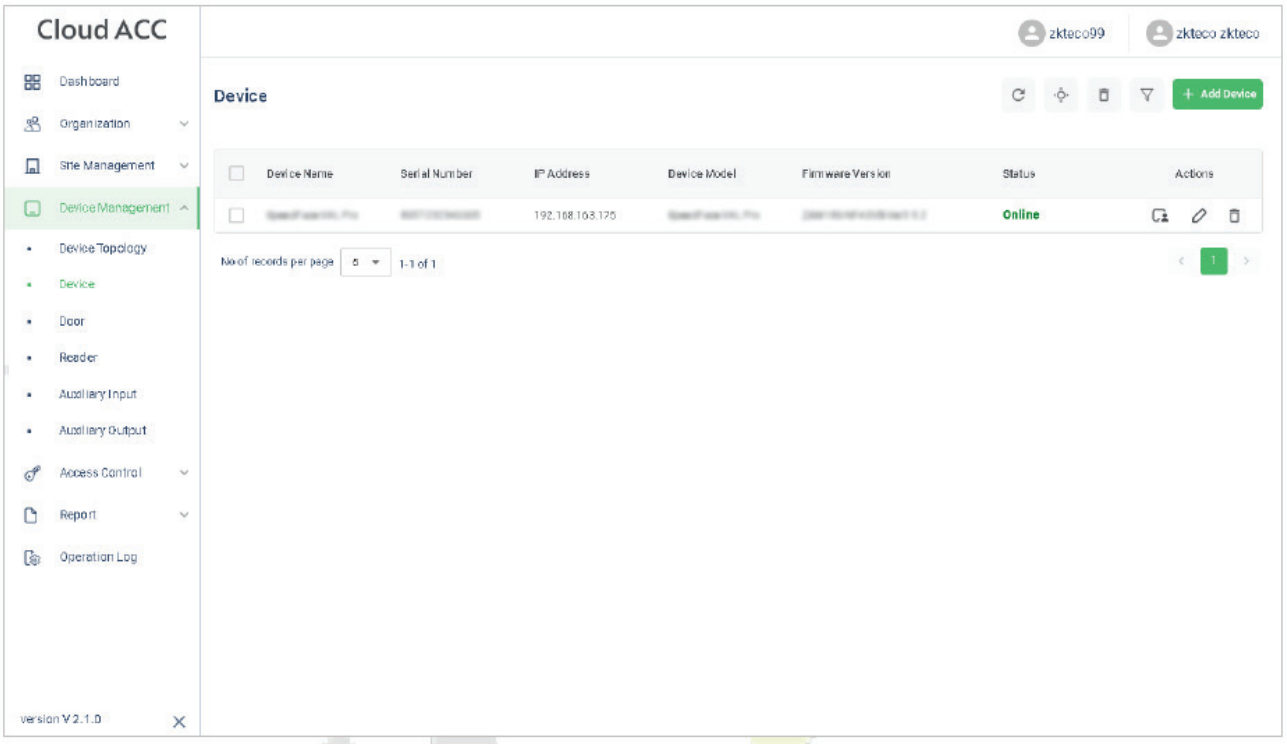
3.Haga clic en  para registrar la contraseña en el dispositivo.



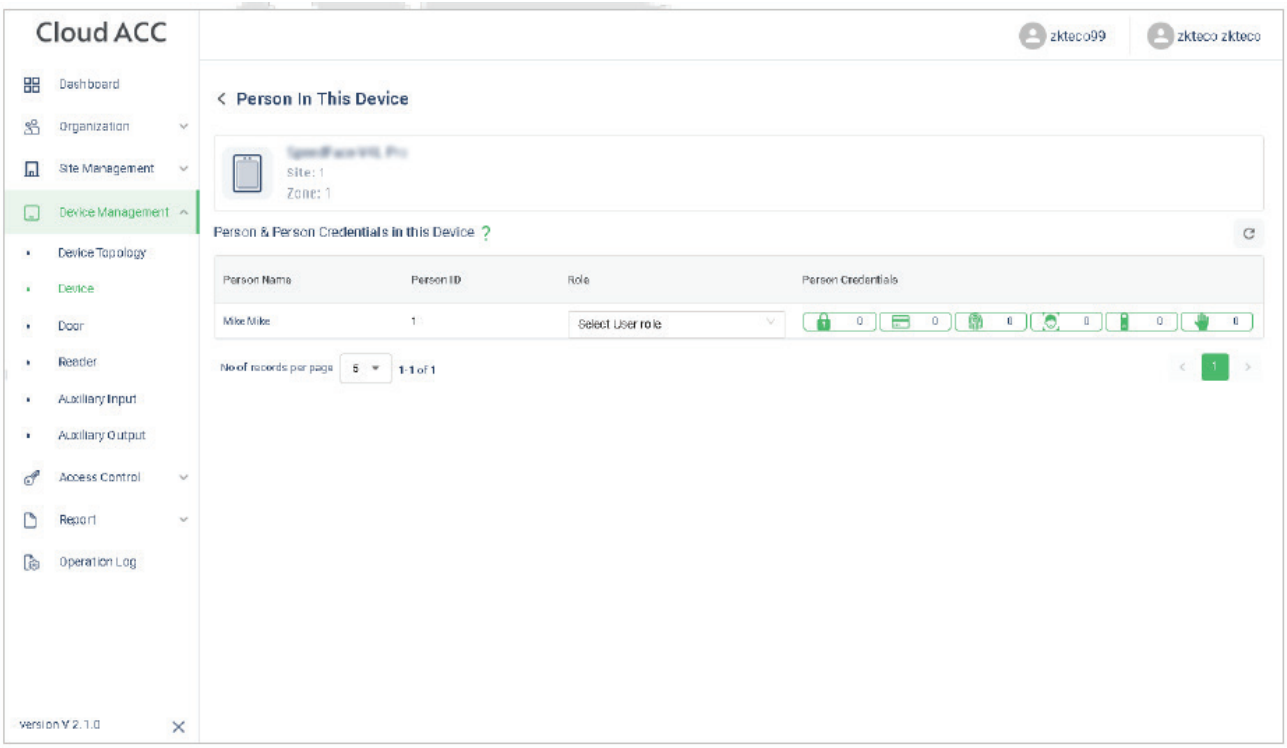
Nota: La contraseña puede contener de uno a ocho dígitos de forma predeterminada

22.5.6 Tarjeta de registro

1.Haga clic en Administración de dispositivos > dispositivo en la interfaz de acceso a la nube de ZKBio para ingresar a la interfaz del dispositivo.
2.Elija un dispositivo y haga clic en Personas en el icono Dispositivo para ver la lista de personas.



