Manual de Usuario

SenseFace 7

Fecha: Nov 2025
Versión: 1.1

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 2025 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 7.

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

DECLARACIÓN DE SEGURIDAD DE DATOS 9
MEDIDAS DE SEGURIDAD 9
1 INSTRUCCIONES DE USO 11
1.1 POSICIONAMIENTO DEL DEDO 11
1.2 POSICIÓN DE PIE, POSTURA Y EXPRESIÓN FACIAL 11
1.3 REGISTRO DE PLANTILLA FACIAL 12
1.4 INTERFAZ EN ESPERA 14
1.5 TECLADO VIRTUAL 15
1.6 MODO DE VERIFICACIÓN 16
1.6.1 VERIFICACIÓN DE HUELLA DACTILAR 16
1.6.2 VERIFICACIÓN DE CÓDIGO QR 19
1.6.3 VERIFICACIÓN CON TARJETA 19
1.6.4 VERIFICACIÓN FACIAL 22
1.6.5 VERIFICACIÓN DE CONTRASEÑA 24
1.6.6 VERIFICACIÓN COMBINADA 26
2. VISIÓN GENERAL (OVERVIEW) 26
2.1 APARIENCIA 26
2.2 DESCRIPCIÓN DE TERMINALES Y CABLEADO 28
2.3 DESCRIPCIÓN DEL CABLEADO 28
2.3.1 CONEXIÓN DE ALIMENTACIÓN (ENERGÍA) 28
2.3.2 CONEXIÓN ETHERNET 29
2.3.3 CONEXIÓN DE BOTÓN DE SALIDA, SENSOR DE PUERTA Y AUXILIAR 29
2.3.4 CONEXIÓN RS485 30
2.3.5 CONEXIÓN DE RELÉ DE CERRADURA (LOCK) 30
2.3.6 CONEXIÓN DE LECTOR WIEGAND 31
3. INSTALACIÓN 32
3.1 ENTORNO DE INSTALACIÓN 32
3.2 INSTALACIÓN DEL DISPOSITIVO 32
4. MENÚ PRINCIPAL 33
5. GESTIÓN DE USUARIOS 35
5.1 REGISTRO DE USUARIO 35
5.1.1 ID DE USUARIO Y NOMBRE 35
5.1.2 ROL DE USUARIO 36
5.1.3 HUELLA DACTILAR ★ 36
5.1.4 PLANTILLA FACIAL 37
5.1.5 TARJETA 38
5.1.6 CONTRASEÑA 39
5.1.7 FOTO DE PERFIL 39
5.1.8 ROL DE CONTROL DE ACCESO 40
5.2 BÚSQUEDA DE USUARIOS 41

5.3 EDITAR USUARIO 41
5.4 ELIMINAR USUARIO 42
5.5 ESTILO DE VISUALIZACIÓN 42
6. ROL DE USUARIO 44
7. CONFIGURACIÓN DE COMUNICACIÓN 46
7.1 CONFIGURACIÓN DE RED 46
7.2 COMUNICACIÓN SERIAL 47
7.3 CONEXIÓN A PC 48
7.4 RED INALÁMBRICA ★ 49
7.5 CONFIGURACIÓN DEL SERVIDOR EN LA NUBE (CLOUD) 52
7.6 CONFIGURACIÓN WIEGAND 52
7.6.1 ENTRADA WIEGAND 53
7.6.2 SALIDA WIEGAND 55
7.7 DIAGNÓSTICO DE RED 56
8. CONFIGURACIÓN DEL SISTEMA 57
8.1 FECHA Y HORA 57
8.2 CONFIGURACIÓN DE REGISTROS DE ACCESO (LOGS) 59
8.3 PARÁMETROS DE PLANTILLA FACIAL 60
8.4 PARÁMETROS DE HUELLA DACTILAR ★ 62
8.5 AJUSTE DE TIPO DE DISPOSITIVO 63
8.6 CONFIGURACIÓN DE SEGURIDAD 64
8.7 ACTUALIZACIÓN POR USB 65
8.8 ACTUALIZAR FIRMWARE EN LÍNEA 65
8.9 RESTABLECIMIENTO DE FÁBRICA 66
9. AJUSTES DE PERSONALIZACIÓN 67
9.1 CONFIGURACIÓN DE INTERFAZ DE USUARIO 67
9.2 CONFIGURACIÓN DE VOZ 68
9.3 HORARIOS DE TIMBRE (CAMPANA) 69
10. GESTIÓN DE DATOS 71
10.1 ELIMINAR DATOS 71
11. INTERCOMUNICADOR 74
11.1 CONFIGURACIÓN SIP 74
11.1.1 CONFIGURACIÓN LOCAL 75
11.1.2 OPCIONES DE AUDIO 76
11.1.3 OPCIONES DE VÍDEO 77
11.1.4 OPCIONES DE LLAMADA 77
11.1.5 LISTA DE CONTACTOS 78
11.1.6 CONFIGURACIÓN DE ACCESO DIRECTO DE LLAMADA 79
11.1.7 CONFIGURACIÓN AVANZADA 81
11.2 CONFIGURACIÓN DEL TIMBRE 81
11.2.1 CONECTAR EL TIMBRE INALÁMBRICO★ 82
11.3 CONFIGURACIÓN DE ONVIF 83

12. CONTROL DE ACCESO 87
12.1 OPCIONES DE CONTROL DE ACCESO 88
12.2 CONFIGURACIÓN DE REGLAS DE TIEMPO 89
12.3 DÍAS FESTIVOS 91
12.4 GRUPOS DE ACCESO ★ 92
12.5 VERIFICACIÓN COMBINADA 93
12.6 CONFIGURACIÓN ANTIPASSBACK 94
12.7 OPCIONES DE COACCIÓN 95
13. GESTOR USB 97
13.1 DESCARGA USB 97
13.2 CARGA USB 98
14. BÚSQUEDA DE ASISTENCIA 100
15. AUTOTEST 102
16. INFORMACIÓN DEL SISTEMA 103
17. CONECTAR AL SOFTWARE ZKBIO CVSECURITY 104
17.1 CONFIGURAR LA DIRECCIÓN DE COMUNICACIÓN 104
17.2 AÑADIR DISPOSITIVO EN EL SOFTWARE 105
17.3 AÑADIR PERSONAL EN EL SOFTWARE Y REGISTRO DE HUELLAS DACTILARES/ROSTRO EN LÍNEA 106
18. CONECTAR AL SOFTWARE ZKBIOTIME 109
18.1 CONFIGURAR LA DIRECCIÓN DE COMUNICACIÓN 109
18.2 AÑADIR DISPOSITIVO EN EL SOFTWARE 109
18.3 AÑADIR PERSONAL EN EL SOFTWARE Y REGISTRO DE HUELLAS DACTILARES EN LÍNEA 110
19. CONEXIÓN AL TIMBRE INALÁMBRICO ★ 112
19.1 CONECTAR EL TIMBRE INALÁMBRICO 112
19.2 DESVINCULAR EL TIMBRE INALÁMBRICO 112
20. INTERCOMUNICADOR DE VÍDEO SIP 113
20.1 USO DE LA RED DE ÁREA LOCAL 113
20.1.1 LISTA DE CONTACTOS DE LLAMADAS 119
20.1.2 PERSONALIZAR LAS TECLAS DE ACCESO RÁPIDO PARA LLAMADAS 120
20.1.3 LLAMADAS DIRECTAS 121
20.2 SERVIDOR SIP 122
20.2.1 CONFIGURACIÓN DEL SERVIDOR SIP 123
20.2.2 AÑADIR DISPOSITIVO 126
20.2.3 CREAR NÚMEROS DE EXTENSIÓN 128
20.2.4 LISTA DE CONTACTOS 129
20.2.5 ASIGNACIÓN DE NÚMEROS DE EXTENSIÓN Y CUENTAS SIP 131
20.2.6 FUNCIONALIDAD DEL CLIENTE PC 137
20.2.7 REALIZAR UNA LLAMADA 140
21. CONEXIÓN A LA APLICACIÓN MÓVIL ZKBIO ZLINK 146
21.1 INICIAR SESIÓN EN LA APLICACIÓN MÓVIL 146

21.2 AÑADIR DISPOSITIVO EN LA APLICACIÓN MÓVIL.....147
21.2.1 INTERCOMUNICADOR DE VÍDEO 148
22. CONEXIÓN AL PORTAL WEB ZKBIO ZLINK.....150
22.1 INICIAR SESIÓN EN EL PORTAL WEB 150
22.2 AÑADIR DISPOSITIVO EN EL PORTAL WEB 150
APÉNDICE 1.....153
REQUISITOS PARA LA RECOPILACIÓN EN VIVO Y EL REGISTRO DE PLANTILLAS FACIALES CON LUZ VISIBLE 153
REQUISITOS PARA LOS DATOS DE PLANTILLAS FACIALES DIGITALES CON LUZ VISIBLE.....154
APÉNDICE 2.....155
POLÍTICA DE PRIVACIDAD.....155
OPERACIÓN ECOLÓGICA.....157

Declaración de seguridad de datos

ZKTeco, como proveedor de productos inteligentes, también puede necesitar conocer y recopilar cierta información personal sobre usted para ayudarle mejor a utilizar los productos y servicios de ZKTeco, y tratará su privacidad con cuidado mediante el desarrollo de una Política de privacidad.

Lea y comprenda completamente todas las normas y puntos clave de la política de protección de la privacidad que aparecen en el dispositivo antes de utilizar los productos de ZKTeco.

Como usuario del producto, debe cumplir con las leyes y normativas aplicables relacionadas con la protección dedatos personales al recopilar, almacenar y utilizar datos personales, lo que incluye, entre otras cosas, tomarmedidas de protección de los datos personales, como llevar a cabo una gestión razonable de los derechos de losdispositivos, reforzar la seguridad física de los escenarios de aplicación de los dispositivos, etc.

Medidas de seguridad

Las siguientes precauciones tienen por objeto garantizar la seguridad del usuario y evitar cualquier daño. Léalas atentamente antes de la instalación.

1. **Lea, siga y conserve las instrucciones:** todas las instrucciones de seguridad y funcionamiento deben leerse y seguirse correctamente antes de poner en servicio el dispositivo.
2. **No ignore las advertencias:** respete todas las advertencias que figuran en la unidad y en las instrucciones de funcionamiento
3. **Accesorios:** utilice únicamente accesorios recomendados por el fabricante o vendidos con el producto. No utilice ningún otro componente que no sea el material sugerido por el fabricante.
4. **recauciones para la instalación:** no coloque este dispositivo sobre un soporte o bastidor inestable. Podría caerse y causar lesiones graves a las personas y daños al dispositivo.
5. **Servicio técnico:** no intente reparar esta unidad usted mismo. Abrir o retirar las cubiertas puede exponerle a voltajes peligrosos u otros riesgos.
6. **Daños que requieren reparación:** desconecte el sistema de la fuente de alimentación principal de CA o CC y consulte al personal de servicio en las siguientes condiciones:
   - Cuando el cable o el control de conexión se vean afectados.
   - Cuando se haya derramado líquido o se haya caído algún objeto dentro del sistema.
   - Si el sistema se expone al agua y/o a condiciones climáticas adversas (lluvia, nieve, etc.).
   - Si el sistema no funciona normalmente según las instrucciones de funcionamiento.

Cambie únicamente los controles definidos en las instrucciones de funcionamiento. El ajuste incorrecto de otros controles puede provocar daños y requerir la intervención de un técnico cualificado para que el dispositivo vuelva a funcionar con normalidad.

7. **Piezas de repuesto:** cuando se requieran piezas de repuesto, los técnicos de servicio solo deben utiliza piezas de repuesto proporcionadas por el proveedor. Los sustitutos no autorizados pueden provocarquemaduras, descargas eléctricas u otros peligros
8. **Comprobación de seguridad:** una vez finalizado el servicio o la reparación de la unidad, pida al técnico de servicio que realice comprobaciones de seguridad para garantizar el correcto funcionamiento de la un dad.

9. **Fuentes de alimentación:** utilice el sistema únicamente con la fuente de alimentación indicada en la etiqueta. Si no tiene claro qué tipo de fuente de alimentación debe utilizar, llame a su distribuidor.
10. **Rayos:** se pueden instalar pararrayos externos para proteger contra tormentas eléctricas. Esto evita que las sobrecargas destruyan el sistema

Los dispositivos deben instalarse en zonas de acceso restringido.

1. Instrucciones de uso

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

1.1 Posición de los dedos

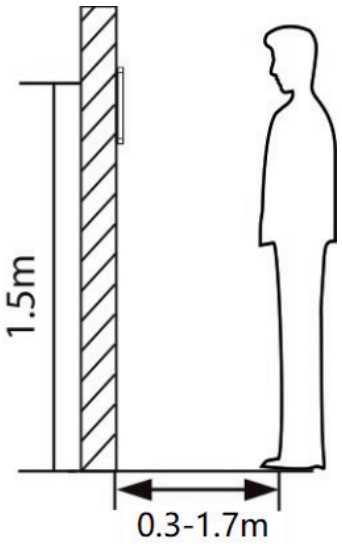
Dedos recomendados: se recomienda utilizar los dedos índice, medio o anular, y evitar el pulgar o el meñique, ya que son difíciles de colocar correctamente en el lector de huellas dactilares.



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 derivarse de un uso incorrecto del producto. Nos reservamos el derecho de interpretación y modificación finales en relación con este punto*

1.2 Posición de pie, postura y expresión facial

- **Distancia recomendada**



Se recomienda que la distancia entre el dispositivo y un usuario cuya altura esté comprendida entre 1,55 m y 1,85 m sea de 0,3 m a 1,7 m. Los usuarios pueden moverse ligeramente hacia adelante o hacia atrás para mejorar la calidad de las imágenes faciales capturadas.

- **Postura de pie y expresión facial recomendadas:**



Postura de pie

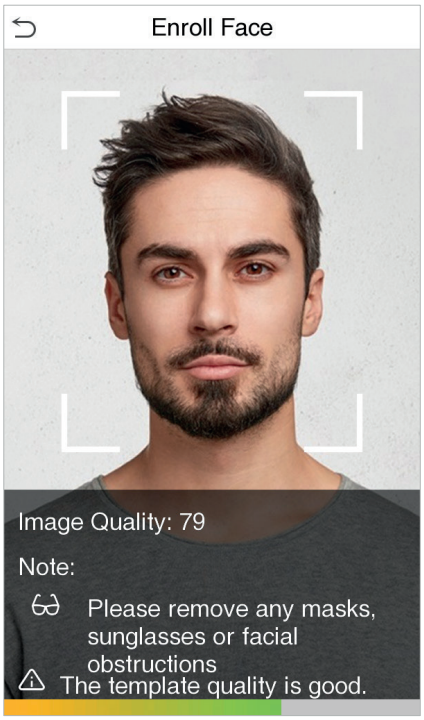


Expresión facial

Nota: *Durante el registro y la verificación, mantenga una expresión facial y una postura de pie naturales*

1.3 Registro de la plantilla facial

Asegúrese de que la plantilla facial se encuentre 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 tener el aspecto de la imagen siguiente:



Método correcto de registro y autenticación de la plantilla facia

- **Recomendaciones para registrar una plantilla facial**

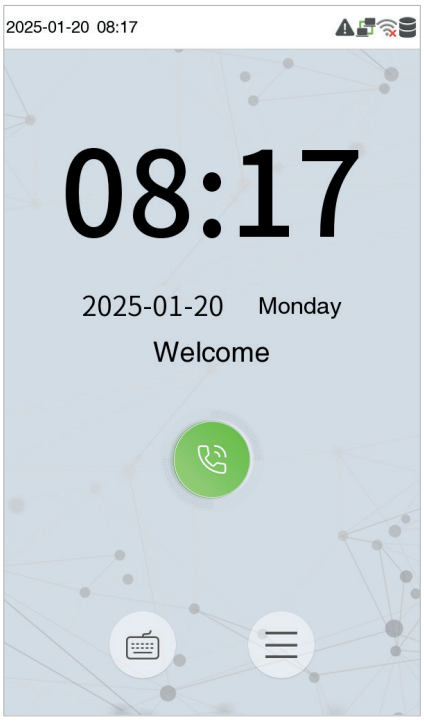
Al registrar una plantilla facial, mantenga una distancia de entre 40 cm y 80 cm entre el dispositivo y la plantilla facial.

- Tenga cuidado de no cambiar su expresión facial. (Plantilla facial sonriente, plantilla facial dibujada, guiño, etc.)
- Si no sigue las instrucciones que aparecen en pantalla, el registro de la plantilla facial puede tardar más tiempo o fallar.
- Tenga cuidado de no cubrir los ojos ni las cejas.
- No lleve gorras, máscaras, gafas de sol ni gafas graduadas.
- Tenga cuidado de no mostrar dos plantillas faciales en la pantalla. Registre a una persona cada vez.
- Se recomienda que los usuarios que lleven gafas registren ambas plantillas faciales, con y sin gafas.

- **Recomendación para autenticar una plantilla facial**
  - Asegúrese de que la plantilla facial aparezca dentro de la guía que se muestra en la pantalla del dispositivo
  - Si se han cambiado las gafas, es posible que la autenticación falle. Si se ha registrado la plantilla facial sin gafas, autentique la plantilla facial sin gafas. Si se ha registrado la plantilla facial con gafas, autentique la plantilla facial con las gafas que llevaba anteriormente.
  - Si una parte de la plantilla facial está cubierta por un sombrero, una máscara, un parche en el ojo o gafas de sol, es posible que falle la autenticación. No cubra la plantilla facial, permita que el dispositivo reconozca tanto las cejas y la plantilla facial.

1.4 Interfaz de espera

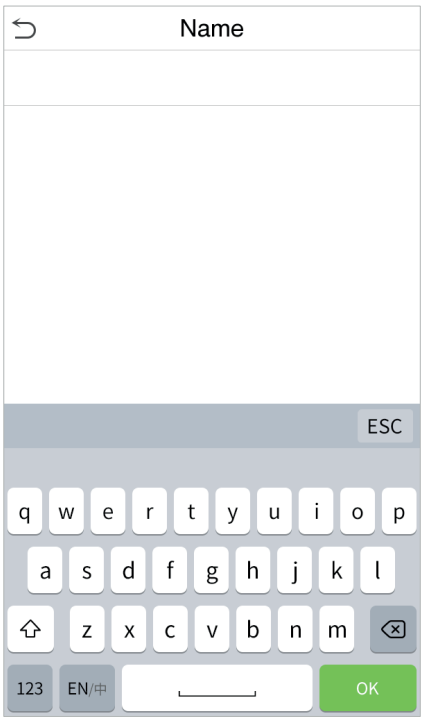
Después de conectar la fuente de alimentación, se muestra la siguiente plantilla de interfaz en espera:



- Haga clic en el icono para acceder a la plantilla de la interfaz de entrada del ID de usuario
- Cuando no hay ningún superadministrador configurado en el dispositivo, pulse el icono para acceder al menú.
- Después de configurar el superadministrador en el dispositivo, se requiere la verificación del superadministrador antes de acceder a las funciones del menú.

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

1.5 Teclado virtual



Nota:

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

- Haga clic en **EN** para cambiar al teclado en inglés.
- Pulse **123** para cambiar al teclado numérico y de símbolos.
- Haga clic en **ABC** para volver al teclado alfabético.
- Haga clic en el cuadro de entrada y aparecerá el teclado virtual.
- Haga clic en **ESC** para salir del teclado virtual.

1.6 Modo de verificación

1.6.1 Verificación de huellas dactilares★

Nota: *Esta función solo está disponible para SenseFace 7A.*

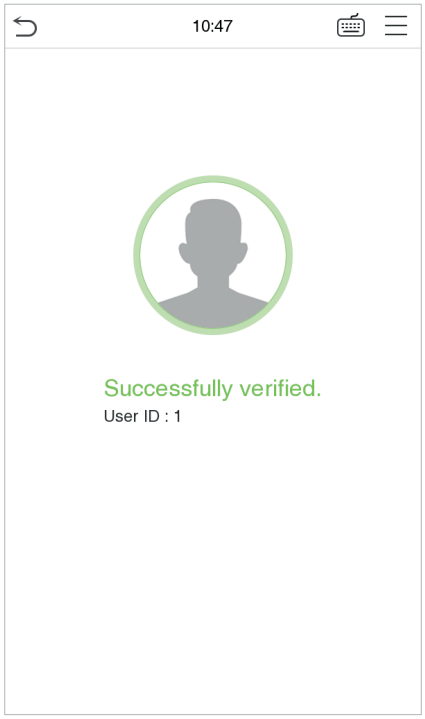
- **1: N Modo de verificación de huellas dactilares**

El dispositivo compara la huella dactilar actual con los datos de huellas dactilares disponibles almacenados en su base de datos.

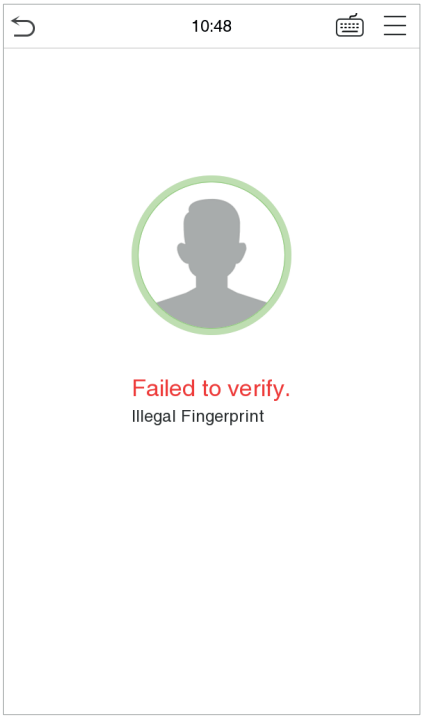
El modo de autenticación por huella dactilar se activa cuando el usuario coloca el dedo sobre el escáner de huellas dactilares.

Siga las instrucciones recomendadas para colocar el dedo sobre el sensor. Para obtener más información, consulte la sección Posición del dedo.

La verificación se ha realizado correctamente:



La verificación ha fallado:

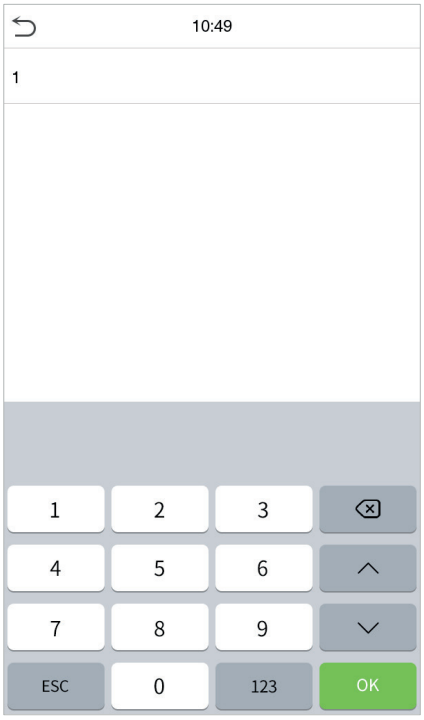


- **1: 1 Modo de verificación de huella dactilar**

El dispositivo compara la huella dactilar actual con las huellas dactilares vinculadas al ID de usuario introducido a través del teclado virtual.

Si los usuarios no pueden acceder utilizando el método de autenticación 1:N, pueden intentar verificar su identidad utilizando el modo de verificación 1:1.

Haga clic en el botón  en la pantalla principal para acceder al modo de verificación de huella digital 1:1. Introduzca el ID de usuario y pulse «OK»

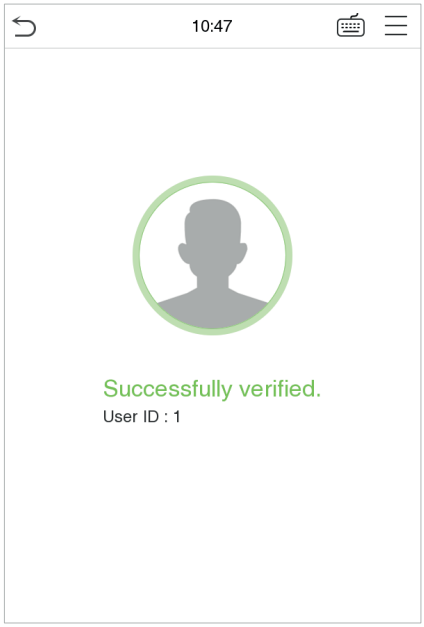


Si el usuario ha registrado una plantilla facial, una tarjeta y una contraseña además de sus huellas dactilares y el método de verificación está configurado como «Verificación de contraseña/huella dactilar/tarjeta/plantilla facial», aparecerá la siguiente. Seleccione el icono de huella dactilar para y entrar en el modo de verificación de huellas dactilares.

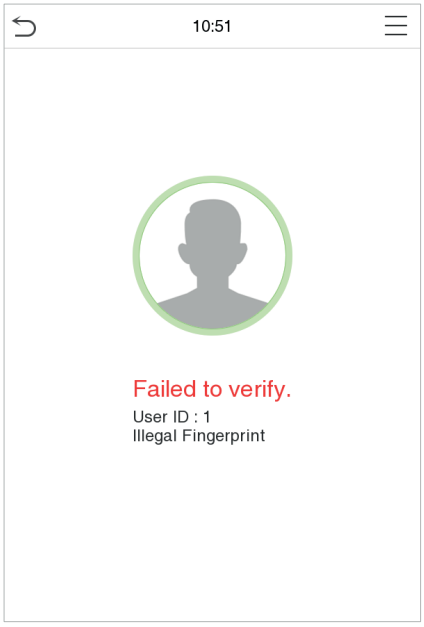


Presione la huella digital para verificar.

La verificación se ha realizado correctamente:



La verificación ha fallado:



1.6.2 Verificación del código QR★

Nota: *Esta función solo está disponible para SenseFace 7C.*

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

Toque «**Credencial móvil**» en la página móvil de ZKBioAccess y aparecerá un código QR que incluye la identificación del empleado y el número de tarjeta (el código QR estático solo incluye el número de tarjeta). El código QR puede sustituir a una tarjeta física en un dispositivo específico para lograr una autenticación sin contacto. Consulte 15.4 Credencial móvil

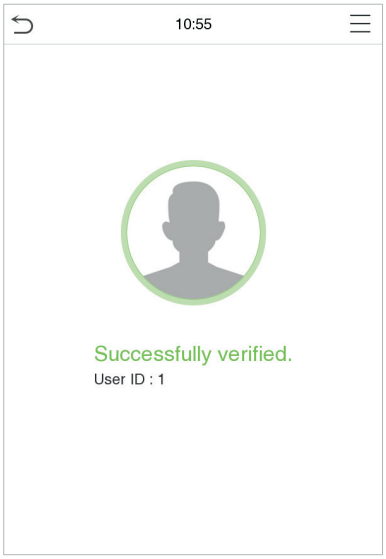


1.6.3 Verificación de tarjetas

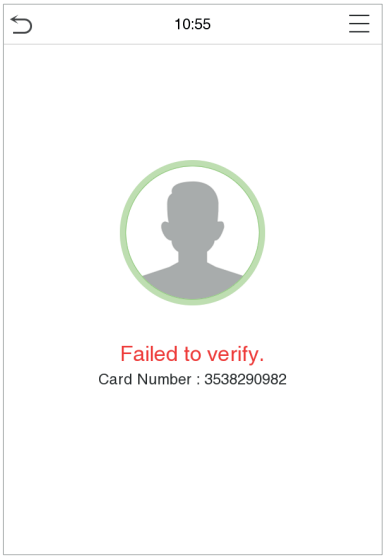
- **1:N Verificación de tarjetas**

El modo de verificación de tarjetas 1:N compara el número de tarjeta en el área de inducción de tarjetas con todos los datos de números de tarjetas registrados en el dispositivo. Coloque la tarjeta en el área de recopilación para su verificación.

La verificación se ha realizado correctamente:



La verificación ha fallado:

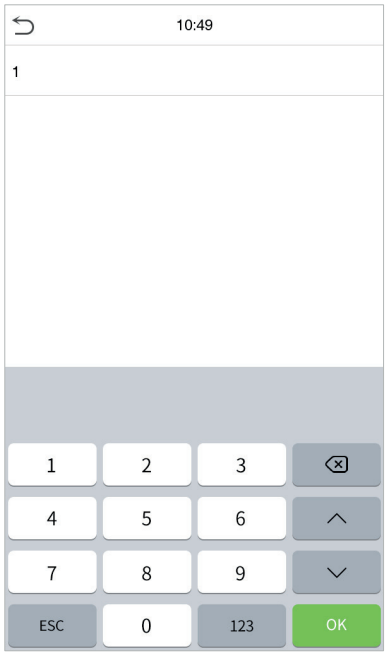


- **1:1 Verificación de tarjetas**

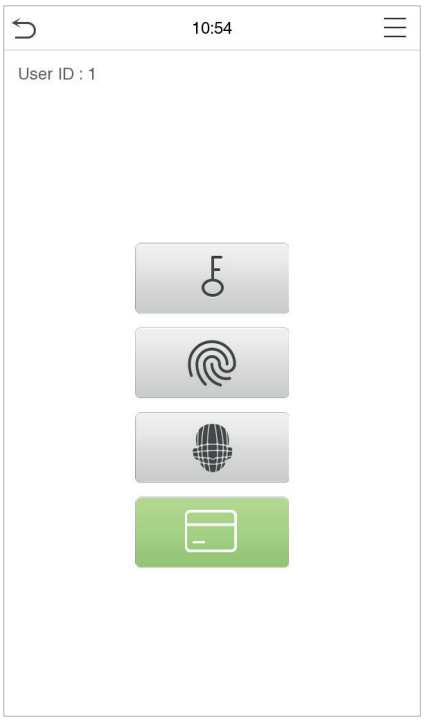
El modo de verificación de tarjetas 1:1 compara el número de la tarjeta en el área de inducción de tarjetas con el número asociado al ID de usuario del empleado registrado en el dispositivo

Pulse en la plantilla de la interfaz principal para abrir el modo de verificación de tarjetas 1:1

Introduzca el ID de usuario y haga clic en **Aceptar.**

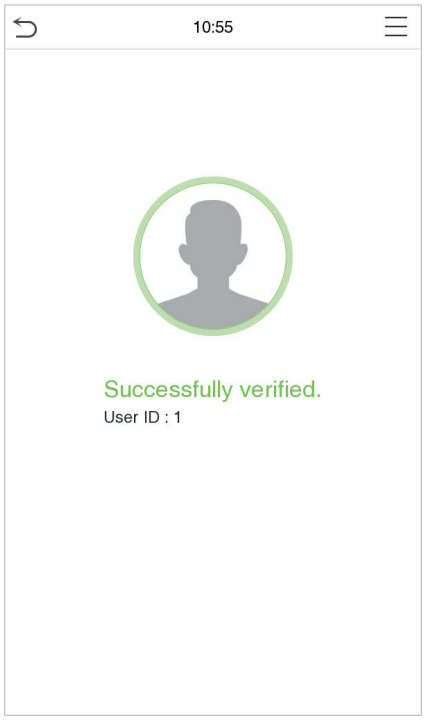


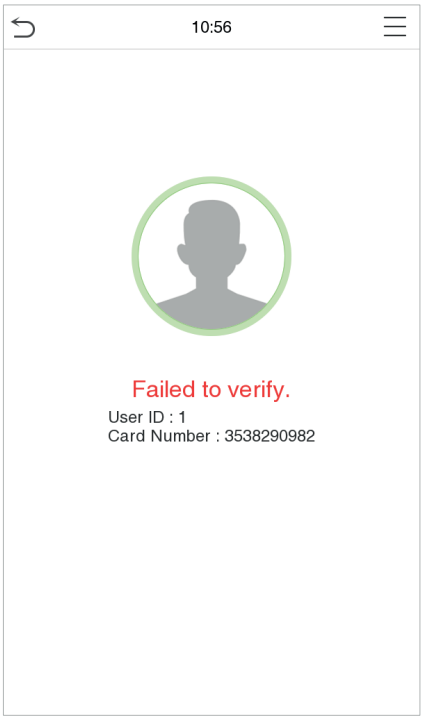
Si el usuario ha registrado una plantilla facial, una tarjeta y una contraseña además de su tarjeta, y el método de verificación está configurado como Contraseña/Huella dactilar/Tarjeta/Verificación facial, aparecerá la siguiente pantalla. Seleccione el icono (Verificación de tarjeta) para acceder al modo de verificación de tarjeta.



Coloque la tarjeta en el área de recogida para su verificación.

La verificación se ha realizado correctamente:	La verificación ha fallado:

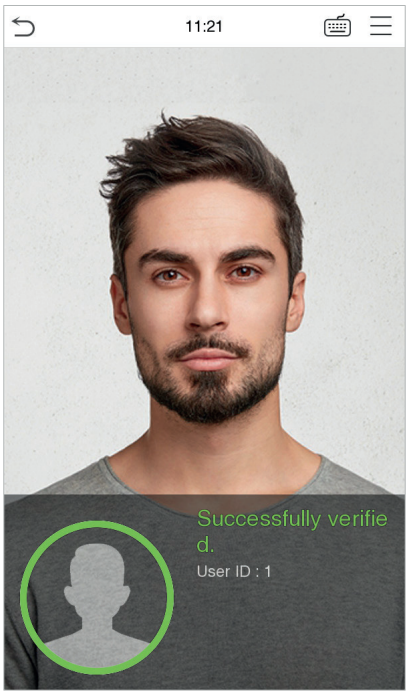




1.6.4 Verificación facial

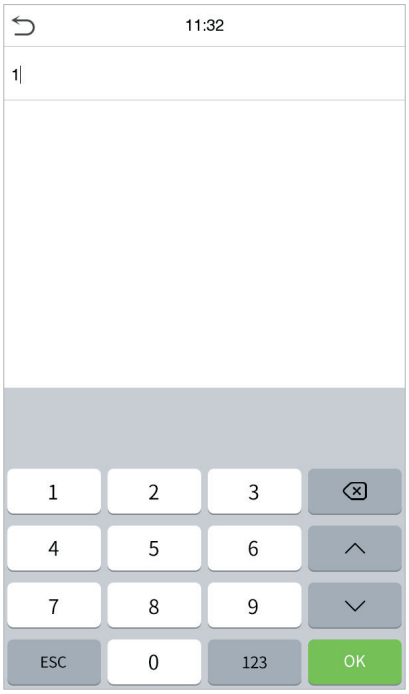
- **1:N Verificación facial**

El dispositivo compara las imágenes faciales adquiridas actualmente con todos los datos de plantillas faciales registrados almacenados en su base de datos. A continuación se muestra el cuadro emergente que muestra el resultado de la comparación.



- **1:1 Verificación facial**

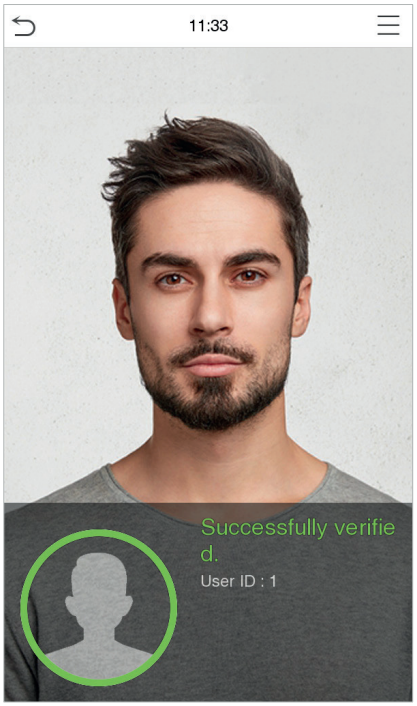
En este modo de verificación, el dispositivo compara la plantilla facial capturada por la cámara con la plantilla facial relacionada con el ID de usuario introducido. Pulse el icono en la interfaz principal, introduzca el ID de usuario y haga clic en «OK».



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



Tras una verificación satisfactoria, el cuadro de mensaje muestra «**Verificación correcta**», como se muestra a continuación:

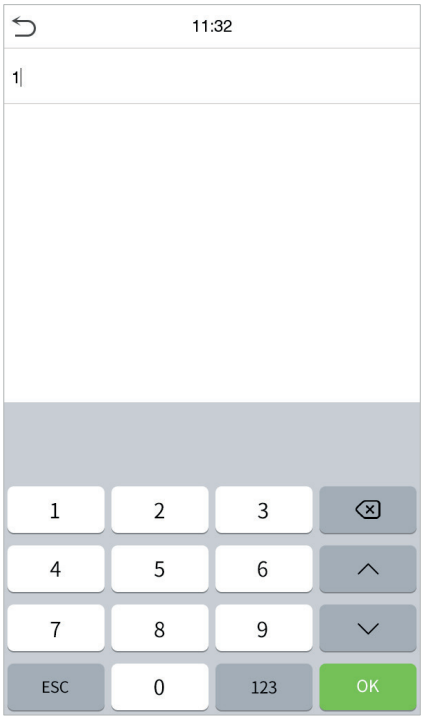


Si la verificación falla, aparecerá el mensaje **«¡Ajuste su posición!».**

1.6.5 Verificación de contraseña

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

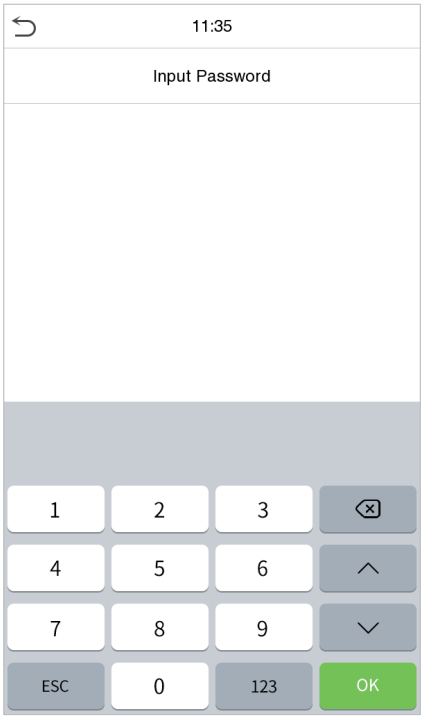
Haga clic en el botón (Verificar contraseña) de la pantalla principal para acceder al modo de verificación de contraseña 1:1. A continuación, introduzca el ID de usuario y pulse «OK».



Si el usuario ha registrado una plantilla facial y una tarjeta además de la contraseña, y el método de verificación está configurado como Contraseña/Huella dactilar/Tarjeta/Verificación facial, aparecerá la siguiente pantalla.
Seleccione el icono « » (Contraseña/Huella dactilar/Tarjeta/Verificación facial) para entrar en el modo de verificación de contraseña.

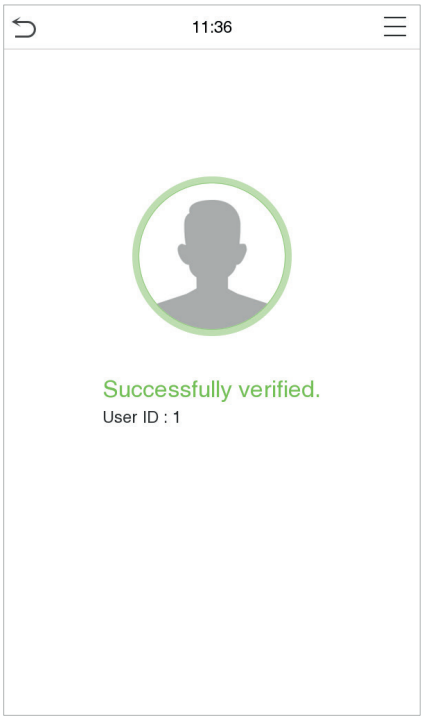


Introduzca la contraseña y pulse «OK»

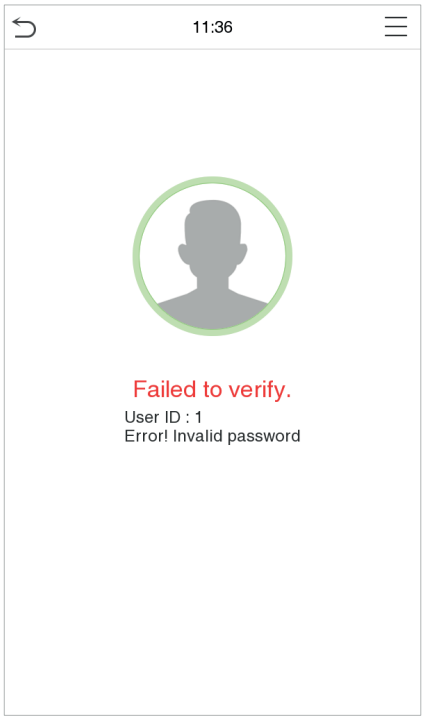


La siguiente pantalla se muestra después de introducir una contraseña correcta y una contraseña incorrecta, respectivamente.

La verificación se ha realizado correctamente:



La verificación ha fallado:

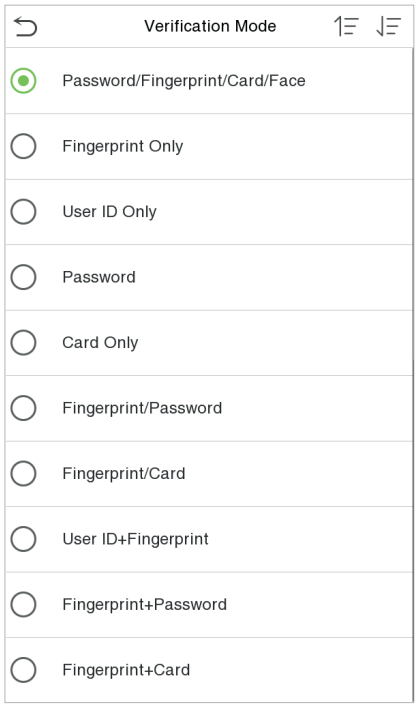


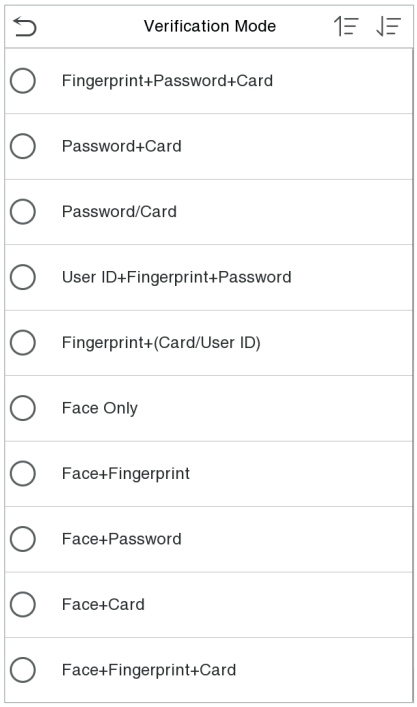
1.6.6 Verificación combinada

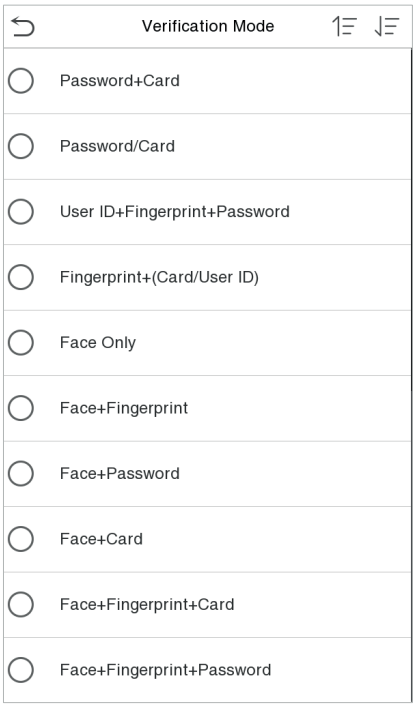
Para aumentar la seguridad, este dispositivo ofrece la opción de utilizar múltiples formas de métodos de verificación. Se pueden utilizar un total de 21 combinaciones de verificación diferentes, como se muestra a continuación:

Verificación combinada Definición de símbolos:

Simbolo Definición		Explicación
/	or	Este método compara la verificación introducida de una persona con la plantilla de verificación relacionada almacenada previamente para ese ID de personal en el dispositivo.
+	y	Este método compara la verificación introducida de una persona con todas las plantillas de verificación almacenadas previamente para ese ID de personal en el dispositivo.