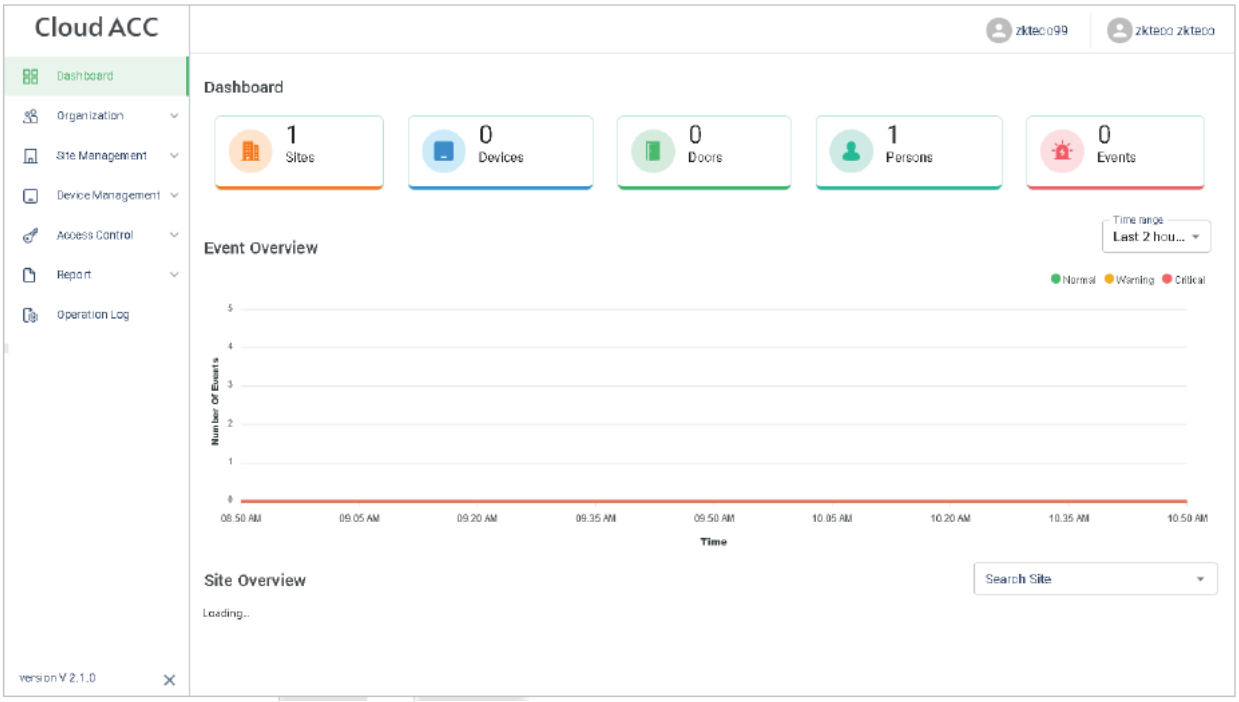
3.Haga clic en para registrar la contraseña en el dispositivo.



22.6 Búsqueda de datos

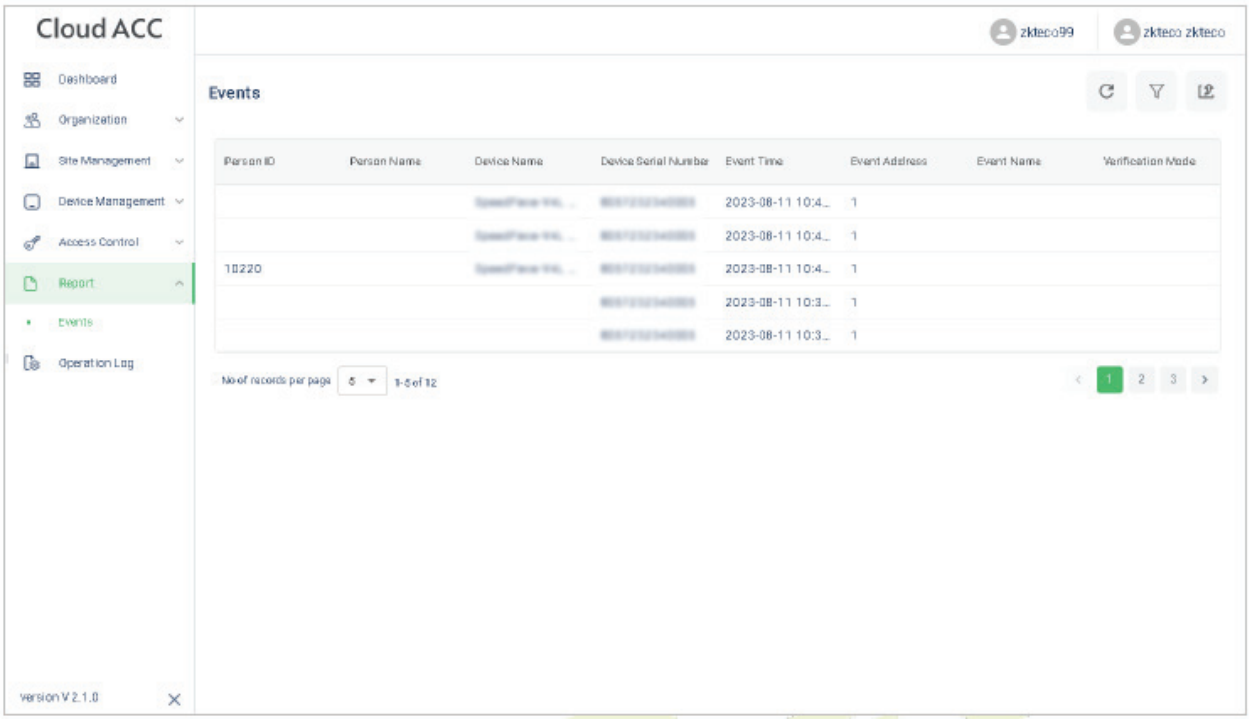
22.6.1 Panel de control

En la interfaz de ZKBio Cloud Access, haga clic en Panel de control para verificar los sitios, dispositivos, puertas, persona de esta aplicación, gráfico de descripción general de eventos y mapa de descripción general de sitios.



22.6.2 Informe de eventos

En ZKBioCloud Accessinterfaz, haga clic en Informar > eventos para verificar la información específica de los eventos de los dispositivos fallantes.