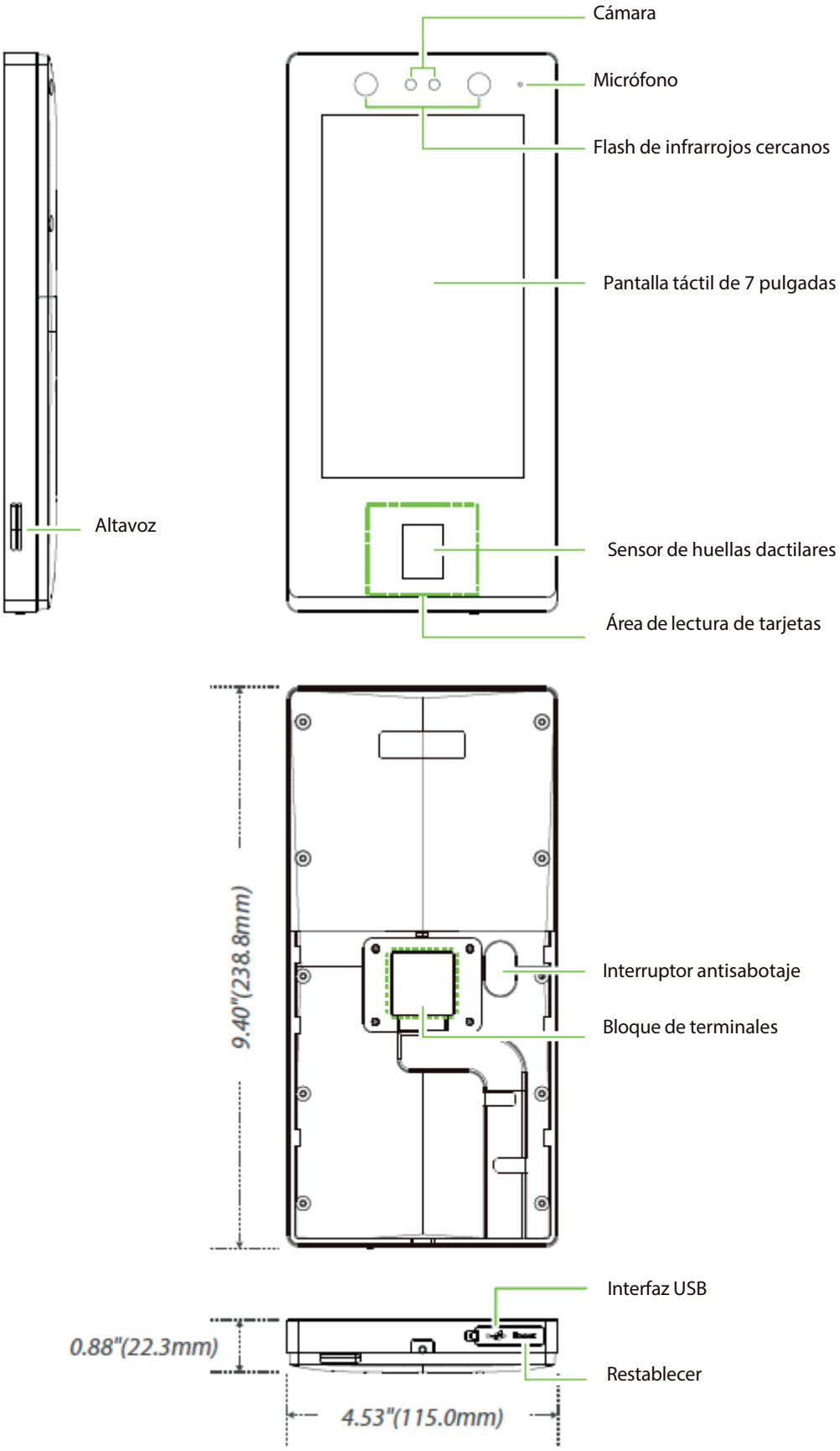
Procedimiento para configurar el modo de verificación combinada:

- La verificación combinada requiere que el personal registre todos los diferentes métodos de verificación. De lo contrario, los empleados no podrán verificar correctamente el proceso de verificación combinada
- Por ejemplo, cuando un empleado solo ha registrado los datos, pero el modo de verificación del dispositivo está configurado como «Rostro + Contraseña», el empleado no podrá completar con éxito el proceso de verificación
- Esto se debe a que el dispositivo compara la plantilla facial escaneada de la persona con plantilla de verificación registrada (tanto la plantilla facial como la contraseña) almacenada previamente en ese ID de personal en el dispositivo.
- Pero como el empleado solo ha registrado la plantilla facial y no la contraseña, la verificación no se completará y el dispositivo mostrará «Verificación fallida».

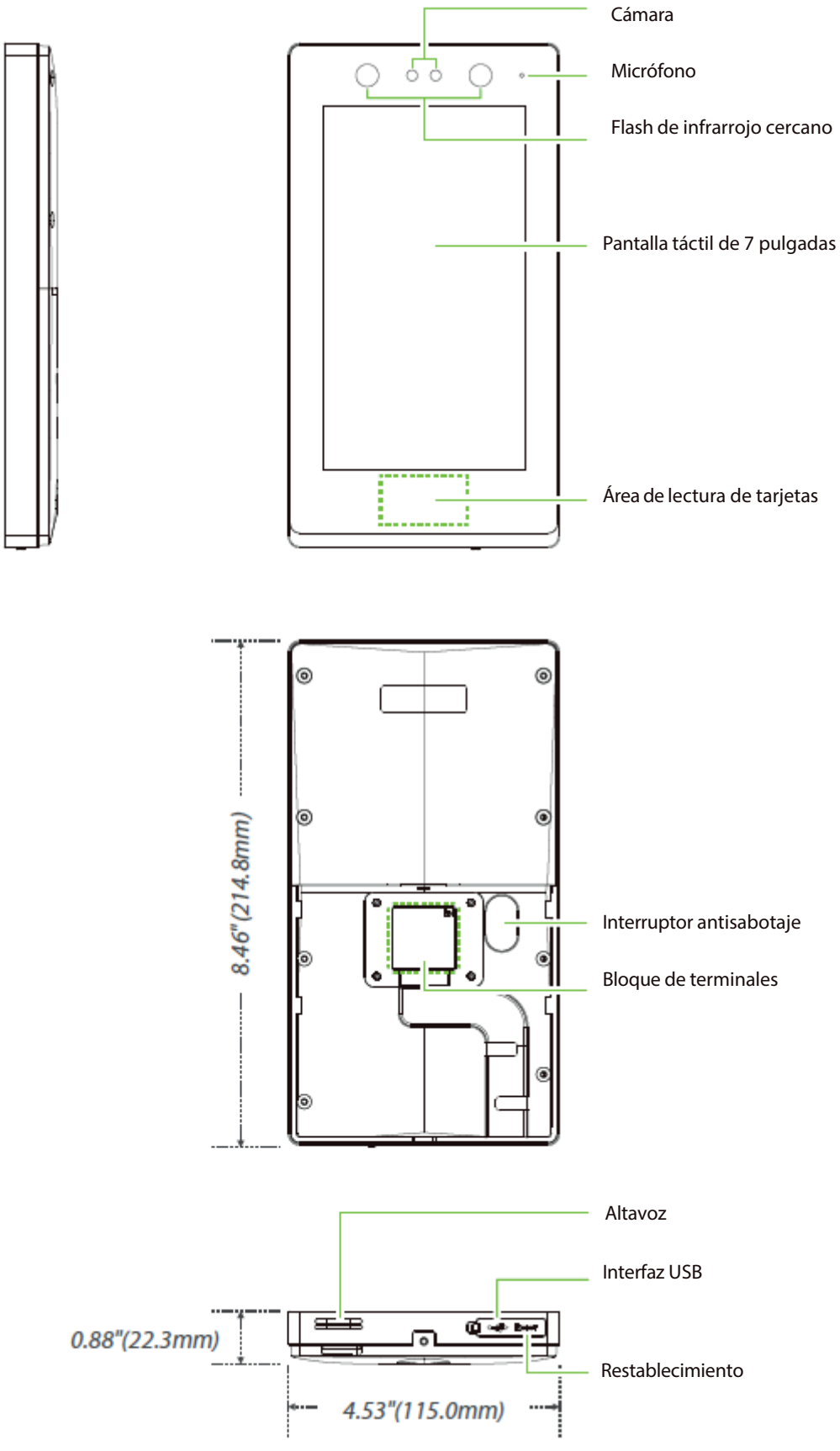
2. Descripción general

2.1 Apariencia

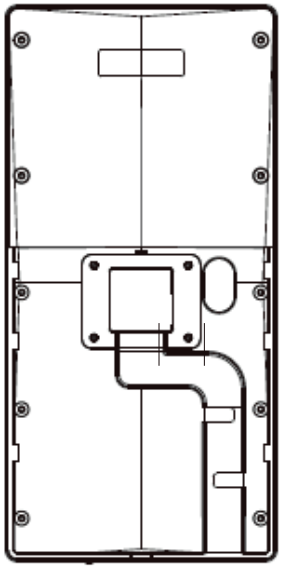
SenseFace 7A/7C

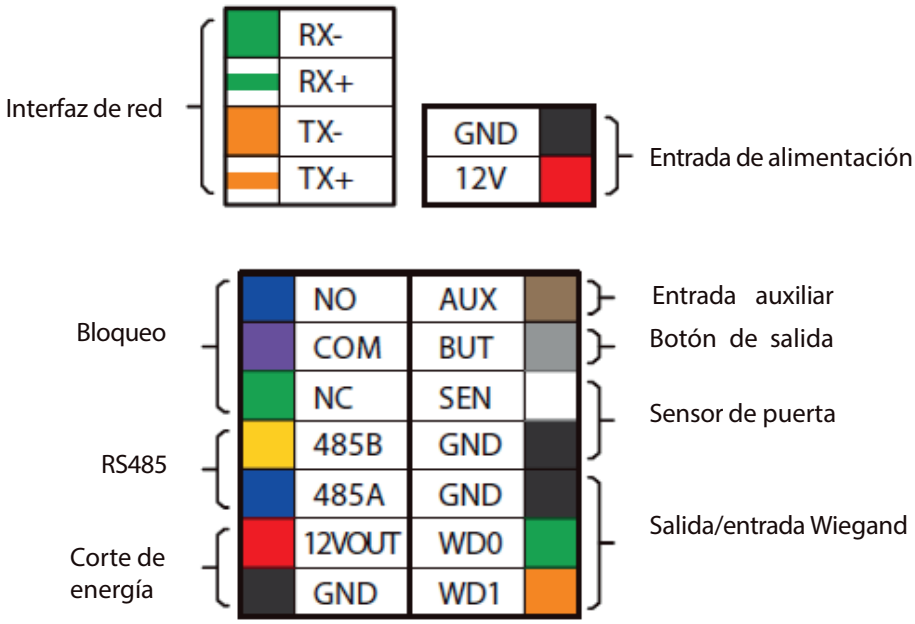


SenseFace 7B



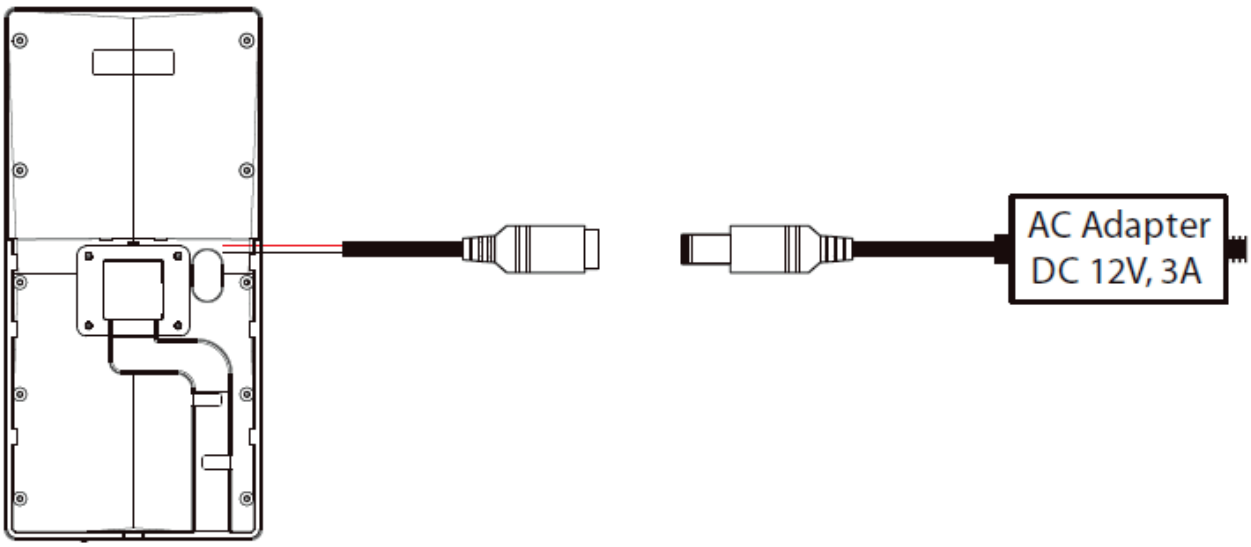
2.2 Descripción de los terminales y el cableado





2.3 Descripción del cableado

2.3.1 Conexión de alimentación

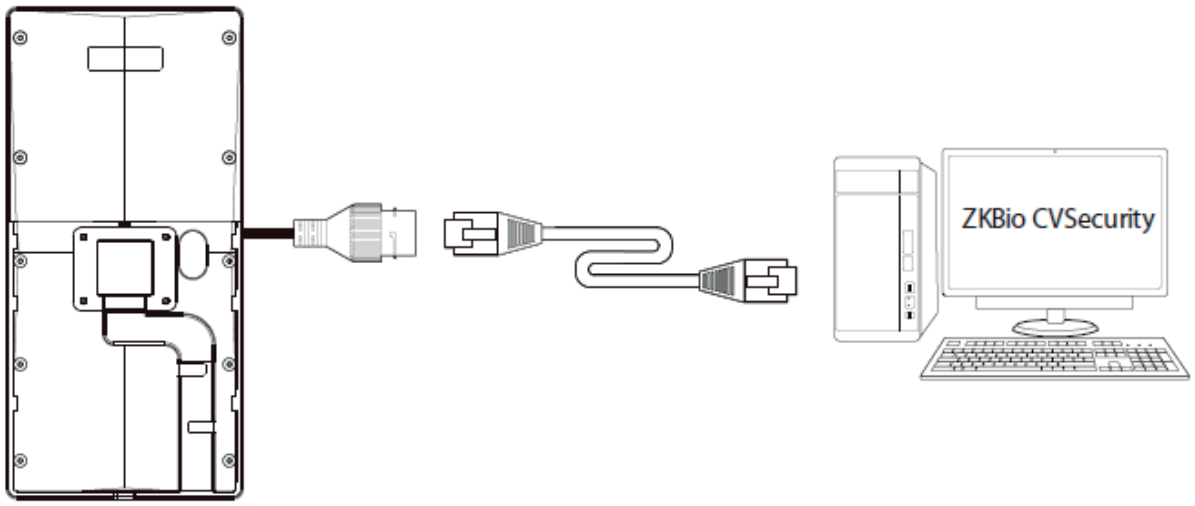


Fuente de alimentación recomendada

- Adaptador de CA recomendado: **12V, 3A**.
- Para compartir la alimentación con otros dispositivos, utilice un adaptador de CA con una intensidad nominal superior.

2.3.2 Conexión Ethernet

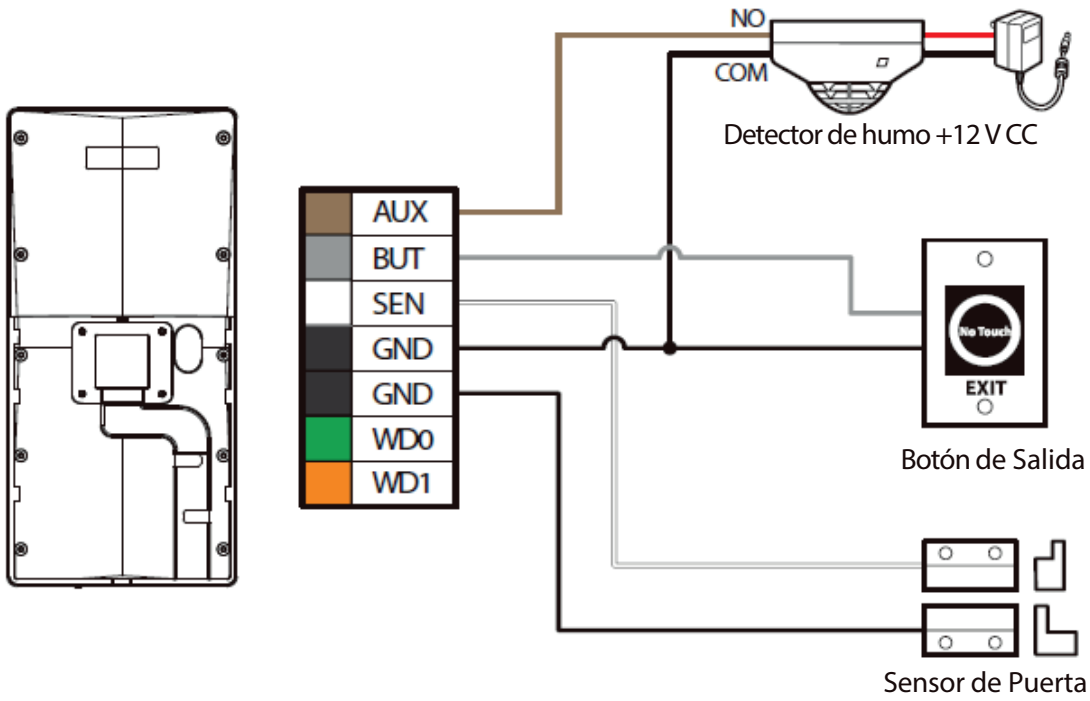
Conecte el dispositivo al software del ordenador mediante un cable Ethernet. A continuación se muestra un ejemplo:



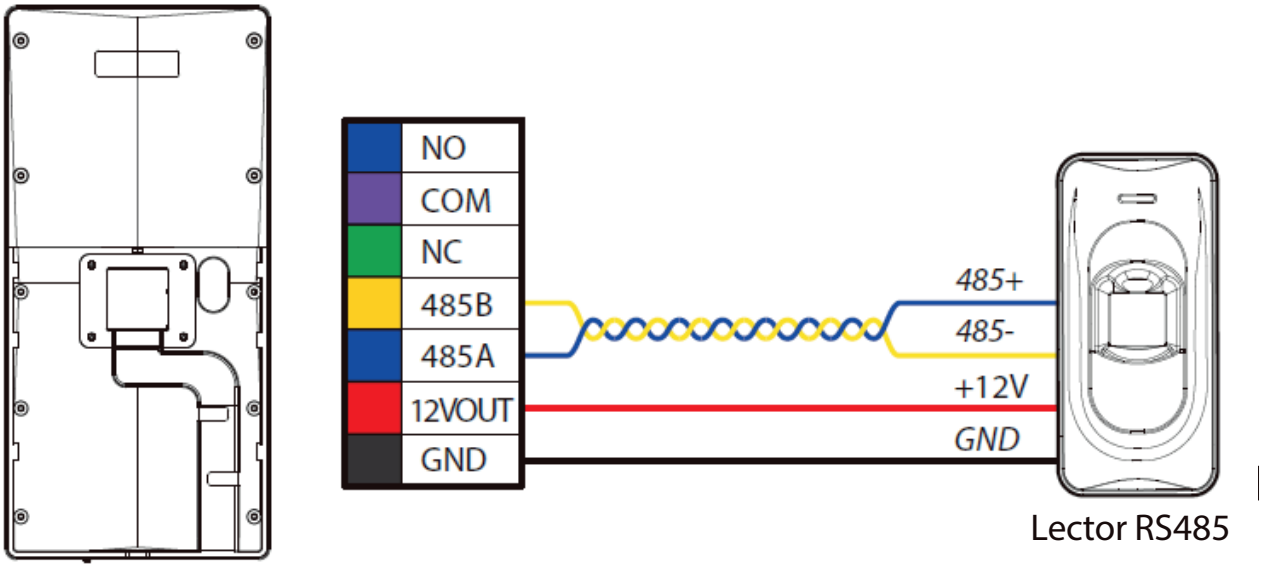
Haga clic en **Comm.** > **Ethernet** > **Dirección IP** para introducir la dirección IP.

Nota: En LAN, la dirección IP del servidor (PC) y del dispositivo deben estar en el mismo segmento de red al conectarse al software.

2.3.3 Botón de salida, sensor de puerta y conexión auxiliar



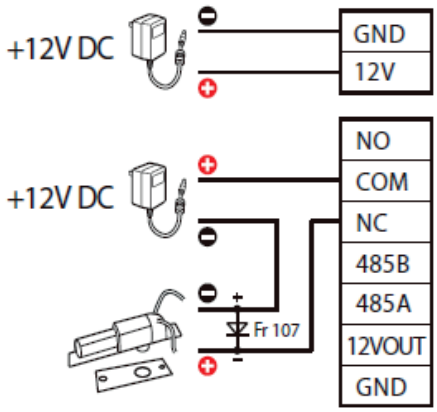
2.3.4 Conexión RS485



2.3.5 Conexión del relé de bloqueo

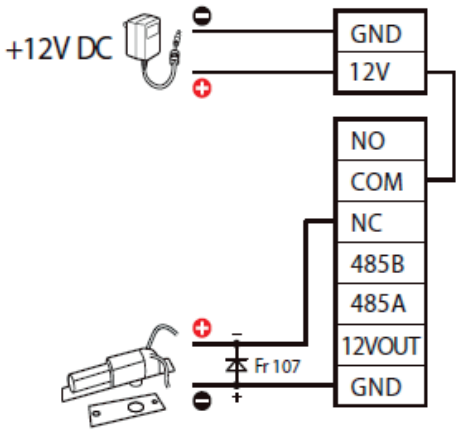
El sistema admite tanto cerraduras normalmente abiertas como cerraduras normalmente cerradas. La cerradura NO (normalmente abierta cuando está alimentada) se conecta con los terminales «NO» y «COM», y la cerradura NC (normalmente cerrada cuando está alimentada) se conecta con los terminales «NC» y «COM». La alimentación se puede compartir con la cerradura o se puede utilizar por separado para la cerradura, como se muestra en el ejemplo con cerradura NC a continuación:

1) Dispositivo que no comparte la alimentación con la cerradura alimentación con la cerradura



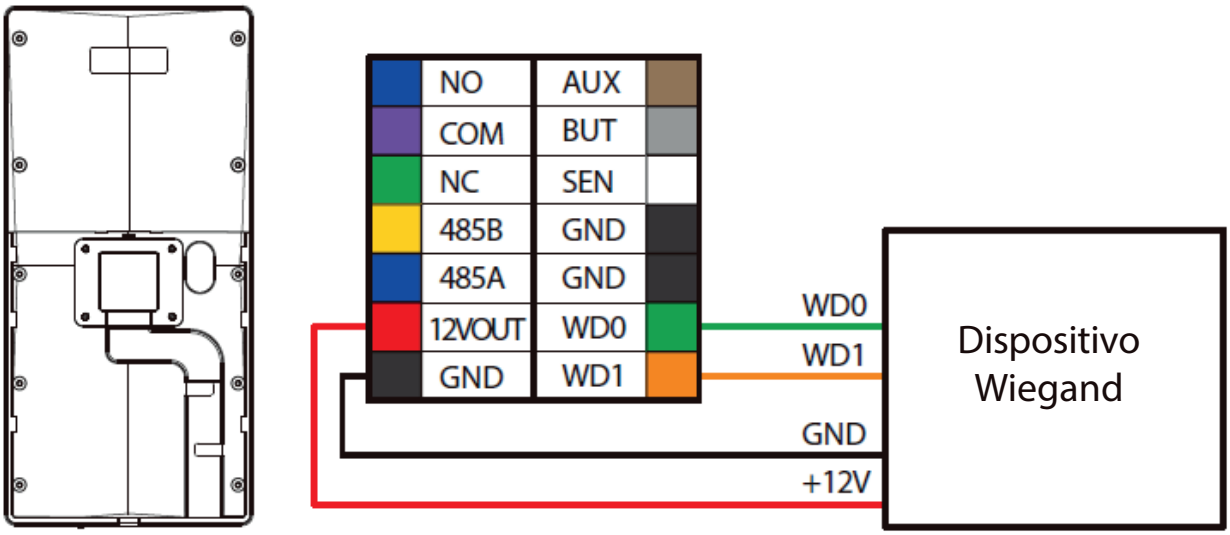
Bloqueo normalmente cerrado

2) Dispositivo para compartir energía con el bloqueo



Cerradura normalmente cerrada

2.3.6 Conexión del lector Wiegand



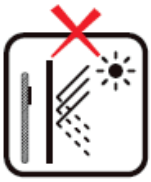
3. Instalación

3.1 Entorno de instalación

Consulte las siguientes recomendaciones para la instalación.



INSTALAR ÚNICAMENTE EN INTERIORES



EVITE LA INSTALACIÓN CERCA DE VENTANAS DE CRISTAL



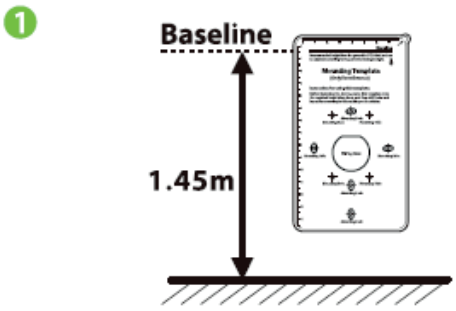
EVITE LA LUZ SOLAR DIRECTA Y LA EXPOSICIÓN

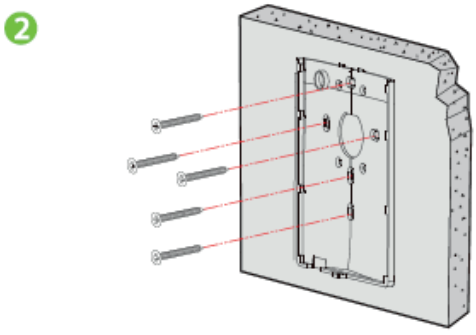


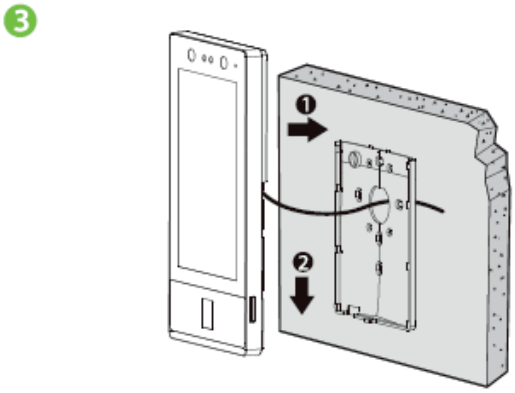
EVITE EL USO DE CUALQUIER FUENTE DE CALOR CERCA DEL DISPOSITIVO

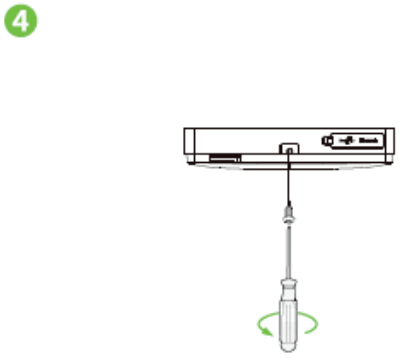
3.2 Instalación del dispositivo

1. Pegue la plantilla de montaje adhesiva a la pared y taladre los agujeros según las indicaciones del papel de montaje.
2. Fije la placa trasera a la pared con los tornillos de montaje en pared
3. Después de pasar los cables por el orificio de cableado y conectarlos al dispositivo, encaje el dispositivo en la placa posterior y empújelo hacia abajo hasta que encaje en su sitio.
4. Fije el dispositivo a la placa trasera con un tornillo de seguridad.



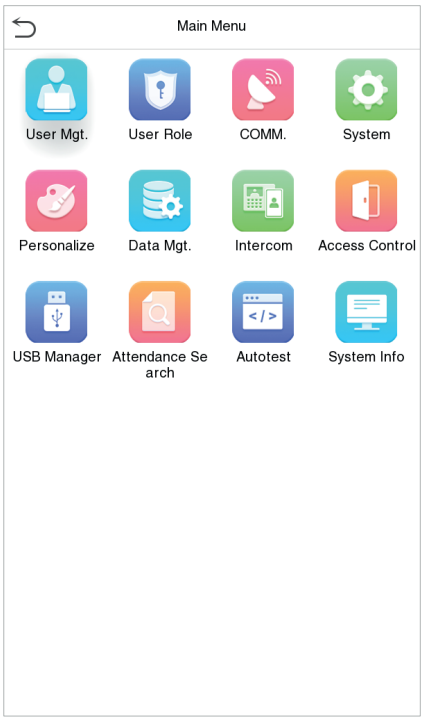






4. Menú principal

Pulse « » (Abrir menú principal) en la interfaz de espera para acceder al menú principal. Se mostrará la siguiente pantalla:

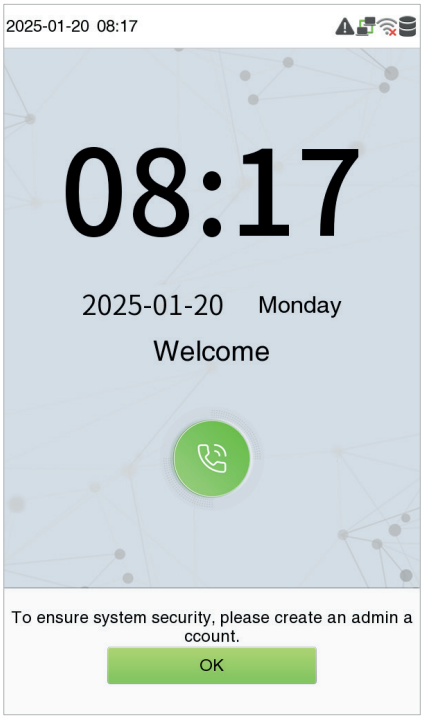


Descripción de la función

Menu	Descriptions
Gestión de usuarios	Añadir, editar, ver y eliminar información básica de un usuario.
Rol de usuario	Establecer el alcance de los permisos del rol personalizado y del registrador para los usuarios, es decir, los derechos para operar el sistema.
COMM.	Configurar los parámetros relevantes de red, comunicación serie, conexión a PC, red inalámbrica, servidor en la nube, Wiegand y diagnóstico de red.
Sistema	Para configurar los parámetros relacionados con el sistema, incluyendo la fecha y la hora, la configuración de los registros de acceso, los parámetros de la plantilla facial y las huellas dactilares ★, la configuración del tipo de dispositivo, la configuración de seguridad, la actualización del firmware en línea, la actualización USB y el restablecimiento de los ajustes de fábrica.
Personalizar	Incluye la interfaz de usuario, la voz, los horarios de las campanas, las opciones de estado de asistencia y la configuración de las asignaciones de teclas de acceso directo
Gestión de datos	Para eliminar todos los datos relevantes del dispositivo.
Intercom	Para configurar los parámetros relacionados con el SIP y el NVR.
Control de acceso	Para configurar los parámetros de la cerradura y el dispositivo de control de acceso relevante, incluyendo opciones como reglas de tiempo, configuración de días festivos, verificación combinada y configuración de opciones de coacción.

Menu	Descriptions
Administrador USB	Para cargar o descargar datos específicos mediante una unidad USB.
Búsqueda de asistencia	Para consultar los registros de eventos especificados, compruebe las fotos de asistencia y las fotos de asistencia de la lista de bloqueados..
Auto-comprobación	Para comprobar automáticamente si cada módulo funciona correctamente, incluyendo la pantalla LCD, el audio, el micrófono, la cámara, el sensor de huellas dactilares★ y el reloj en tiempo real.
Información del sistema	Para ver la capacidad de datos, la información del dispositivo y del firmware, y la políticade privacidad del dispositivo.

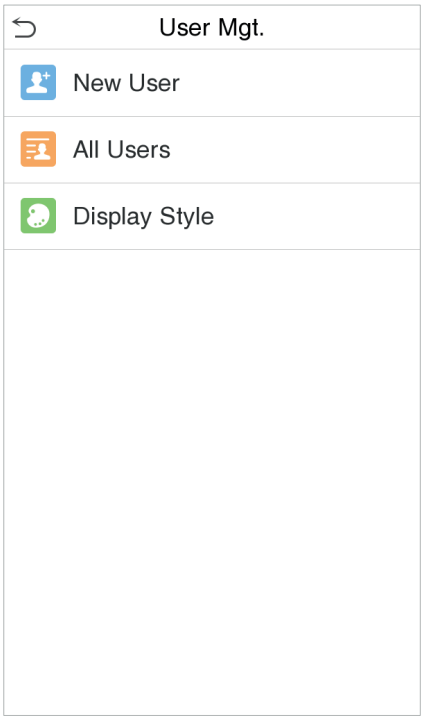
Nota: *Cuando los usuarios utilicen el producto por primera vez, deberán configurar los privilegios de administrador antes de utilizarlo. Toque* **«Gestión de usuarios»** *para añadir un administrador o editar los permisos de usuario como superadministrador. Si el producto no tiene una configuración de administrador, el sistema mostrará un mensaje de comando de configuración de administrador cada vez que acceda al menú del dispositivo.*



5. Gestión de usuarios

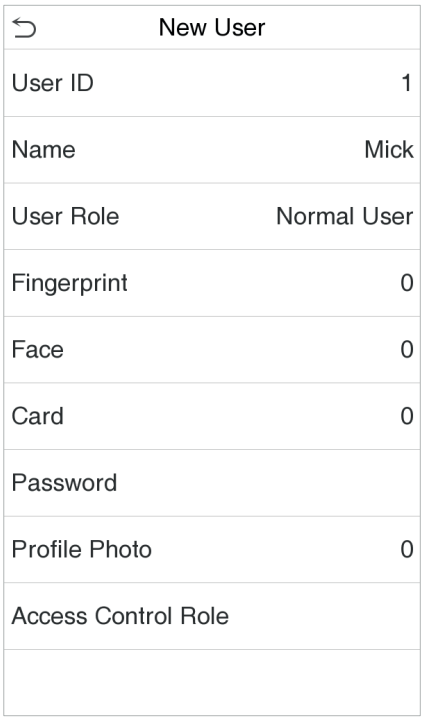
5.1 Registro de usuarios

Haga clic en **«Gestión de usuarios»** en el menú principal.



5.1.1 ID de usuario y nombre

Pulse **Nuevo usuario.** Introduzca el **ID de usuario y el nombre.**



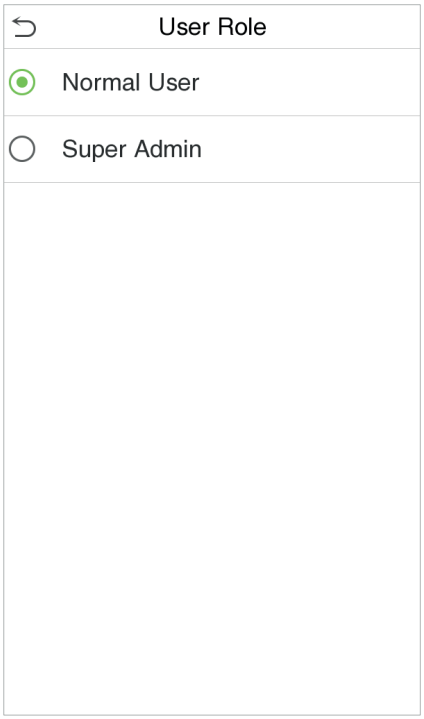
Notas:

- *Un nombre de usuario puede contener un máximo de 34 caracteres.*
- *El ID de usuario puede contener de 1 a 14 dígitos de forma predeterminada.*
- *Durante el registro inicial, puede modificar su ID, que no se puede modificar después del registro.*
- *Si aparece el mensaje «¡Duplicado!», debe elegir otro ID, ya que el ID de usuario introducido ya existe.*

5.1.2 Rol de Usuario

En la interfaz Nuevo usuario, pulse en **Rol de usuario** para establecer el rol del usuario como **Usuario normal** o **Superadministrador**

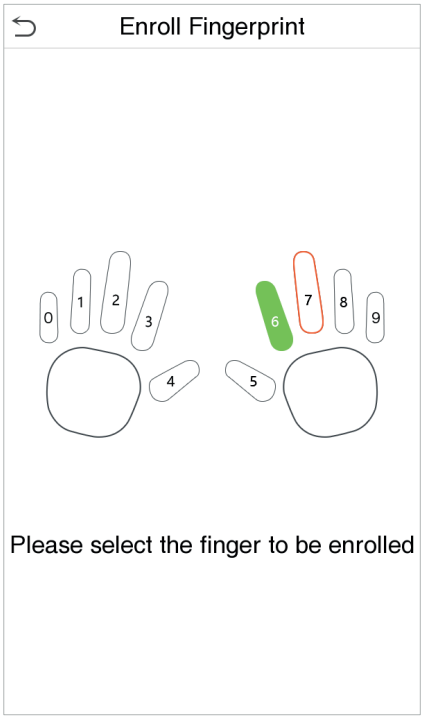
- **Superadministrador:** El superadministrador tiene todos los privilegios de administración del dispositivo
- **Usuario normal:** Si el superadministrador ya está registrado en el dispositivo, los usuarios normales no tendrán privilegios para gestionar el sistema y solo podrán acceder a las verificaciones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



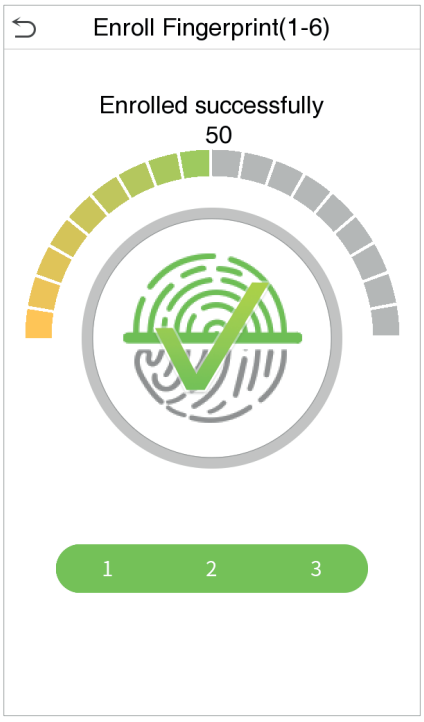
Nota: *Si el rol de usuario seleccionado es el de superadministrador, el usuario debe pasar la autenticación de identidad para acceder al menú principal. La autenticación se basa en los métodos de autenticación que haya registrado el superadministrador. Consulte 1.6 Modo de verificación.*

5.1.3 Huella dactilar★

Haga clic en **Huella dactilar** para acceder a la página de registro de huellas dactilares. Seleccione el dedo que desea registrar.



Presiona tres veces con el mismo dedo sobre el lector de huellas dactilares. La luz verde indica que la huella dactilar se ha registrado correctamente.

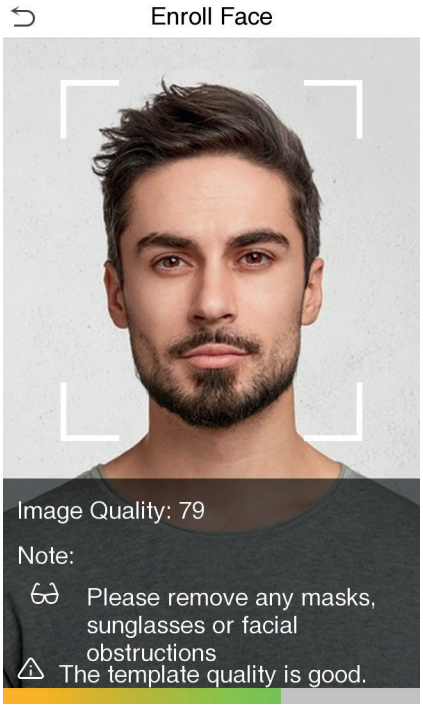


5.1.4 Plantilla facial

Toque Cara en la interfaz Nuevo usuario para acceder a la página de registro de la plantilla facial.

Míre hacia la cámara, coloque su plantilla facial dentro del cuadro guía blanco y permanezca quieto durante el registro de la plantilla facial.

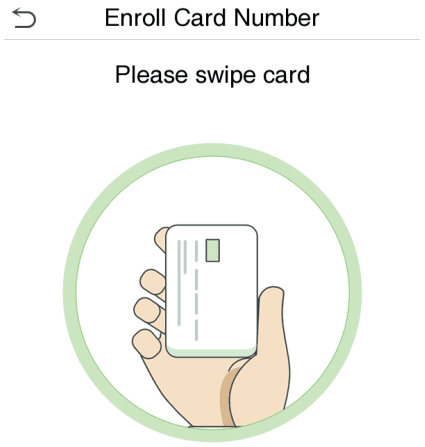
- Aparecerá una barra de progreso durante el registro de la plantilla facial y, cuando se complete, se mostrará el mensaje «Registrado correctamente».
- Si la plantilla facial ya está registrada, aparecerá el mensaje «Rostro duplicado». La interfaz de registro es la siguiente:



5.1.5 Tarjeta

Toque **Tarjeta** en la interfaz de **Nuevo usuario** para acceder a la página de registro de tarjetas.

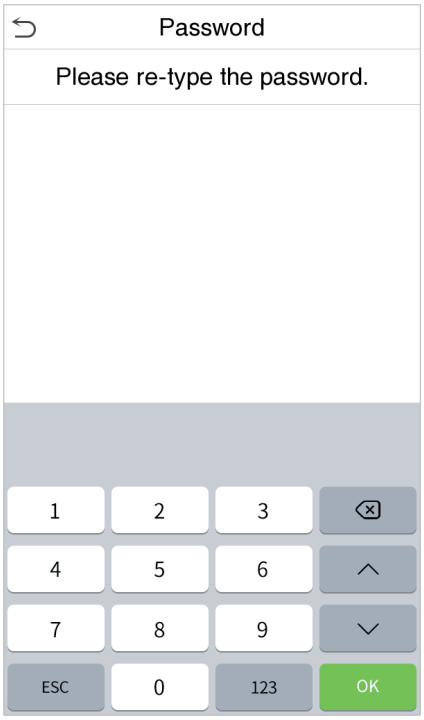
- En la interfaz Tarjeta, deslice la tarjeta por debajo del área de lectura de tarjetas. El registro de la tarjeta se realizará correctamente.
- Si la tarjeta ya está registrada, aparecerá el mensaje «**Tarjeta duplicada**». La interfaz de registro es la siguiente:



5.1.6 Contraseña

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

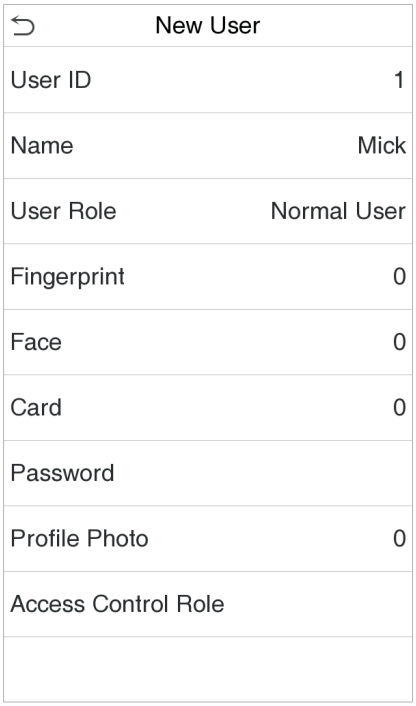
- En la interfaz Contraseña, introduzca la contraseña requerida y vuelva a introducirla para confirmarla y pulse **Aceptar.**
  - Si la contraseña introducida de nuevo es diferente de l a introducida inicialmente, el dispositivo mostrará el mensaje «**¡Contraseña no coincidente!**», y el usuario deberá volver a confirmar la contraseña.

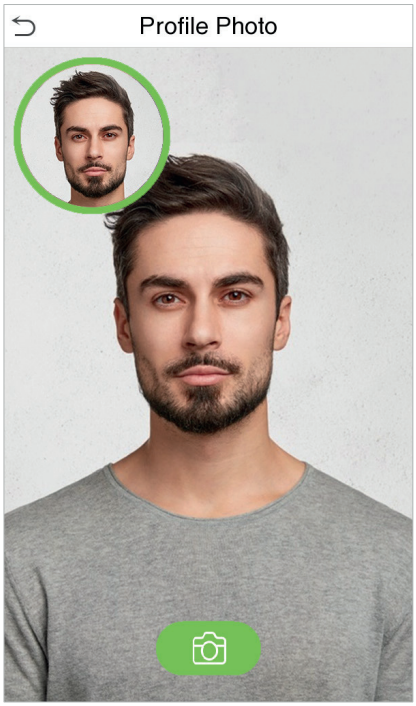


Nota: *La contraseña puede contener de 6 a 8 dígitos de forma predeterminada.*

5.1.7 Foto de perfil

Pulsa en **Foto de perfil** en la interfaz **Nuevo usuario** para ir a la página de registro de la foto de perfil.





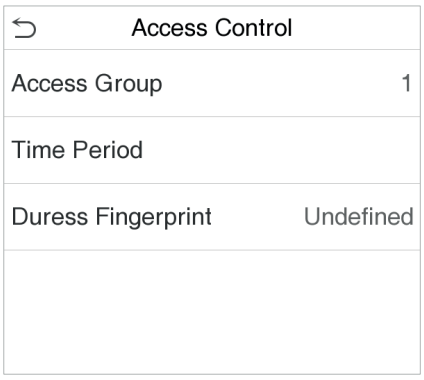
- Cuando un usuario registrado con una foto supera la autenticación, se mostrará la foto registrada.
- Toca la foto de perfil, se abrirá la cámara del dispositivo, luego toca el icono de la cámara para tomar una foto. La foto capturada se muestra en la esquina superior izquierda de la pantalla y la cámara se abre de nuevo para tomar una nueva foto, después de tomar la foto inicial.

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 establece automáticamente la foto capturada durante el registro como la foto predeterminada.*

5.1.8 Función de control de acceso

La función de control de acceso establece el privilegio de acceso a la puerta para cada usuario. Esto incluye el grupo de acceso, la huella digital de coacción y facilita establecer el período de tiempo de acceso al grupo.

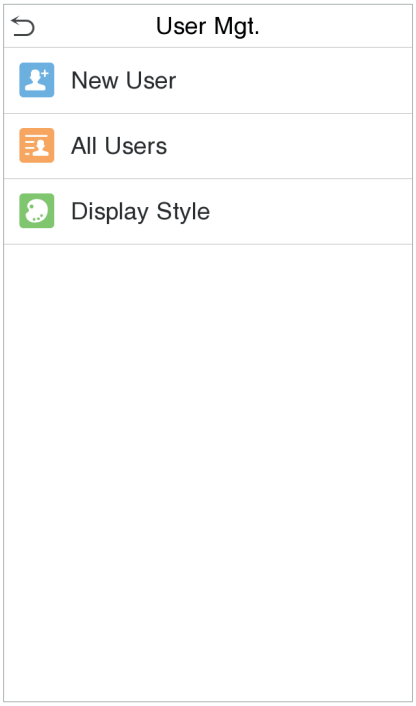
- Toque Rol de control de acceso > grupo de acceso, para asignar los usuarios registrados a diferentes grupos para una mejor administración. Los nuevos usuarios pertenecen al Grupo 1 de forma predeterminada y se pueden reasignar a otros grupos. El dispositivo admite hasta 99 grupos de control de acceso.
- Toque Período de tiempo para seleccionar el período de tiempo que desea usar.