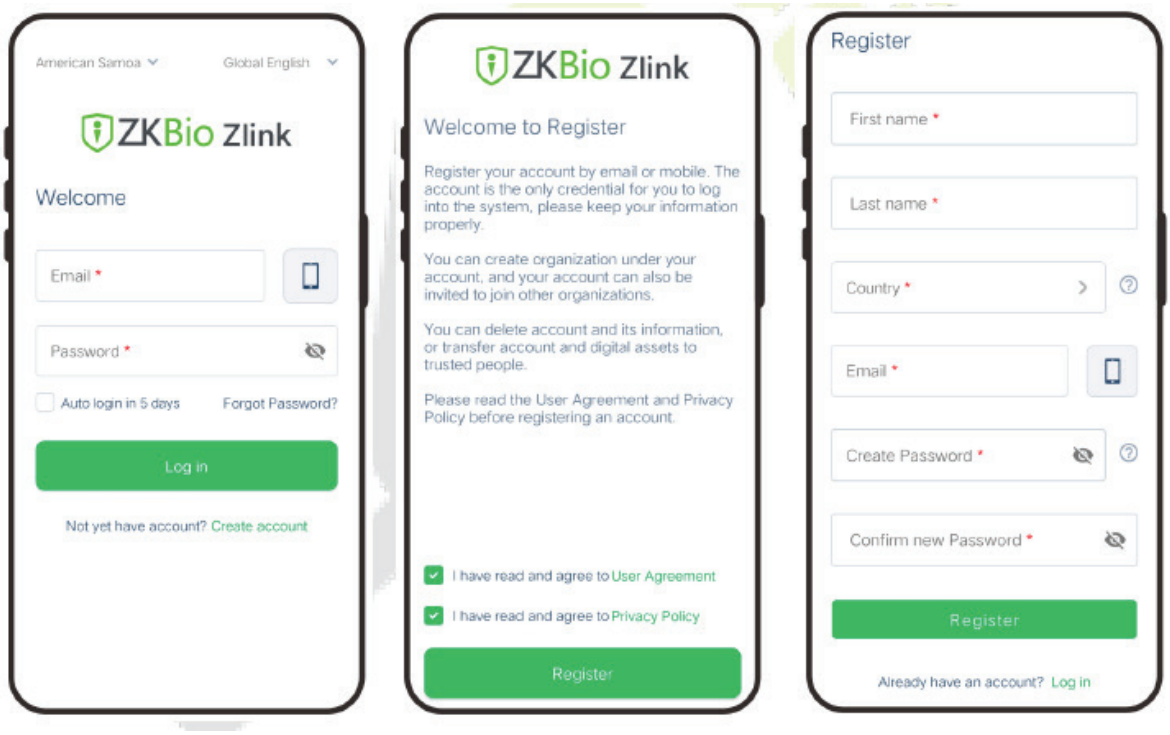

Cloud ACC
zkteco99
zkteco zkteco
Dashboard
Organization
Site Management
Device Management
Access Control
Report
Events
Operation Log
Events
Person ID
Person Name
Device Name
Device Serial Number
Event Time
Event Address
Event Name
Verification Mode
10220
2023-08-11 10:4...
2023-08-11 10:3...
No of records per page
1-5 of 12
version V 2.1.0

23 Conexión a la aplicación ZKBio Zlink

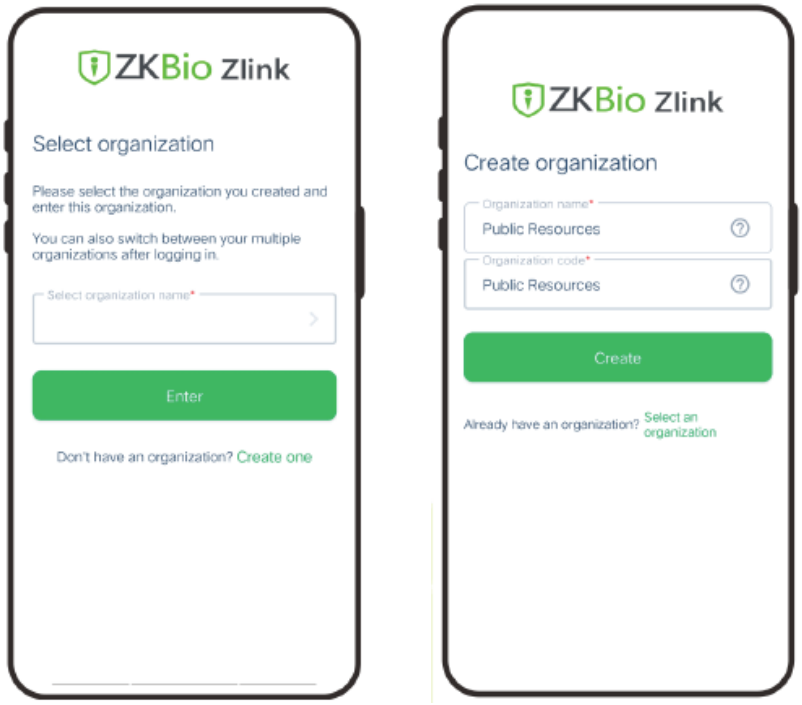
Cambie el protocolo de comunicación del dispositivo al protocolo BEST, entonces el dispositivo podrá ser gestionado por ZKBio Zlink. Consulte el apartado 11.5 Configuración del tipo de dispositivo. Los usuarios pueden utilizar la cuenta creada para acceder a la aplicación ZKBio Zlink y conectar dispositivos, desbloquear el dispositivo de forma remota y consultar registros.

23.1 Cuenta de registro

1. Busque la aplicación ZKBioZlink en Apple App Store o Google Play Store y descargue la aplicación en su teléfono inteligente.
2. Abra la aplicación ZKBioZlink y si no tiene una cuenta, haga clic en Crear cuenta para agregar una nueva cuenta.
3. Lea y acepte Acuerdo de usuario y Política de privacidad, luego haga clic en Registrarse .
4. Ingrese información del usuario y establezca contraseña, luego haga clic en Registrarse .

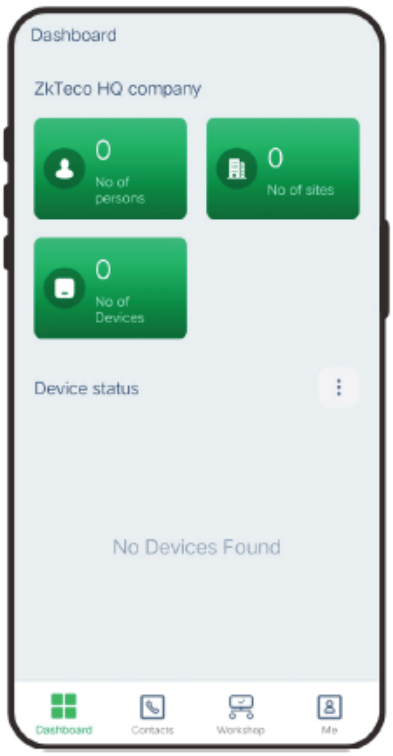


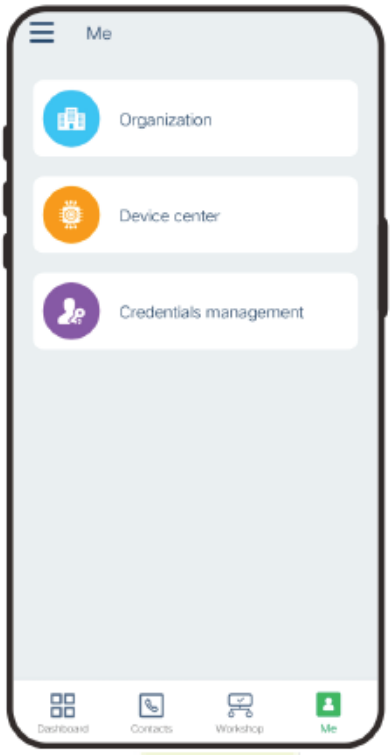
5.Elija una organización, haga clic en Entrar y, a continuación, complete el registro. Si no tiene una organización, haga clic en Crear una

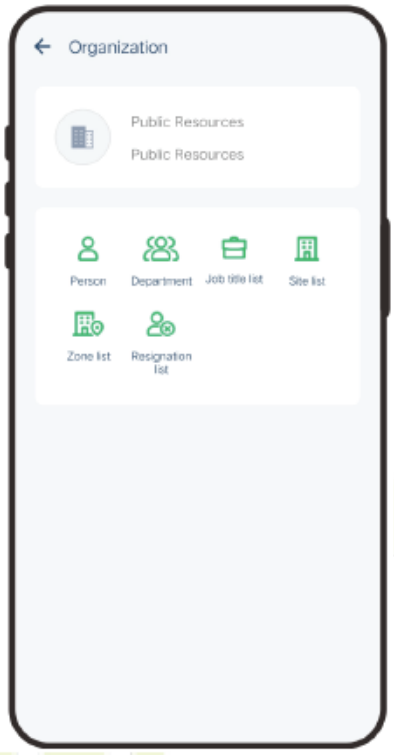


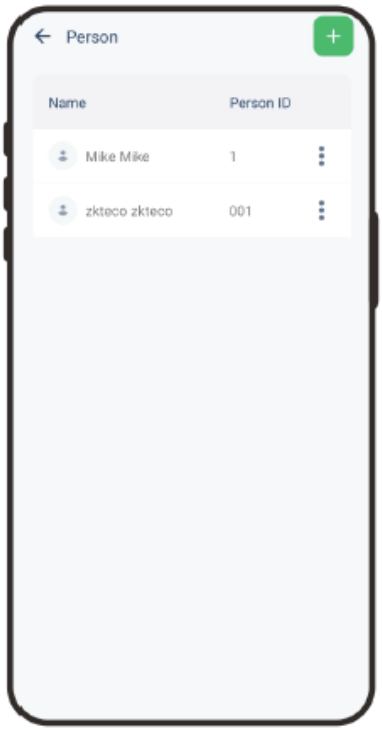
23.2 Agregar persona

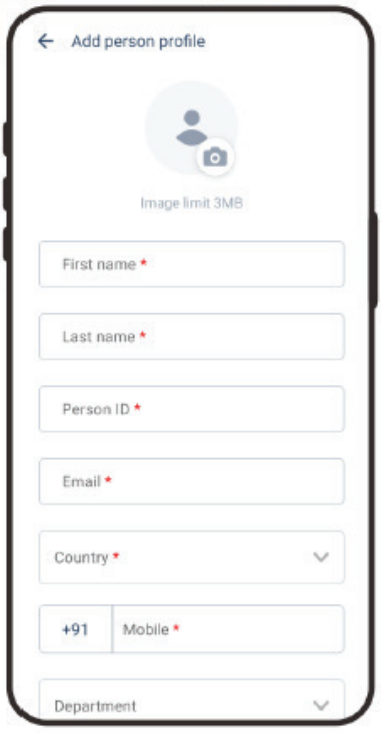
1.Haga clic en Yo > organización > persona en el menú principal.
2.Haga clic en + para agregar una nueva persona. Introduzca la información y haga clic en Guardar.


Dashboard
ZkTeco HQ company
0
No of persons
0
No of sites
0
No of Devices
Device status
No Devices Found
Dashboard
Contacts
Workshop
Me


Me
Organization
Device center
Credentials management
Dashboard
Contacts
Workshop
Me


Organization
Public Resources
Public Resources
Person
Department
Job title list
Site list
Zone list
Resignation list