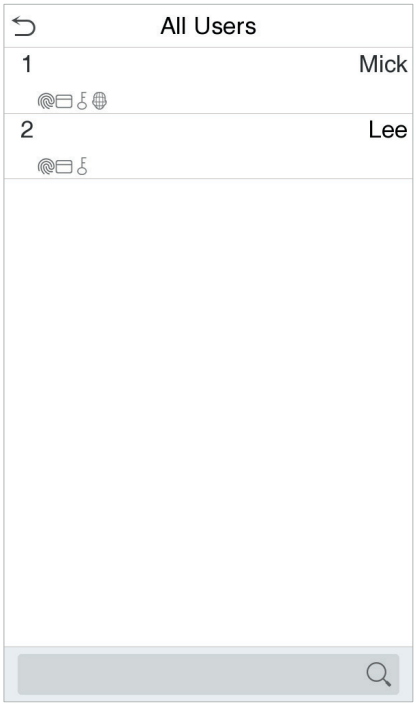


5.2 Búsqueda de usuarios

En el menú principal, pulse «Gestión de usuarios» y, a continuación, pulse «Todos los usuarios» para buscar un usuario.

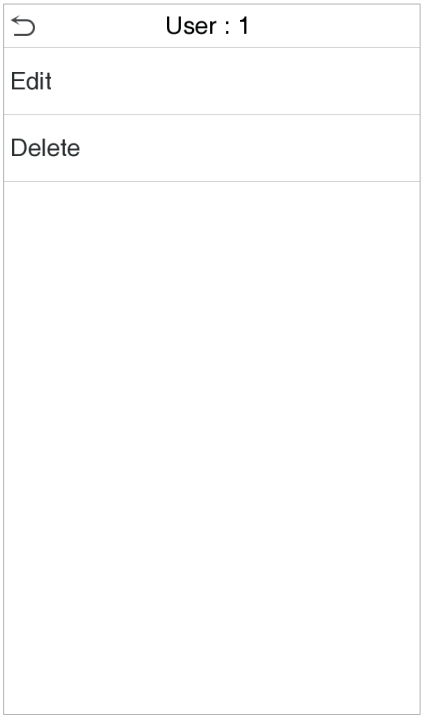
- En la interfaz Todos los usuarios, toque la barra de búsqueda en la lista de usuarios para ingresar la palabra clave de recuperación requerida (donde la palabra clave puede ser el ID de usuario, apellido o nombre completo) y el sistema buscará la información de usuario relacionada

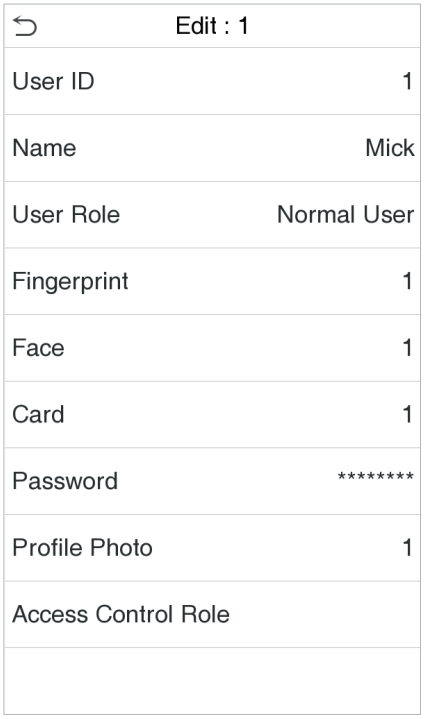




5.3 Editar usuario

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





Nota: *El proceso de edición de un usuario es el mismo que el de agregar un usuario, excepto que el ID de usuario no se puede modificar al editar los detalles de un usuario. El proceso en detalle se refiere a "3. Gestión de Usuarios".*

5.4 Eliminar usuario

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

- **Operaciones de eliminación**

Eliminar usuario: Toda la información del usuario se eliminará (elimina el usuario seleccionado en su totalidad) del dispositivo.

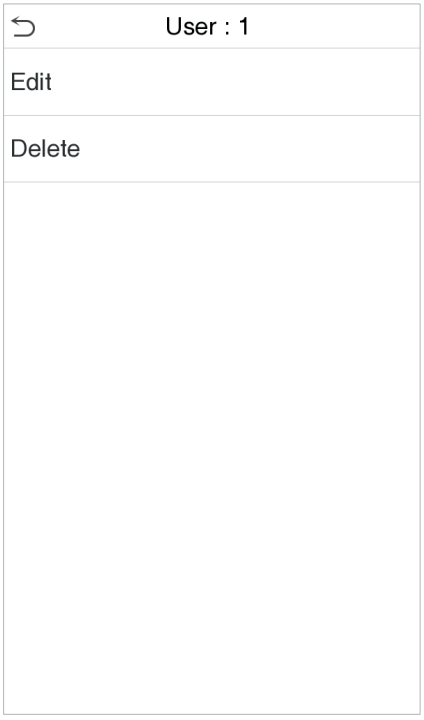
Eliminar solo huella digital: Elimina la información de huellas dactilares del usuario seleccionado.

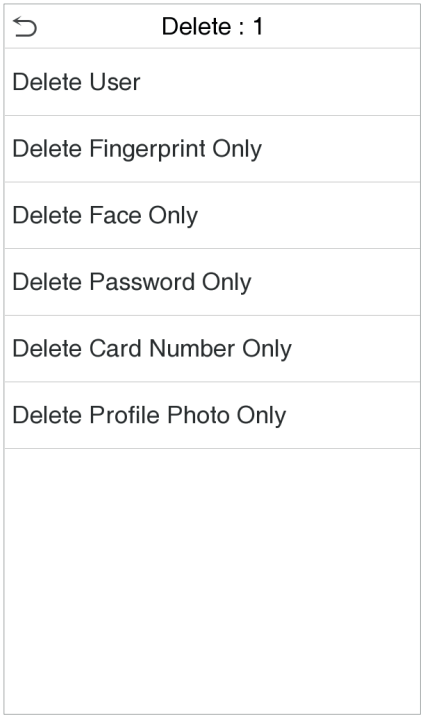
Eliminar solo cara: Elimina la información de la plantilla de cara del usuario seleccionado.

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.

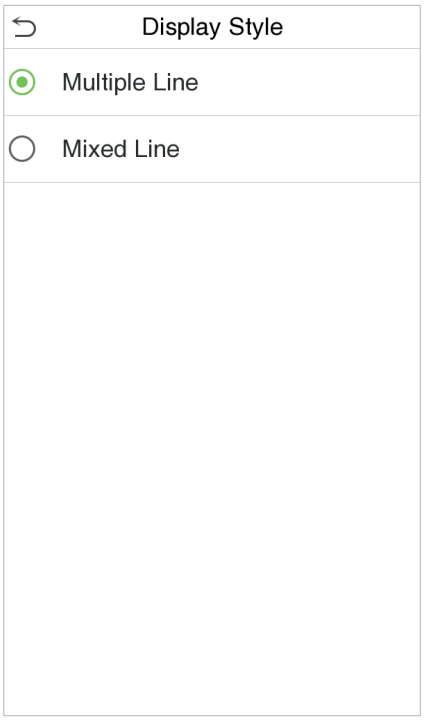
Eliminar solo foto de perfil: Elimina la foto de perfil del usuario seleccionado.





5.5 Estilo de visualización

Toque Administrador de usuario > Estilo de visualización para elegir el estilo de la lista de la interfaz Todos los usuarios.

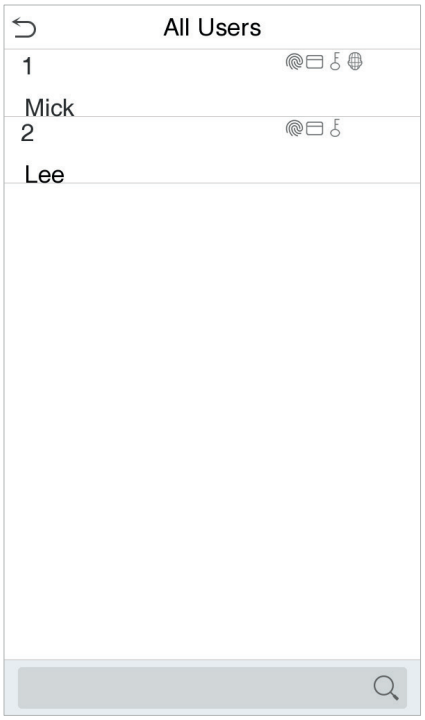


Los diferentes estilos de visualización se muestran a continuación:

Línea múltiple:



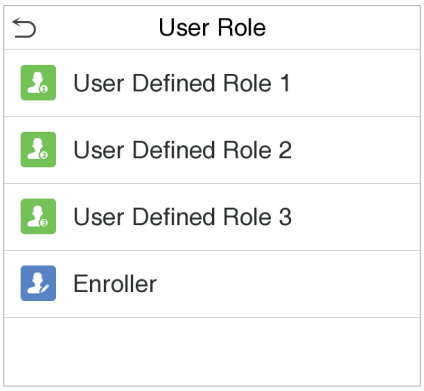
Línea Mixta:



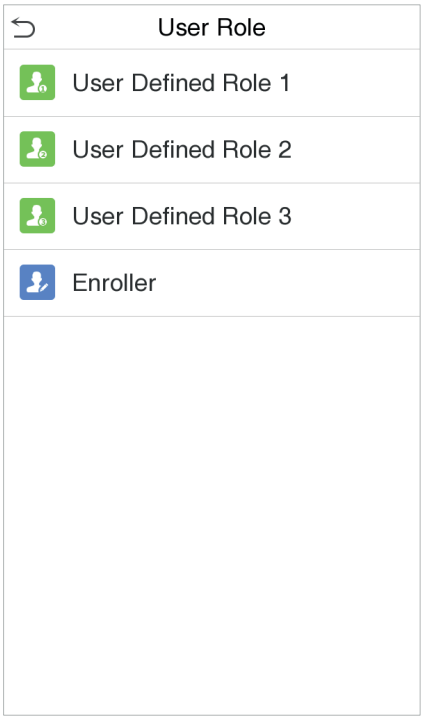
6. Rol de usuario

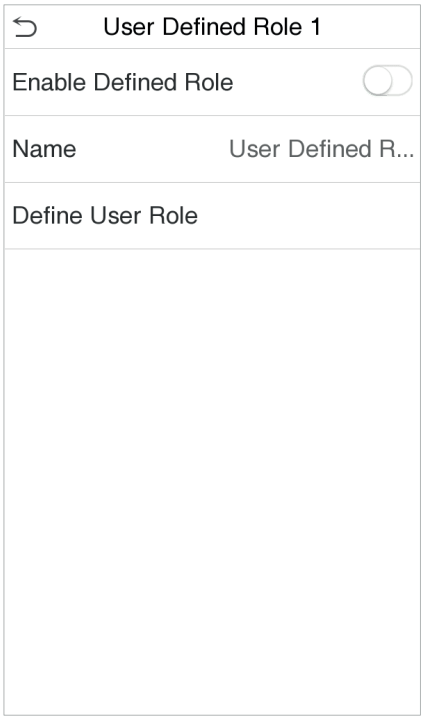
El rol de usuario facilita la asignación de algunos permisos específicos a usuarios específicos, en función del requisito.

- En el menú principal, toque Rol de usuario y luego toque el Rol definido por el usuario para establecer el usuario permisos definidos.
- El alcance de permisos del rol personalizado se puede configurar hasta 3 roles, es decir, el funcionamiento personalizado alcance de las funciones del menú del usuario.



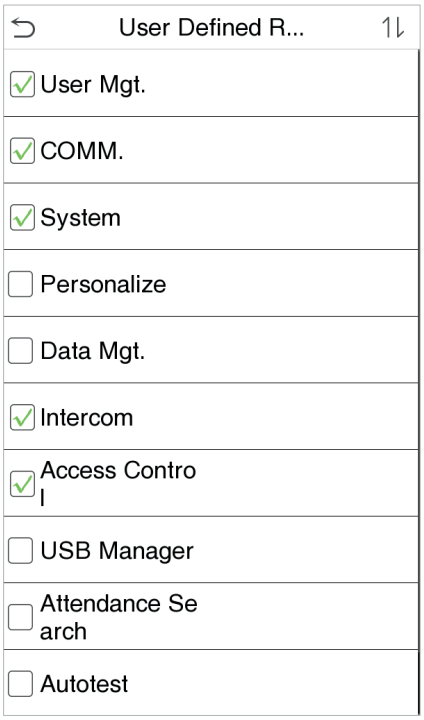
- En la interfaz de rol definido por el usuario, active Habilitar rol definido para habilitar o deshabilitar el usuario rol definido
- **Toque Nombre e ingrese el nombre personalizado del rol.**

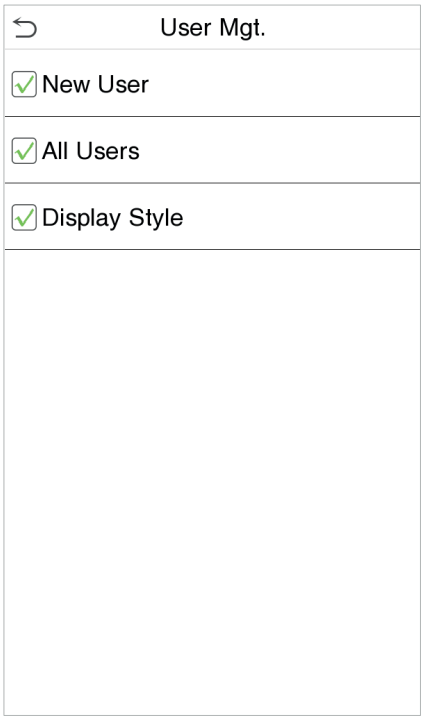




- Luego, toque Rol definido por el usuario y seleccione los privilegios necesarios para asignar al nuevo rol, y luego toque el botón Volver
- Durante la asignación de privilegios, los nombres de las funciones del menú principal se mostrarán a la izquierda y sus submenús se enumerarán a su derecha

Primero toque el nombre de la función del menú principal requerida y luego seleccione los submenús requeridos de la lista.

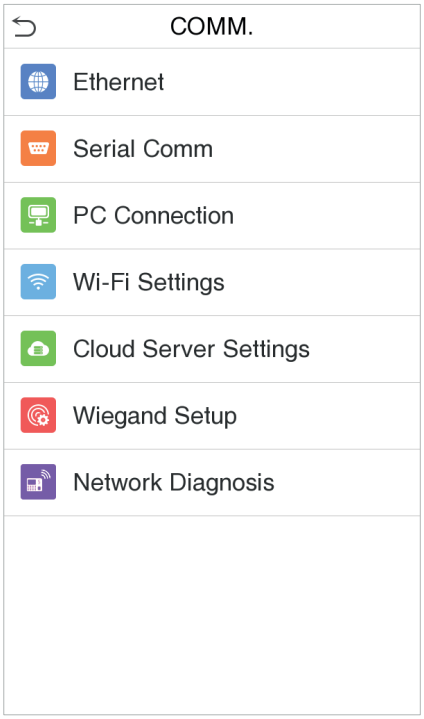




Nota: *Si el rol de usuario está habilitado para el dispositivo, toque Mgt. de usuario > nuevo usuario > rol de usuario para asignar los roles creados a los usuarios requeridos. Pero si no hay un superadministrador registrado en el dispositivo, el dispositivo solicitará "¡Inscriba primero al superadministrador!" al habilitar la función de rol de usuario.*

7. Configuración de comunicación

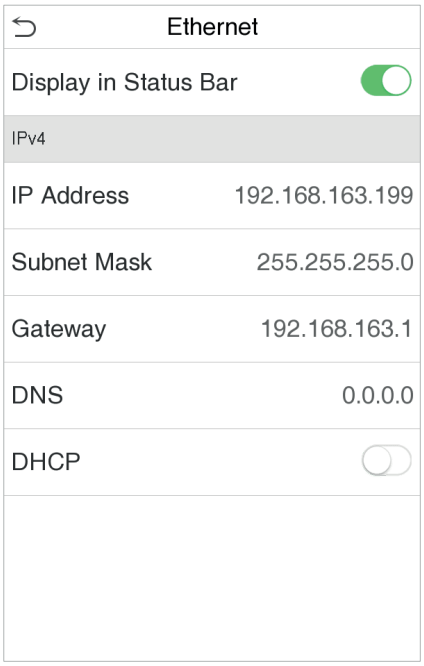
Toque COMM. en el menú principal para configurar los parámetros relevantes de Red, Comunicación en serie, Conexión a PC, Red inalámbrica, Servidor en la nube, Wiegand y Diagnóstico de red



7.1 Configuración de red

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

Toque Ethernet en la interfaz de configuración de comunicaciones para configurar los ajustes.



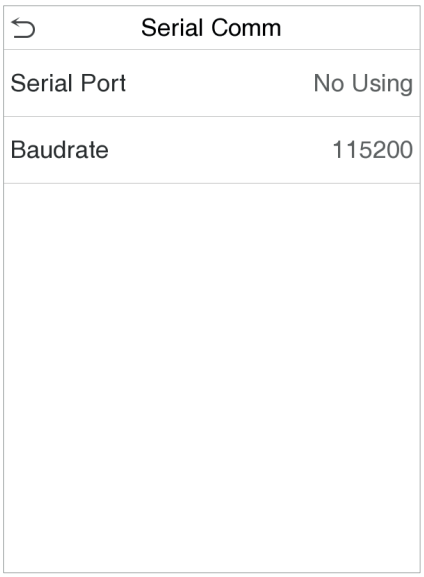
Descripción de la función

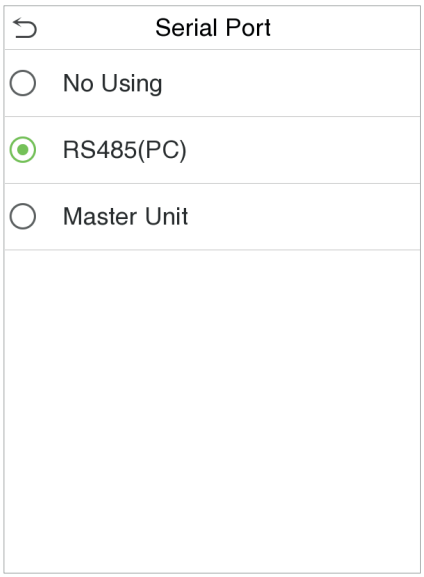
Nombre de la función	Descripciones
Visualización en la barra de estado	Alternar para establecer si se muestra el icono de red en la barra de estado.
Dirección IP	La dirección IP predeterminada es 192.168.1.201. Se puede modificar según la disponibilidad de la red.
Máscara de subred	La máscara de subred 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 consiste en asignar dinámicamente la dirección IP de los clientes a través del servidor.

7.2 Comunicación en serie

La función de comunicación en serie facilita el establecimiento de comunicación con el dispositivo a través de un puerto serie (RS485 / unidad maestra).

Toque Comunicación serie en la interfaz de configuración de comunicación





Descripción de la función

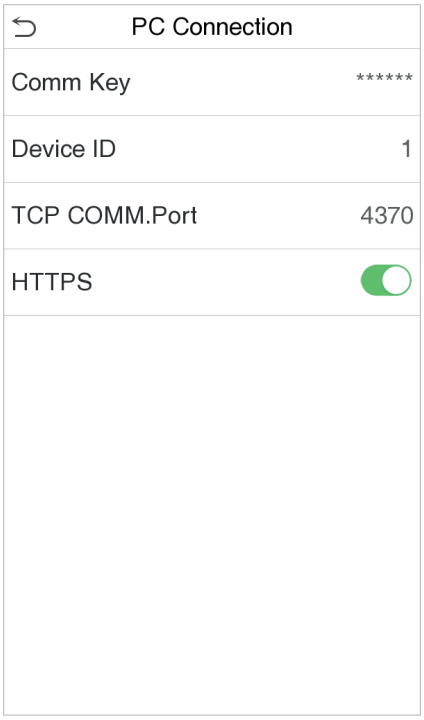
Nombre de la función	Descripciones
Puerto serie	No usando: No se comunique con el dispositivo a través del puerto serie. RS485 (PC): Se comunica con el dispositivo a través del puerto serie RS485. Unidad maestra: Cuando se utiliza RS485 como función de "unidad maestra", el dispositivo actuará como una unidad maestra y se puede conectar al lector de tarjetas RS485.

Nombre de la función	Descripciones
Velocidad	The rate at which the data is communicated with PC, there are 4 options of baud rate: 115200 (default), 57600, 38400, and 19200. The higher is the baud rate, the faster is the communication speed, but also the less reliable. Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.

7.3 Conexión a PC

Para mejorar la seguridad de los datos, establezca una clave de comunicación para la comunicación entre el dispositivo y la PC. Es necesario introducir la contraseña de conexión antes de que el dispositivo pueda conectarse al software del PC si se ha establecido una clave de comunicación.

Toque Conexión a PC en la interfaz de configuración de comunicaciones para configurar los ajustes de comunicación



Descripción de la función

Function Name	Descriptions
Tecla de comunicación	La contraseña predeterminada es 0 y se puede cambiar. La clave de comunicación debe tener 6 dígitos
ID de dispositivo	Número de identidad del dispositivo, que oscila entre 1 y 254.Si el método de comunicación es RS232/RS485, debe ingresar este ID de dispositivo en la interfaz de comunicación del software.
Puerto TCP COMM	El valor predeterminado del puerto TCP COMM es 4370. Se puede modificar según la disponibilidad de la red.

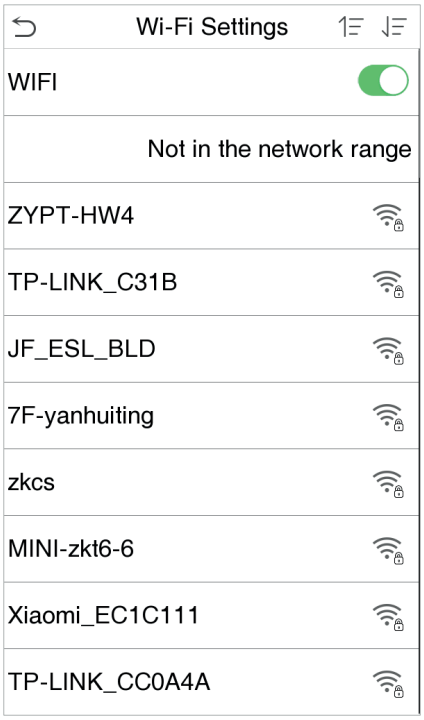
Function Name	Descriptions
HTTPS	Para aumentar la seguridad del acceso al software, los usuarios pueden habilitar el protocolo HTTPS para crear una transmisión de red segura y encriptada y garantizar la seguridad de los datos enviados a través de la autenticación de identidad y la comunicación encriptada. 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.

7.4 WIFI★

El dispositivo proporciona un módulo Wi-Fi, que se puede integrar dentro del molde del dispositivo o se puede conectar externamente.

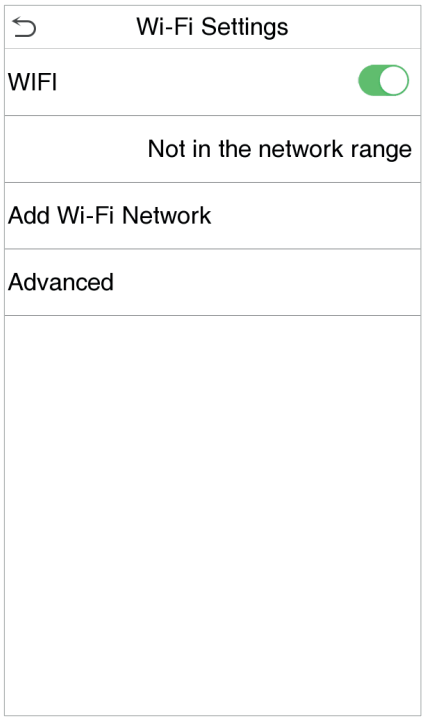
El módulo Wi-Fi permite la transmisión de datos a través de Wi-Fi (Wireless Fidelity) y establece un entorno de red inalámbrica. Wi-Fi está habilitado de forma predeterminada en el dispositivo. Si no necesita usar la red Wi-Fi, puede alternar el botón Wi-Fi para deshabilitar.

Toque Red inalámbrica en la interfaz de configuración de comunicaciones para configurar los ajustes de Wi-Fi.



- **Buscar en la red Wi-Fi**

- WIFI está habilitado en el dispositivo de forma predeterminada. Activar para activar o desactivar WIFI.
- Una vez que se enciende el Wi-Fi, el dispositivo buscará el Wi-Fi disponible dentro de la red.
- Elija el nombre de Wi-Fi apropiado de la lista disponible e ingrese la contraseña correcta en la interfaz de contraseña y, a continuación, pulse **Conectar a Wi-Fi (Aceptar)**.



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

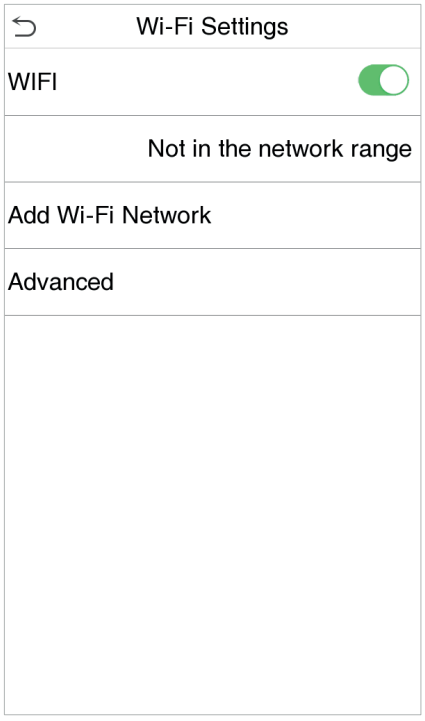


Toque el campo de contraseña para ingresar el contraseña , y luego toque Conectar a Wi-Fi (OK)

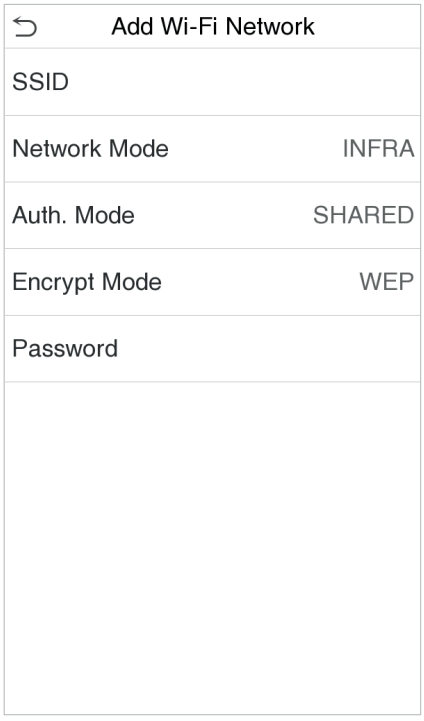
Cuando el Wi-Fi se conecta correctamente, la interfaz inicial mostrará el logo Wi-Fi.

- **Agregar red WIFI 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

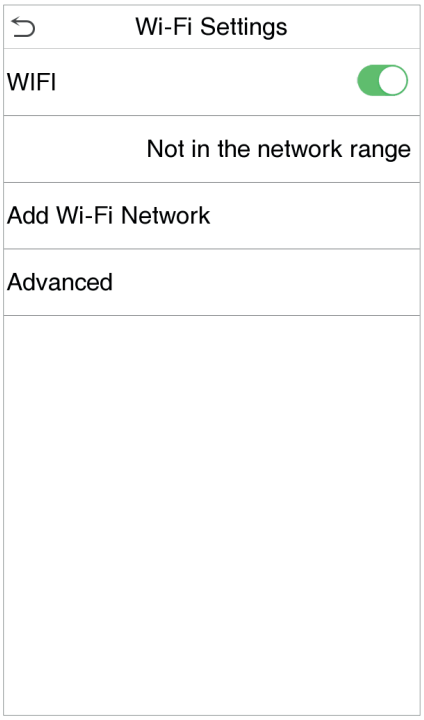


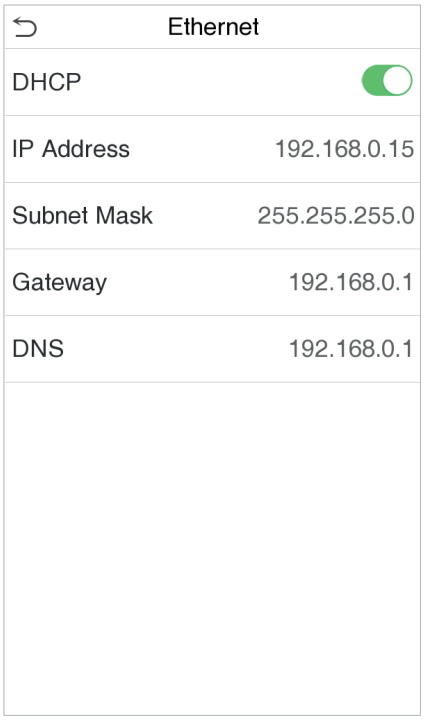
On this interface template, enter the Wi-Fi network parameters. (The added network must exist.)

Nota: *Después de agregar con éxito el WIFI manualmente, siga el mismo proceso para buscar el nombre de WIFI agregado. Haga clic aquí para ver el proceso de búsqueda de la red WIFI*

- **Configuración Avanzada**

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



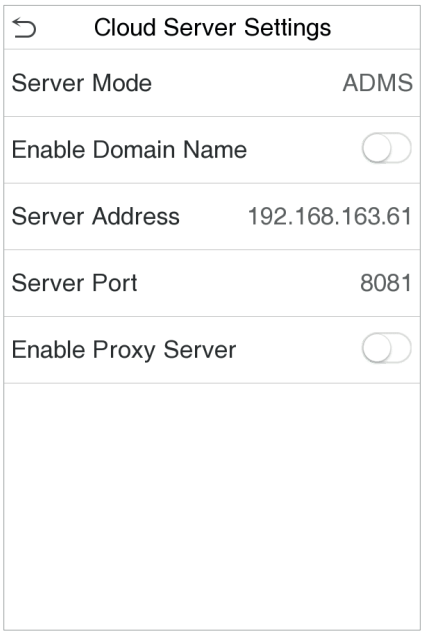


Descripción de la función

Function Name	Description
DHCP	El protocolo de configuración dinámica de host (DHCP) asigna dinámicamente la dirección IP a los clientes de red. Si el DHCP está habilitado, la IP no se puede configurar manualmente.
Dirección IP	Dirección IP para la red WIFI, el valor predeterminado es 0.0.0.0. Se puede modificar según la disponibilidad de la red.
Máscara de subred	La máscara de subred predeterminada de la red WIFI es 255.255.255.0. Se puede modificar según la disponibilidad de la red.
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 de acuerdo con la disponibilidad de la red.

7.5 Configuración del servidor en la nube

Toque Configuración del servidor en la nube en la interfaz de configuración de comunicaciones para conectarse con el servidor ADMS



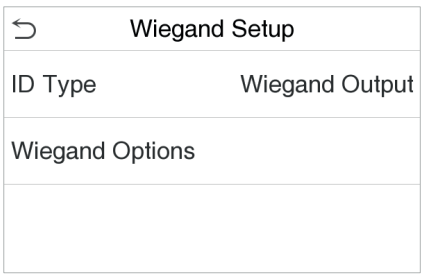
Descripción de la función

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.

7.6 Configuración de Wiegand

Para establecer los parámetros de entrada y salida de Wiegand.

Toque Wiegand Setup en la interfaz de configuración de COMM. para establecer los parámetros de entrada o salida de Wiegand.

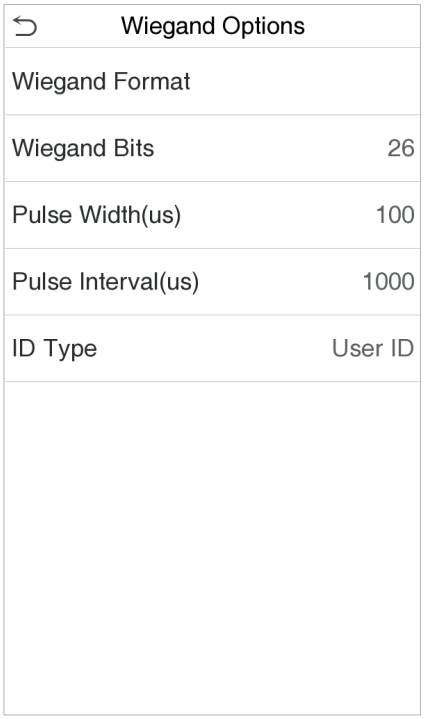


Nota: La interfaz Wiegand es compartida y el usuario puede elegir utilizar la función de entrada o salida Wiegand para interactuar con diferentes dispositivos Wiegand.

7.6.1 Entrada de Wiegand

Toque Tipo de ID en la Configuración de Wiegand, seleccione Entrada de Wiegand y, a continuación, toque Opciones de Wiegand en la Configuración de Wiegand.





Descripción de la función

Function Name	Descriptions
Formato Wiegand	Los valores oscilan entre 26 bits, 32 bits, 34 bits, 36 bits, 37 bits, 50 bits y 64 bits.
Bits Wiegand	Número de bits de datos de Wiegand.
Ancho de pulso (us)	El valor del ancho de pulso enviado por Wiegand es de 100 microsegundos de forma predeterminada, que se puede ajustar dentro del rango de 20 a 400 microsegundos.
Intervalo de pulso (us)	El valor predeterminado es 1000 microsegundos, que se puede ajustar dentro del rango de 200 a 20000 microsegundos.
Tipo de ID	Seleccione entre ID de usuario y número de tarjeta

Varios Descripción de formatos comunes de Wiegand

Wiegand Format	Description

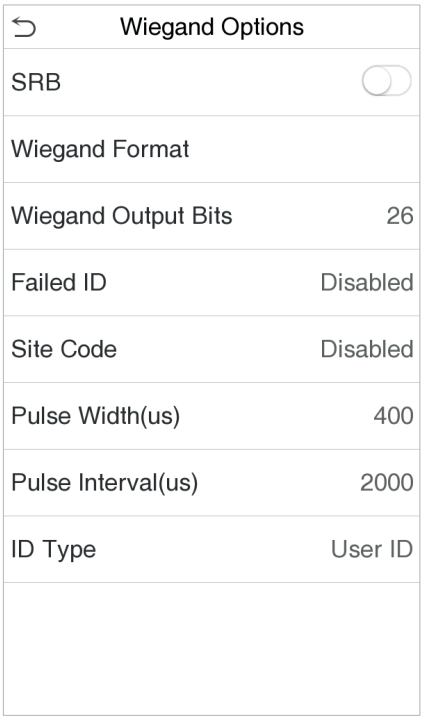
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El primer bit es el bit de paridad par de los bits 2 a 13, mientras que el bit 26 es el bit de paridad impar de los bits 14 a 25. Los bits 2 a 25 son los números de la tarjeta.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El primer bit es el bit de paridad par de los bits del 2º al 13º, mientras que el bit 26 es el bit de paridad impar de los bits del 14º al 25º. Los bits del 2º al 9º son los códigos de sitio, mientras que los bits del 10º al 25º son los números de tarjeta.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El primer bit es el bit de paridad par de los bits del 2º al 13º, mientras que el bit 26 es el bit de paridad impar de los bits del 14º al 25º. Los bits del 2º al 9º son los códigos de sitio, mientras que los bits del 10º al 25º son los números de tarjeta.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El primer bit es el bit de paridad par de los bits del 2 al 17, mientras que el bit 34 es el bit de paridad impar de los bits del 18 al 33. Los bits del 2 al 9 son los códigos de sitio, mientras que los bits del 10 al 25 son los números de tarjeta.
Wiegand36	OFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El primer bit es el bit de paridad par de los bits del 2º al 18º, mientras que el bit 36 es el bit de paridad impar de los bits del 19º al 35º. Los bits del 2º al 19º son los códigos de dispositivo, y los bits del 20º al 35º son los números de tarjeta.
Wiegand36a	EFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consta de 36 bits de código binario. El primer bit es el bit de paridad par de los bits del 2º al 18º, mientras que el bit 36 es el bit de paridad impar de los bits del 19º al 35º. Los bits del 2º al 19º son los códigos del dispositivo, y los bits del 20º al 35º son los números de tarjeta.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE Consta de 37 bits de código binario. El primer bit es el bit de paridad impar de los bits 2 a 18, mientras que el bit 37 es el bit de paridad par de los bits 19 a 36. Los bits del 2º al 4º son los códigos del fabricante. Los bits del 5º al 16º son los códigos del sitio, y los bits del 21º al 36º son los números de la tarjeta.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCO Consta de 37 bits de código binario. El primer bit es el bit de paridad par de los bits 2 a 18, mientras que el bit 37 es el bit de paridad impar de los bits 19 a 36. Los bits del 2º al 4º son los códigos del fabricante. Los bits del 5º al 14º son los códigos del dispositivo, los del 15º al 20º son los códigos del sitio y los del 21º al 36º son los números de tarjeta.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 50 bits de código binario. El primer bit es el bit de paridad par de los bits del 2 al 25, mientras que el bit 50 es el bit de paridad impar de los bits del 26 al 49. Los bits del 2 al 17 son los códigos de sitio, y los bits del 18 al 49 son los números de tarjeta.

"C" denota el número de tarjeta; "E" denota el bit de paridad par; "O" denota el bit de paridad impar; F" denota el código de la instalación; "M" denota el código del fabricante; "P" denota el bit de paridad; y "S" denota el código del sitio.

7.6.2 Salida Wiegand

Toque Tipo de ID en la Configuración de Wiegand, seleccione Salida de Wiegand y, a continuación, toque Opciones de Wiegand en la Configuración de Wiegand





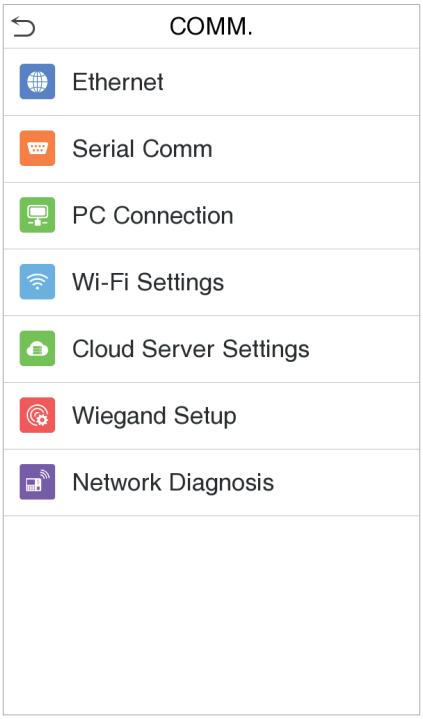
Descripción de la función

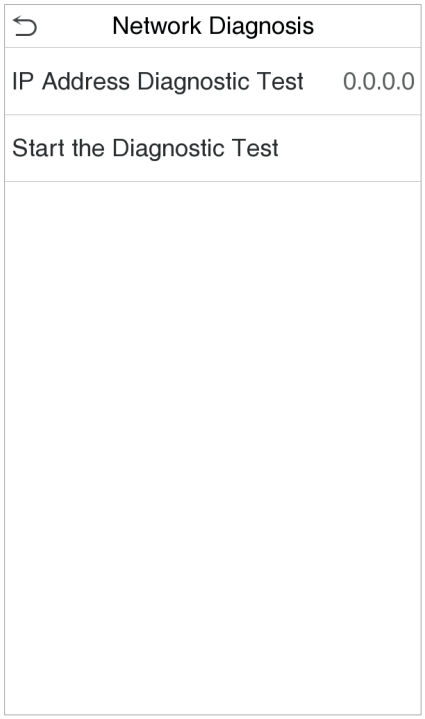
Nombre de la función	Descripción
SRB★	Cuando SRB está habilitado, el SRB controla el bloqueo para evitar que el bloqueo se abra debido a la extracción del dispositivo..
Formato Wiegand	Los valores oscilan entre 26 bits, 32 bits, 34 bits, 36 bits, 37 bits, 50 bits y 64 bits
Bits de salida Wiegand	Después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

7.7 Diagnóstico de la red

Para establecer los parámetros de diagnóstico de red.

Toque Diagnóstico de red en la interfaz de configuración de COMM. para establecer el diagnóstico de la dirección IP e iniciar los parámetros de diagnóstico.

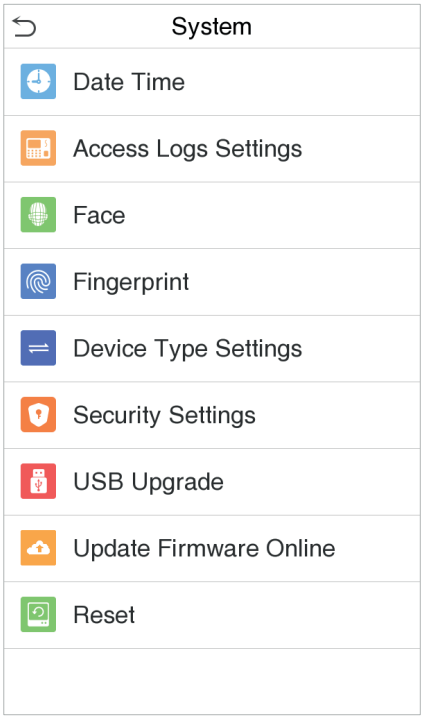




8. Configuración del sistema

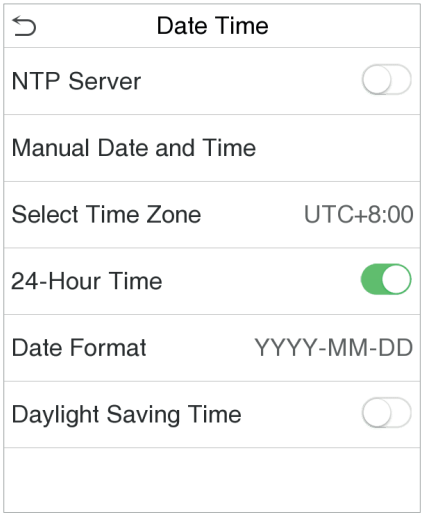
Establezca los parámetros del sistema relacionados para optimizar el rendimiento del dispositivo.

Toque Sistema en la interfaz del menú principal para configurar los parámetros del sistema relacionados para optimizar el rendimiento del dispositivo

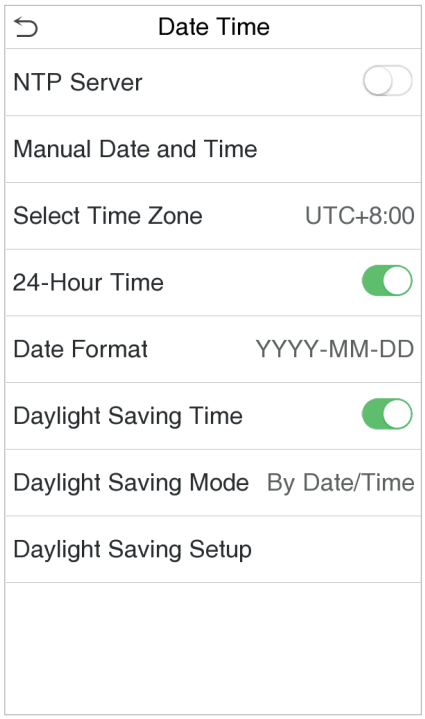


8.1 Fecha y hora

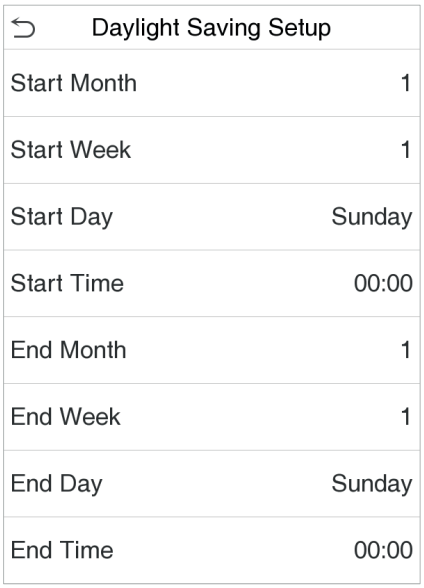
Toque Fecha y hora en la interfaz del sistema para establecer la fecha y la hora.

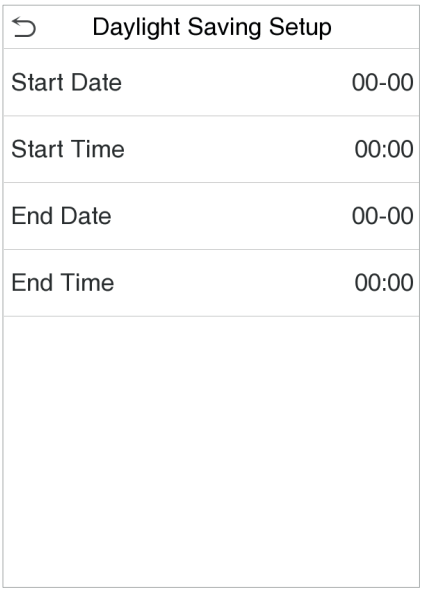


- El producto admite el sistema de sincronización horaria NTP de forma predeterminada. Esta función se activa después de habilitar el servidor NTP y configurar el enlace de dirección del servidor NTP correspondiente.
- Si los usuarios necesitan configurar la fecha y la hora manualmente, desactive primero el servidor NTP y, a continuación, pulse Datos y hora manuales para configurar la fecha y la hora y pulse Confirmar para guardar.



- Pulsa en «Formato de 24 horas» para activar o desactivar este formato. Si lo activas, selecciona el «Formato de fecha» para establecer el formato de fecha.
- Toque «Horario de verano» para activar o desactivar la función. Si está activada, toque «Modo horario de verano» para seleccionar un modo de horario de verano y, a continuación, toque «Configuración del horario de verano» para establecer la hora de cambio. Modo semanal Modo de fecha.



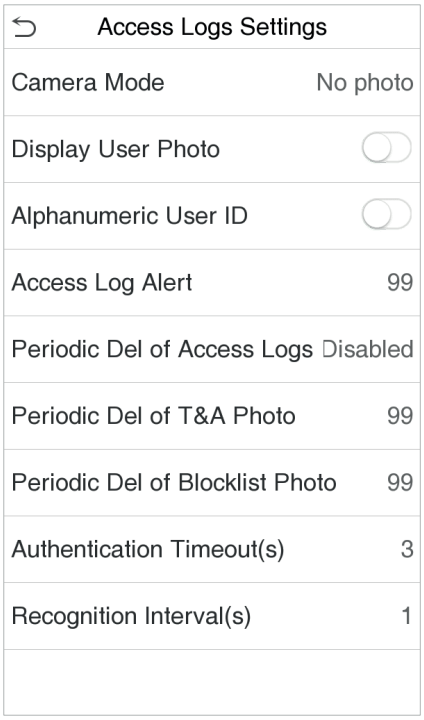


- Al restaurar la configuración de fábrica, se pueden restaurar la hora (24 horas) y el formato de fecha (AAAA-MM-DD), pero no se pueden restaurar la fecha y la hora del dispositivo.

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

8.2 Configuración de registros de acceso

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



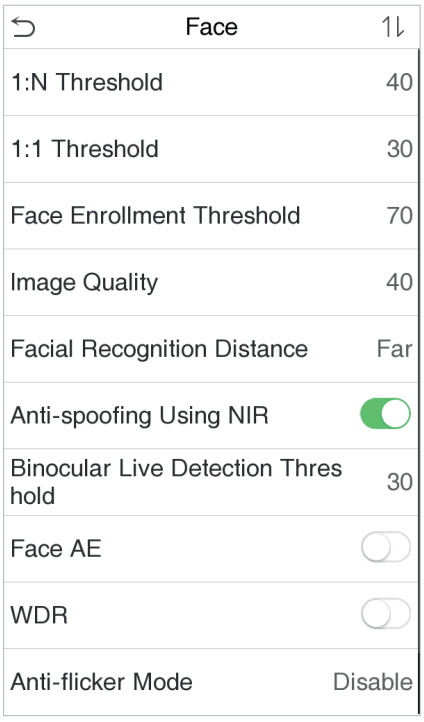
Descripción de la función

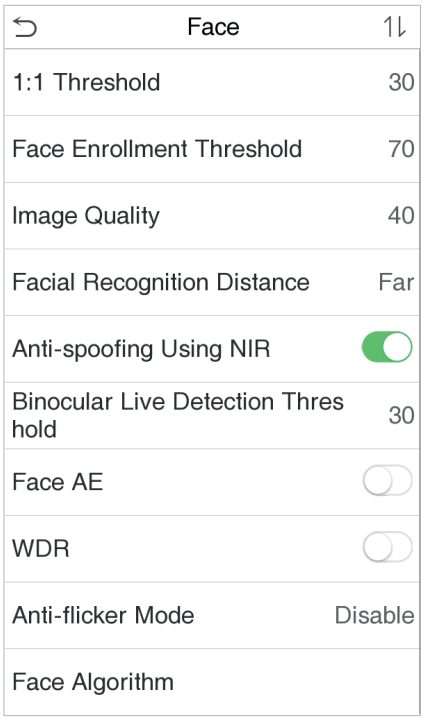
Nombre de la función	Descripción
Modo de cámara	Esta función está desactivada de forma predeterminada. Cuando esté habilitado, aparecerá un mensaje de seguridad y el sonido del obturador en la cámara se activará obligatoriamente.Hay 5 modos: Sin foto: No se toma ninguna foto durante la verificación del usuario. Tomar foto, no guardar: Se toma la foto, pero no se guarda durante la verificación. Tomar foto y guardar: Se toma la foto y se guarda durante la verificación. Guardar si la verificación es satisfactoria: Se toma la foto y se guarda cada vez que la verificación es satisfactoria. Guardar si la verificación falla: Se toma la foto y se guarda solo cuando la verificación falla.
Mostrar foto de usuario	Esta función está desactivada de forma predeterminada. Cuando está habilitado, habrá un mensaje de seguridad.
ID de usuario alfanumérico	Decide si se admiten letras en un ID de usuario.
Alerta de registros de acceso	Cuando el espacio de registro del acceso de asistencia alcanza el valor de umbral máximo, el dispositivo mostrará automáticamente la advertencia de espacio de memoria. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999.

Eliminación periódica de registros de acceso	Cuando los registros de acceso hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de registros de acceso antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 999.
Eliminación periódica de fotos T&A	Cuando las fotos de asistencia hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos de asistencia antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Eliminación periódica de fotos de la lista de bloqueados	Cuando las fotos de la lista de bloques hayan alcanzado su capacidad completa, el dispositivo eliminará 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	Se muestra la duración del mensaje de verificación correcta. Valor válido: 1~9 segundos.
Intervalo(s) de reconocimiento	Para establecer el intervalo de tiempo de coincidencia de la plantilla facial según sea necesario. Valor válido: 0~9 segundos.

8.3 Parámetros de la plantilla facial

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





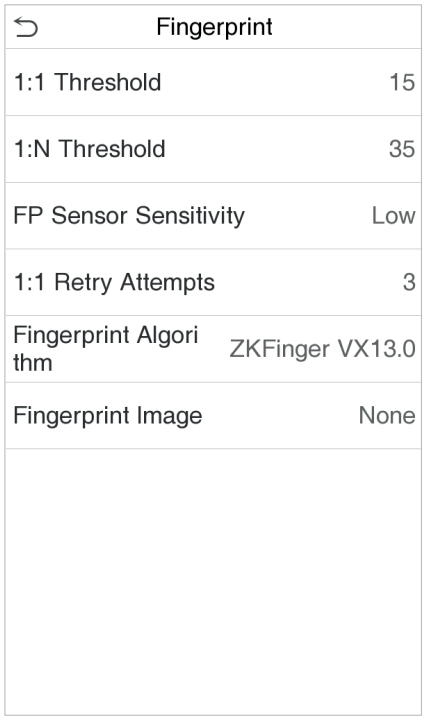
FRR	FAR	Umbrales de coincidencia recomendados	
		1:N	1:1
Alto	Bajo	85	80
Medio	Medio	82	75
Bajo	Medio	80	70

Descripción de la función

Nombre de la función	Descripción
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 oscilentre 0 y 100. Cuanto más altos sean los umbrales, menor será la tasa de rechazo, y viceversa. Se recomienda establecer el valor predeterminado de 75.
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 rechazo, y viceversa. Se recomienda establecer el valor predeterminado de 63.
Umbral de inscripción facial	Durante la inscripción de la plantilla de rostro, 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 este umbral, indica que la plantilla facial ya se ha registrado.
Calidad de imagen	Calidad de imagen para el registro y la comparación facial. Cuanto mayor sea el valor, más clara será la imagen.
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 esteparámetro puede ajustar la distancia de comparación más lejana de las caras.
Antifalsificación mediante NIR	Uso de imágenes de espectros de infrarrojo cercano para identificar y prevenir ataques de fotos y videos falsos
Umbral de detección binocular en vivo	Es conveniente juzgar si las imágenes espectrales del infrarrojo cercano son falsas de foto y video. 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 oscurecen
WDR	El amplio rango dinámico (WDR) equilibra la luz y amplía la visibilidad de la imagen para vídeos de vigilancia en escenas de iluminación de alto contraste y mejora la identificación de objetos en entornos brillantes y oscuros.
Modo antiparpadeo	Se utiliza cuando WDR está desactivado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea a la misma frecuencia que la luz.
Algoritmo de cara	Información relacionada con el algoritmo facial y pausa de la actualización de la plantilla facial.
Notas	Un ajuste incorrecto de los parámetros de exposición y calidad puede afectar gravemente al rendimiento del dispositivo. Ajuste el parámetro de exposición solo bajo la guía del personal de servicio posventa de nuestra empresa.

8.4 Parámetros de huellas dactilares ★

Haga clic en Huella digital en la interfaz del sistema



FRR	FAR	Umbrales de coincidencia recomendados	
		1:N	1:1
Alto	Bajo	45	25
Medio	Medio	35	15
Bajo	Alto	25	10

Function Description

Function Name	Descriptions
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.
Sensor FP Sensibilidad	Para establecer la sensibilidad de la adquisición de huellas dactilares. Se recomienda utilizar el nivel predeterminado "Medio". Cuando el entorno 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".
1:1 Intentos de reintento	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, Finger VX13.0 o FingerVX10.0.

Function Name	Descriptions
Imagen de huella dactilar	Esta función está desactivada de forma predeterminada. Después de desactivarla, la imagen de la huella dactilar no se mostrará al registrar y verificar las huellas dactilares. La interfaz del menú permite activar o desactivar esta función, y hay avisos de seguridad al cambiarla. Hay cuatro opciones disponibles: **Mostrar para el registro:** para mostrar la imagen de la huella dactilar en la pantalla solo durante el registro. **Mostrar para la comparación:** 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 el registro y la verificación. **Ninguna:** para no mostrar la imagen de la huella dactilar

8.5 Configuración del tipo de dispositivo

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

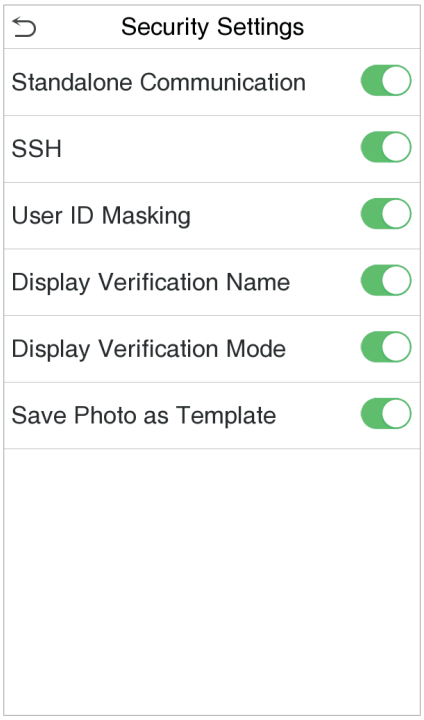


Descripción de la función

Nombre de la función	Descripción
Protocolo de comunicación	Establezca el protocolo de comunicación del dispositivo. (El protocolo BEST es administrado por ZKBio Zlink, consulte 15 Conexión a ZKBio Zlink Web y 16Conexión a la aplicación ZKBio Zlink).
Tipo de dispositivo	Configure el dispositivo como terminal de asistencia de tiempo (T&A PUSH) o terminal de control de acceso (A&C PUSH).

8.6 Configuración de seguridad

Toque Configuración de seguridad en la interfaz del sistema.



Descripción de la función

Nombre de la función	Descripción
Comunicación independiente	De forma predeterminada, esta función está deshabilitada. Esta función se puede activar o desactivar a través de la interfaz del menú. Cuando se enciende, aparece un mensaje de seguridad y el dispositivo se reiniciará después de que confirme.
SSH	El dispositivo no es compatible con la función Telnet, por lo que SSH se utiliza normalmente para la depuración remota. De forma predeterminada, SSH está habilitado. La interfaz del menú le permite habilitar y deshabilitar SSH. Cuando esté habilitado, habrá un mensaje de seguridad, pero no será necesario reiniciar el dispositivo después de la confirmación.
Ocultar ID de usuario	Después de habilitado, el ID de usuario se mostrará parcialmente después del resultado de la verificación del personal (solo el ID de usuario con más de 2 dígitos admite la visualización de solicitudes), y está habilitado de forma predeterminada.
Nombre de verificación de pantalla	Una vez habilitado, el nombre del usuario se mostrará después del resultado de la verificación de personal. El resultado de la verificación no mostrará el nombre después de deshabilitarlo.
Modo de verificación de pantalla	Una vez habilitado, el resultado de la verificación de personal mostrará el modo de verificación del usuario. El resultado de la verificación no mostrará el modo de verificación después de desactivarlo.
Guardar foto como plantilla	Después de deshabilitar esta función, es necesario volver a registrar la plantilla facial después de una actualización del algoritmo.

8.7 Actualización USB

Toque Actualización USB en la interfaz del sistema.

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

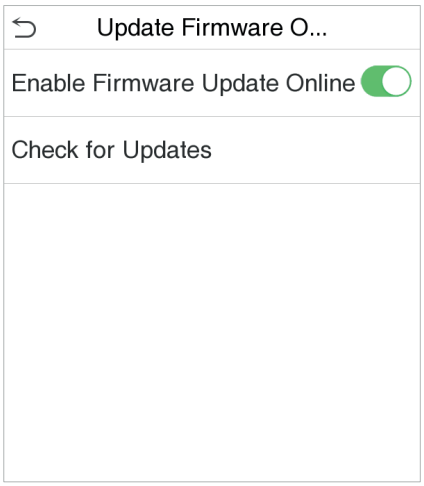


Nota: *Si necesita un archivo de actualización, póngase en contacto con nuestro soporte técnico. La actualización del firmware no se reinicia en circunstancias normales.*

8.8 Actualizar firmware en línea

Haga clic en Actualizar firmware en línea en la interfaz del sistema.

Haga clic en «Habilitar función de actualización de firmware en línea». El dispositivo le avisará de que la actualización puede suponer algunos riesgos para la seguridad de los datos, lo que requiere la confirmación manual por parte del usuario (si la función de configuración de seguridad está desactivada, la advertencia de riesgo no se mostrará cuando se active la actualización en línea).



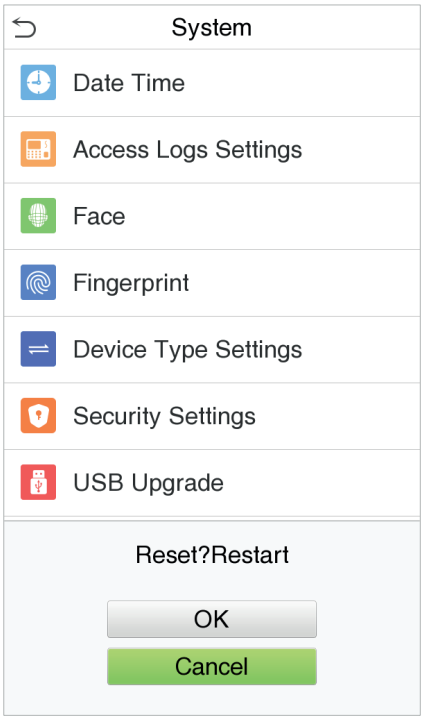
Haga clic en Buscar actualizaciones, puede tener los siguientes 3 escenarios:

- Si la consulta falla, la interfaz solicitará "Error de consulta".
- Si la versión de firmware del dispositivo es la más reciente, solicitará que el firmware actual La versión ya es la más reciente.
- Si la versión del firmware del dispositivo no es la más reciente, 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.

8.9 Restablecimiento de fábrica

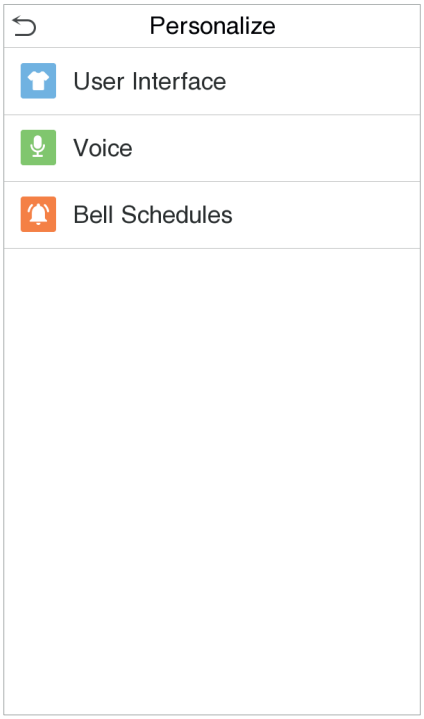
La función de restablecimiento de fábrica restaura la configuración del dispositivo, como la configuración de comunicación y la configuración del sistema, a la configuración predeterminada de fábrica (esta función no borra los datos de usuario registrados).

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



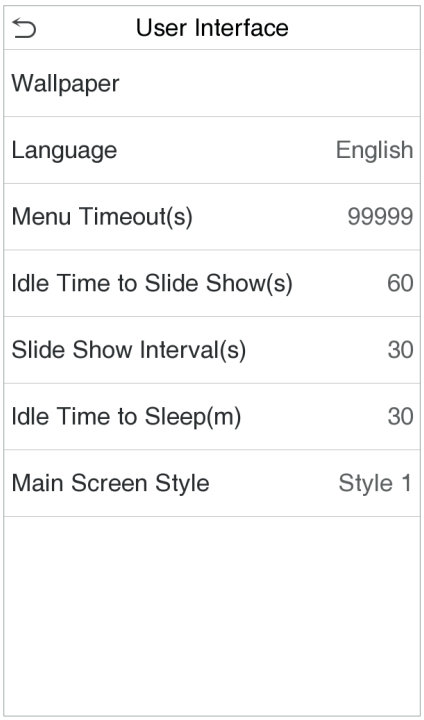
9. Personaliza la configuración

Toque Personalizar en la interfaz del menú principal para personalizar la configuración de la interfaz, la voz y el timbre



9.1 Configuración de la interfaz de usuario

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

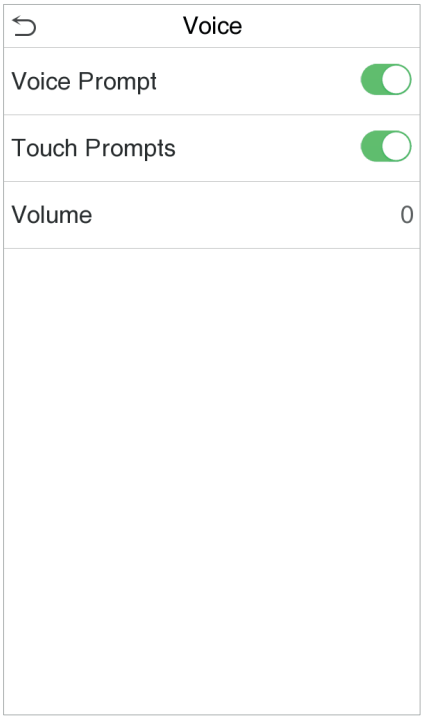


Descripción de la función

Nombre de la función	Descripción
Fondo de pantalla	El fondo de pantalla de la pantalla principal se puede seleccionar según las preferencias del usuario.
Idioma	Seleccione el idioma del dispositivo.
Tiempo de espera del menú (s)	Cuando no hay operación y el tiempo excede el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. La función se puede desactivar o establecer el valor requerido entre 60 y 99999 segundos.
Tiempo de inactividad hasta la presentación de diapositivas (s)	Cuando no hay ninguna operación y el tiempo supera el valor establecido, se reproducirá una presentación de diapositivas. La función se puede desactivar, o puede establecer el valor entre 3 y 999 segundos.
Intervalo de presentación de diapositivas (s)	Es el intervalo de tiempo para cambiar entre diferentes fotos de presentación de diapositivas. La función se puede desactivar, o puede establecer el intervalo entre 3 y 999 segundos.
Tiempo de inactividad para suspender	Si el modo de suspensión está activado y cuando no hay operación en el dispositivo, el dispositivo entrará en modo de espera. Toque la pantalla en cualquier lugar para reanudar el modo de trabajo normal. Esta función se puede desactivar o establecer un valor en 1-999 minutos.
Estilo de la pantalla principal	El estilo de la pantalla principal se puede seleccionar según las preferencias del usuario.

9.2 Ajustes de voz

Pulse Voz en la interfaz Personalizar para configurar los ajustes de voz

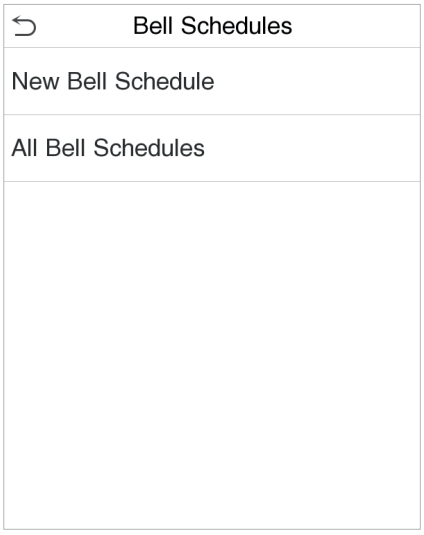


Descripción de la función

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

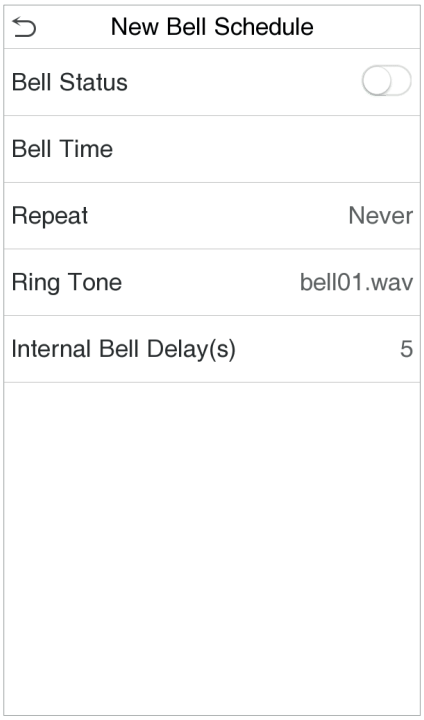
9.3 Ajustes de campana

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



- **Nuevo horario de campanas**

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



Descripción de la función

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 activará automáticamente para hacer sonar la campana durante ese tiempo.
Repetir	Establezca el número requerido de conteos 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. Los valores válidos oscilan entre 1 y 999 segundos.

- **Todos los horarios de campanas:**

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

- **Edite la campana programada:**

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

- **Eliminar una campana:**

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

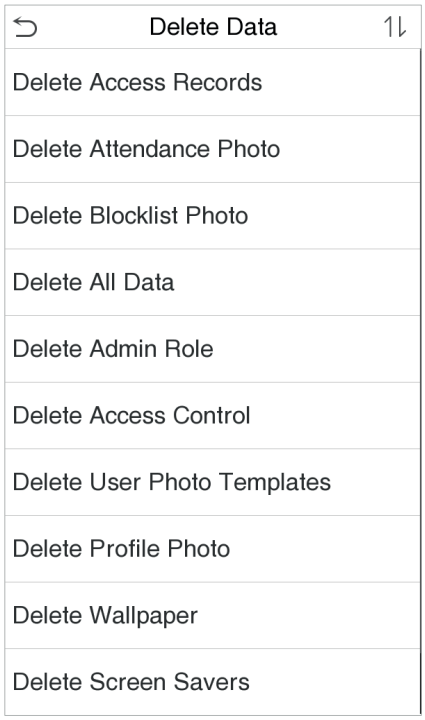
10. Gestión de datos

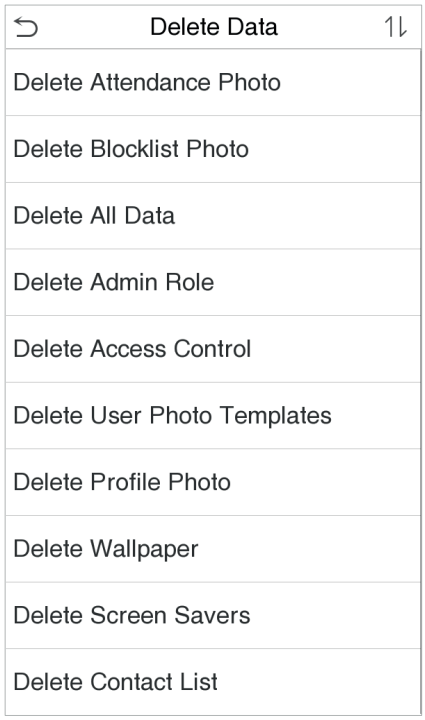
En el menú principal, toque Gestión de datos para eliminar los datos relevantes en el dispositivo



10.1 Eliminar datos

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





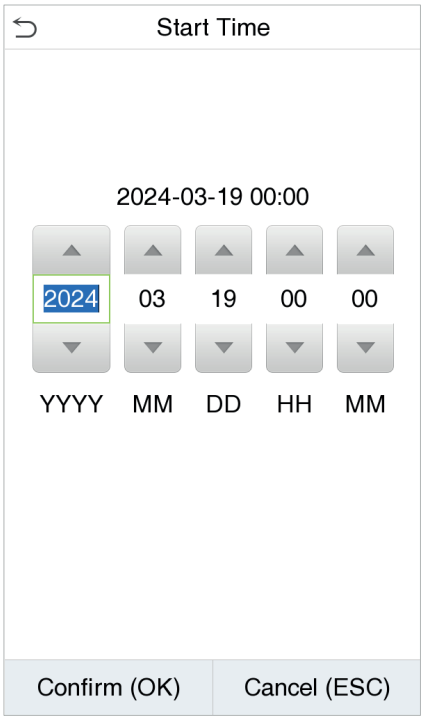
Descripción de la función

Nombre de la función	Descripción
Eliminar registros de acceso	Para eliminar registros de acceso condicionalmente.
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	Para eliminar la información y los registros de asistencia/registros de acceso 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 un nuevo registro facial después de una actualización del algoritmo"
Eliminar foto de perfil	Para eliminar todas las fotos de usuario en el dispositivo.
Eliminar fondo de pantalla	Para eliminar todos los fondos de pantalla del dispositivo.
Eliminar protectores de pantalla	Para eliminar los salvapantallas 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, las fotos de asistencia o las fotos de la lista de bloques. Al seleccionar Eliminar por rango de tiempo, debe establecer un rango de tiempo específico para eliminar todos los datos dentro de un período específico.



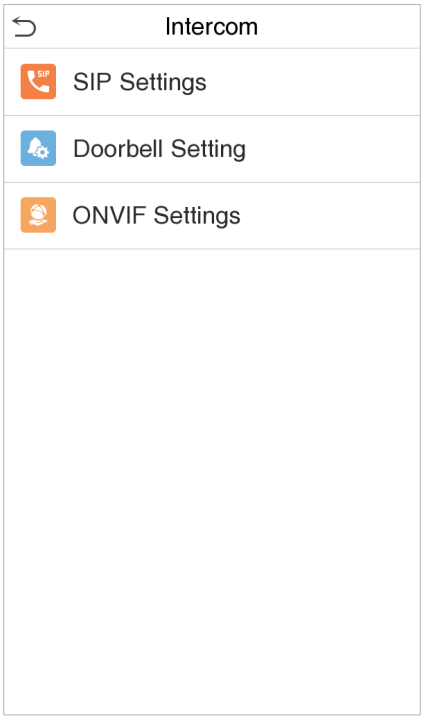
Seleccione Eliminar por intervalo de tiempo



Establezca el intervalo de tiempo y haga clic en Aceptar

11. Intercomunicador

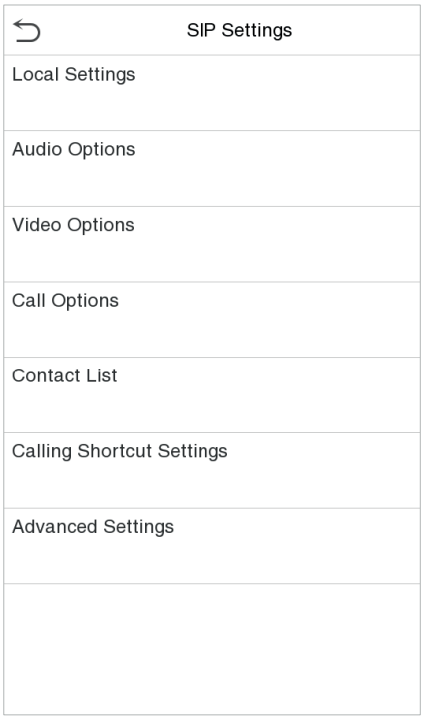
Haga clic en Parámetros del videoportero en la interfaz del sistema.



11.1 Configuración de SIP

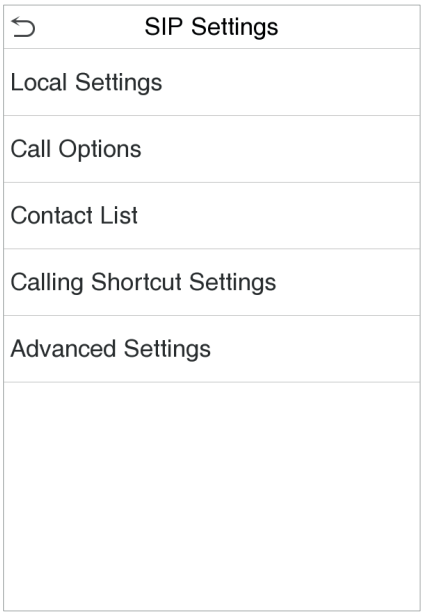
Nota: *Esta función debe utilizarse con la estación interior.*

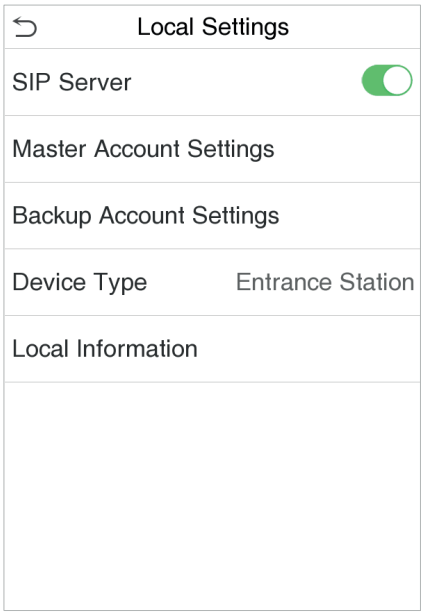
Toque Configuración SIP en la interfaz Parámetros del videoportero para ir a la configuración SIP de monitoreo



11.1.1 Configuración local

Toque Configuración local en la interfaz de Configuración SIP.



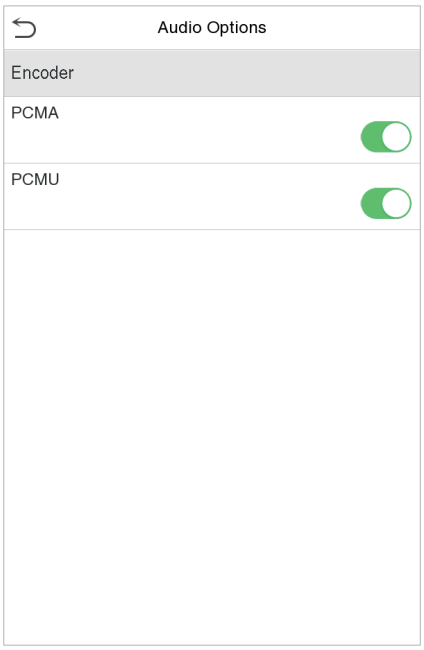


Descripción de la función

Function Name	Description
Servidor SIP	Seleccione si desea habilitar el servidor SIP. Cuando está habilitado, se debe establecer la cuenta SIP. Nota: Cada vez que se active o desactive esta función, la lista de contactos se reiniciará.
Configuración de la cuenta principal	Después de asignar la cuenta SIP al dispositivo en el ZKBio CVAccess, la información de la cuenta se sincronizará automáticamente con el dispositivo. No es necesario configurarlo manualmente.
Configuración de la cuenta de respaldo	Seleccione si desea habilitar la configuración de la cuenta de copia de seguridad.
Información local	Tipo de dispositivo: Configure el tipo de dispositivo como estación de entrada o terminal de valla. Y configure la información de ubicación específica del dispositivo, incluyendo el bloque, la unidad (se puede desactivar) y el número de habitación. Cuando se configura como terminal de valla, la página de llamada mostrará el bloque, la unidad y el número de habitación. Nota: La lista de contactos se borrará después de cambiar el tipo de dispositivo.
Lista de contactos de llamadas	Seleccione si desea habilitar la lista de contactos en la página de llamadas. Cuando está habilitada, puede hacer clic en el icono para abrir la lista de contactos en la página de llamadas.
Tipo de número de llamada	Seleccione si desea habilitar la lista de contactos en la página de llamadas. Cuando está habilitada, puede hacer clic en el icono para abrir la lista de contactos en la página de llamadas.

11.1.2 Opciones de audio

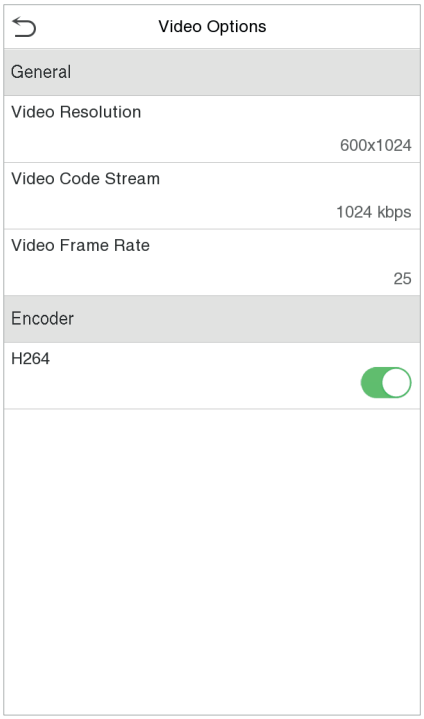
Toque Opciones de audio en la interfaz de configuración SIP.



Seleccione el codificador de audio para el intercomunicador. Tanto PCMU como PCMA proporcionan una mejor calidad de voz, pero ocupan más ancho de banda, requiriendo 64 kbps.

11.1.3 Opciones de vídeo

Toque Opciones de video en la interfaz de configuración SIP.

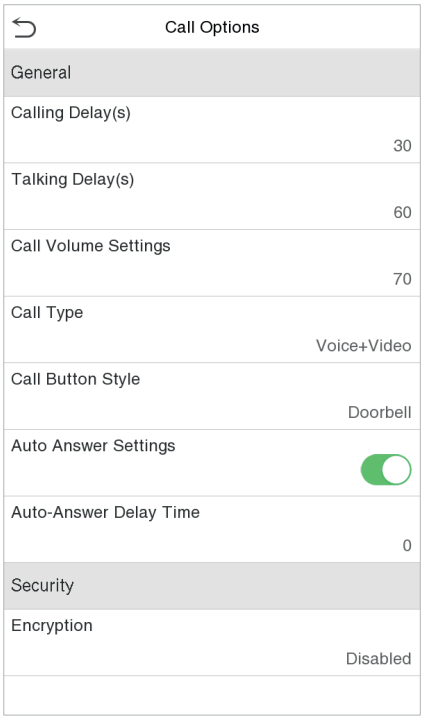


Descripción de la función

Nombre de la función	Descripción
Resolución de video	Seleccione la resolución de vídeo del intercomunicador, 1024 x 576 (para pantalla horizontal) o 600 x 1024 (para pantalla vertical). Se sugiere que el dispositivo se configure como 600 x 1024.
Flujo de código de vídeo	Seleccione el flujo de código de video del intercomunicador, cuanto mayor sea el valor, mayor será la calidad de imagen y sonido del video y mayores serán los requisitos de red.
Velocidad de fotogramas de vídeo	Se refiere al número de fotogramas por segundo de la pantalla de video del intercomunicador, cuanto mayor sea el valor, más suave, el dispositivo predeterminado es 25Hz, no admite modificación.
Codificador	Si se va a habilitar el codificador H264.

11.1.4 Opciones de compra

Toque Opciones de llamada en la interfaz de configuración de SIP.



Descripción de la función

Nombre de la función	Descripción
Retraso(s) de llamadas	Establezca la hora de la llamada, valor válido de 30 a 60 segundos.
Retraso(s) de conversación	Establezca la hora del intercomunicador, valor válido de 60 a 120 segundos. Se sugiere establecer como 60s.

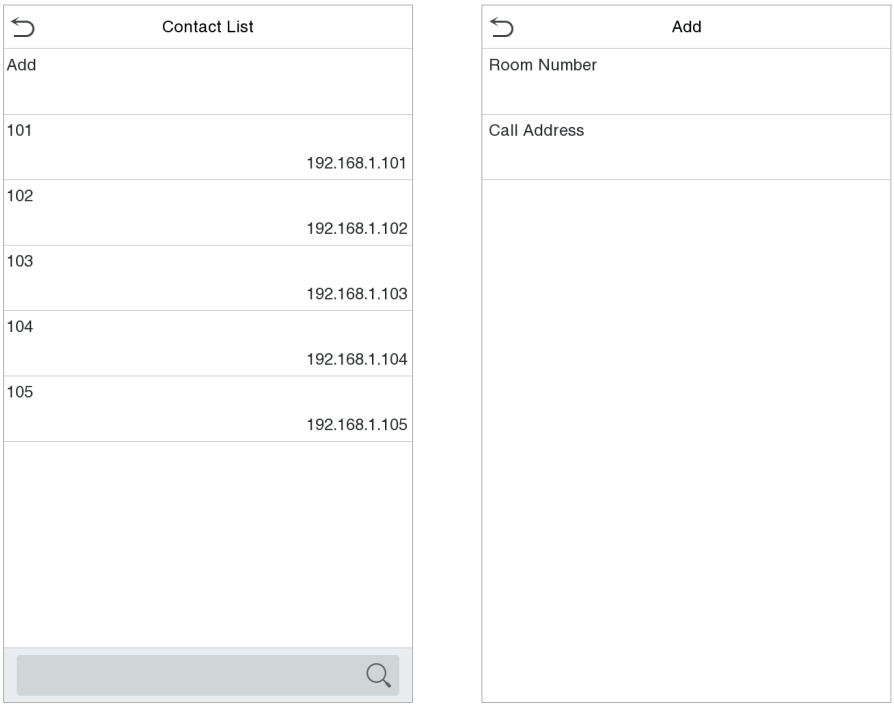
Nombre de la función	Descripción
Configuración del volumen de llamadas	Establezca el volumen de la llamada, con un valor válido que oscile entre 0 y 100.
Tipo de llamada	Establezca el tipo de llamada en Solo voz o Voz+Vídeo.
Estilo de botón de llamada	Cambie el botón de llamada del intercomunicador visual en la interfaz de espera del dispositivo, etiquetadora de timbre opcional o etiqueta de teléfono.
Configuración de respuestas automáticas	Seleccione si desea habilitar la función de respuesta automática. Cuando está habilitado, el dispositivo responderá automáticamente si el monitor interior llama.
Tiempo de retardo de respuesta automática	El dispositivo responderá automáticamente tras el tiempo de retardo establecido si llama el monitor interior, valor válido de 0 a 10 segundos.
Encriptación	Está deshabilitado de forma predeterminada.

11.1.5 Lista de contactos

Toque Lista de contactos en la interfaz de configuración de SIP.

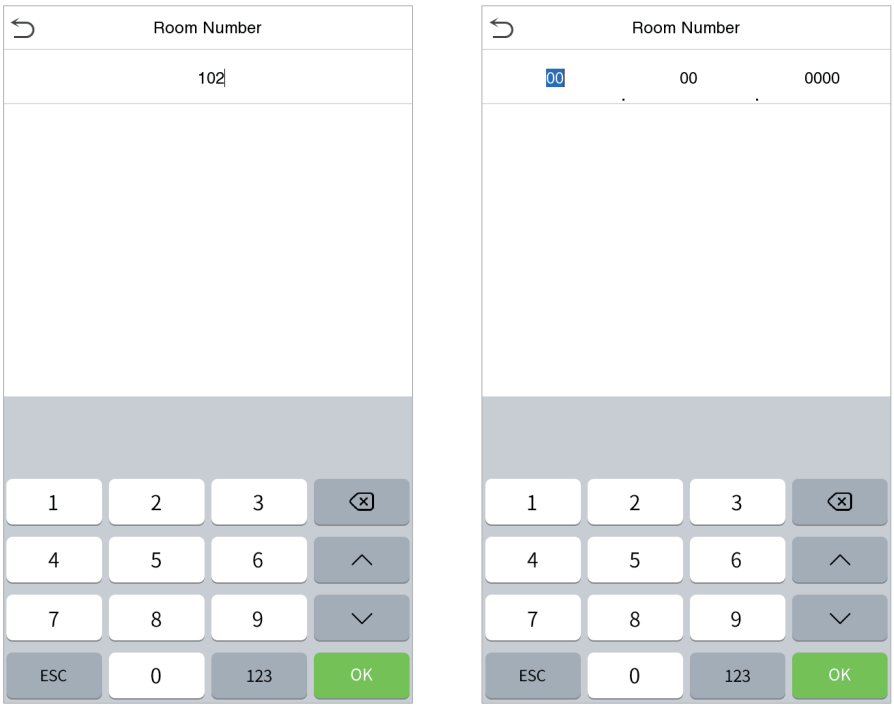
En el modo de servidor SIP, el servidor ZKBio CVSecurity sincroniza la lista de contactos con el dispositivo. La lista de contactos solo se puede ver, no se puede editar. Cuando el servidor SIP está deshabilitado, aquí se puede agregar el número de habitación y la dirección de llamada de los monitores interiores.

Haga clic en Agregar para ingresar a la interfaz Agregar lista de contactos



Número de habitación: Personalice el número del monitor interior.

Cuando el tipo de dispositivo se establece como Estación de entrada, el número de habitación puede ser de 1 ~ 4 dígitos. Cuando el tipo de dispositivo se establece como Terminal de cerca, debe ingresar el bloque, la unidad y el número de habitación. Por ejemplo, si el monitor interior está en el Bloque 3, Unidad 2, Sala 2601, ingrese "03.02.2601".

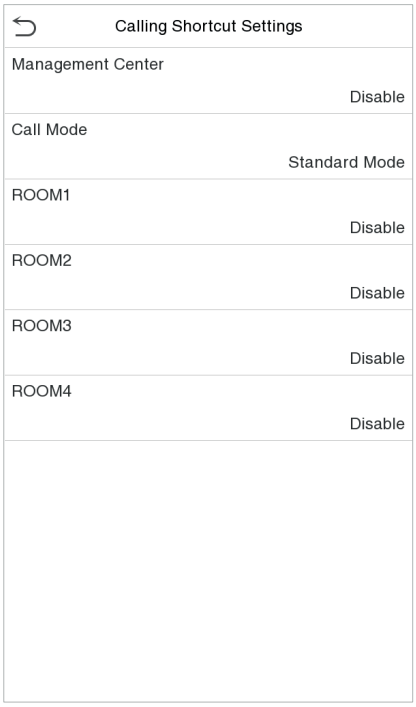


Entrance Station　　Fence Terminal

Dirección de llamada: Es la dirección IP del monitor interior

11.1.6 Configuración de acceso directo de llamadas

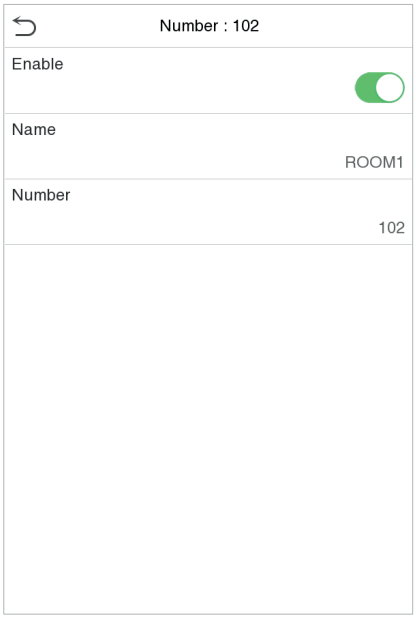
Toque Configuración de acceso directo de llamadas en la interfaz de configuración de SIP.



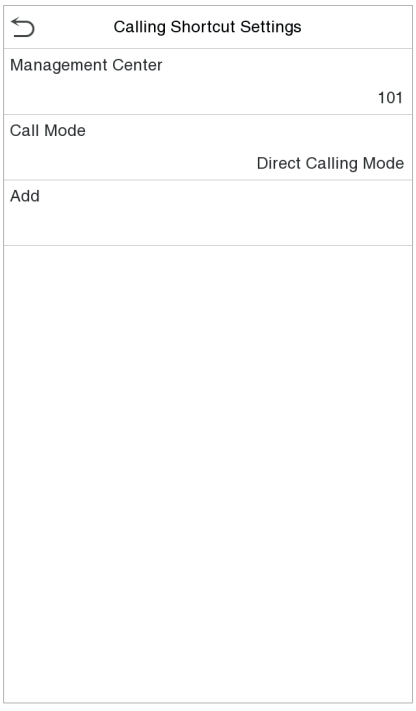
Centro de gestión: seleccione  si desea habilitar el Centro de gestión y establezca su número. Después de habilitarlo, puede hacer clic en el icono para llamar directamente al administrador en la página de llamadas

Modo de llamada: Se puede configurar como modo estándar o modo de llamada directa.

- En el modo estándar, hay **2** teclas de acceso directo que se pueden habilitar y definir en el dispositivo: **ROOM1 y ROOM.** Puede configurar una tecla de acceso directo para llamar al monitor interior rápidamente sin ingresar el número del monitor interior cada vez. **Nombre:** Personaliza el nombre de las teclas de método abreviado. **Número:** Seleccione el número de habitación que se estableció en el menú de la lista de contactos.



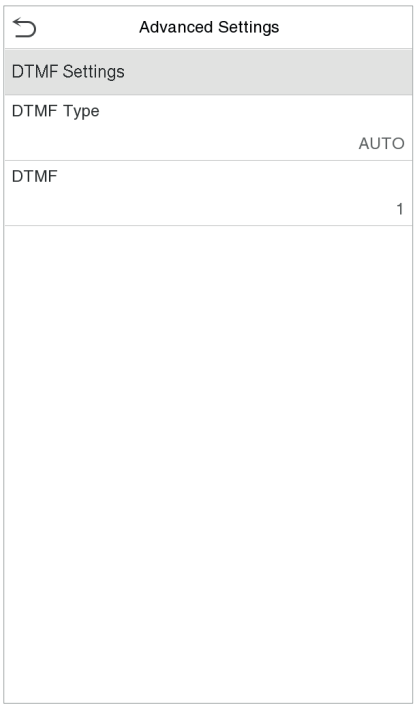
- En el modo de llamada directa, el usuario puede llamar directamente a varios monitores interiores. Haga clic en **Modo de llamada > Modo de llamada directa> Agregar**, seleccione los monitores interiores a los que desea llamar, luego los monitores interiores se mostrarán en la lista.





11.1.7 Configuración avanzada

Toque Configuración avanzada en la interfaz de configuración SIP.

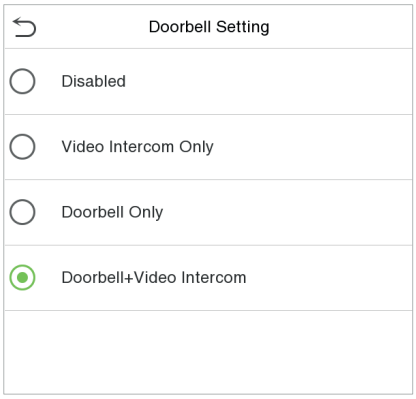


Descripción de la función

Nombre de la función	Descripción
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 el monitor interior.