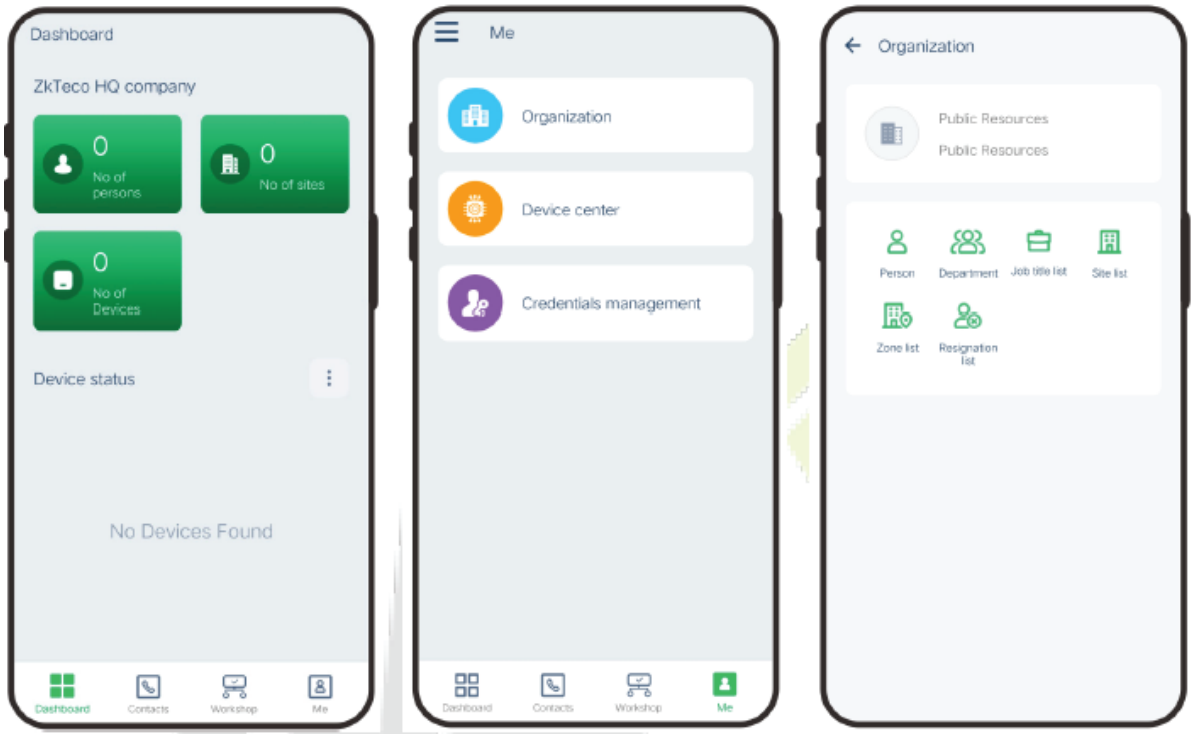

Person
Name
Person ID
Mike Mike
1
zkteco zkteco
001

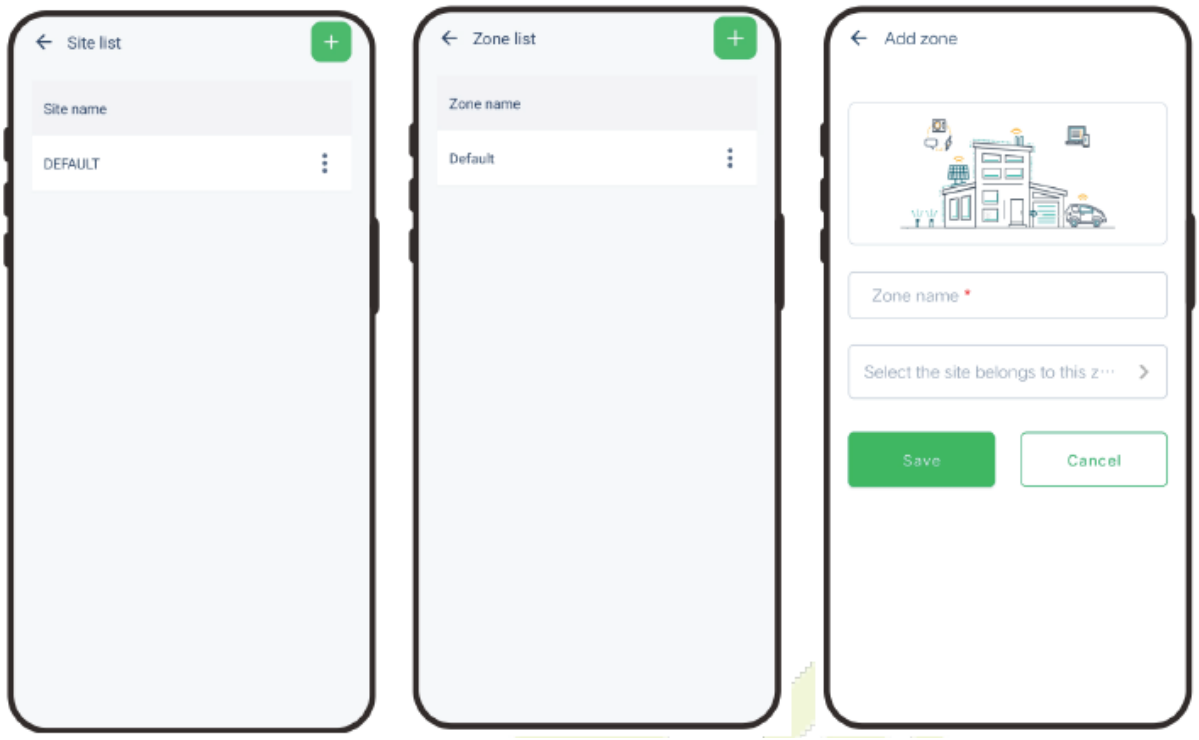

Add person profile
Image limit 3MB
First name *
Last name *
Person ID *
Email *
Country *
+91
Mobile *
Department