11.2 Configuración del timbre

Toque Configuración del timbre en la interfaz Parámetros del videoportero para ir a la configuración del timbre de monitoreo.



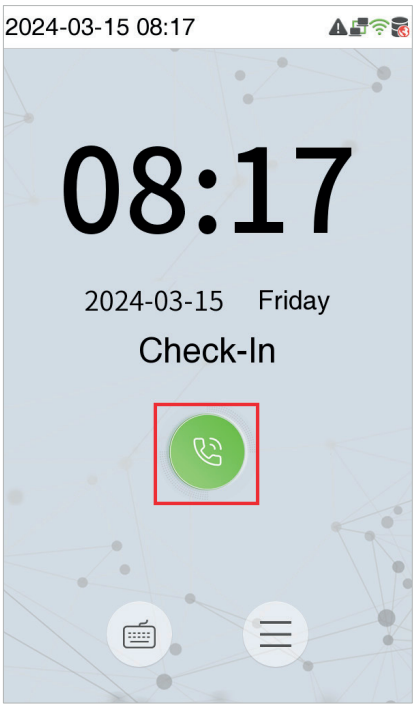
Descripción de la función

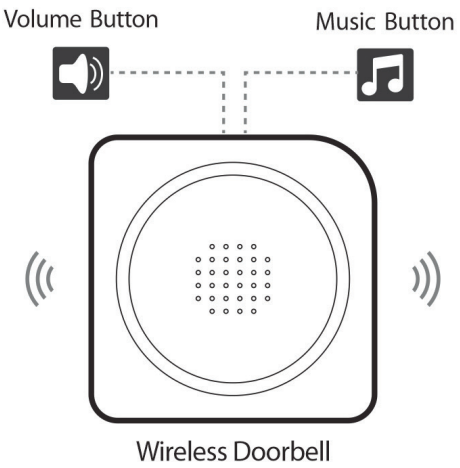
Function Name	Description
Solo videoportero	Toque el icono o en la interfaz de espera para llamar a la unidad interior para el videoportero
Solo timbre	Toque el icono o en la interfaz de espera, suena el timbre.
Timbres + Videoporteros	Toque el icono o en la interfaz de espera, el timbre sonará y llamará a la unidad interior para el videoportero.

11.2.1 Conecte el timbre inalámbrico ★

Nota: *Esta función debe utilizarse con el timbre inalámbrico.*

1. En primer lugar, 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, haga clic en el icono del dispositivo SenseFace 7 Series. Si el timbre inalámbrico suena y el indicador parpadea, significa que la conexión se ha realizado correctamente.





2. Una vez emparejado correctamente, al hacer clic en el icono del dispositivo SenseFace Serie 7 sonará el timbre inalámbrico.

Nota: *Por lo general, todos los dispositivos de la serie SenseFace 7 se conectan al timbre inalámbrico.*

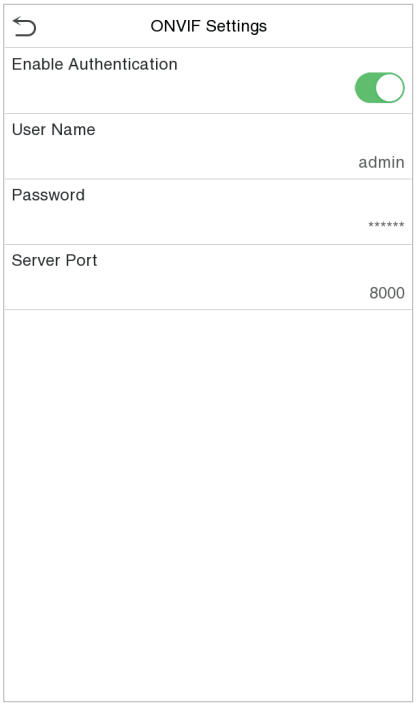
- **Desvincular el timbre inalámbrico**

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.

11.3 Configuración de ONVIF

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

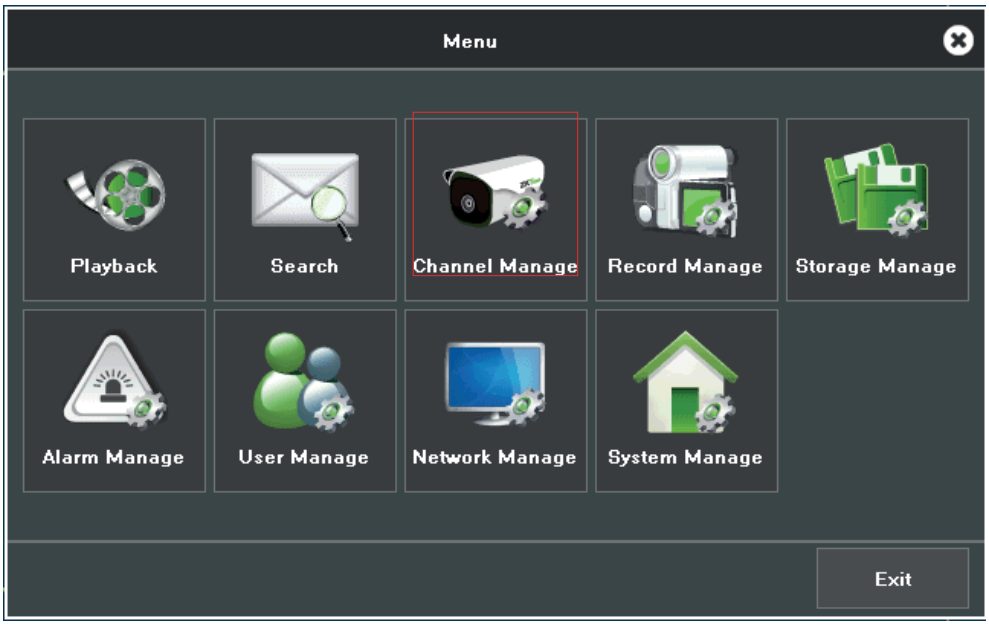
1. Configure el dispositivo en el mismo segmento de red que el NVR.
2. Toque **Configuración de ONVIF** en la interfaz Parámetros del videoportero.



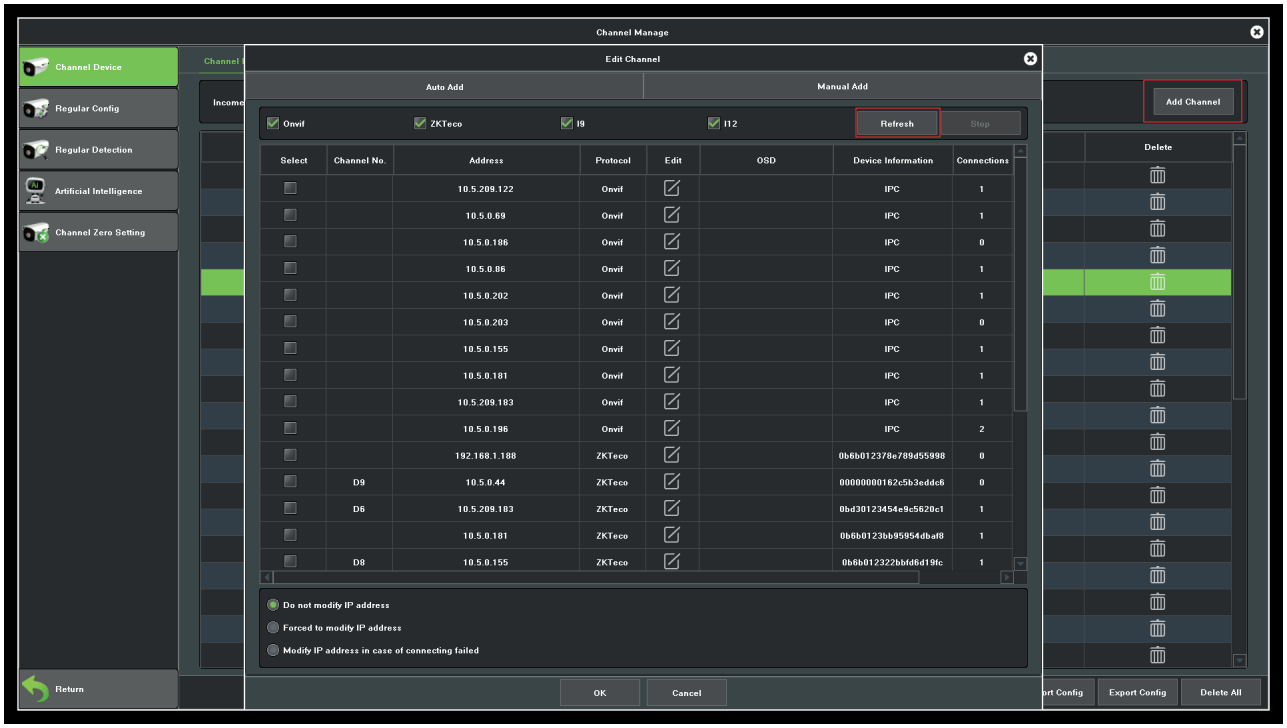
Descripción de la función

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.

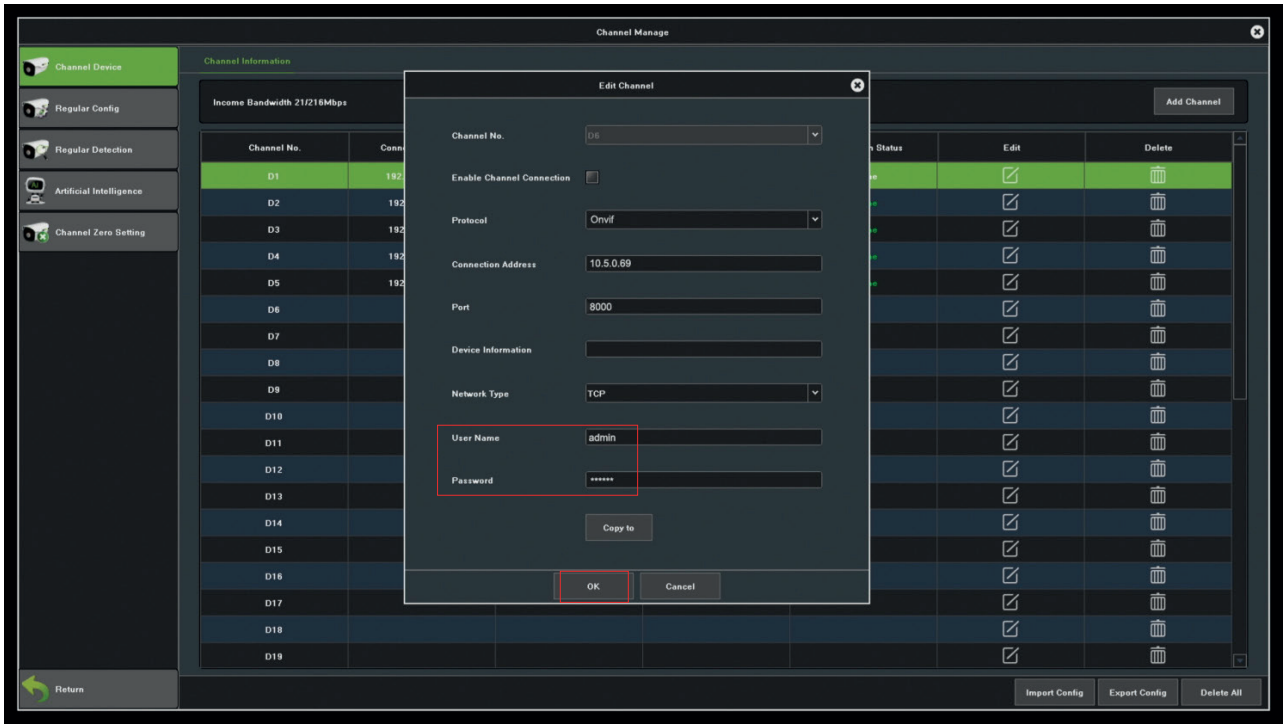
3. En el sistema NVR, haga clic en [Inicio] > [Menú], luego aparecerá el menú principal.



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

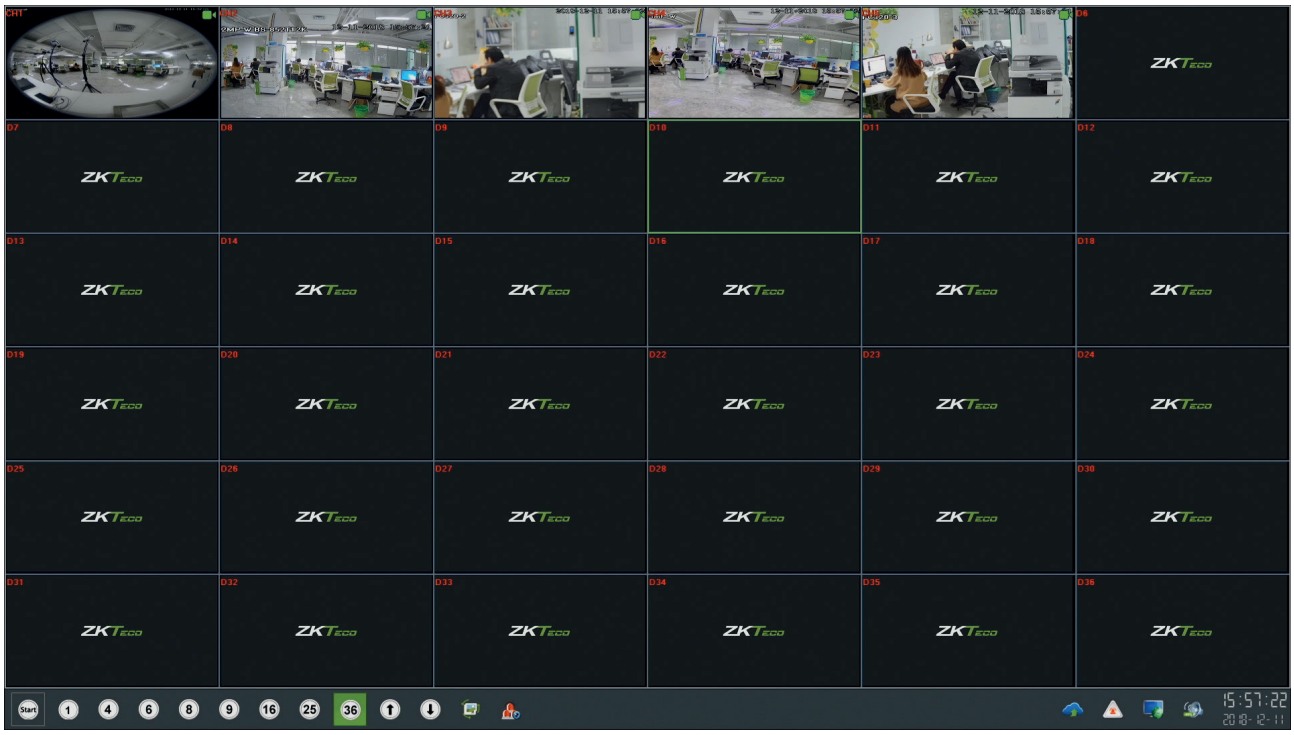


5. Seleccione la casilla de verificación del dispositivo que desea agregar y edite los parámetros en el campo de texto correspondiente, luego haga clic en [Aceptar] para agregarlo a la lista de conexiones.



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

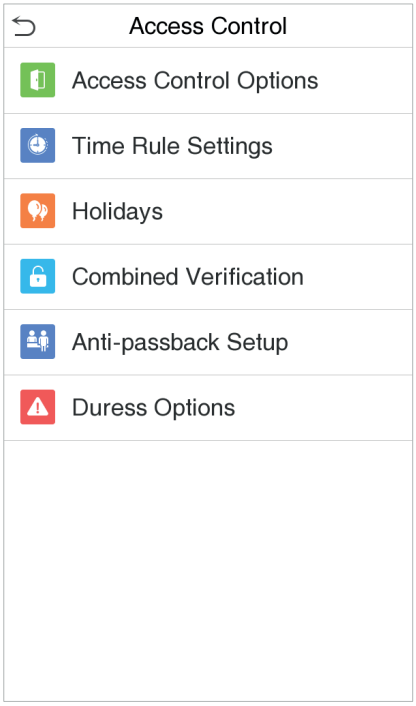
6. Después de agregar con éxito, la imagen de video obtenida del dispositivo se puede ver en tiempo real.



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

12. Control de acceso

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

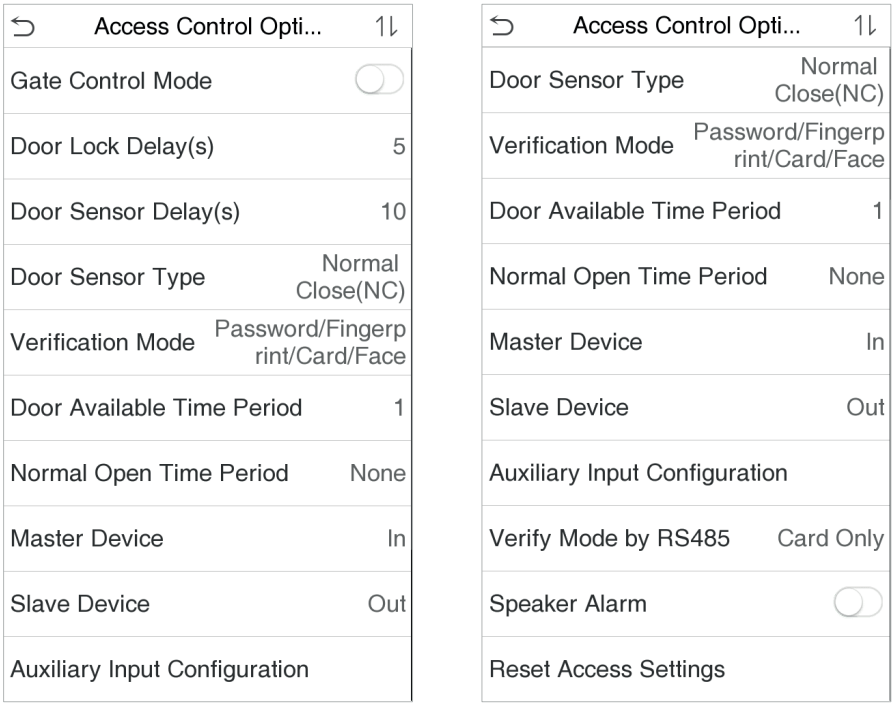


- **Para obtener acceso, el usuario registrado debe cumplir con las siguientes condiciones:**

- La hora actual de desbloqueo de la puerta correspondiente debe estar dentro de cualquier zona horaria válida del período de tiempo del usuario.
- El grupo de usuarios correspondiente debe estar ya configurado en la combinación de desbloqueo de la puerta (y si hay otros grupos configurados en la misma combinación de acceso, también se requerirá la verificación de los miembros de esos grupos para desbloquear la puerta).
- En la configuración predeterminada, los nuevos usuarios se asignan al primer grupo con la zona horaria predeterminada del grupo, donde el combo de acceso es «1» y está configurado en estado desbloqueado de forma predeterminada.

12.1 Opciones de control de acceso

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



Descripción de la función

Nombre de la función	Descripción
Modo de control de puerta	Cambie entre el interruptor ON (Activado) u OFF (Desactivado) para entrar o salir del modo de control de puerta. Cuando se establece en ON (Activado), esta interfaz eliminará las opciones Relé de bloqueo de puerta, Relé 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 ~ 10 segundos; 0 segundos representa la desactivación de la función.
Por sensor Retardo(s)	Si la puerta no está cerrada con llave y se deja abierta durante un determinado periodo de tiempo (retardo del sensor de puerta), se activará una alarma. El valor válido del retardo del sensor de puerta oscila entre 1 y 255 segundos.
Tipo de sensor de puerta	Hay tres tipos de sensores: **Ninguno, Normal abierto y Normal cerrado.** **Ninguno:** significa que el sensor de la puerta no está en uso. **Normal abierto:** significa que la puerta permanece siempre abierta cuando hay suministro eléctrico. **Normal cerrado:** significa que la puerta permanece siempre cerrada cuando hay suministro eléctrico.
Modo de verificación	El modo de verificación compatible incluye contraseña/huella dactilar/tarjeta/rostro, solo huella dactilar, solo ID de usuario, contraseña, solo tarjeta, huella dactilar/contraseña, huella dactilar/tarjeta, ID de usuario + huella dactilar, huella dactilar + contraseña, huella dactilar + tarjeta, huella dactilar + contraseña + tarjeta, contraseña + tarjeta, contraseña/tarjeta, ID de usuario + huella dactilar + contraseña, huella dactilar + (tarjeta/ID de usuario), solo rostro, rostro + huella dactilar, rostro + contraseña, rostro + tarjeta, rostro + huella dactilar + tarjeta y rostro + huella dactilar + contraseña.

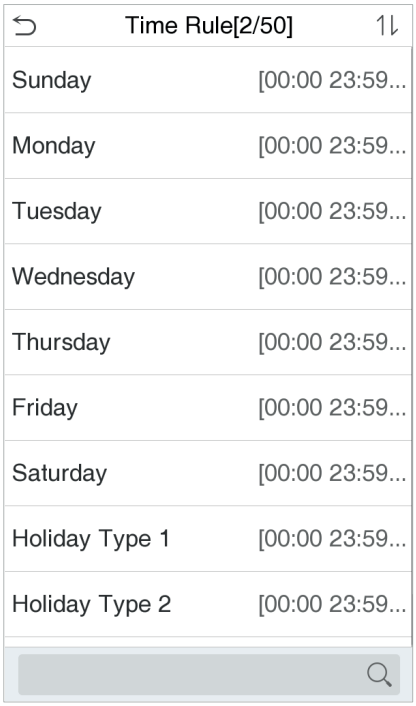
Nombre de la función	Descripción
Periodo de disponibilidad de la puerta	Para establecer el periodo de tiempo de la puerta, de modo que la puerta solo esté disponible durante ese periodo.
Periodo normal de apertura	Periodo de tiempo programado para el modo «Normal abierto», de modo que la puerta permanezca siempre abierta durante este periodo.
Dispositivo maestro	Al configurar el maestro, se puede establecer el estado del maestro para que salga al entrar. Salida: el registro verificado en el host es el registro de salida. Entrada: el registro verificado en el host es el registro de entrada.
Dispositivo esclavo	Al configurar el esclavo, se puede establecer su estado para que salga al entrar. Salida: el registro verificado en el host es el registro de salida. Entrada: el registro verificado en el host es el registro de entrada.
Configuración de la entrada auxiliar	Establece el periodo de tiempo de desbloqueo de la puerta y el tipo de salida auxiliar del dispositivo terminal auxiliar. Los tipos de salida auxiliar incluyen Ninguno, Activar apertura de puerta, Activar alarma, Activar apertura de puerta y alarma.
Modo de verificación por RS485	El modo de verificación se utiliza cuando el dispositivo se utiliza como host o esclavo. El modo de verificación compatible incluye Solo tarjeta y Tarjeta + Contraseña.
Alarma del altavoz	Transmite una alarma sonora o una alarma de desmontaje desde el local. Cuando la puerta está cerrada o la verificación es satisfactoria, el sistema cancela la alarma desde el local.
Restablecer configuración de acceso	Los parámetros de restablecimiento del control de acceso incluyen el retraso del bloqueo de la puerta, el retraso del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el periodo de tiempo de disponibilidad de la puerta, el periodo de tiempo de apertura normal, el dispositivo maestro y la alarma. Sin embargo, se excluyen los datos de control de acceso borrados en Gestión de datos.

12.2 Configuración de reglas de tiempo

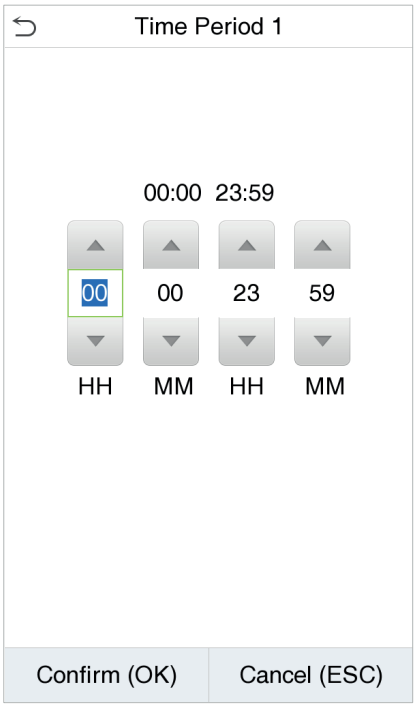
Toque Configuración de regla de tiempo en la interfaz de control de acceso para configurar los ajustes de tiempo.

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

Notas:

- *Cuando la hora de finalización es anterior a la hora de inicio (como 23:57~23:56), indica que el acceso es prohibido todo el día.*
- *Cuando la hora de finalización es posterior a la hora de inicio (como 00:00~23:59), indica que el intervalo es válido.*

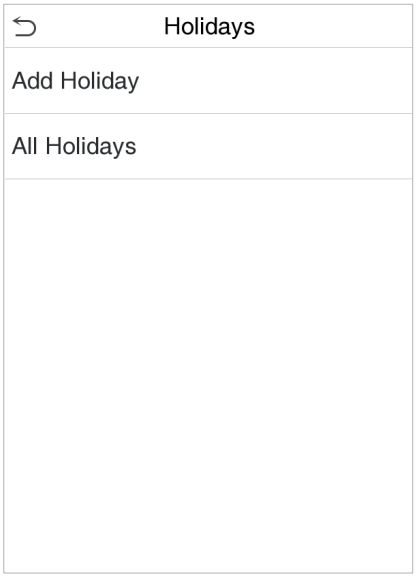
El período de tiempo efectivo para mantener la puerta desbloqueada o abierta todo el día es (00:00 ~ 23:59) o también cuando la hora de finalización es posterior a la hora de inicio (por ejemplo, 08:00~23:59).

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

12.3 Vacaciones

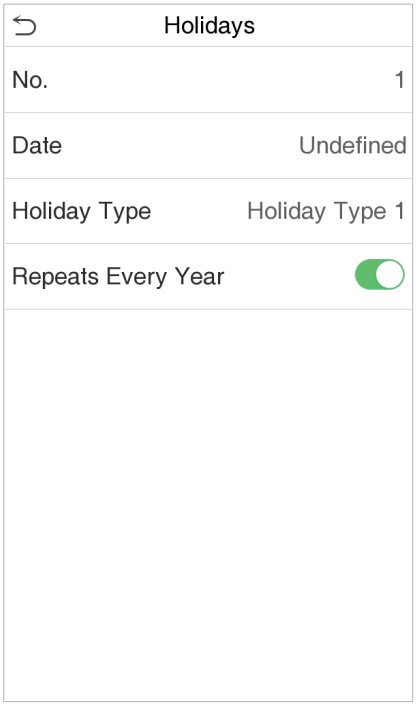
Siempre que haya un día festivo, es posible que necesite un horario de acceso especial; Pero cambiar la hora de acceso de todos uno por uno es extremadamente engorroso, por lo que puede establecer una hora de acceso a las vacaciones que sea aplicable a todos los empleados, y el usuario podrá abrir la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

Toque Días festivos en la interfaz de control de acceso para establecer el acceso a los días festivos.



- **Agregar 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. Toque Editar para modificar los parámetros de vacaciones.

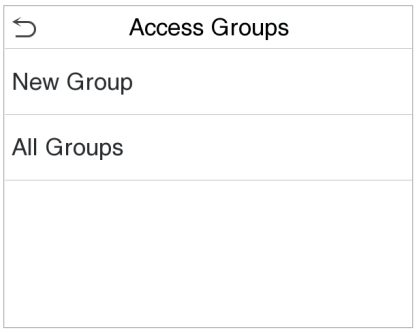
- **Eliminar un día festivo:**

En la interfaz «Días festivos», seleccione el día festivo que desea eliminar y pulse «Eliminar». Pulse «Aceptar» para confirmar la eliminación. Una vez eliminado, este día festivo ya no aparecerá en la interfaz «Todos los días festivos»..

12.4 Grupos de acceso ★

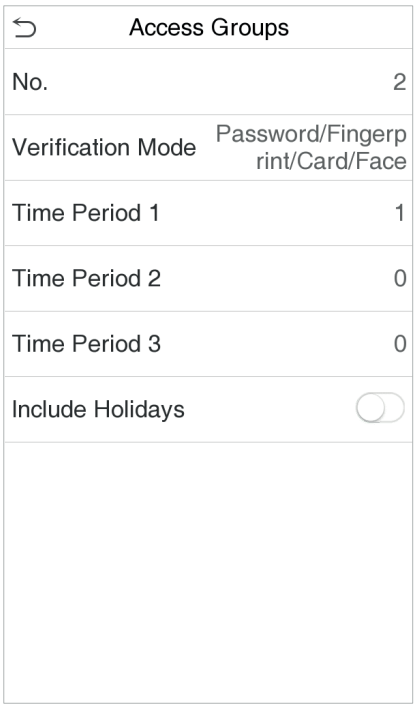
Esto es para administrar fácilmente agrupaciones y usuarios en diferentes grupos de acceso. La configuración de un grupo de acceso, como las zonas horarias de acceso, se aplica a todos los miembros del grupo de forma predeterminada. Sin embargo, los usuarios pueden configurar manualmente las zonas horarias según sea necesario. La autenticación de usuario tiene prioridad sobre la autenticación de grupo cuando los modos de autenticación de grupo se superponen con los métodos de autenticación individuales. Cada grupo puede establecer un máximo de tres zonas horarias. De forma predeterminada, los usuarios recién inscritos se asignan al Grupo de acceso 1; Se pueden asignar a otros grupos de acceso

Haga clic en Grupos de acceso en la interfaz de control de acceso.



- **Agregar un nuevo grupo**

Haga clic en Nuevo grupo en la interfaz Grupos de acceso y establezca los parámetros del grupo de acceso



Notas:

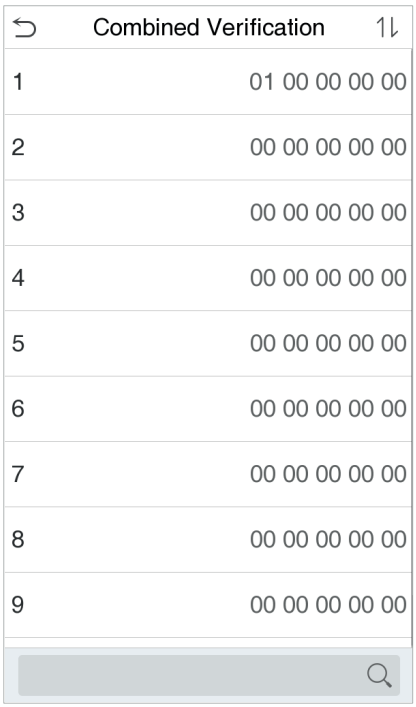
- Esta función solo se utiliza en el marco del empuje de asistencia (T&A PUSH).
- Hay un grupo de acceso predeterminado numerado 1, que no se puede eliminar, pero se puede modificar.
- Un número no se puede modificar después de establecerlo.
- Cuando el día festivo está configurado para ser válido, el personal de un grupo solo puede abrir la puerta cuando la zona horaria del grupo se superpone con el período de tiempo de vacaciones

Cuando el día festivo se establece como no válido, el tiempo de control de acceso del personal de un grupo no se ve afectado durante los días festivos.

12.5 Verificación combinada

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

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



En la interfaz de verificación combinada, toque la combinación de desbloqueo de puerta que se va a configurar, toque las flechas arriba y abajo para ingresar el número de combinación y, a continuación, presione **OK**.

Por ejemplo:

- La combinación de desbloqueo de puerta 1 se establece como (01 03 05 06 08), lo que indica que el desbloqueo La combinación 1 consta de 5 personas, y los 5 individuos pertenecen a 5 grupos, a saber, el Grupo de Control de Acceso 1 (grupo AC 1), el grupo AC 3, el grupo AC 5, el grupo AC 6 y el grupo AC 8, respectivamente.

- La combinación de desbloqueo de puerta 2 se establece como (02 02 04 04 07), lo que indica que el desbloqueo combinación 2 consta de 5 personas; los dos primeros son del grupo AC 2, los dos siguientes son del grupo AC 4 y la última persona es del grupo AC 7.
- La combinación de desbloqueo de puerta 3 se establece como (09 09 09 09 09), lo que indica que hay 5 personas en esta combinación; todos ellos del grupo AC 9
- La combinación de desbloqueo de puerta 4 se establece como (03 05 08 00 00), lo que indica que el desbloque la combinación 4 consta de solo tres personas. La primera persona es del grupo AC 3, la segunda persona es del grupo AC 5 y la tercera persona es del grupo AC 8.

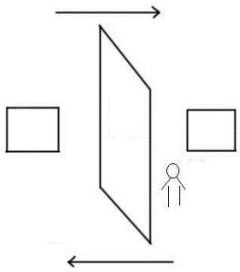
- **Eliminar una combinación de desbloqueo de puertas:**

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

12.6 Configuración anti-retorno

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

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



Toque Configuración anti-retorno en la interfaz de control de acceso.



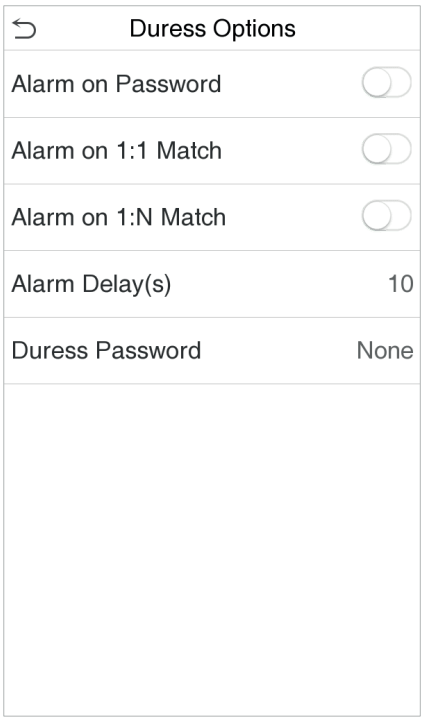
Descripción de la función

Nombre de la función	Descripción
Dirección anti-retorno	Sin anti-retorno: La función anti-retorno está desactivada, lo que significa que una verificación satisfactoria a través del dispositivo maestro o del dispositivo esclavo puede desbloquear la puerta. El estado de asistencia no se guarda en esta opción. Anti-retorno: después de que un usuario salga, solo si el último registro es un registro de entrada, el usuario podrá volver a salir; de lo contrario, se activará la alarma. Sin embargo, el usuario podrá entrar libremente. En Anti-retorno: después de que un usuario se registre, solo si el último registro es un registro de salida, el usuario podrá volver a registrarse; de lo contrario, se activará la alarma. Sin embargo, el usuario podrá salir libremente. Anti-retorno de entrada/salida: después de que un usuario registre su entrada/salida, solo si el último registro es un registro de salida, el usuario podrá volver a registrar su entrada; o si es un registro de entrada, el usuario podrá volver a registrar su salida; de lo contrario, se activará la alarma.

12.7 Opciones de coacción

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

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



Function Description

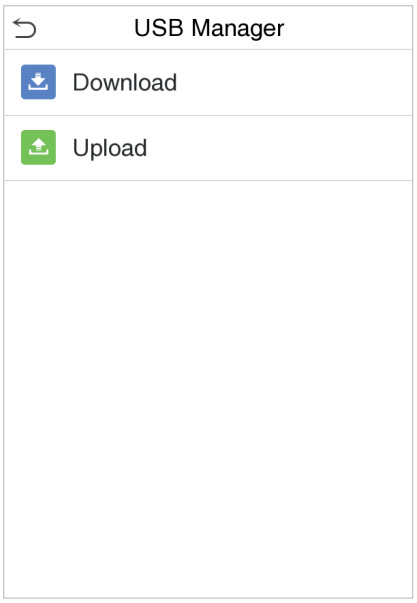
Nombre de la función	Descripción
Alarma con contraseña	Cuando un usuario utiliza el método de verificación de contraseña, se generará una señal de alarma, de lo contrario, no habrá señal de alarma.
Alarma en partido 1:1	Cuando un usuario utiliza cualquier huella dactilar para realizar la verificación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

13. Administrador de USB

Puede importar la información del usuario y los datos de asistencia en la máquina al software de asistencia correspondiente para su procesamiento mediante un disco USB, o importar la información del usuario a otros dispositivos para realizar una copia de seguridad. Antes de cargar/descargar datos desde/hacia el disco USB, inserte primero el disco USB en la ranura USB.

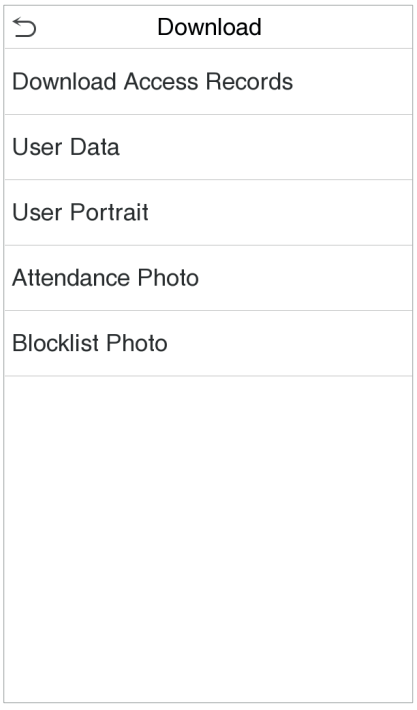
Nota: *Solo se admite el formato FAT32 cuando se descargan datos mediante un disco USB.*

Toque Administrador USB en la interfaz del menú principal.



13.1 Descarga USB

En la interfaz del Administrador USB, toque Descargar.

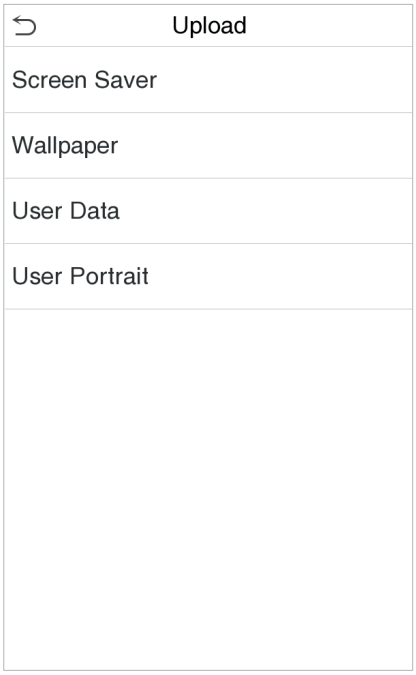


Descripción de la función

Nombre de la función	Description
Descargar registros de acceso	Para descargar todos los registros de acceso en un 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 del usuario	Para descargar todos los retratos de usuario del dispositivo en un disco USB.
Foto de asistencia	Para descargar todas las fotos de asistencia del dispositivo a un disco USB.
Bloquear foto	Para descargar todas las fotos incluidas en la lista de bloqueo (fotos tomadas después de verificaciones fallidas) desde el dispositivo a un disco USB.

13.2 Carga USB

En la interfaz del Administrador USB, toque Descargar.



Descripción de la función

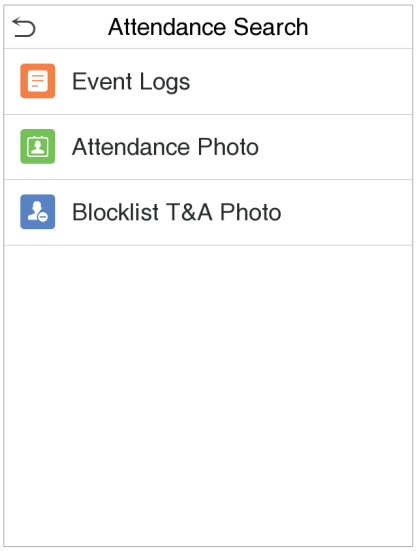
Function Name	Description
Salvapantallas	Para cargar todos los salvapantallas desde un disco USB al dispositivo. Puede elegir entre cargar las fotos seleccionadas o cargar todas las fotos. Las imágenes se mostrarán en la interfaz principal del dispositivo después de la carga.
Fondo de pantalla	Para cargar todos los fondos de pantalla desde un disco USB al dispositivo. Puede elegir entre cargar la foto seleccionada o cargar todas las fotos. Las imágenes se mostrarán en la pantalla después de la carga.
Datos del usuario	Para cargar toda la información del usuario desde el disco USB al dispositivo.

Function Name	Description
Retrato del usuario	Para cargar todos los retratos de usuario desde un disco USB en el dispositivo.

14. Búsqueda de asistencia

Una vez verificada la identidad de un usuario, los registros de eventos se guardarán en el dispositivo. Esta función permite a los usuarios comprobar sus registros de acceso.

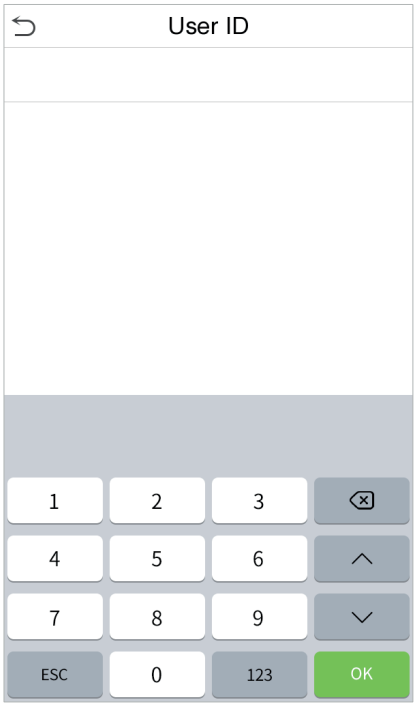
Haga clic en Búsqueda de asistencia en la interfaz del menú principal para buscar el registro de acceso/asistencia requerido.



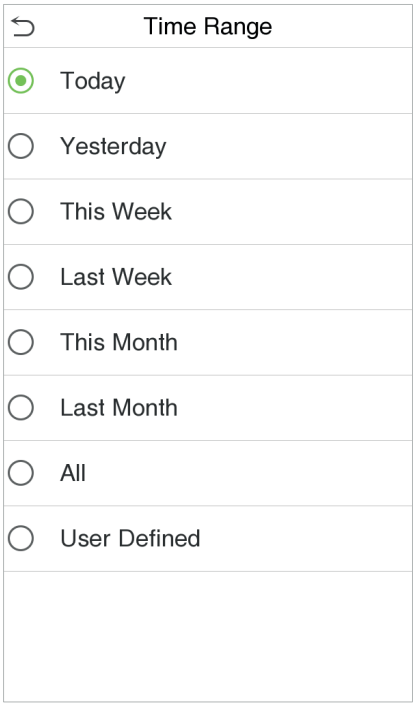
El proceso de búsqueda de fotos de asistencia y listas de bloqueo es similar al de búsqueda de registros de eventos. A continuación se muestra un ejemplo de búsqueda de registros de eventos

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

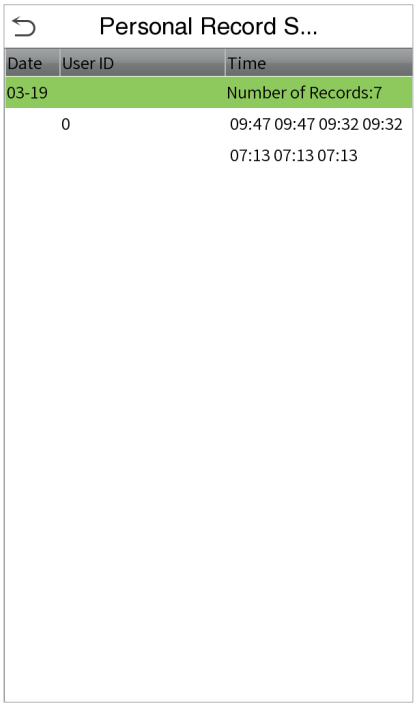
1. Introduzca el ID de usuario que desea buscar y haga clic en Aceptar. Si desea buscar los registros de todos los usuarios, haga clic en Aceptar sin introducir ningún ID de usuario.



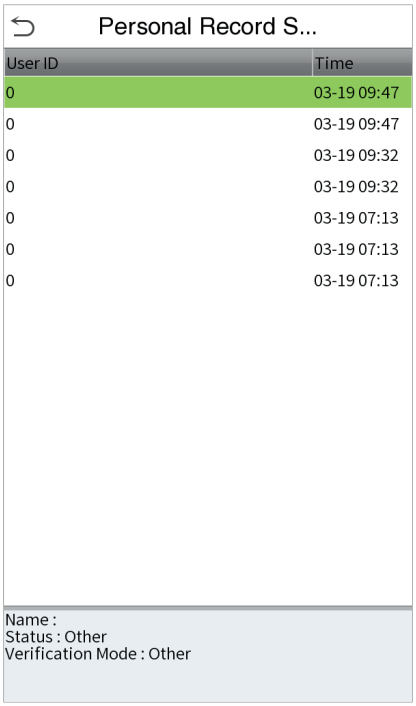
2. Seleccione el intervalo de tiempo en el que se deben buscar los registros.



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

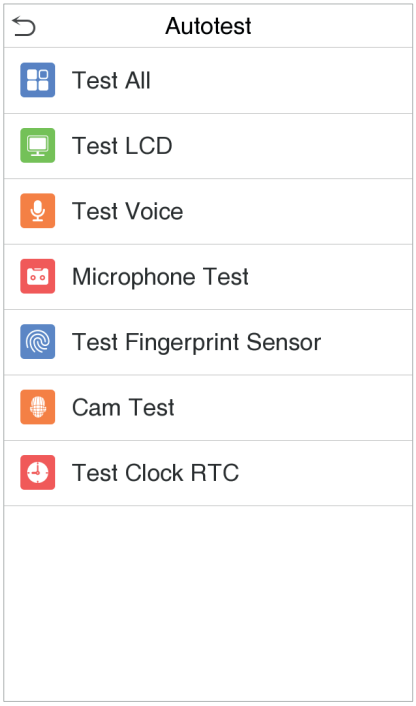


4. La siguiente figura muestra los detalles del registro seleccionado.



15. Autoprueba

En el menú principal, toque Autotest para comprobar automáticamente si todos los módulos del dispositivo funcionan correctamente, incluidos la pantalla LCD, la voz, la cámara y el reloj en tiempo real (RTC).

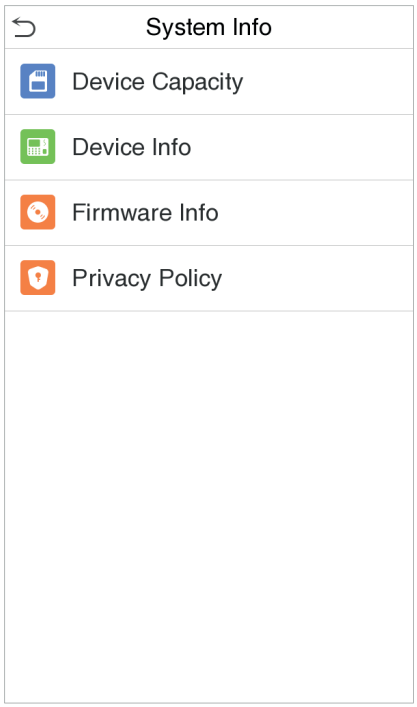


Descripción de la función

Function Name	Description
Probar todo	Para probar automáticamente si la pantalla LCD, el audio, la cámara y el 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.
Prueba de micrófono	Compruebe si el micrófono está funcionando hablando con el micrófono y reproduciendo la grabación del micrófono.
Prueba del sensor de huellas dactilares	Para probar el sensor de huellas dactilares presionando un dedo en el escáner para verificar si la imagen de huellas dactilares adquirida es clara. Cuando presione un dedo en el escáner, la imagen de la huella digital se mostrará en la pantalla.
Prueba de cámara	Para probar si la cámara funciona correctamente revisando las fotos tomadas para ver si son lo suficientemente claras. 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. Toque la pantalla para comenzar a contar y presiónela nuevamente para detener el conteo.

16. Información del sistema

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



Descripción de la función

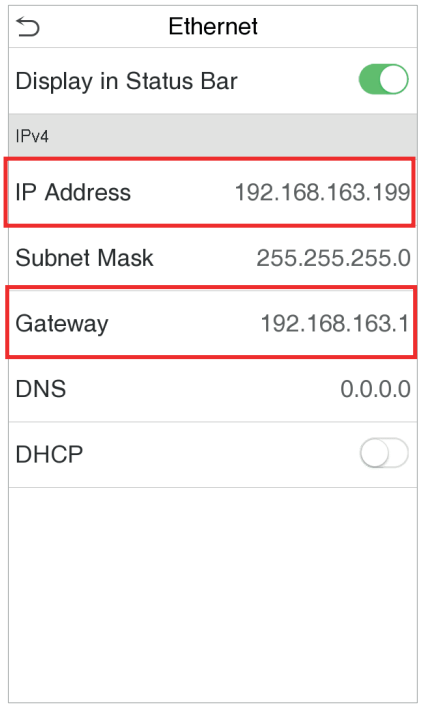
Nombre de la función	Descripción
Capacidad del dispositivo	Muestra el almacenamiento de usuario del dispositivo actual, la contraseña, la plantilla de rostro, el almacenamiento de huellas dactilares y tarjetas, los registros de acceso, las fotos de asistencia y de lista de bloqueo, y las fotos de perfil.
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la dirección MAC, el algoritmo★ de huellas dactilares, el algoritmo de plantilla facial, la información de la plataforma, la versión de MCU y la fecha de fabricación.
Información de firmware	Muestra la versión del firmware y otra información de la versión del dispositivo.
Política de privacidad	El control de la política de privacidad aparecerá cuando el gadget se encienda por primera vez. Después de hacer clic en "Lo he leído", el cliente puede utilizar el producto con regularidad. Haga clic en Información del sistema > Política de privacidad para ver el contenido de la política de privacidad. El contenido de la política de privacidad no permite la exportación de discos U. Nota: El texto de la política de privacidad actual solo está disponible en chino simplificado/inglés. Sin embargo, la traducción de otros contenidos multilingües está en curso, con reiteraciones.

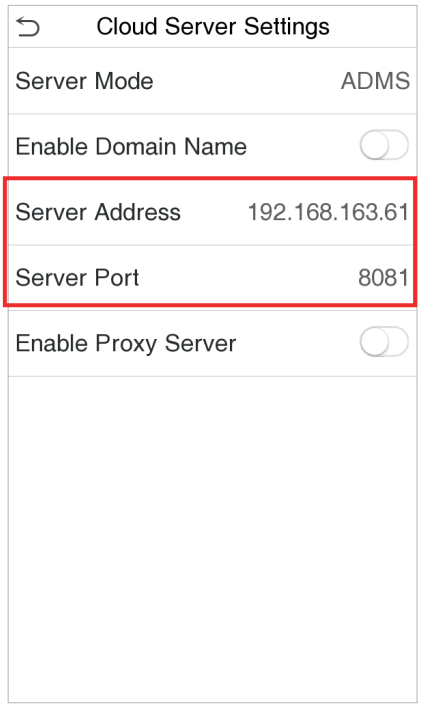
17. Conéctese al software ZKBio CVSecurity

17.1 Establecer la dirección de comunicación

- **Lado del dispositivo**

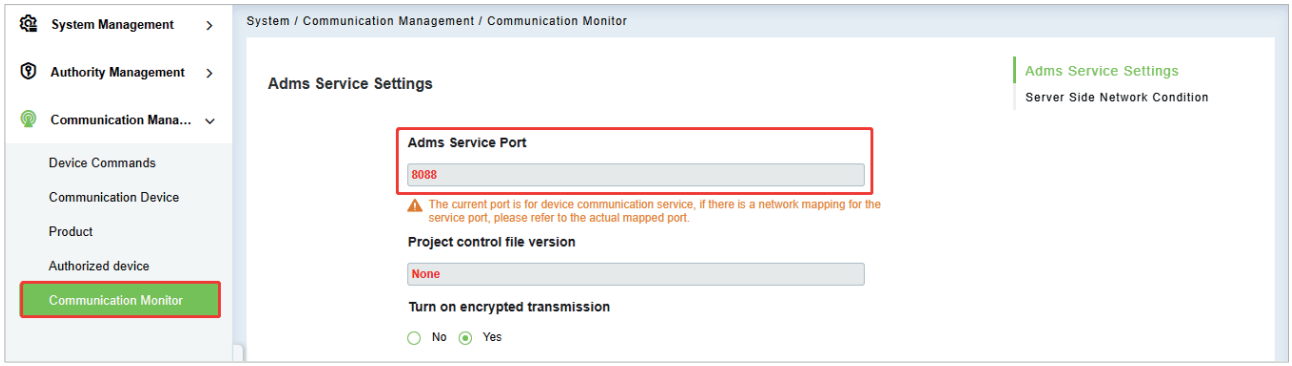
1. Toque COMM. > Ethernet en el menú principal para configurar la dirección IP y la puerta de enlace del dispositivo. Nota: Asegúrese de que la dirección IP esté en el mismo segmento de red que la dirección del servidor y pueda comunicarse con el servidor ZKBio CVSecurity
2. En el menú principal, haga clic en 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 a partir del servidor ZKBio CVSecurity. Puerto del servidor: Establezca el puerto del servidor a partir de ZKBio CVSecurity.





- **Lado del software**

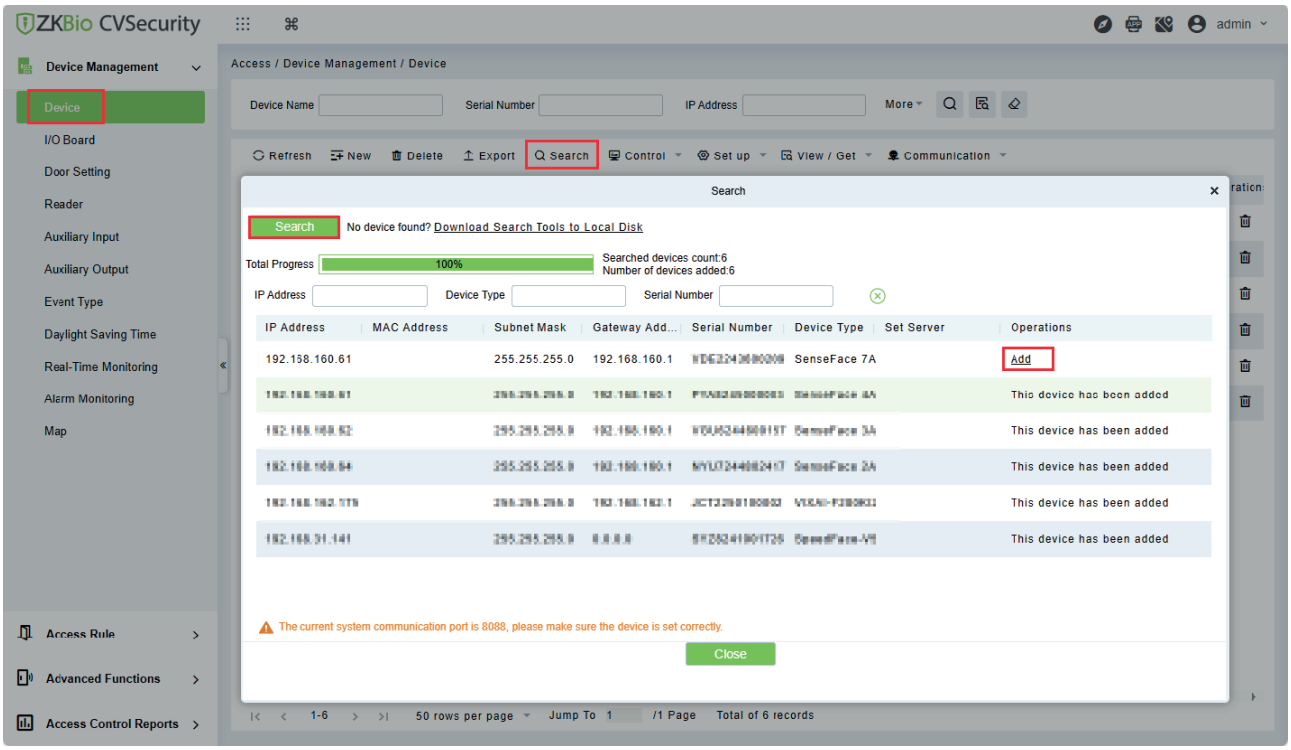
Inicie sesión en el software ZKBio CVSecurity, haga clic en System > Communication > Communication Monitor para configurar el puerto de servicio ADMS, como se muestra en la figura a continuación:



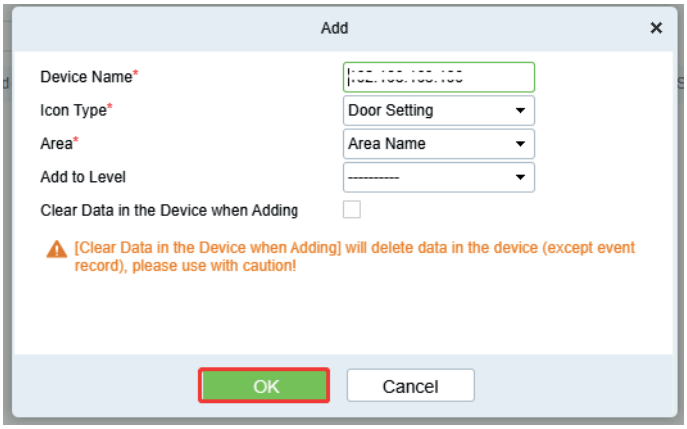
17.2 Agregar dispositivo en el software

Agregue el dispositivo mediante la búsqueda. El proceso es el siguiente:

1. Haga clic en Acceder > dispositivo > buscar para abrir la interfaz de búsqueda en el software.
2. Haga clic en Buscar y aparecerá la opción Buscar…….
3. Después de buscar, se mostrará la lista y el número total de controladores de acceso.



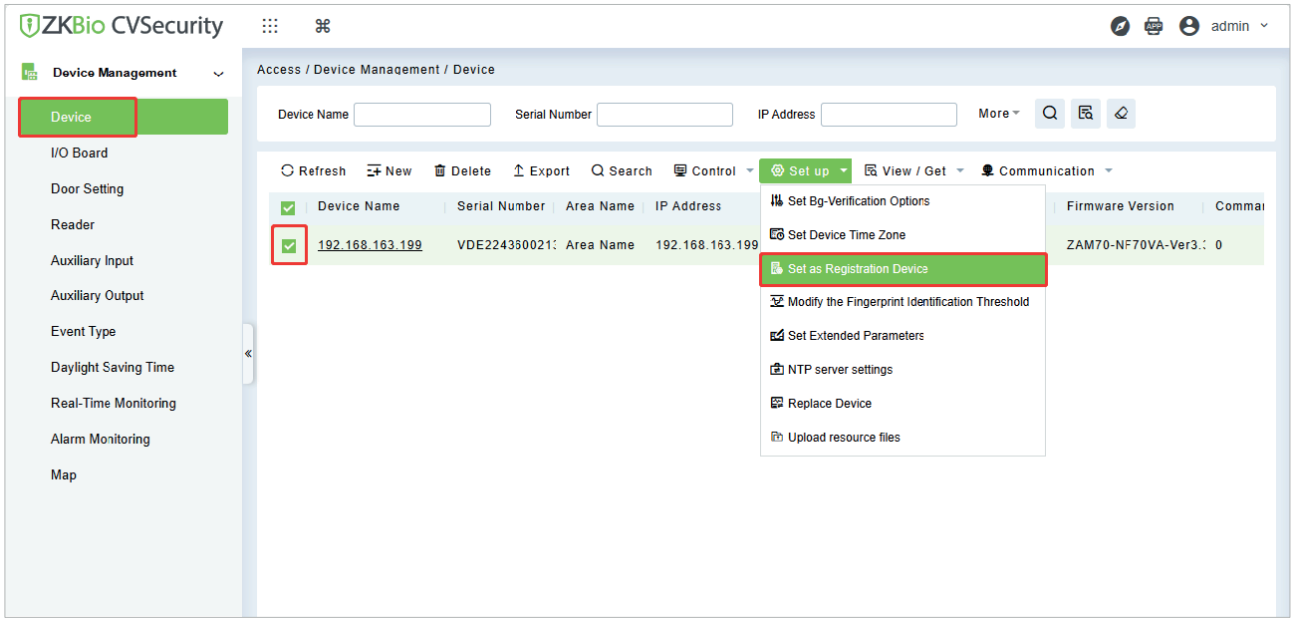
4. Haga clic en Agregar en la columna de operación, aparecerá una nueva ventana. Seleccione Tipo de icono, Área y Agregar al nivel en cada menú desplegable y haga clic en Aceptar para agregar el dispositivo



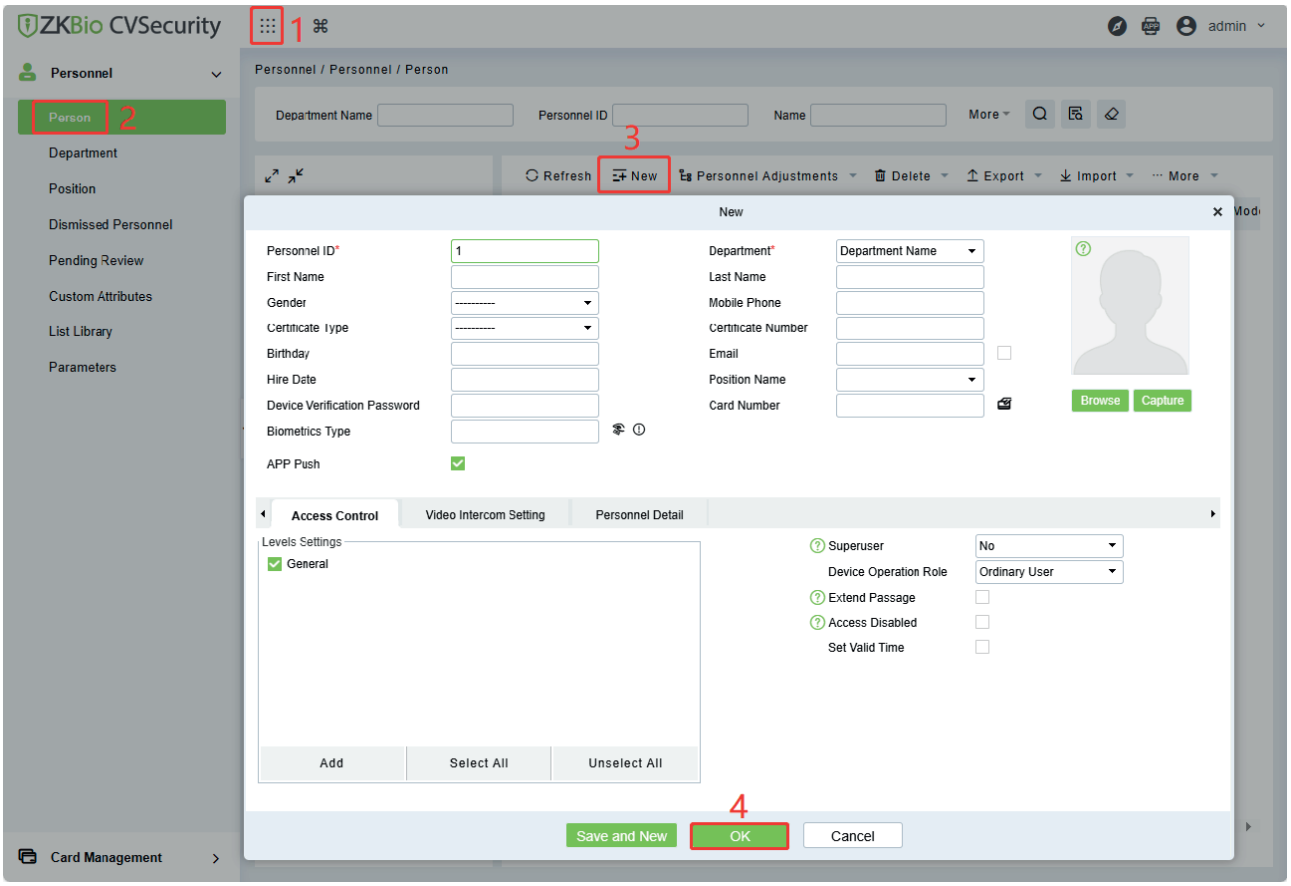
5. Una vez que la adición se haya realizado correctamente, el dispositivo se mostrará en la lista de dispositivos.

17.3 Añadir personal en el software y registro de huellas dactilares/rostro en línea

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

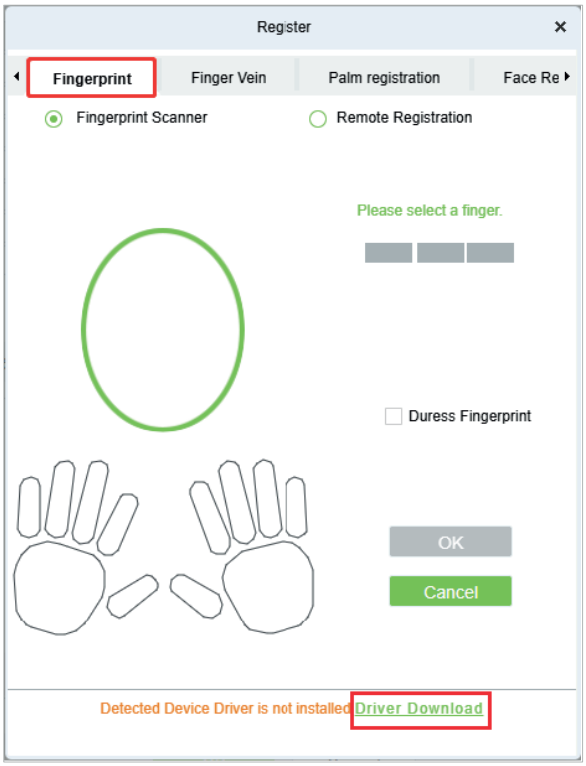


2. Haga clic en Personal > Persona > Nuevo:

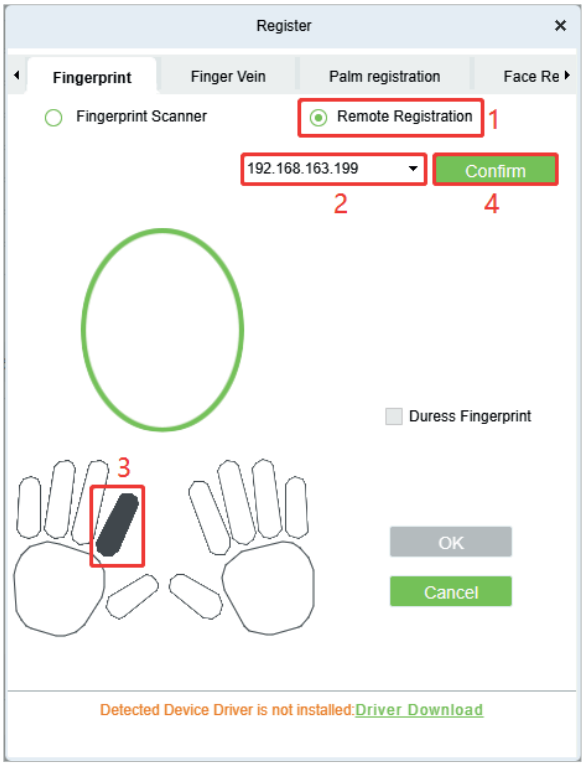


3. Rellene todos los campos obligatorios del usuario y haga clic y seleccione Huella dactilar para acceder a la interfaz de registro de huellas dactilares en línea.

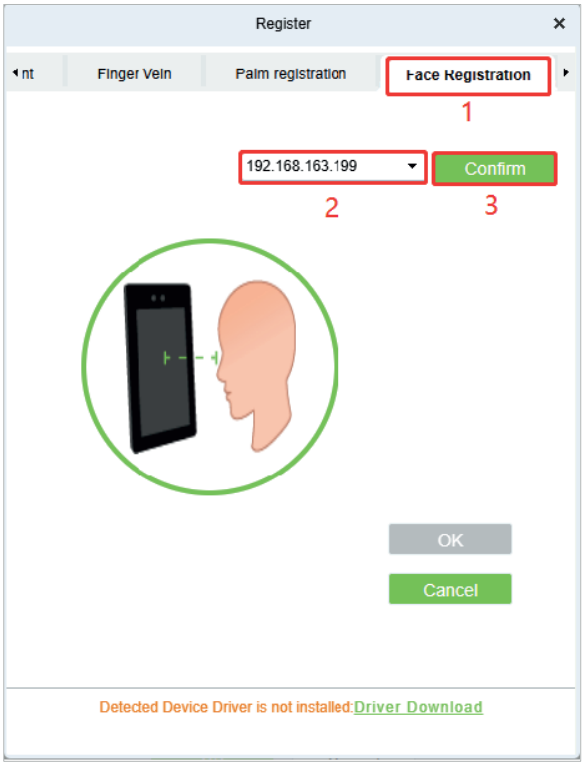
4. Haga clic en Descargar controlador para instalar primero el controlador.



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 en 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 digital de coacción:** En cualquier caso, se genera una alarma de coacción cuando una huella digital coincide con una huella digital 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 indicará "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.

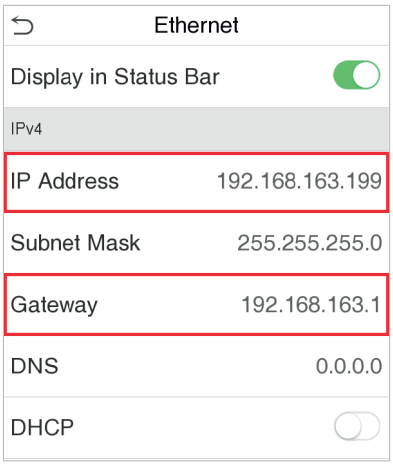
Nota: Para otras operaciones específicas, consulte el Manual de usuario de ZKBio CVSecurity.

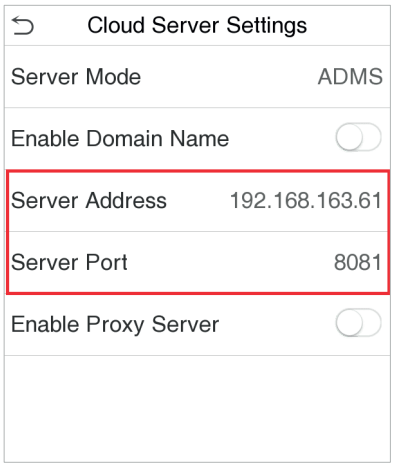
18. Conéctese al software ZKBioTime

18.1 Establecer la dirección de comunicación

1. Toque COMM. > Ethernet en el menú principal para configurar la dirección IP y la puerta de enlace del dispositivo. Nota: La dirección IP debe ser capaz de comunicarse con el servidor de tiempo ZKBio, preferiblemente en el mismo segmento de red que la dirección del servidor
2. En el menú principal, haga clic en 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 a partir de la hora de ZKBio (el valor predeterminado es 8081)

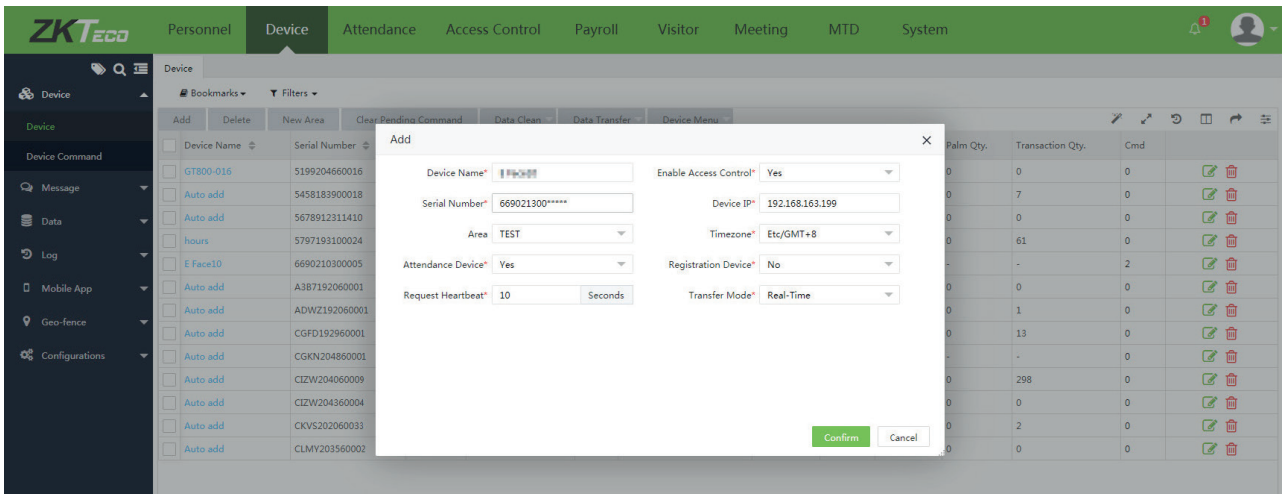




18.2 Agregar dispositivo en el software

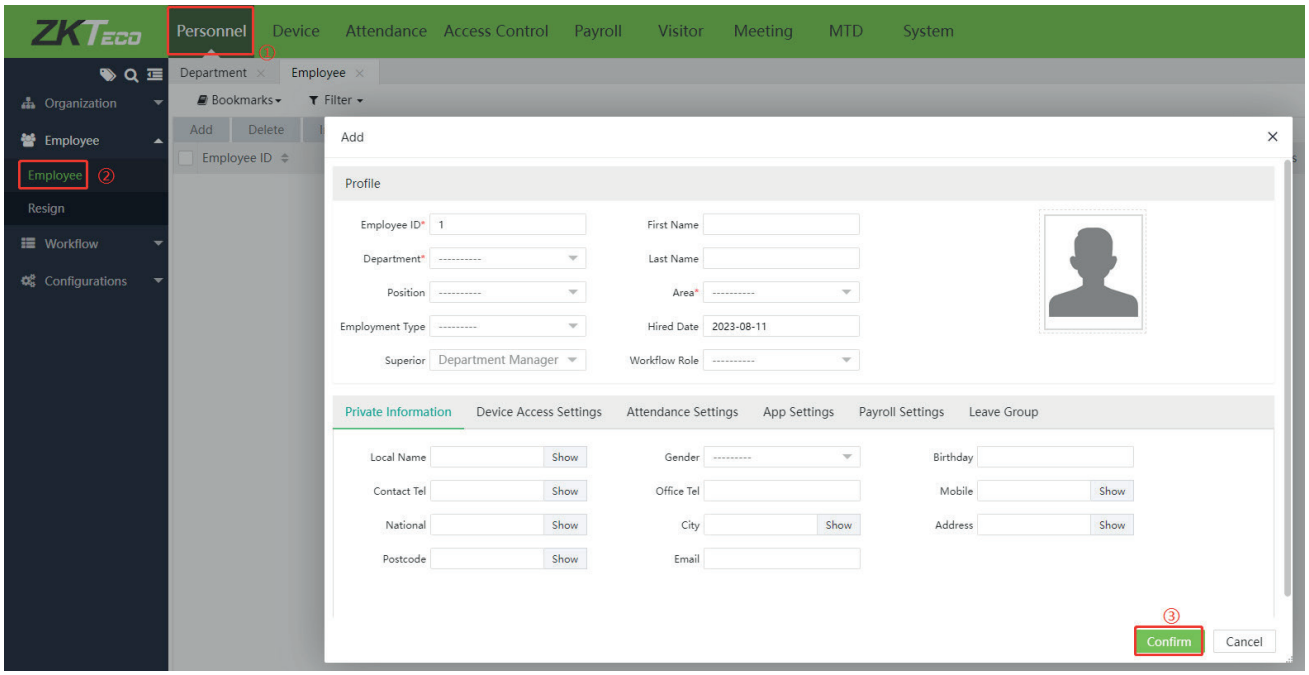
Agregue el dispositivo mediante la búsqueda. El proceso es el siguiente:

1. Haga clic en Dispositivo > Dispositivo > Agregar para agregar el dispositivo en el software.
2. Aparecerá una nueva ventana al hacer clic en Agregar. Ingrese la información requerida sobre el dispositivo y haga clic en Confirmar, luego los dispositivos agregados se muestran automáticamente



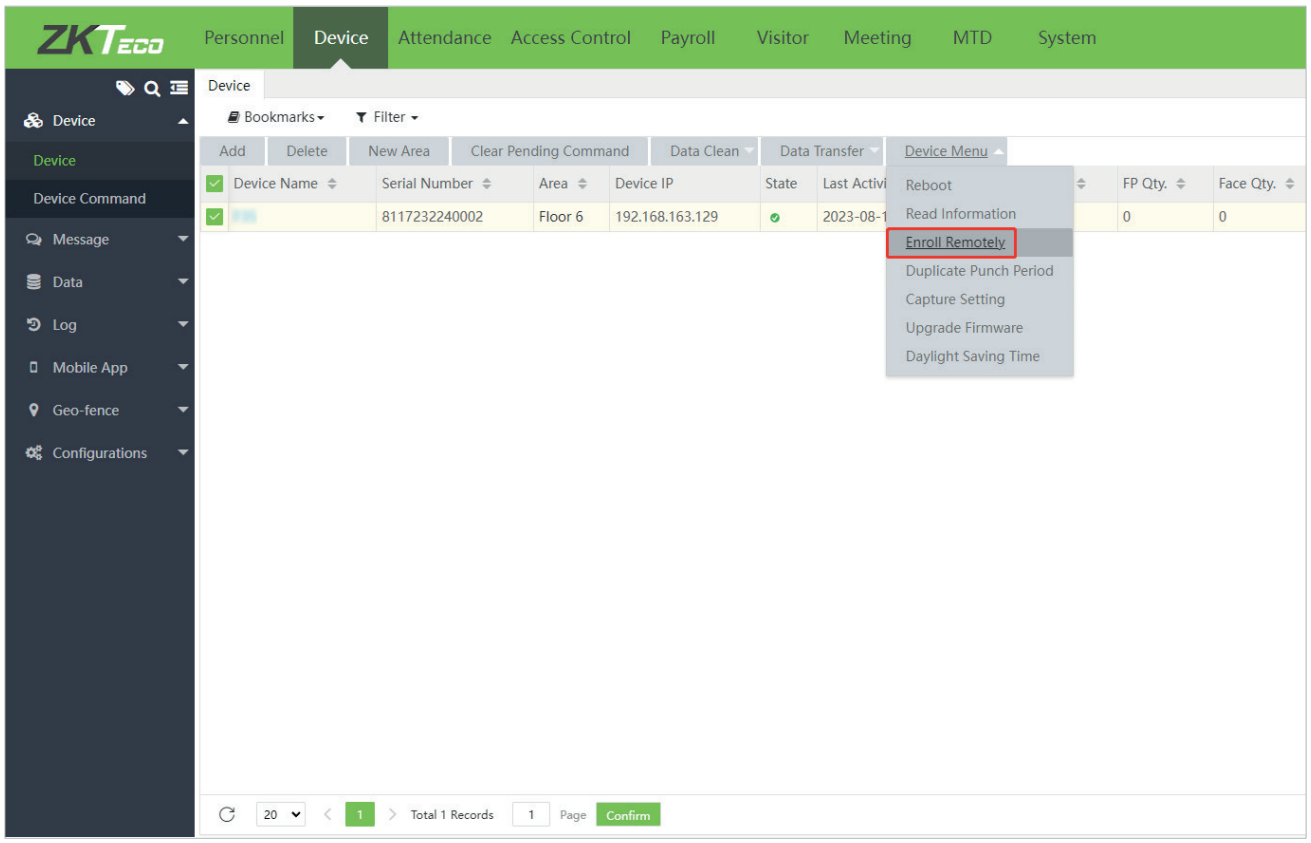
18.3 Agregue personal en el software y registro de huellas dactilares en línea

1. Haga clic en Personal > Empleado > agregar:

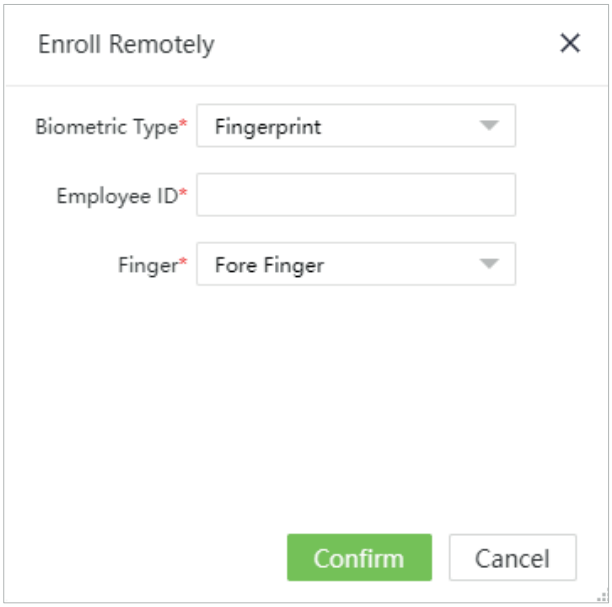


2. Rellene todos los campos obligatorios y haga clic en Confirmar para registrar un nuevo usuario.

3. Haga clic en Dispositivo > dispositivo, seleccione el dispositivo y haga clic en Menú de dispositivo > Inscribir de forma remota.



4. Ingrese el 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 dactilar se registra correctamente, el dispositivo solicitará "Inscrito correctamente".



5. Haga clic en Dispositivo > Dispositivo > Transferencia de datos > Sincronizar datos con el dispositivo para sincronizar todos los datos con el dispositivo, incluidos los nuevos usuarios.

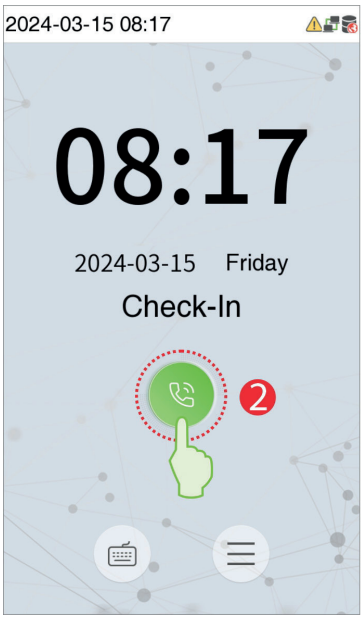
Nota: *Para otras operaciones específicas, consulte el Manual del usuario de ZKBio Time.*

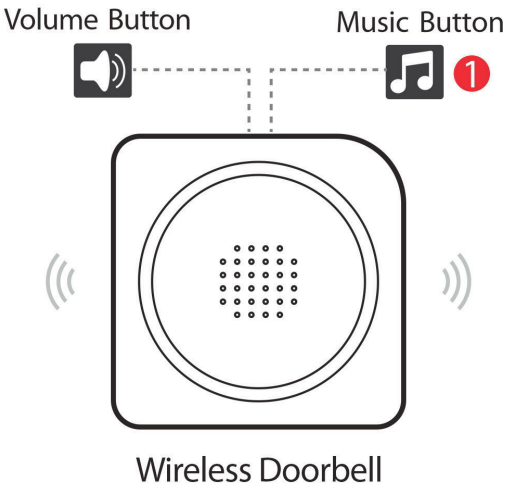
19. Conexión al timbre inalámbrico ★

Nota: Esta función debe utilizarse con el timbre inalámbrico

19.1 Conectar el timbre inalámbrico

1. En primer lugar, 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 emparejarlo correctamente, al pulsar el botón del timbre del dispositivo sonará 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 SenseFace 7 solo admite un timbre inalámbrico.
3) Los clientes deben adquirir ellos mismos el timbre inalámbrico.

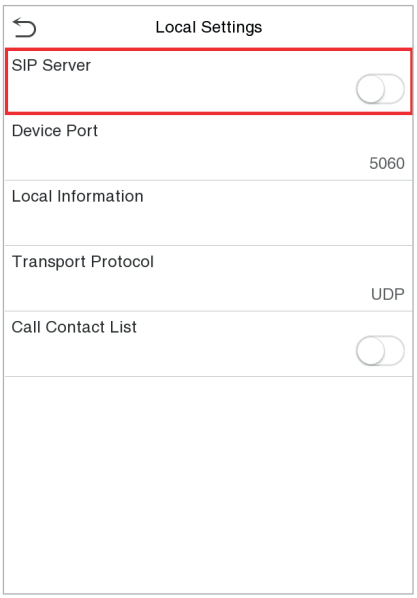
19.2 Desvincular el timbre inalámbrico

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.

20. Intercomunicador de video SIP

20.1 Uso de la red de área local

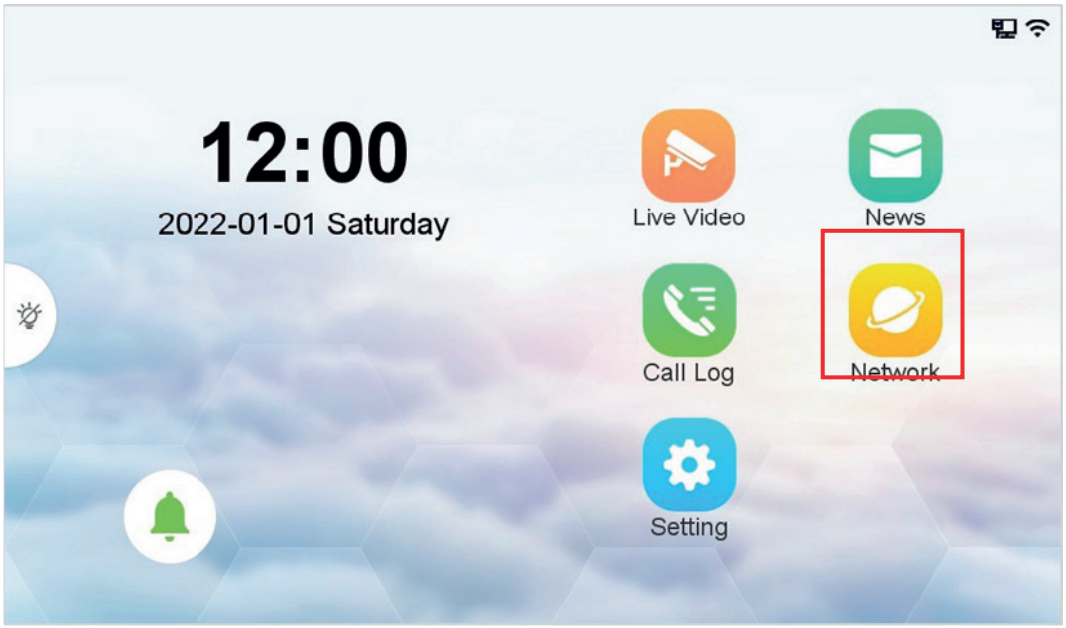
En este modo, asegúrese de que el servidor SIP del dispositivo esté deshabilitado.
Haga clic en Intercomunicador > Configuración SIP > Configuración local para desactivar el servidor SIP.



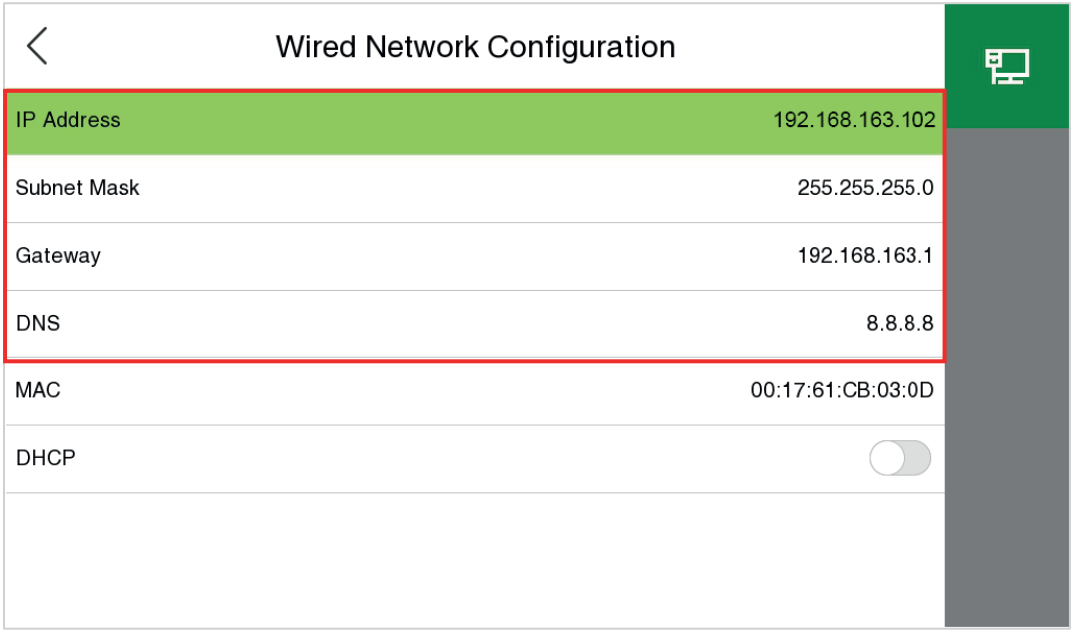
Esta función debe utilizarse con el monitor de interior VT07-B01.

En el monitor interior:

1. Toque Red > para acceder a la interfaz de configuración de la red cableada. (Contraseña predeterminada: 123456)

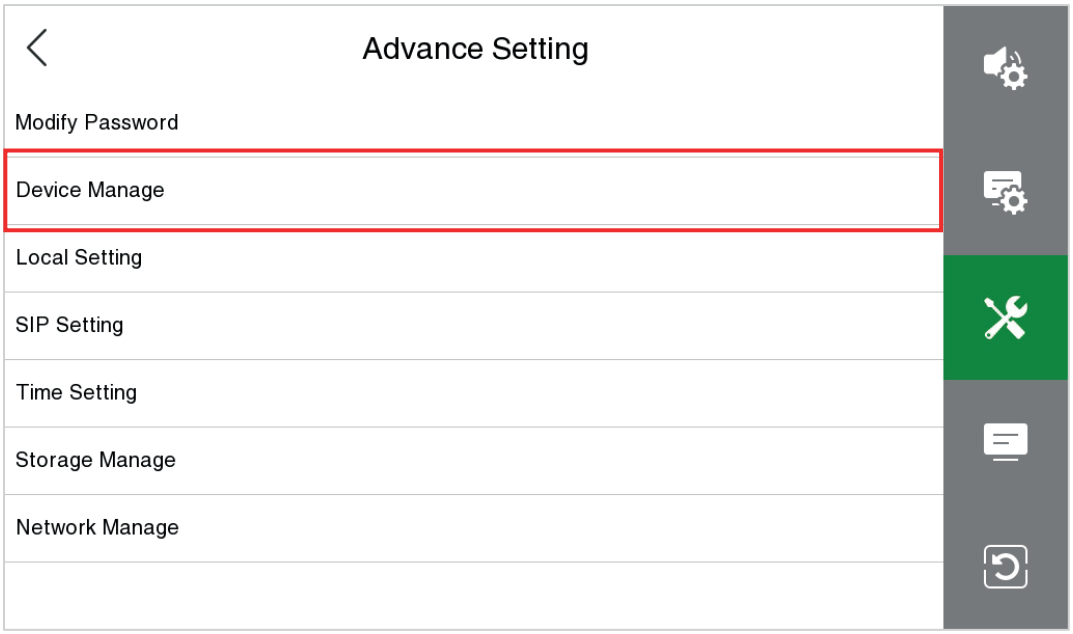


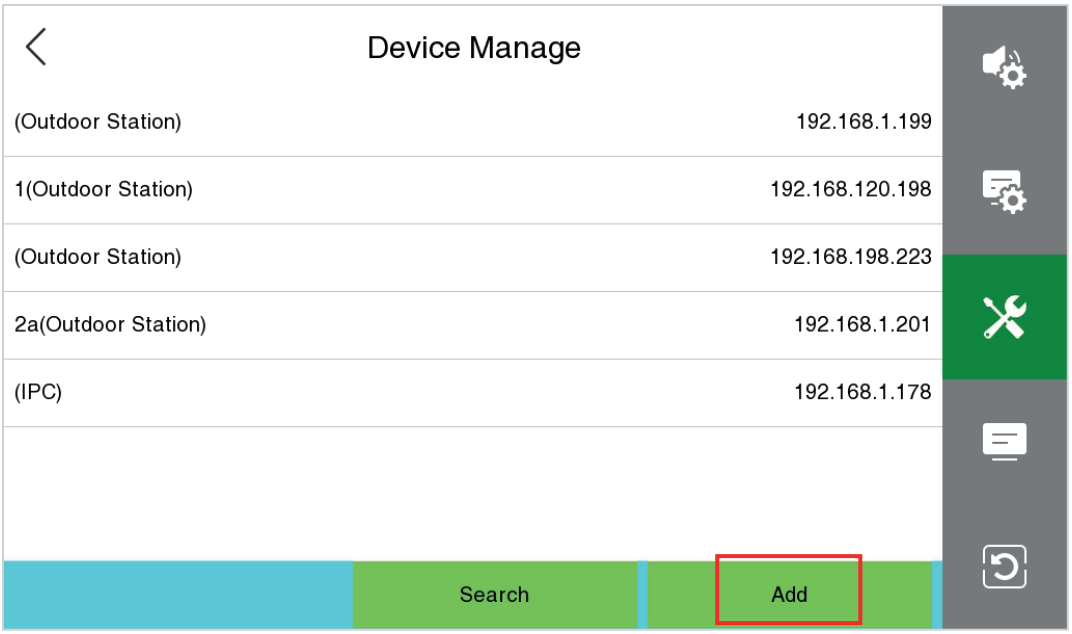
2. Configure la dirección IP y la puerta de enlace del monitor interior. (Nota: La dirección IP debe estar en el mismo segmento de red que el dispositivo).