23.3 Agregar dispositivo

23.3.1 Agregar sitio y zona

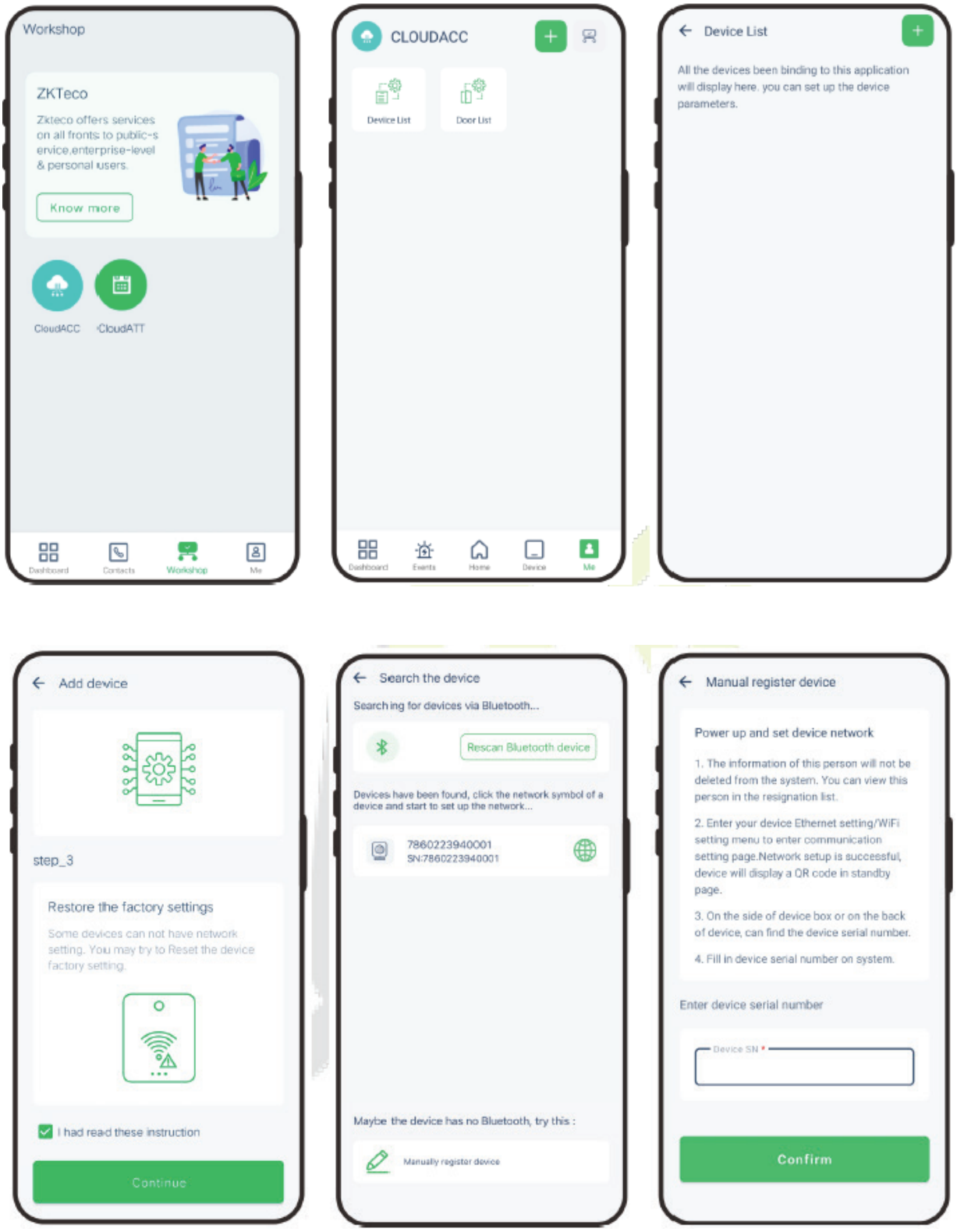
1. Haga clic en Yo > organización > sitio (o zona) en el menú principal.
2. Haga clic en el icono + para añadir un nuevo sitio o zona. Introduzca la información y haga clic en Guardar.



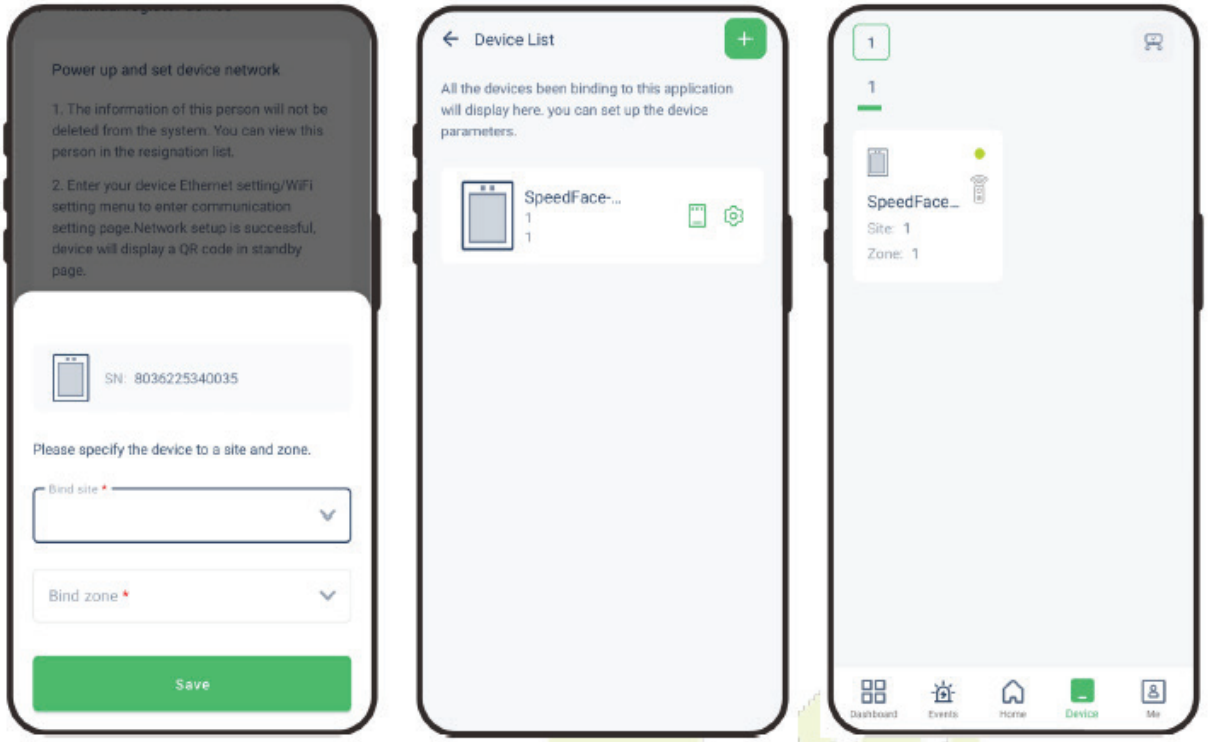


23.3.2 Agregar dispositivo

1.Presione M/OK e ingrese COMM. > Ethernet en el dispositivo para configurar la dirección IP y la puerta de enlace del dispositivo.
2.Haga clic en Workshop > CloudACC en el menú principal para ingresar a la interfaz de ZKBio Cloud Access.
3.Haga clic en Yo > lista de dispositivos para ingresar a la interfaz del dispositivo. Y haga clic en + para agregar un nuevo dispositivo.
4.Haga clic en Registrar dispositivo manualmente.
5.Lea y verifique las instrucciones, luego haga clic en Continuar.
6.Introduzca el número de serie del dispositivo y, a continuación, haga clic en Confirmar. (Presione M/OK e ingrese Información del sistema >Información del dispositivo en el dispositivo para ver el número de serie).



7.Elija un sitio y una zona, luego haga clic en Guardar para finalizar.
8. Luego haga clic en Dispositivo, los usuarios pueden ver el estado del dispositivo y desbloquearlo de forma remota en esta interfaz.