3. Toca Configuración > Configuración avanzada > Administración de dispositivos > Añadir para añadir el dispositivo.







4. Establezca la información relacionada con el dispositivo, luego haga clic en Guardar.

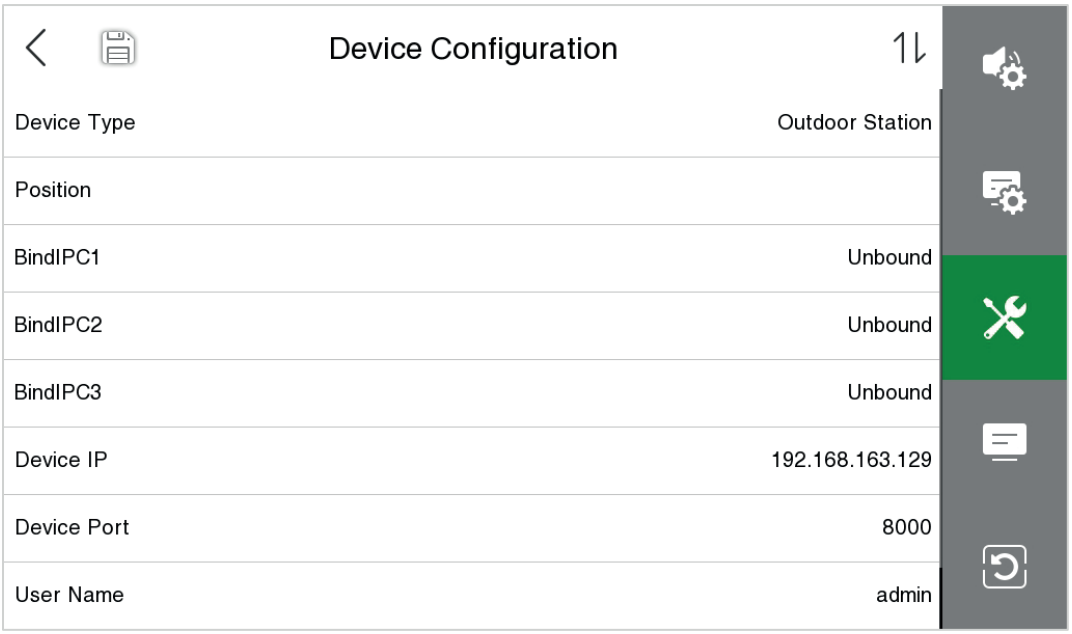
Tipo de dispositivo: Establecer como estación exterior.

IP del dispositivo: Ingrese la dirección IP del dispositivo.

Puerto del dispositivo: 8000.

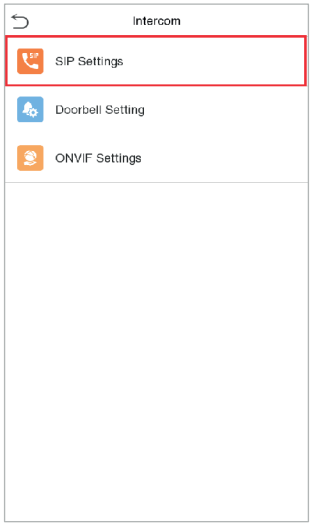
Nombre de usuario: admin.

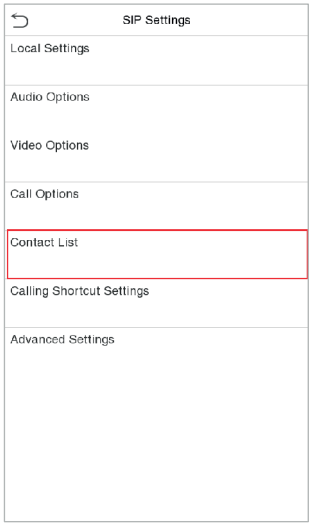
Contraseña: 123456.



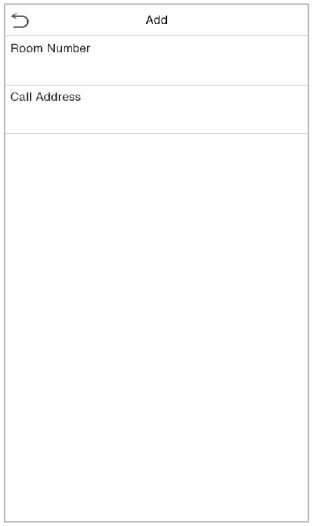
En el dispositivo:

1. En el dispositivo: Haga clic en [Intercomunicador] > [Configuración SIP] > [Lista de contactos] > [Agregar] para agregar los monitores interiores conectados



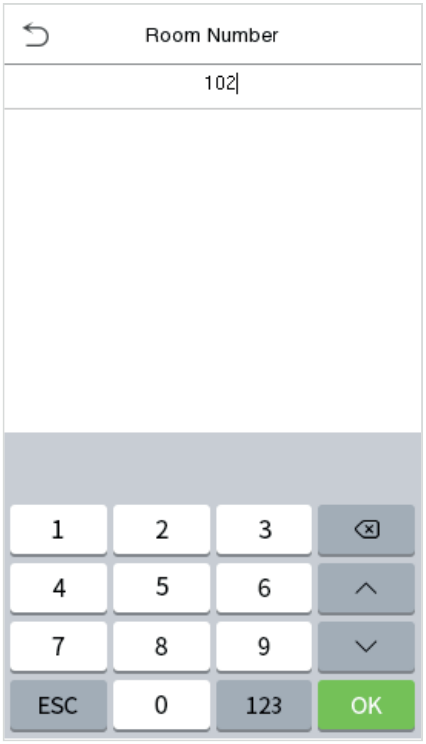




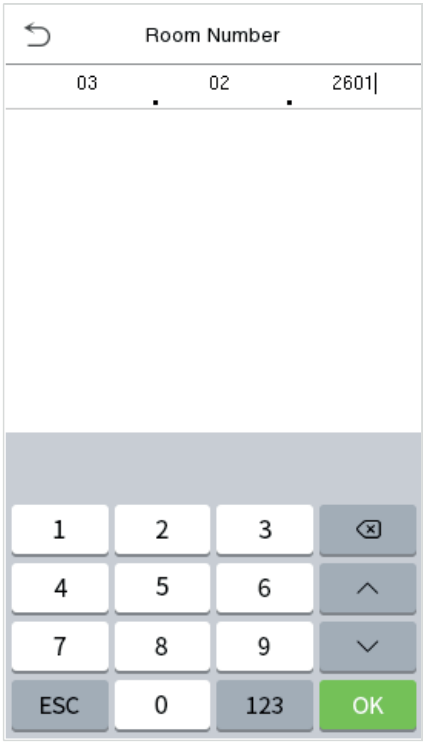


Número de habitación: Personalice el número del monitor interior.

Cuando el tipo de dispositivo se establece como Estación de entrada, el número de habitación puede ser de 1 ~ 4 dígitos. Cuando el tipo de dispositivo se establece como Terminal de cerca, debe ingresar el bloque, la unidad y el número de habitación. Por ejemplo, si el monitor interior está en el Bloque 3, Unidad 2, Sala 2601, ingrese "03.02.2601".



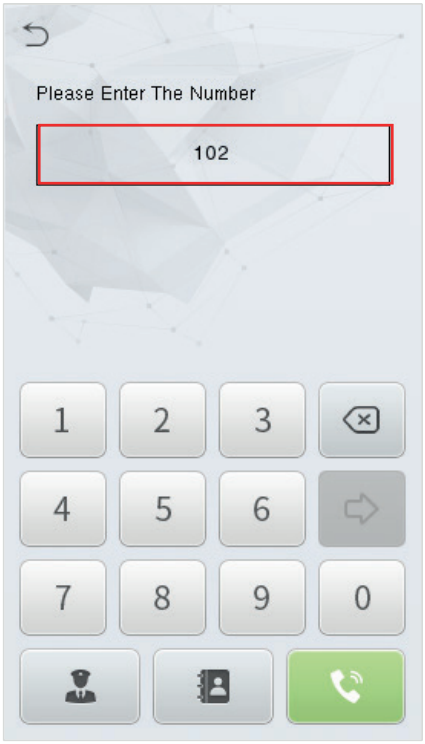
Estación de entrada

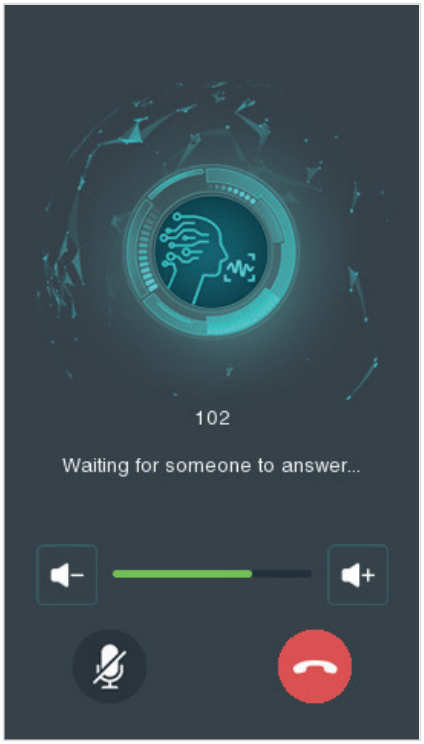


Terminal de valla

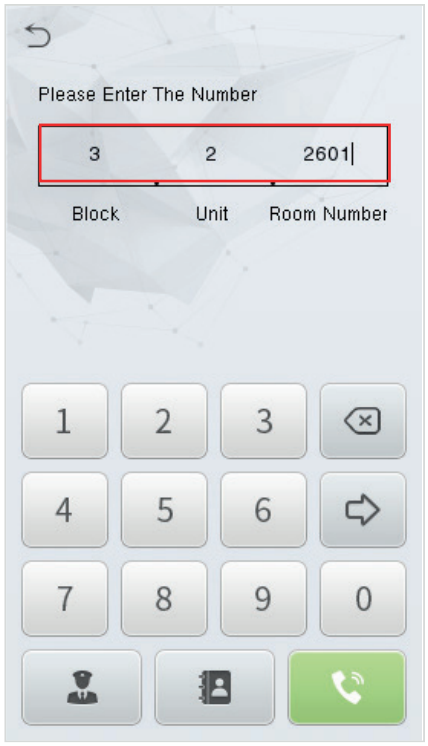
Dirección de llamada: Es la dirección IP del monitor interior.

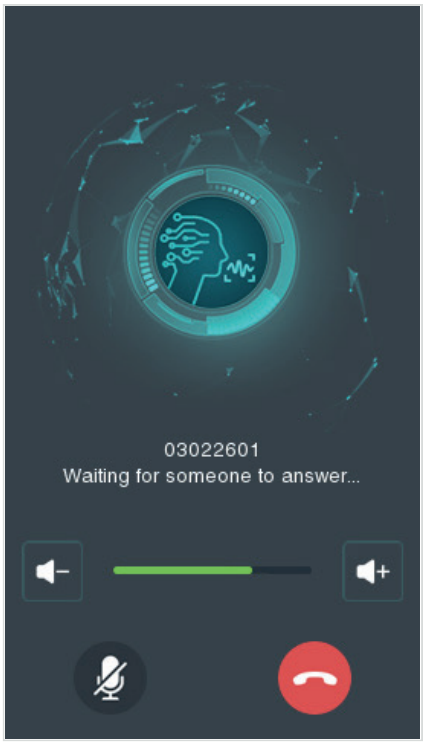
2. Para habilitar la función de videoportero, haga clic en el icono del dispositivo e introduzca el número o la dirección IP del monitor interior en la interfaz proporcionada.





Estación de entrada



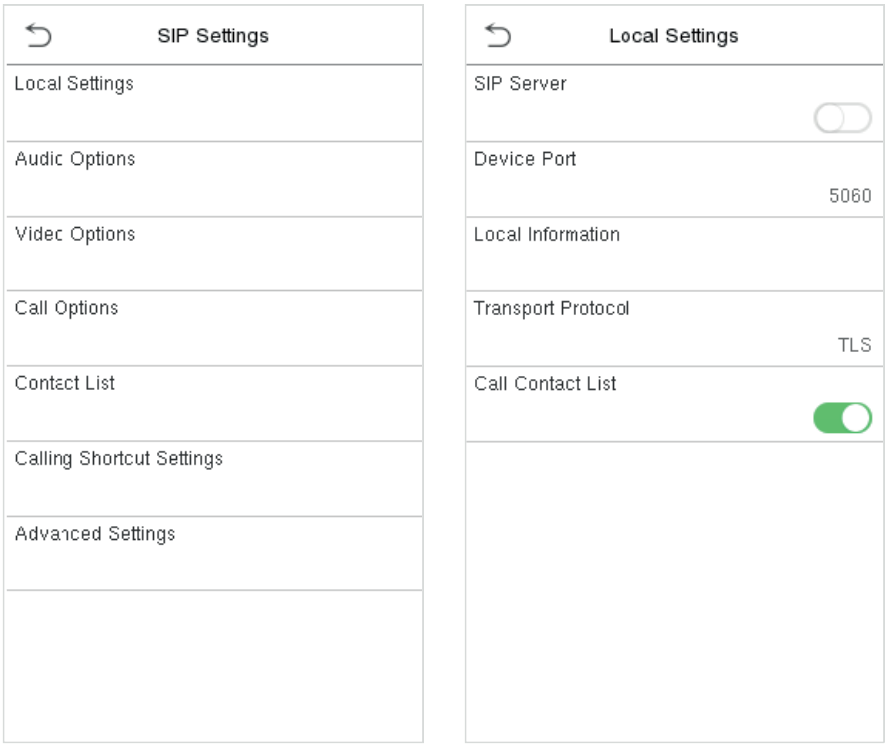


Extremos de la valla

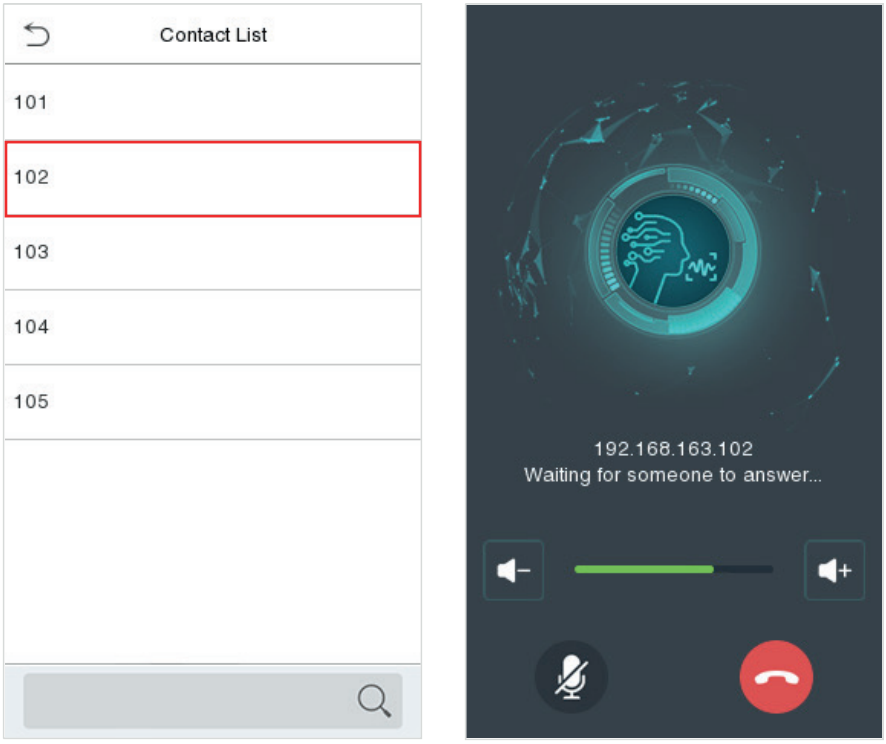


20.1.1 Lista de contactos de llamadas

1. En la interfaz de configuración SIP, toque Configuración local > Lista de contactos de llamadas para habilitar la lista de contactos de llamadas.

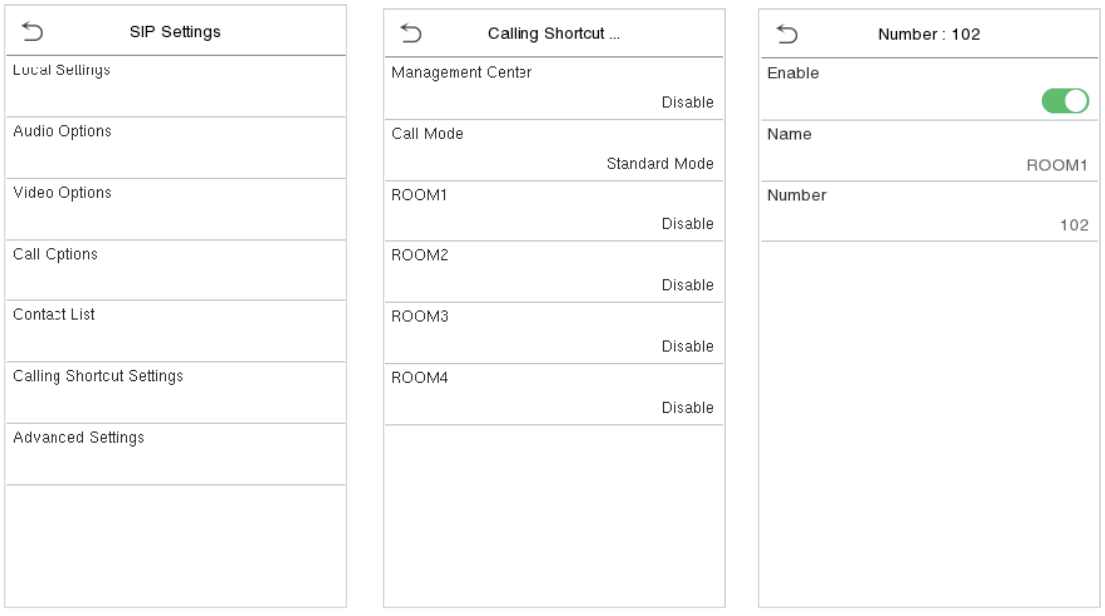


2. Haga clic en el icono del dispositivo para acceder a la página de llamadas. A continuación, haga clic en el icono para abrir la lista de contactos y seleccione el número del monitor interior al que desea llamar.



20.1.2 Personalizar las teclas de acceso directo de llamada

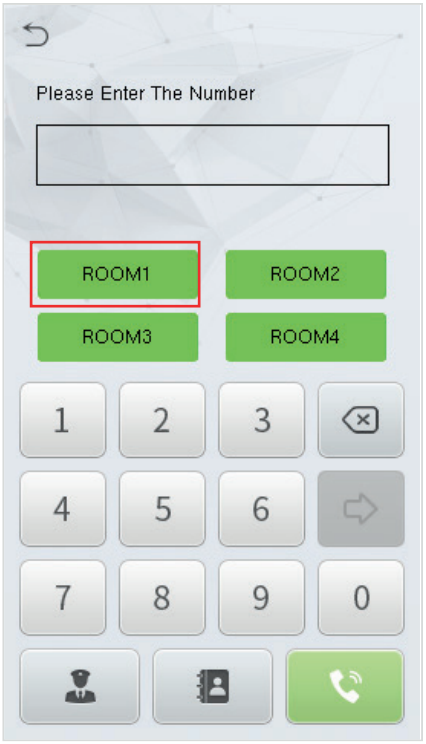
1. En la interfaz Configuración de SIP, toque Configuración de acceso directo de llamada para habilitar y definir las teclas de acceso directo.

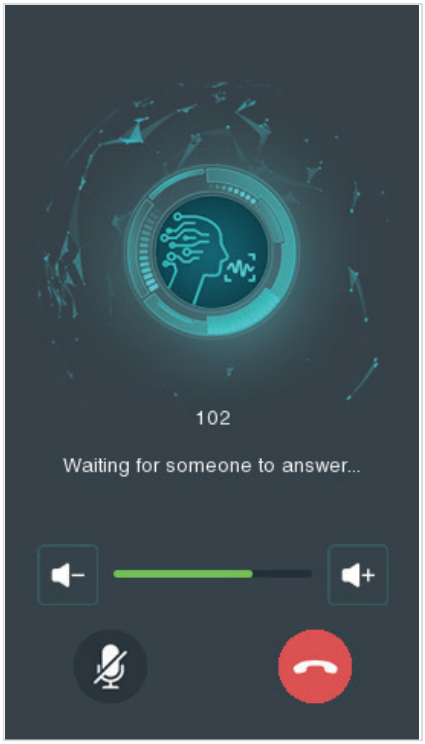


Nombre: Personaliza el nombre de las teclas de método abreviado.

Número: Es el número de habitación que se establece en el menú de la lista de contactos..

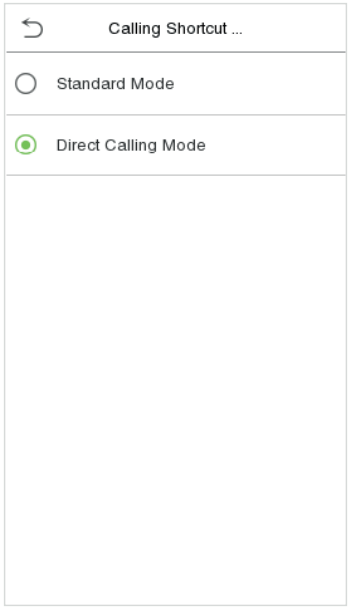
2. A continuación, puede hacer clic en el icono del dispositivo y seleccionar las teclas de acceso rápido para llamar al monitor interior.

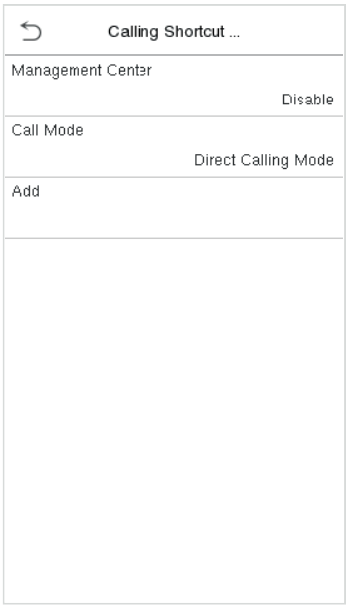




20.1.3 Llamadas directas

1. En la interfaz de configuración de SIP, haga clic en Configuración de acceso directo de llamadas > Modo de llamada > Modo de llamada directa > Agregar. Seleccione la dirección IP de los monitores interiores a los que desea llamar, luego los monitores interiores se mostrarán en la lista.

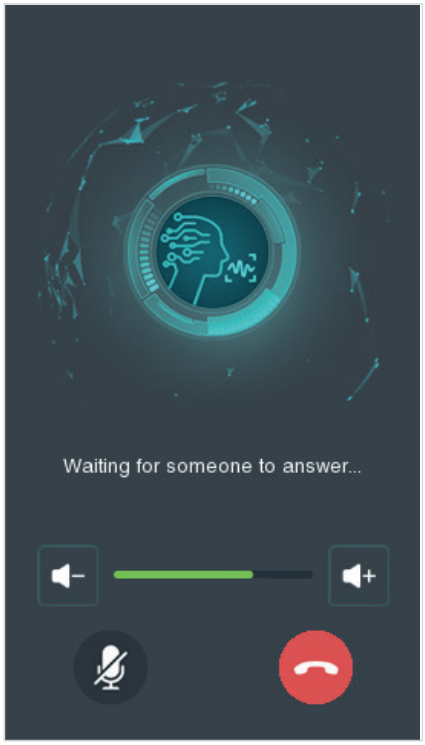






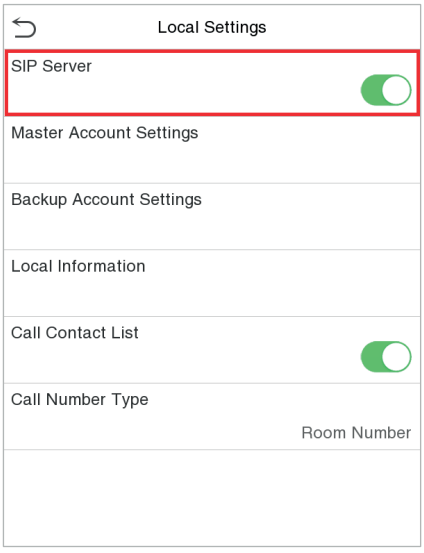
2. A continuación, puede hacer clic en el icono del dispositivo para llamar directamente a los monitores interiores.





20.2 Servidor SIP

En este modo, asegúrese de que el servidor SIP del dispositivo esté habilitado.
Haga clic en Intercomunicador > Configuración SIP > Configuración local para habilitar el servidor SIP



Esta función debe utilizarse con el servidor ZKBio CVSecurity, la aplicación móvil ZKBio Zexus, el monitor interior VT07-B26L-W / VT07-B22L y el cliente para PC BioTalk Pro.

ZKBio CVSecurity admite dos tipos de servidores SIP: SIP en la nube y servidor PBX. Los usuarios pueden elegir uno según la situación real.

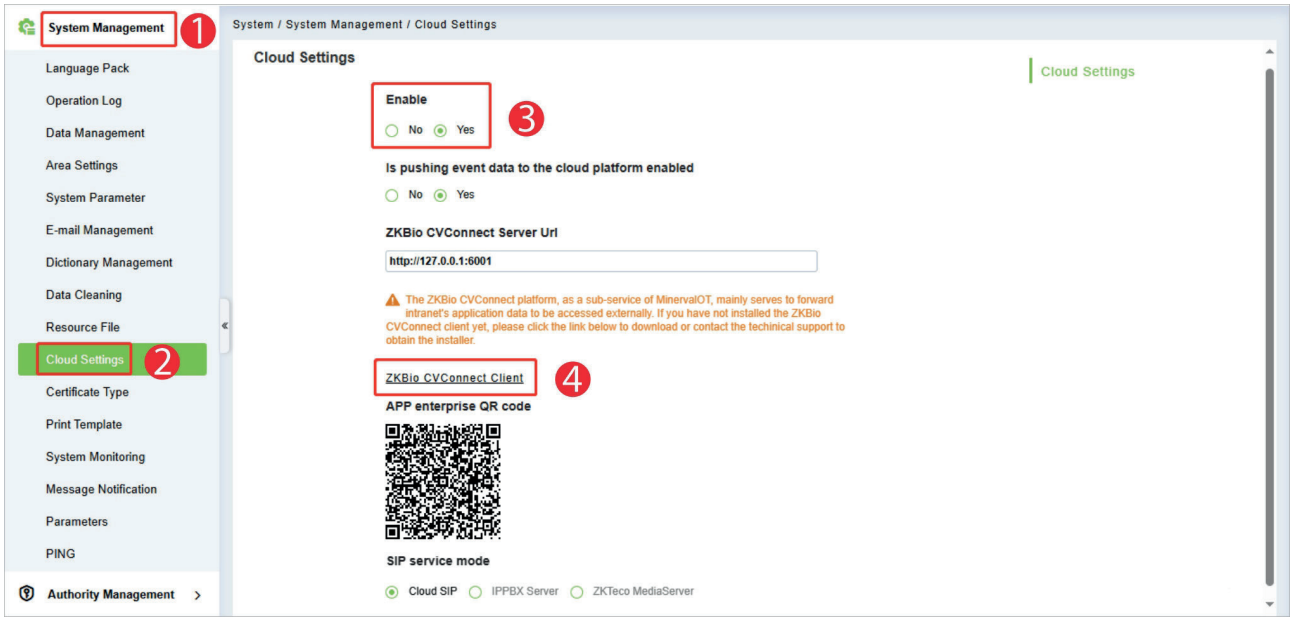
- **Modo SIP en la nube:** Los usuarios no necesitan comprar un servidor SIP adicional, solo necesitan permiso de la cuenta.

- **Servidor PBX:** Debe comprar un servidor PBX para la implementación local. No es necesario comprar una cuenta SIP adicional.

En el siguiente texto se presenta principalmente el modo SIP en la nube.

20.2.1 Configuración del servidor SIP

1. En ZKBio CVSecurity, haga clic en System > System Management > Cloud Setting para habilitar el servicio CloudSIP
2. Haga clic en ZKBio CVConnect Client para descargarlo e instalarlo. (Nota: La instalación y activación del cliente puede ver el Manual del usuario de la aplicación móvil ZKBio Zexus).

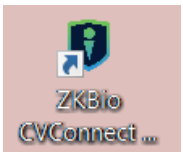


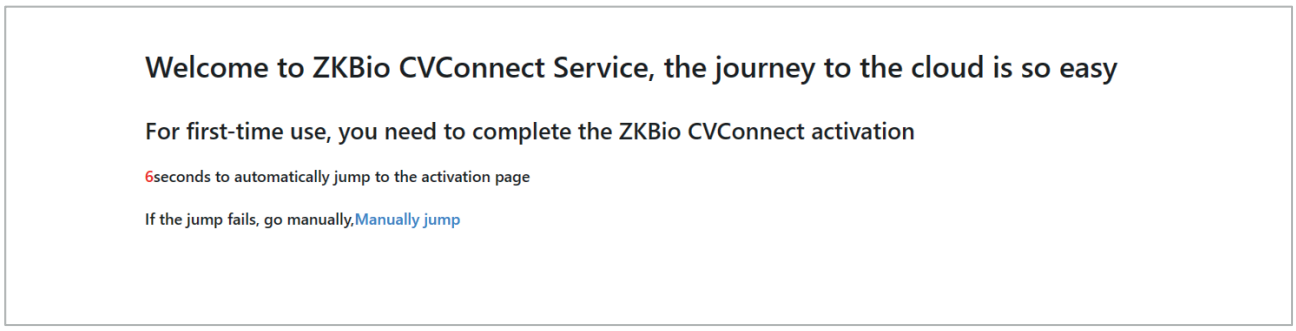
Nota:

1) Asegúrese de que el cliente ZKBio CVConnect esté instalado si Cloud SIP está activado.
2) Después de habilitar Cloud SIP, la red del dispositivo debe poder conectarse a la red externa antes de que pueda ser utilizado.

- **Pasos de activación del cliente ZKBio CVConnect**

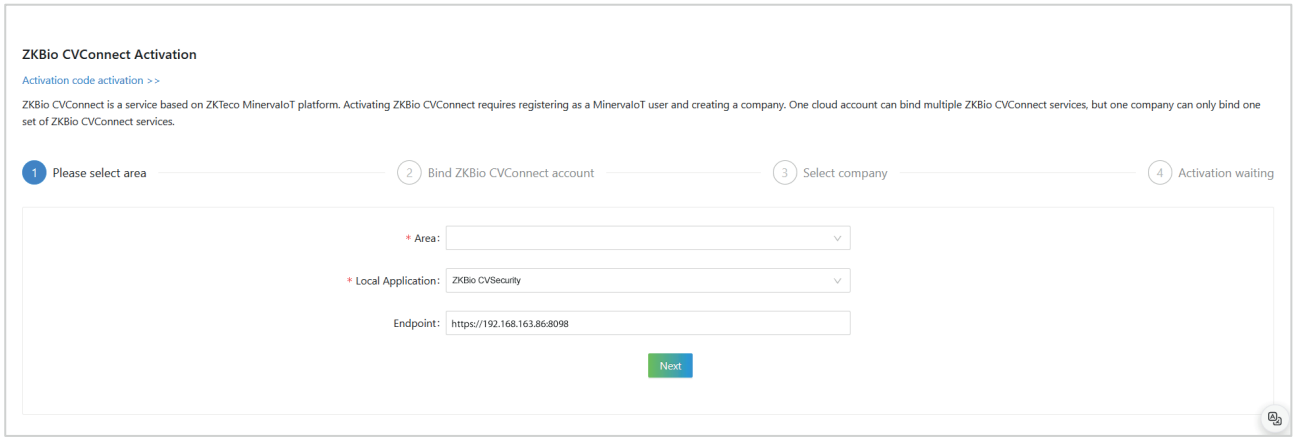
Paso 1: Haz doble clic en la tecla de acceso directo del escritorio. Vaya a la página del navegador.





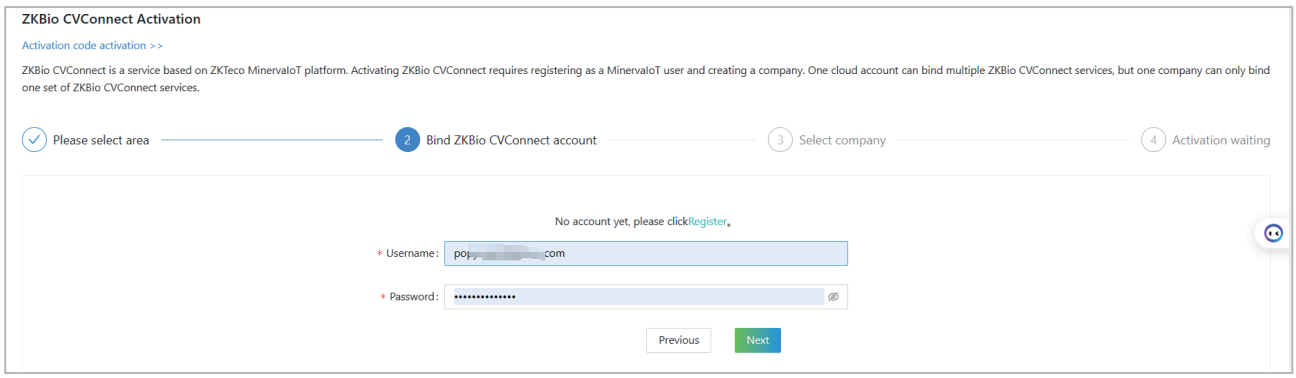
Paso 2: Siga los pasos de la página para completar la activación.

1. Seleccionar área

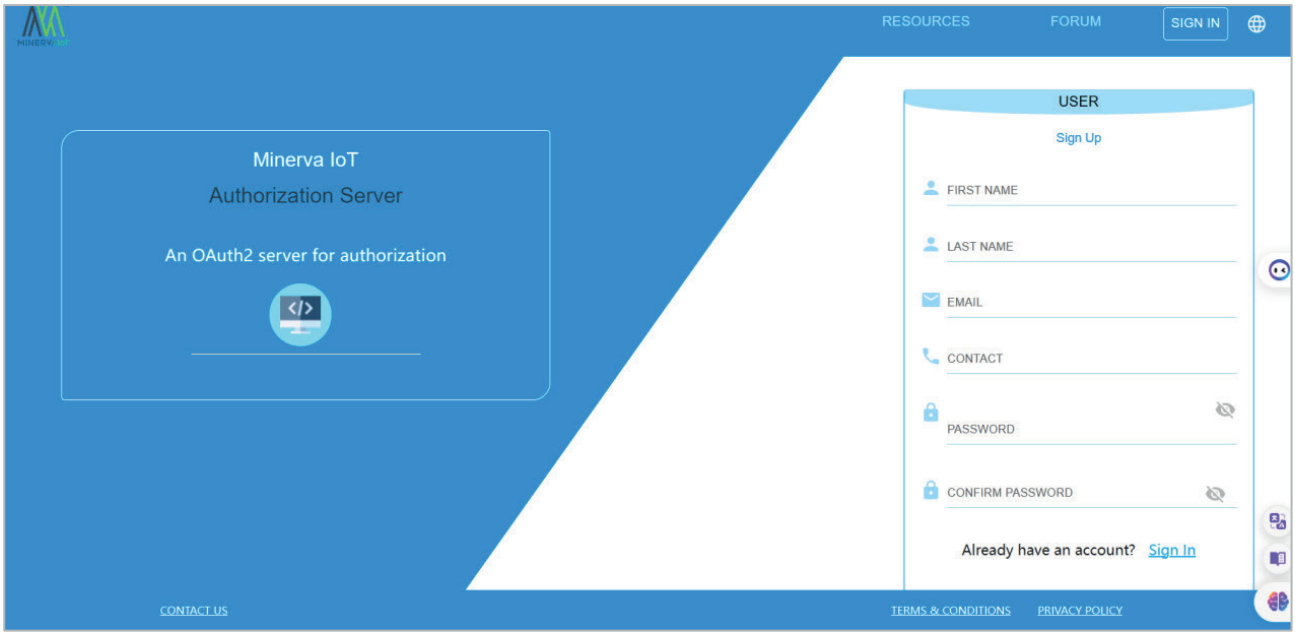


- **Área:** Seleccione el área del servidor en la nube, actualmente solo están disponible China, Singapur y América, otras áreas se agregarán más adelante.
- **Aplicación local:** Establezca como ZKBio CVSecurity
- **EndPoint:** La dirección del servidor de su aplicación local. Por ejemplo, si su aplicación local es ZKBio CVSecurity con una dirección de servidor https://192.168.163.86:8098, introduzca aquí esta dirección de servidor para que ZK-Bio CVConnect pueda reenviar correctamente los datos desde su servidor local para que la aplicación móvil pueda acceder a ellos.

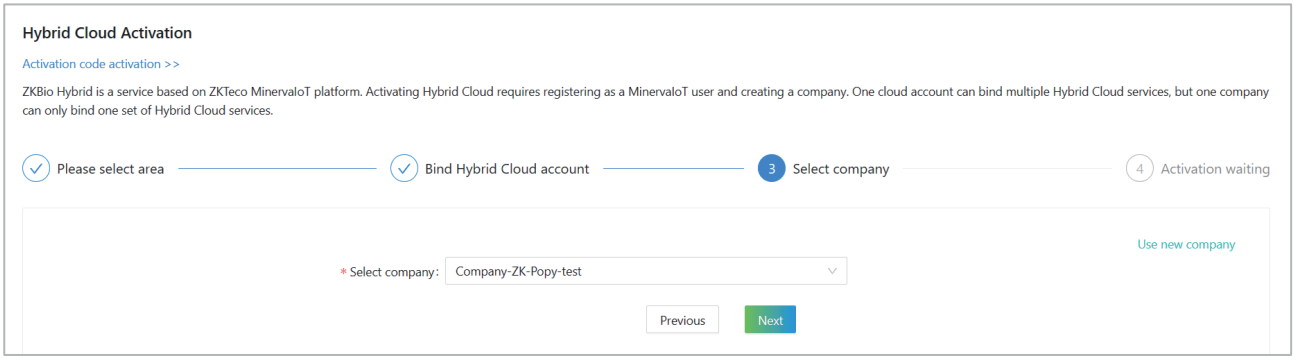
2 Vincular cuenta ZKBio CVConnect



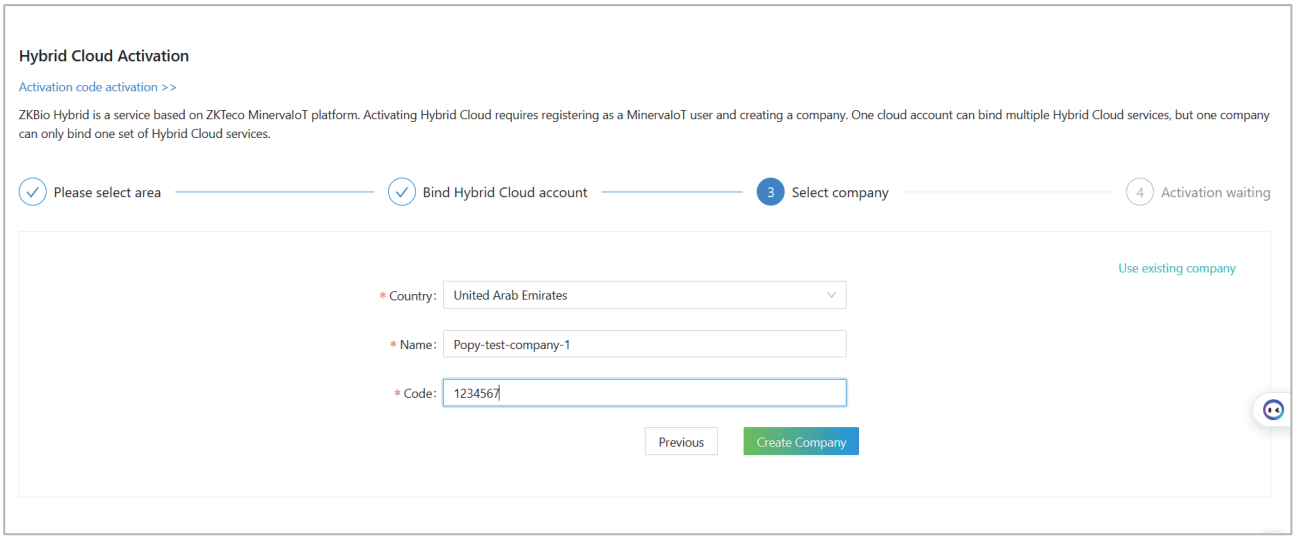
Si ya tiene una cuenta de Minerva IoT, puede usarla e iniciar sesión; de lo contrario, haga clic en Registrarse, luego vaya a la página de registro de Minerva IoT y registre su cuenta.



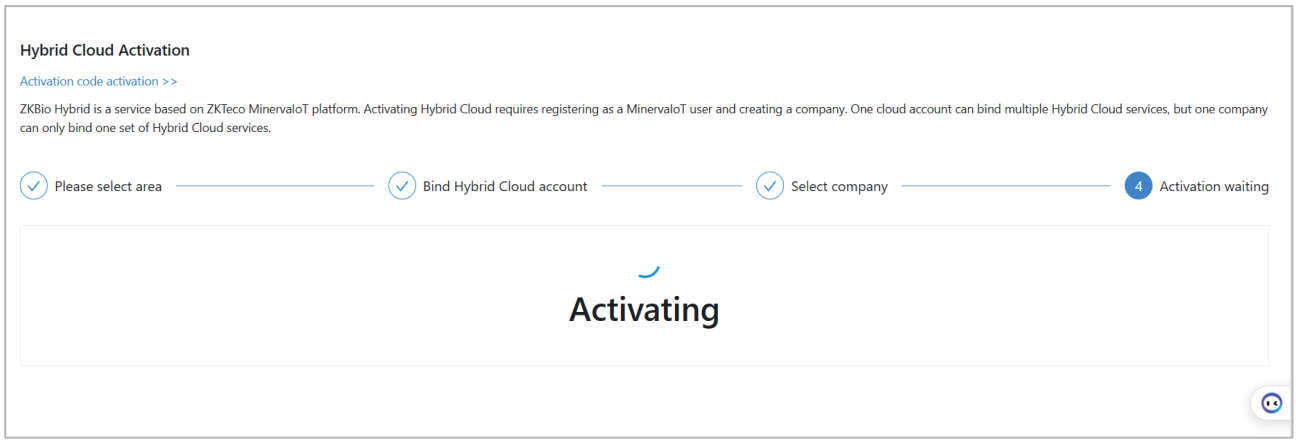
3 Seleccione la empresa



Si actualmente no tiene una empresa, puede optar por crear una haciendo clic en Usar nueva empresa.



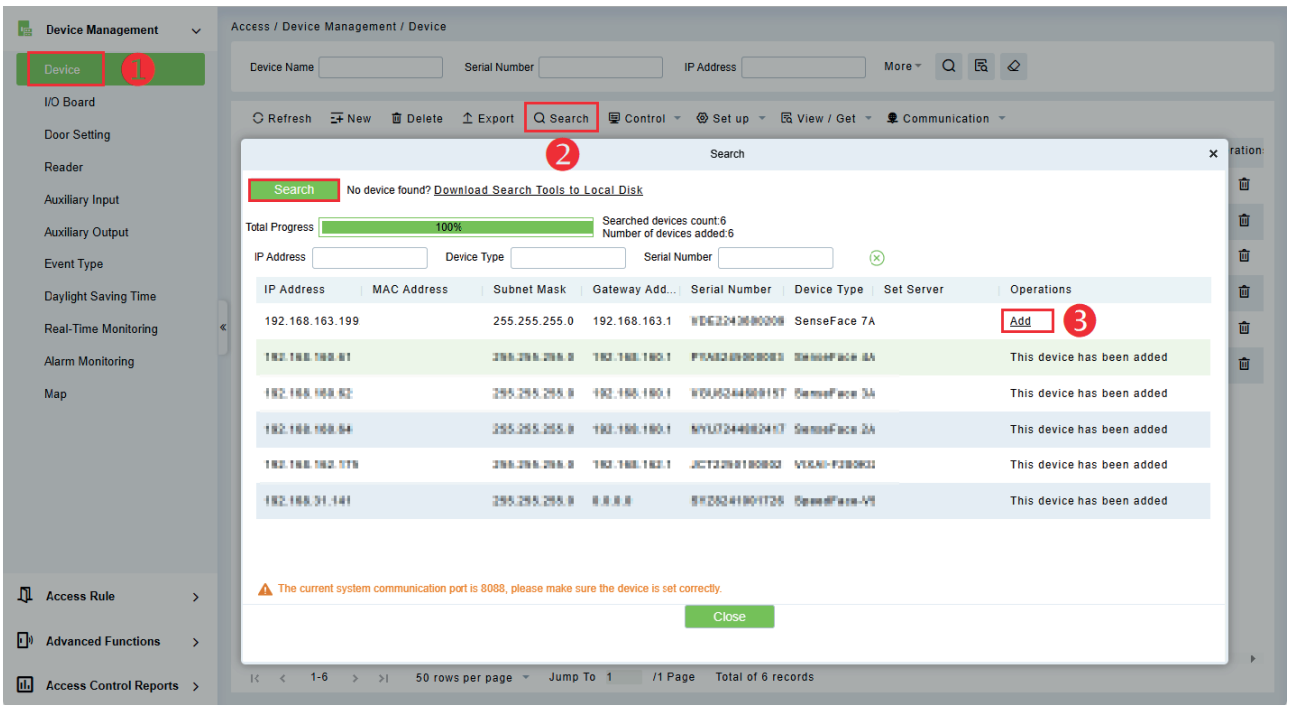
Comience a activar y espere 1-2 minutos hasta que la activación esté completa.