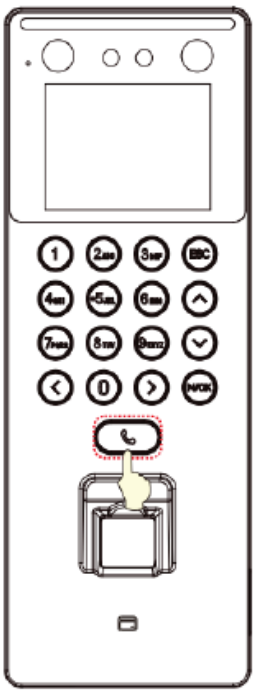

Power up and set device network
1. The information of this person will not be deleted from the system. You can view this person in the resignation list.
2. Enter your device Ethernet setting/WiFi setting menu to enter communication setting page.Network setup is successful, device will display a QR code in standby page.
SN: 8036225340035
Please specify the device to a site and zone.
Bind site *
Bind zone *
Save
Device List
All the devices been binding to this application will display here. you can set up the device parameters.
SpeedFace-...
1
1
1
1
SpeedFace...
Site: 1
Zone: 1
Dashboard
Events
Home
Device
Me

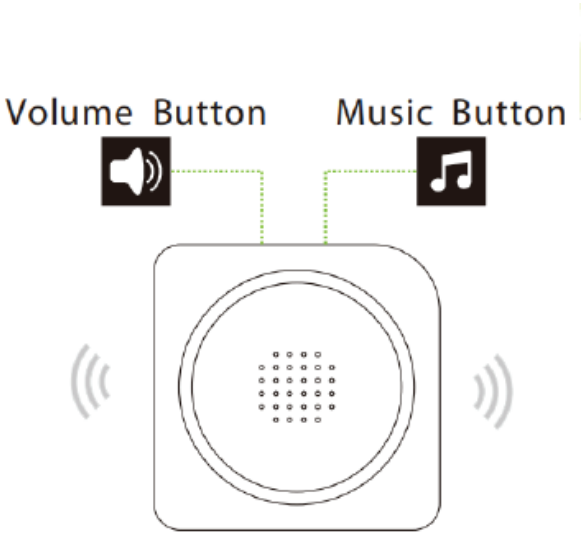
24 Conexión al timbre inalámbrico ★

Nota: Esta función debe utilizarse con el timbre inalámbrico.

24.1 Conecte el timbre inalámbrico

1. Primero, encienda el timbre inalámbrico. A continuación, mantenga pulsado el botón de música durante 1,5 segundos hasta que el indicador parpadee para indicar que está en modo de emparejamiento. Después, pulse el botón del timbre en el dispositivo; si el timbre inalámbrico suena y el indicador parpadea, significa que el emparejamiento se ha realizado correctamente.





2. Después de un emparejamiento exitoso, presione el botón del timbre de la puerta en el dispositivo hará sonar el timbre inalámbrico.

Nota:

1. Para utilizar esta función, debe acceder al menú ([Intercomunicador] > [Configuración del timbre]) y seleccionar la opción «Solo timbre» o «Timbre + videoportero».
2. Cada F35 solo admite un timbre inalámbrico.
3. El timbre inalámbrico debe ser adquirido por los propios clientes.

24.2 Desvincular el timbre inalámbrico

Apague primero el timbre inalámbrico y, a continuación, vuelva a instalar las pilas mientras mantiene pulsado el botón de música hasta que se encienda el indicador, lo que indica que la desvinculación se ha realizado correctamente.

Apéndice

Requisitos de la recopilación en vivo y el registro de plantillas de rostros VisibleLight

1) Se recomienda realizar el registro en un ambiente interior con una luz adecuada
fuente sin subexposición o sobreexposición.
2) No coloque el dispositivo cerca de fuentes de luz exteriores como puertas o ventanas u otra luz intensa
fuentes.
3) Se recomiendan prendas de color oscuro, diferentes del color de fondo para el registro.
4) Exponga su plantilla de cara y frente correctamente y no cubra su plantilla de cara y
cejas con el cabello.
5) Se recomienda mostrar una expresión facial sencilla. (Una sonrisa es aceptable, pero no cierre sus ojos, o
inclinar la cabeza a cualquier orientación).
6) Se requieren dos plantillas para una persona con anteojos, una plantilla con anteojos y el
otros sin los anteojos.
7) No use accesorios como una bufanda o mascarilla que pueda cubrir su boca o barbilla.
8) Mire la plantilla directamente hacia el dispositivo de captura y ubique su plantilla de cara en el
área de captura de la plantilla como se muestra en la plantilla a continuación.
9) No incluya más de una plantilla de cara en el área de captura.
10) Se recomienda una distancia de 50 cm a 80 cm para capturar la plantilla. (La distancia es
ajustable, sujeto a la altura del cuerpo).



Requisitos para los datos de la plantilla de rostro digital de luz visible

La foto digital debe ser de bordes rectos, coloreada, medio retratada con una sola persona, y la persona debe ser inexplorada y en ropa casual. Las personas que usan anteojos deben permanecer para ponerse los anteojos olvidando la foto capturada

● Distancia ocular
Se recomienda una distancia mínima de 115 píxeles y un máximo de 200 píxeles.
● Expresión facial
Se recomienda una expresión facial neutra o una sonrisa con los ojos abiertos de forma natural.
● Gestos y ángulos
El ángulo de rotación horizontal no debe superar los ±10°, la elevación no debe superar los ±10° y el ángulo de depresión no debe superar los ±10°.
● Accesorios
No se permiten máscaras ni gafas de colores. La montura de las gafas no debe cubrir los ojos ni reflejar la luz. Para las personas con monturas de gafas gruesas, se recomienda capturar dos plantillas, una con gafas y otra sin gafas.
● Plantilla facial
Plantilla facial completa con contorno claro, escala real, luz distribuida uniformemente y sin sombras.
● Formato de la plantilla
Debe estar en formato BMP, JPG o JPEG.
● Requisitos de datos
Debe cumplir los siguientes requisitos:

1) Fondo blanco con ropa de color oscuro.
2) Modo de color verdadero de 24 bits.
3) Plantilla comprimida en formato JPG con un tamaño de no más 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 en el mismo nivel horizontal.
7) Los ojos de la persona capturada deben estar abiertos y con el iris claramente visto.
8) Se prefiere una plantilla de rostro o sonrisa neutra, No es preferible mostrar los dientes.
9) La persona capturada debe ser claramente visible, de color natural, sin sombras duras o manchas de luz o reflejo en la plantilla de la cara o en el fondo. El contraste y el nivel de luminosidad deben ser adecuados.

Política de Privacidad

Aviso:
Para ayudarle a utilizar mejor los productos y servicios de ZKTeco (en adelante, "nosotros", "nuestro" o "nos"), proveedor de servicios inteligentes, recopilamos su información personal de forma sistemática. Entendemos la importancia de su información personal, por lo que nos tomamos muy en serio su privacidad y hemos formulado esta política de privacidad para protegerla. A continuación, presentamos las políticas de privacidad para que comprenda con precisión las medidas de protección de datos y privacidad relacionadas con nuestros productos y servicios inteligentes.
Antes de utilizar nuestros productos y servicios, lea atentamente y comprenda todas las normas y disposiciones de esta Política de Privacidad.Si no está de acuerdo con el acuerdo pertinente o alguno de sus términos ,Debes dejar de utilizar nuestros productos y servicios.

I.Información recopilada

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

1.Información de registro de usuario:En su primer registro, la plantilla de funciones (Plantilla de huella dactilar/Plantilla de cara/Plantilla de palma) se guardará en el dispositivo según el tipo de dispositivo seleccionado para verificar la similitud única entre usted y el ID de usuario registrado. Opcionalmente, puede ingresar su nombre y código. Esta información es necesaria para usar nuestros productos. Si no la proporciona, no podrá usar algunas funciones del producto con regularidad.

2.Información del producto:De acuerdo con el modelo del producto y el permiso que usted otorgó cuando instala y utiliza nuestros servicios, la información relacionada con el producto en el que se utilizan nuestros servicios se recopilará cuando el producto se conecte al software, incluido el modelo del producto, el número de versión del firmware, el número de serie del producto y la información de capacidad del producto.Cuando conecte su producto al software, lea atentamente la política de privacidad del software específico.

II.Seguridad y gestión de productos

1.Al utilizar nuestros productos por primera vez, deberá configurar los privilegios de Administrador antes de realizar operaciones específicas. De lo contrario, se le recordará con frecuencia que configure los privilegios de Administrador al acceder a la interfaz del menú principal.Si aún no configura el privilegio de Administrador después de recibir el aviso del sistema, debe tener en cuenta el posible riesgo de seguridad (por ejemplo, los datos pueden modificarse manualmente).

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

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

4.La función de cámara está desactivada en nuestros productos por defecto. Si desea activar esta función para tomarse fotos a sí mismo para registrar la asistencia o a desconocidos para el control de acceso, el producto activará el tono de aviso de la cámara.Una vez que habilite esta función, asumimos que es consciente de los posibles riesgos de seguridad.

5.Todos los datos recopilados por nuestros productos se cifran mediante el algoritmo AES 256. Todos los datos que el Administrador carga en nuestros productos se cifran automáticamente mediante el algoritmo AES 256 y se almacenan de forma segura. Si el Administrador descarga datos de nuestros productos, asumimos que usted necesita procesarlos y que conoce el posible riesgo de seguridad. En tal caso, usted será responsable de almacenarlos. Debe saber que algunos datos no se pueden descargar por motivos de seguridad.

6.Toda la información personal de nuestros productos se puede consultar, modificar o eliminar. Si ya no utiliza nuestros productos, borre sus datos personales.

III.Cómo manejamos la información personal de menores

Nuestros productos, sitio web y servicios están diseñados principalmente para adultos. Los menores no podrán crear su propia cuenta sin el consentimiento de sus padres o tutores. Si es menor de edad, le recomendamos que pida a sus padres o tutores que lean atentamente esta Política y que utilice nuestros servicios o la información que le proporcionamos únicamente con el consentimiento de sus padres o tutores.
Solo utilizaremos o divulgaremos información personal de menores recopilada con el consentimiento de sus padres o tutores si y en la medida en que dicho uso o divulgación esté permitido por la ley o hayamos obtenido el consentimiento explícito de sus padres o tutores, y dicho uso o divulgación sea con el propósito de proteger a los menores.

Al observar que hemos recopilado información personal de menores sin el consentimiento previo de padres verificables, eliminaremos dicha información lo antes posible.

IV.Otros

Puedes visitarnoshttps://www.zkteco.com/cn/index/Index/protección_de_privacidad.html Para obtener más información sobre cómo recopilamos, usamos y almacenamos de forma segura su información personal.
Para mantenernos al día con el rápido desarrollo tecnológico, la adaptación de las operaciones comerciales y satisfacer las necesidades de los clientes, revisaremos y optimizaremos constantemente nuestras medidas y políticas de protección de la privacidad. Le invitamos a visitar nuestro sitio web oficial en cualquier momento para consultar nuestra política de privacidad más reciente.

Operación ecológica

El "período operativo ecológico" del producto se refiere al tiempo durante el cual este producto no descargará ninguna sustancia tóxica o peligrosa cuando se utiliza de acuerdo con los requisitos previos de este manual.
El periodo de funcionamiento ecológico especificado para este producto no incluye baterías ni otros componentes que se desgastan fácilmente y deben reemplazarse periódicamente. El periodo de funcionamiento ecológico de la batería es de 5 años.

Sustancias peligrosas o tóxicas y sus cantidades

Componente Nombre	Sustancia/elemento peligroso/tóxico					
	Plomo (Pb)	Mercurio (Hg)	Cadmio eh (Cd)	Hexava-lente cromo (Cr6+)	Polibromado d Bifenilos (PBB)	Polibromados Éteres de difenilo (PBDE)
Resistencia de chip	×	○	○	○	○	○
Condensador de chip	×	○	○	○	○	○
Inductor de chip	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
ESD componente	×	○	○	○	○	○
Zumbador	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Tornillos	○	○	○	×	○	○

○ Indica que la cantidad total de contenido tóxico en todos los materiales homogéneos está por debajo del límite especificado en SJ/T 11363—2006.
× indica que la cantidad total de contenido tóxico en todos los materiales homogéneos excede el límite especificado en SJ/T 11363—2006.
NotaEl 80 % de los componentes de este producto se fabrican con materiales no tóxicos y ecológicos. Los componentes que contienen toxinas o elementos nocivos se incluyen debido a las limitaciones económicas o técnicas actuales que impiden su sustitución por materiales o elementos no tóxicos.



www.zkteco.com

www.zktecolatinoamerica.com

Derechos de Autor © 2024, ZKTeco CO., LTD. Todos los derechos reservados.
ZKTeco puede, en cualquier momento y sin previo aviso, realizar cambios o mejoras en los productos y servicios o detener su producción o comercialización.
El logo ZKTeco y la marca son propiedad de ZKTeco CO., LTD.