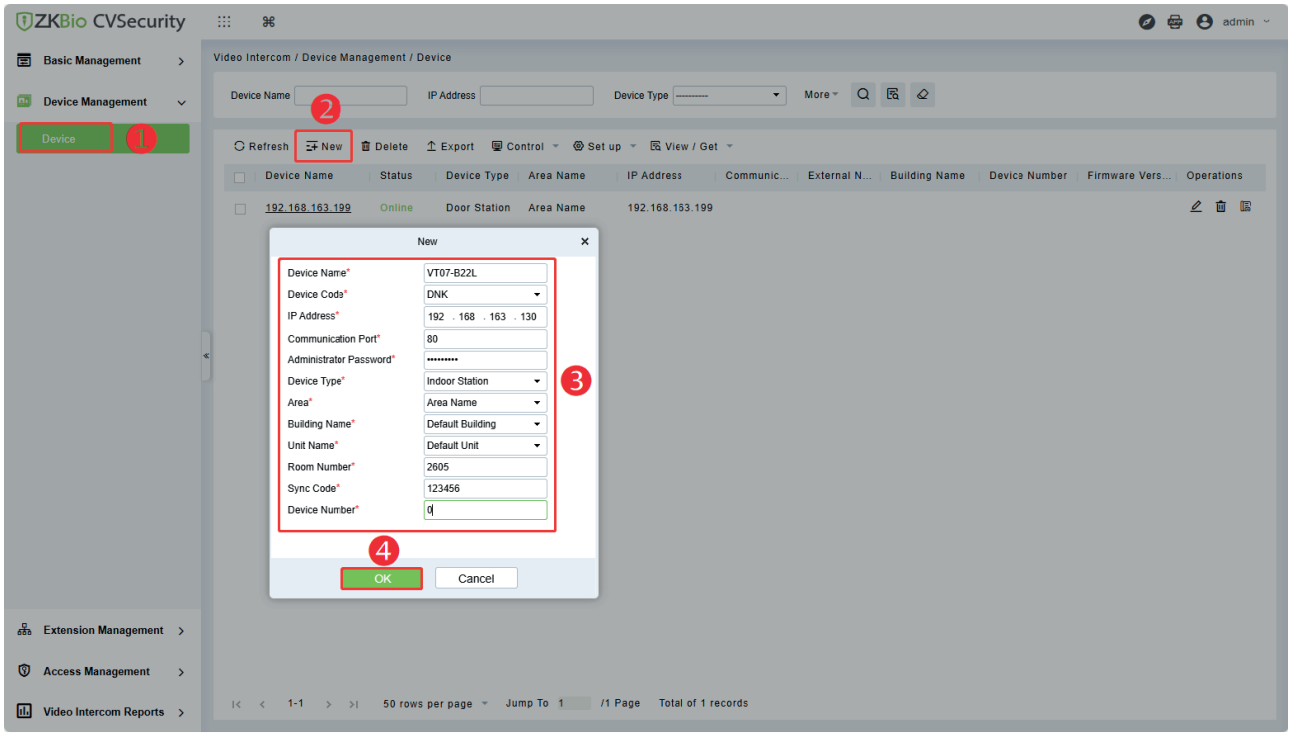
Los pasos específicos de instalación y activación del cliente ZKBio CVConnect pueden consultar el Manual del usuario de la aplicación ZKBio ZexusMobile

20.2.2 Agregar dispositivo

1. En ZKBio CVSecurity, haga clic en Acceso > Administración de dispositivos > Búsqueda > de dispositivos > Buscar >Agregar para agregar el dispositivo mediante la búsqueda. A continuación, el dispositivo se sincronizará automáticamente con el módulo VideoIntercom. (El método de suma puede referirse a 17. Conéctese al software ZKBio CVSecurity)

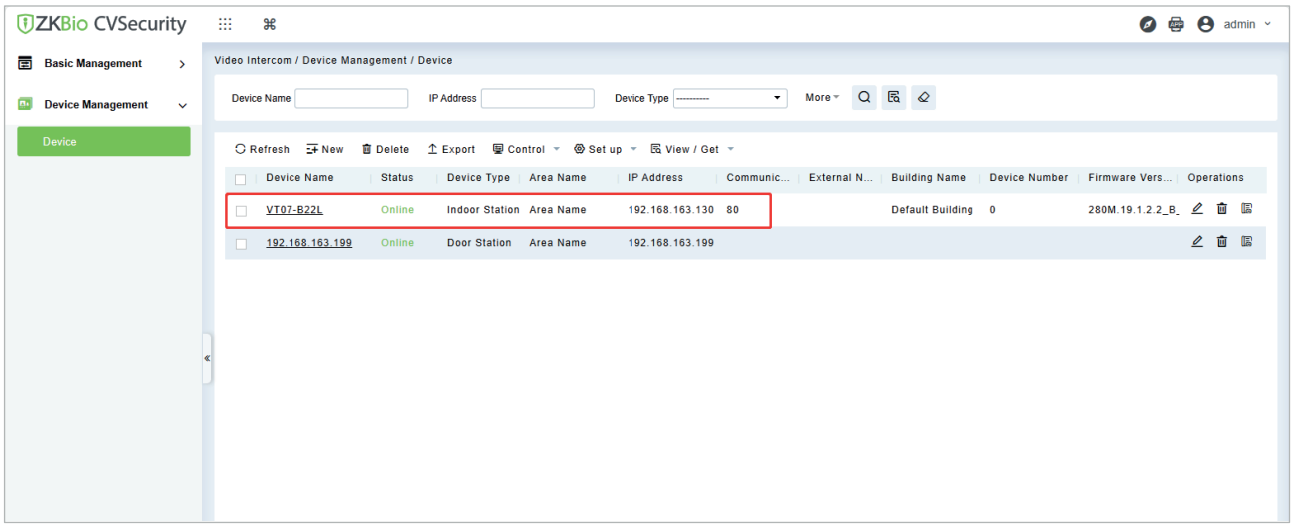


2. Haga clic en Video Intercomunicador > Administración de dispositivos > Dispositivo > Nuevo para agregar el monitor interior.



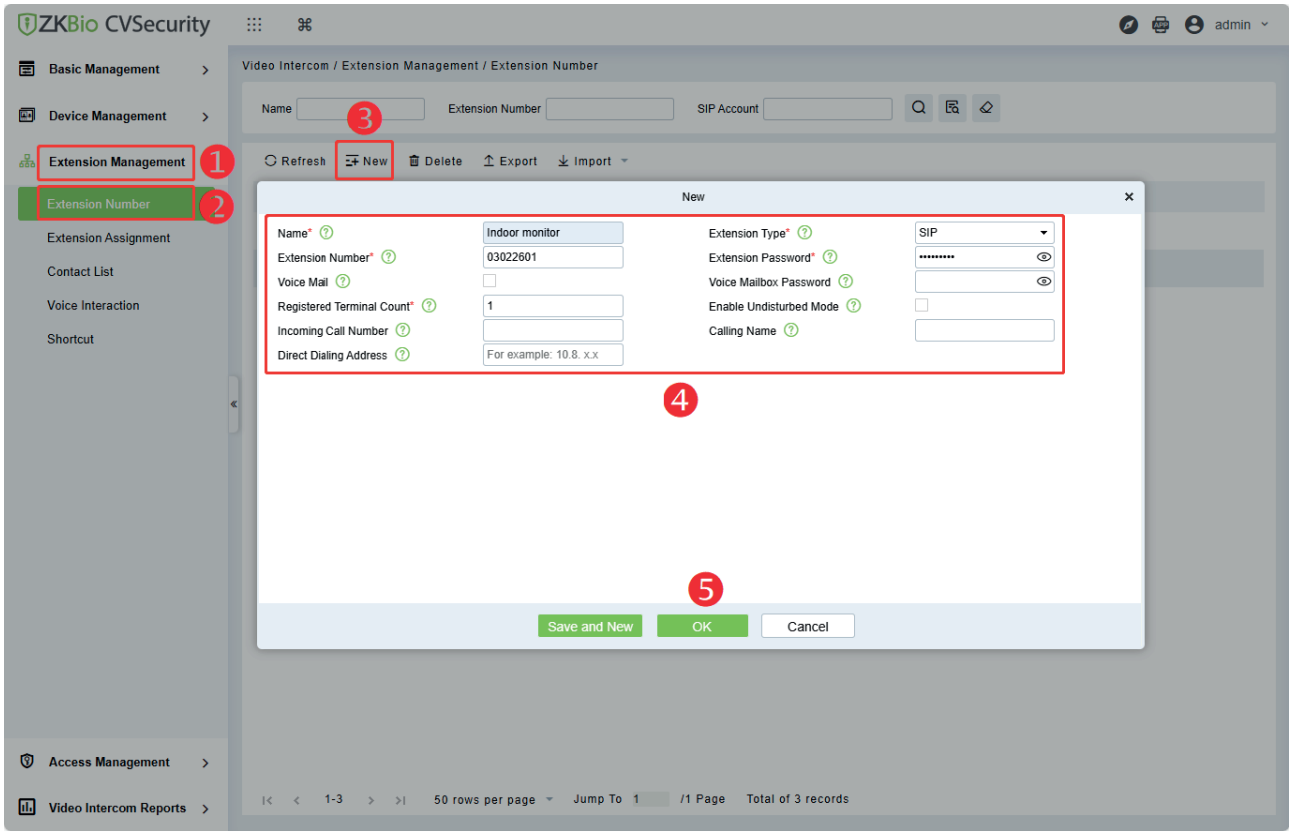
- **Nombre del dispositivo:** Introduzca el nombre del monitor interior.
- **Código del dispositivo:** Establecido como DNK.
- **Dirección IP:** Introduzca la dirección IP del monitor interior.
- **Puerto de comunicación:** 80 de forma predeterminada.
- **Contraseña de administrador:** 123456 de forma predeterminada.
- **Tipo de dispositivo:** Establecer como estación interior.
- **Área/ Nombre del edificio/Nombre de la unidad:** Seleccione de la lista desplegable.
- **Número de habitación:** Personalice el número del monitor interior.
- **Código de sincronización:** El usuario puede personalizarlo. (Se utiliza cuando un residente tiene varios monitores interiores. Los monitores interiores que tengan el mismo código de sincronización se activarán al mismo tiempo).
- **Número de dispositivo:** El rango de configuración es de 0 a 9. Por ejemplo, si solo hay un monitor interior en la habitación, el número de dispositivo será 0. Si hay dos unidades, una será 0 y la otra será 1, y así sucesivamente.

Una vez que la adición se haya realizado correctamente, el monitor interior se mostrará en la lista de dispositivos.



20.2.3 Crear números de extensión

Haga clic en Intercomunicador de vídeo > Administración de extensiones > Número de extensión > Nuevo para agregar números de extensión.



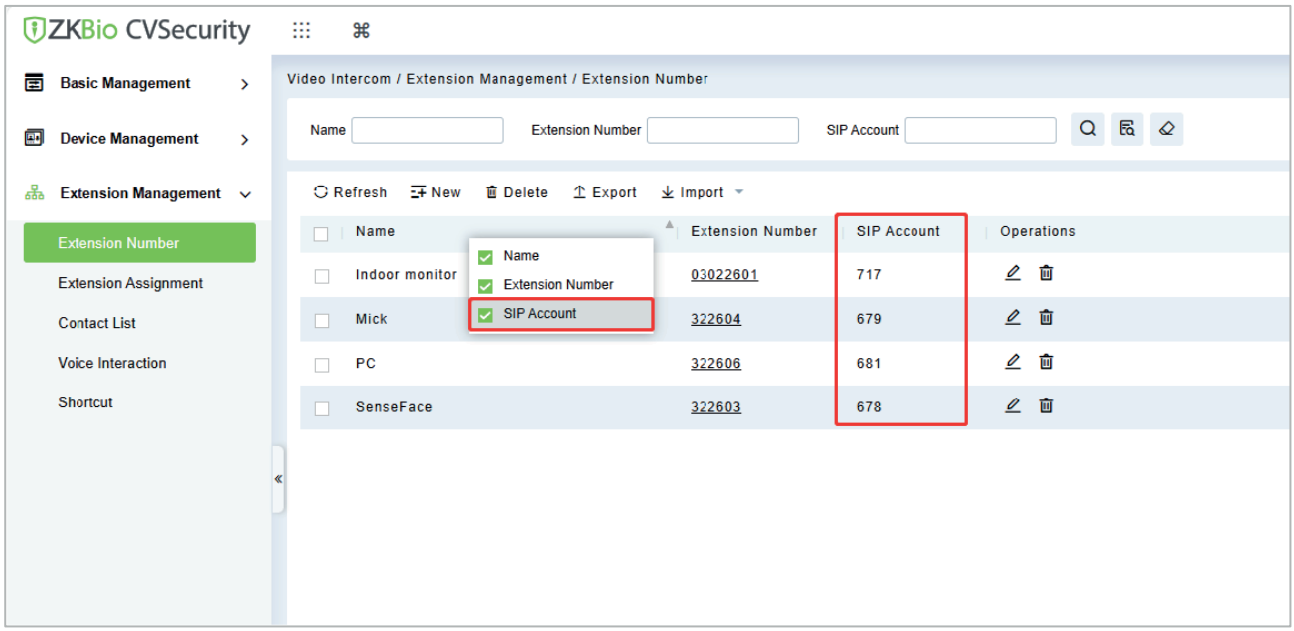
- **Nombre:** Personaliza el nombre de la extensión. Si se trata de una escena residencial, el nombre se puede establecer en el número de habitación; Si se trata de una escena de oficina, el nombre se puede establecer en el número de trabajo y la información del nombre.
- **Tipo de extensión:** SIP por defecto.
- **Número de extensión:** Personalice el número de extensión, puede ser de hasta 8 dígitos; por ejemplo, el número de la habitación 401, unidad 2, edificio 1 se puede definir como 01020401 para una rápida identificación interna.

- **Contraseña de extensión:** Contraseña de la cuenta SIP del usuario, que se puede utilizar para solicitar el registro de la cuenta desde el servicio SIP.
- **Recuento de terminales registrados** El número máximo de terminales que un usuario puede registrar con el mismo número. Cuando el número de registros simultáneos es 1, significa que los nuevos registros pueden adelantarse a la dirección de registro. Cuando el número de registros simultáneos es 2 o más, los nuevos registros se bloquearán automáticamente una vez que el número de registros alcance el límite.

Después de que el usuario cree el número de extensión, el sistema generará automáticamente una cuenta SIP. Por ejemplo, suponiendo que el usuario ha creado el número de extensión 322603, el sistema genera automáticamente la cuenta SIP como 678, por lo que el nombre de usuario SIP utilizado en el terminal es 678.

Nota:

1) La columna Cuenta SIP está oculta de forma predeterminada. Puede hacer clic con el botón derecho en la fila en la que se encuentra Operaciones y verificar la cuenta SIP para mostrarla.

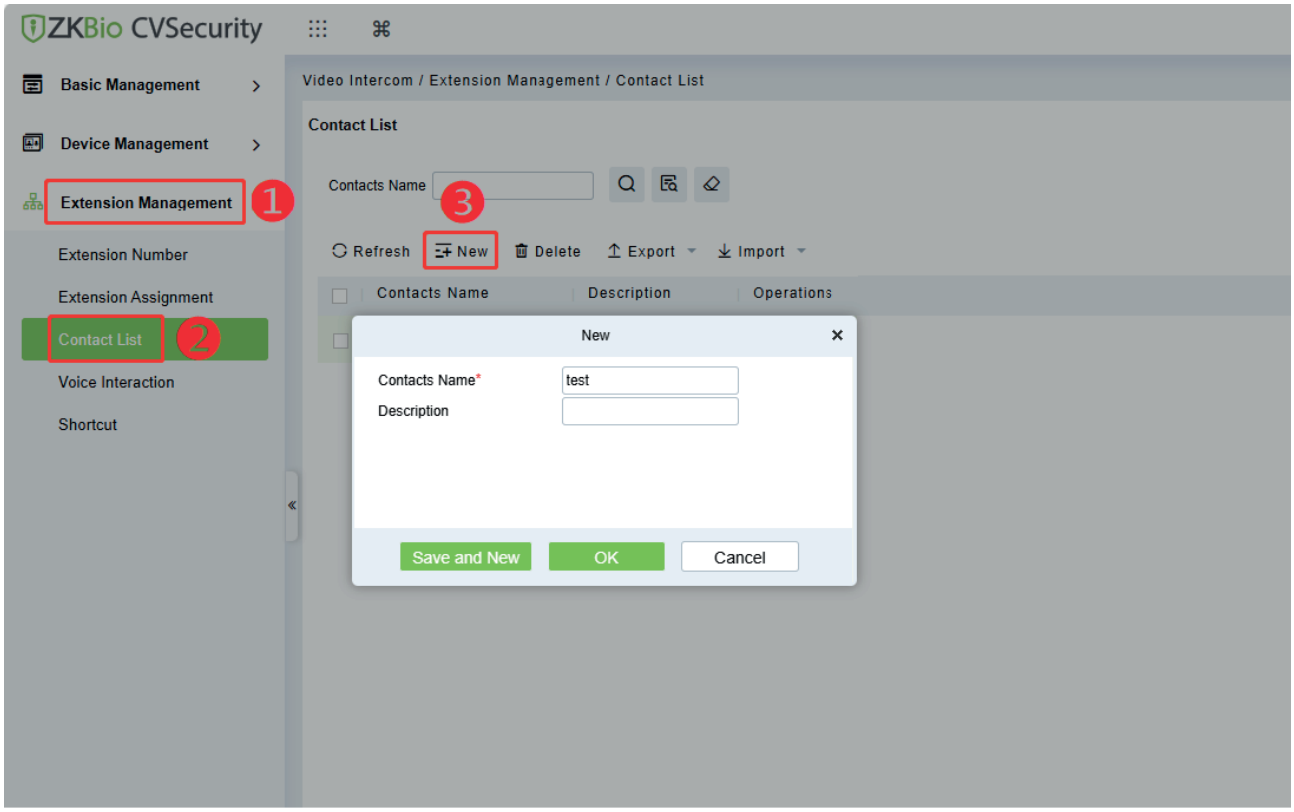


2) Si utiliza una centralita, el número de extensión se utilizará directamente y la lista de cuentas SIP estará vacía.

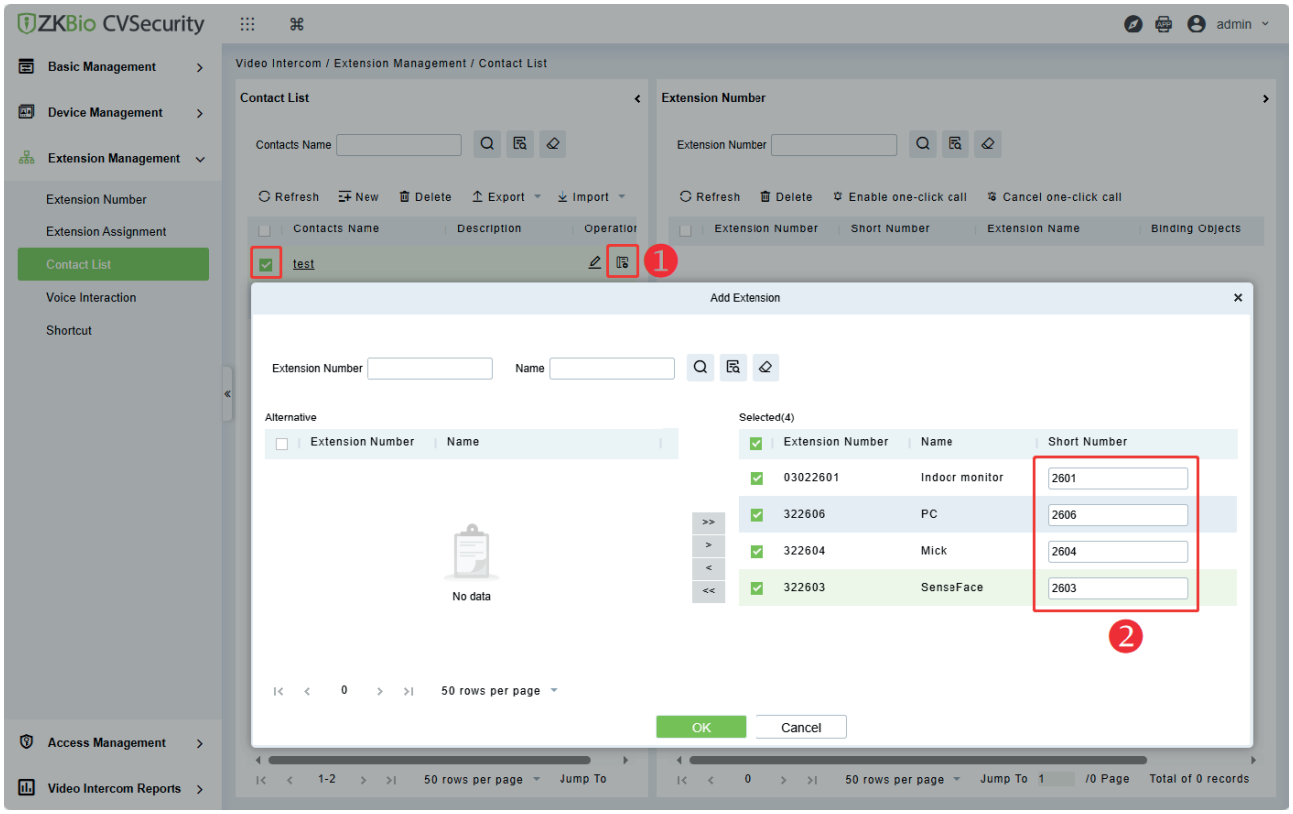
20.2.4 Lista de contactos

Si necesita habilitar diferentes dispositivos o personal para ver un número limitado de contactos, puede configurar la lista de contactos

1. Haga clic en Administración de extensiones > lista de contactos > Nuevo para crear una lista de contactos



2. Haga clic en el icono para añadir números de extensión a la lista de contactos. Durante el proceso de añadir números de extensión, puede definir un número corto para la extensión a la derecha, por ejemplo, si el número de la habitación 1101 se define como 101. Después de definir y sincronizar el número corto con el dispositivo, este podrá marcar el número corto 101 para llamar a esa habitación.



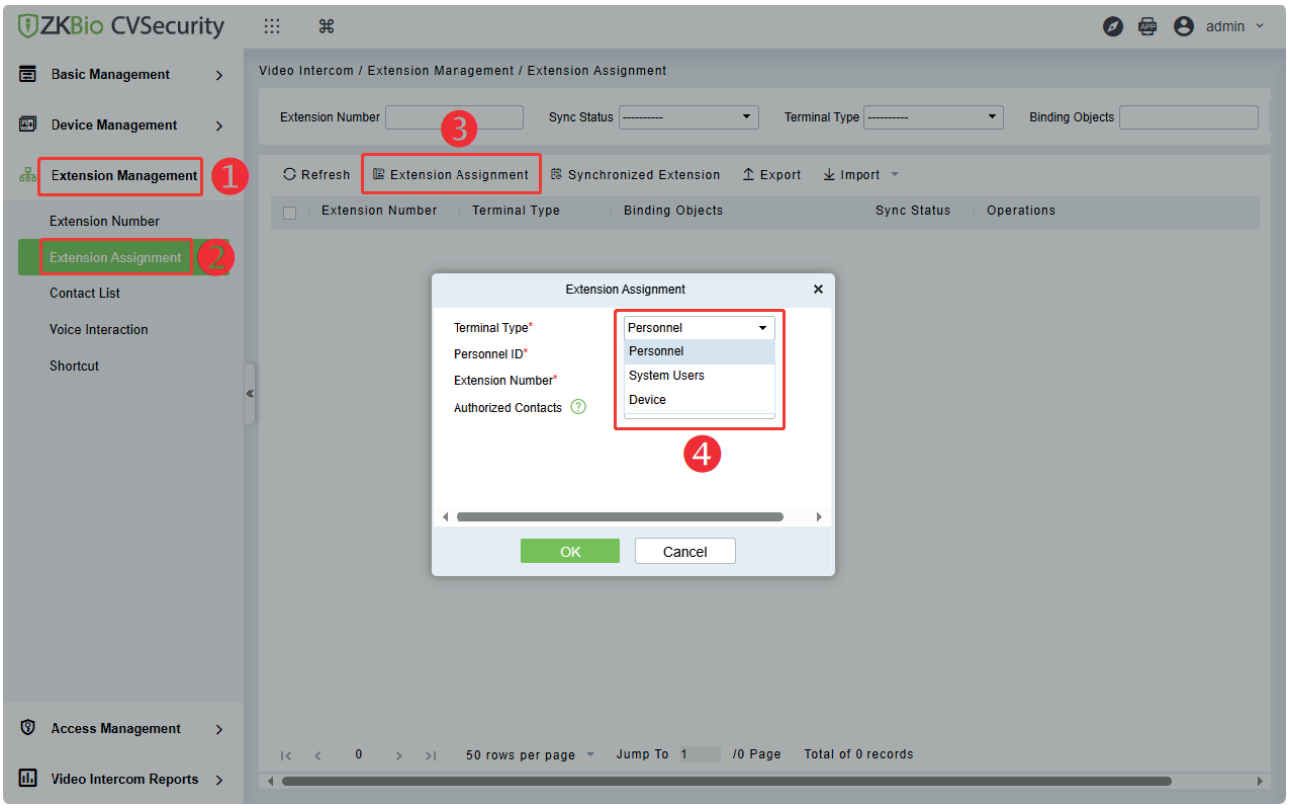
Nota:

1) Si añades un número de extensión a la lista de contactos sin editar el número corto y deseas editarlo más tarde, tendrás que eliminar el número de extensión de ese contacto y luego editarlo al volver a añadirlo, o bien eliminarlo y utilizar la función de importación posteriormente.
2) Si el dispositivo está configurado como terminal de valla, no defina el número corto de los monitores interiores. Solo tiene que introducir el bloque, la unidad y el número de habitación para llamar al monitor interior.

20.2.5 Asignación de números de extensión y cuentas SIP

El número de extensión o la cuenta SIP se puede asignar al personal, a los dispositivos o a los usuarios del sistema. Después de la asignación, el personal y la aplicación de los usuarios podrán utilizar directamente el videoportero para la comunicación. El dispositivo también se puede utilizar directamente sin configuración adicional manual.

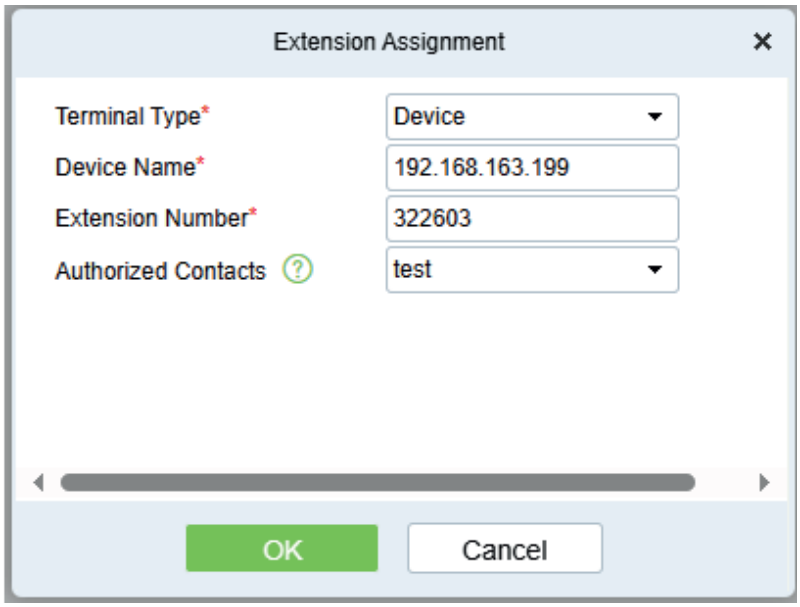
Haga clic en Administración de extensiones > Asignación de extensiones > Asignación de extensiones, seleccione el TerminalType.



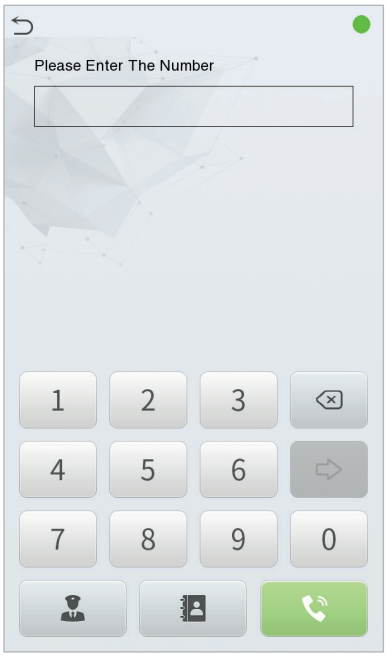
- **Asignación de cuentas de dispositivos**

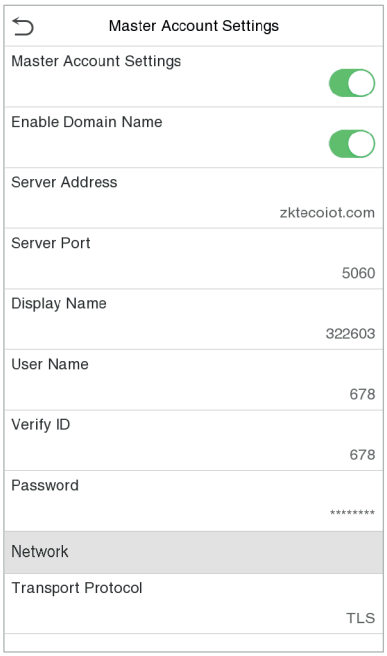
1. Seleccione el tipo de terminal como dispositivo.

2. Seleccione el dispositivo que debe vincularse (dispositivo o monitor interior) y el número de extensión. La información de la cuenta se sincronizará automáticamente con el dispositivo. Seleccione AuthorizedContacts para asignar la lista de contactos al dispositivo; Solo después de la asignación, el dispositivo puede llamar a números de habitación/ números cortos o realizar llamadas a través de la búsqueda de la lista de contactos.



3. Después de una asignación exitosa, aparecerá un punto verde en la esquina superior derecha de la página de llamada, lo que indica que el dispositivo está conectado al servidor. También puede introducir Intercomunicador > Configuración SIP >Configuración local > Configuración de cuenta maestra para ver que la información del servidor SIP y de la cuenta se ha escrito automáticamente, como se muestra en la siguiente figura.

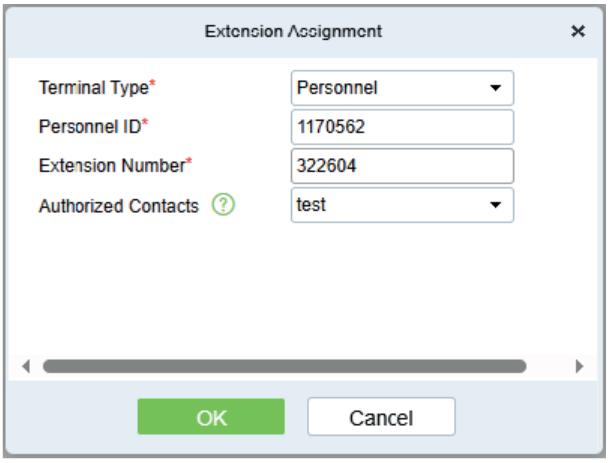




Imputación de personal (aplicación ZKBio Zexus)

1. Seleccione el tipo de terminal como personal.

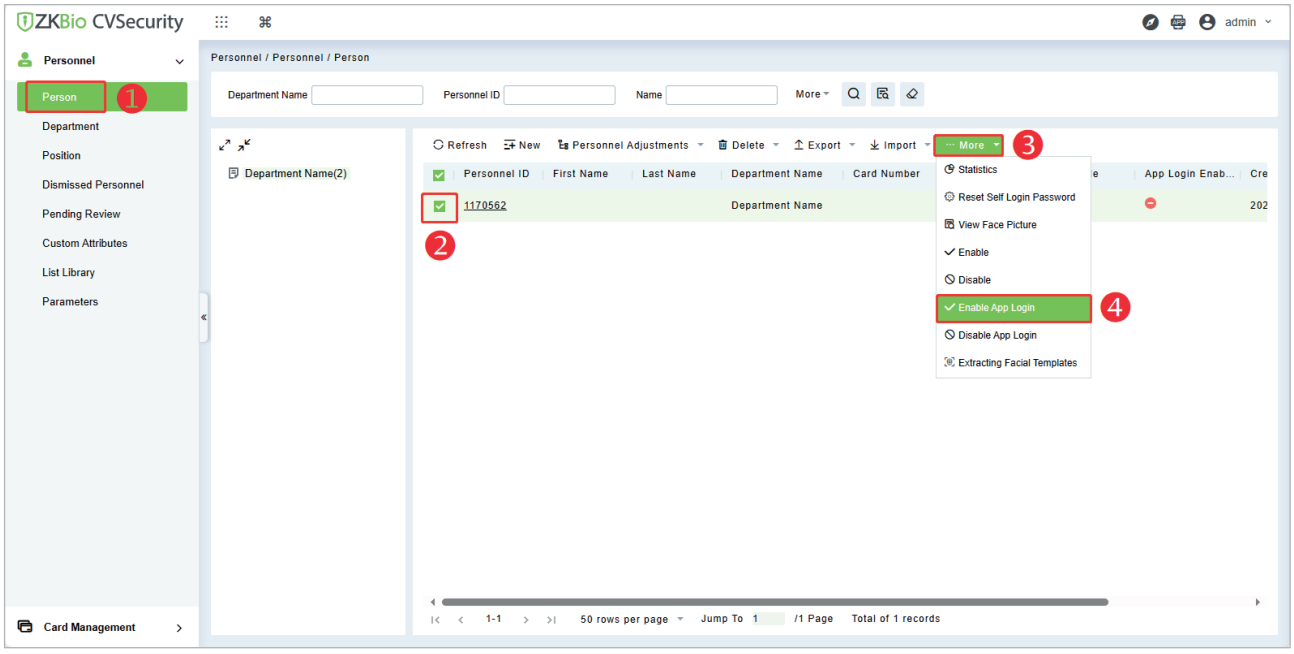
2. Seleccione la persona a la que se le asignará una cuenta y el número de extensión. Seleccione los Contactos autorizados para asignar la lista de contactos a la persona, y después de la asignación, la persona puede ver los contactos en la lista de contactos al iniciar sesión en la aplicación ZKBio Zexus.



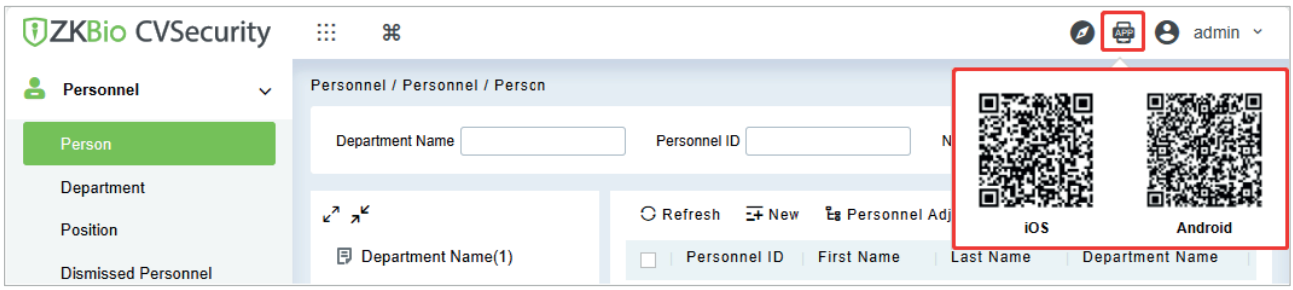
Nota:

1) Antes de asignar una cuenta al personal, primero debe añadir al personal en ZKBio CVSecurity. El método para añadirlo se puede consultar en 17. Conectarse al software ZKBio CVSecurity.

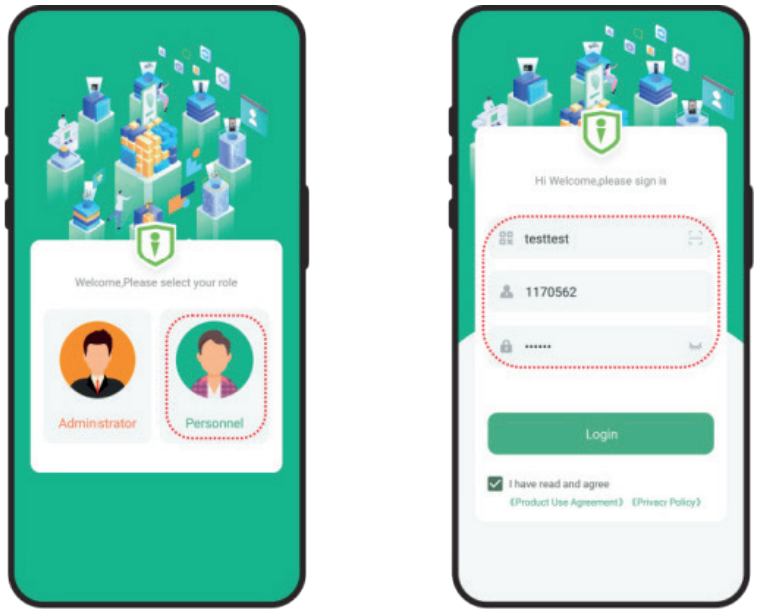
2) El personal debe habilitar el inicio de sesión en la aplicación. (Haga clic en Personal > Personal > Persona > Más > Habilitar inicio de sesión en la aplicación). Una vez que una persona ha habilitado el inicio de sesión en la aplicación, puede acceder directamente a la función de videoportero al iniciar sesión en la aplicación.



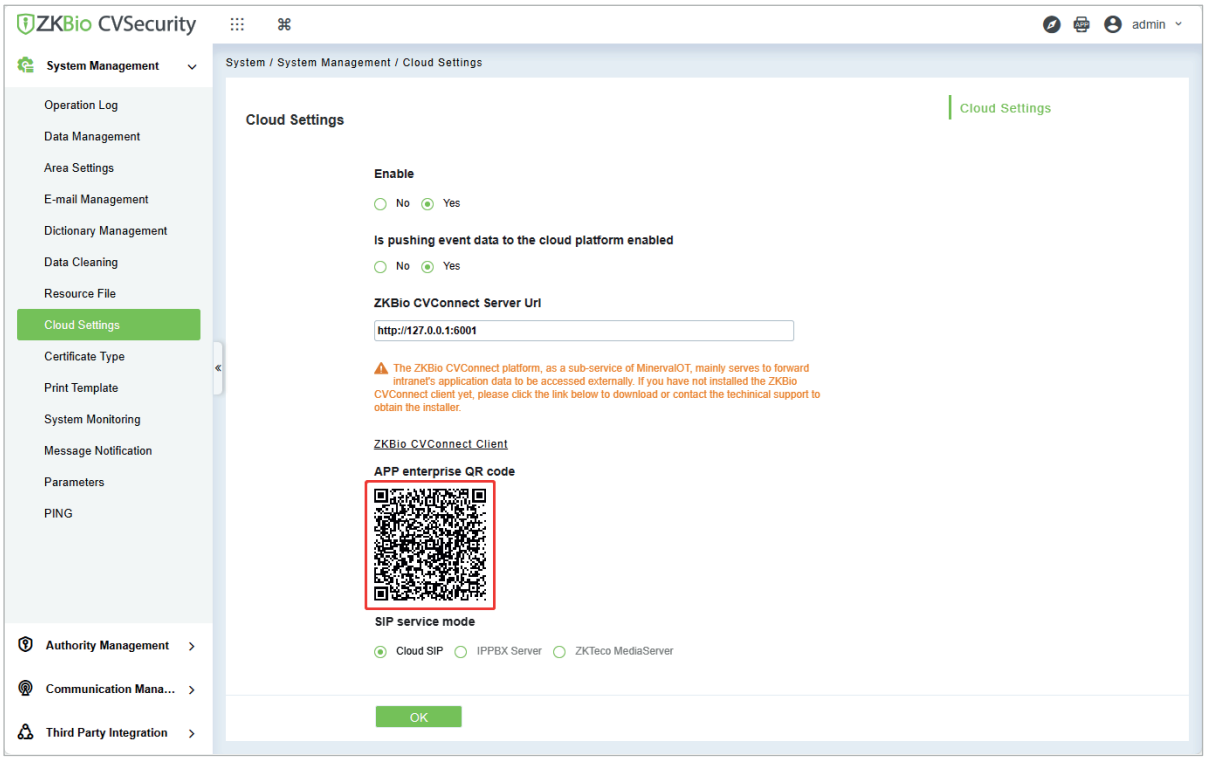
3) Puede hacer clic en el icono  situado en la esquina superior derecha de la interfaz de ZKBio CVSecurity para escanear el código QR e instalar la aplicación ZKBio Zexus.

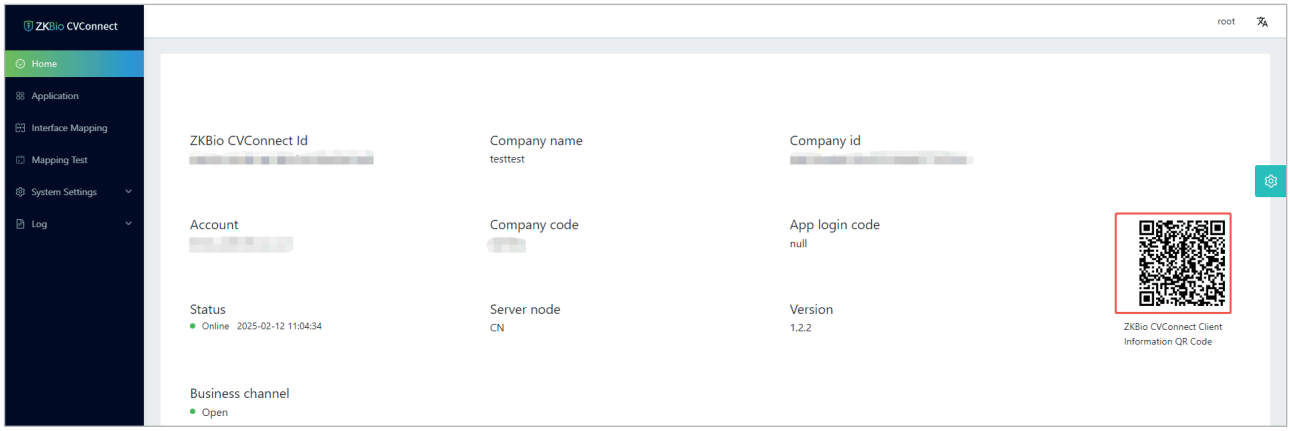


4) Después de una asignación exitosa, el personal puede iniciar sesión en la aplicación. Seleccione el rol-Personal , ingrese la información de la cuenta y haga clic en Iniciar sesión



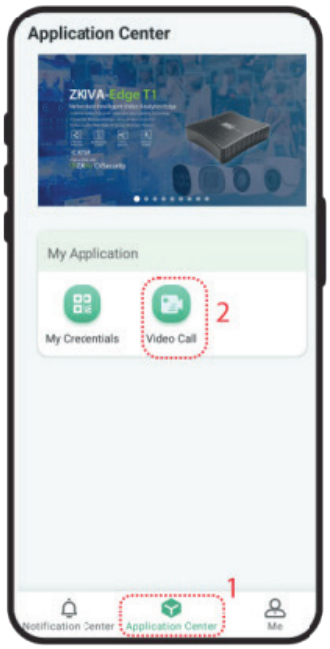
Nombre de la organización: Escanee el código de la organización que obtuvo anteriormente. (Vaya a la web de ZKBio CVSecurity, entre en Sistema > Gestión del sistema > Configuración de la nube > Código QR de la empresa APP, o vaya al cliente ZKBio CVConnect, escanee el código QR de información del cliente ZKBio CVConnect). Cuenta y contraseña: El ID y la contraseña del personal (por defecto: 123456); la misma cuenta y contraseña que ZKBio CVSecurity.



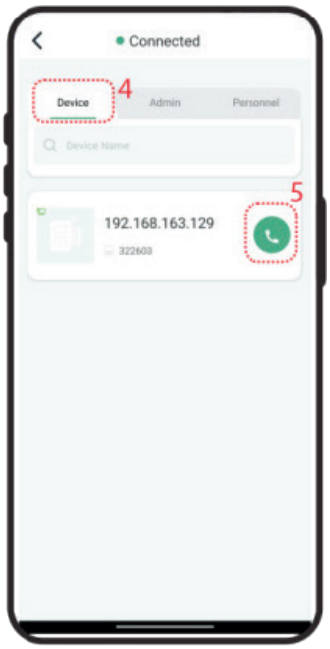


Cuenta y contraseña: El ID y la contraseña del personal (por defecto: 123456); La misma cuenta y contraseña que ZKBio CVSecurity

5) Haga clic en Centro de aplicaciones > Videollamada para acceder a la aplicación de videollamadas, y el estado se mostrará como Conectado. Si la persona no ha asignado un número de extensión, al acceder a la aplicación aparecerá el mensaje «No ha asignado un número de extensión, póngase en contacto con el administrador». A continuación, puede introducir directamente el número de extensión del dispositivo o hacer clic en el icono para buscar el dispositivo y llamarlo.

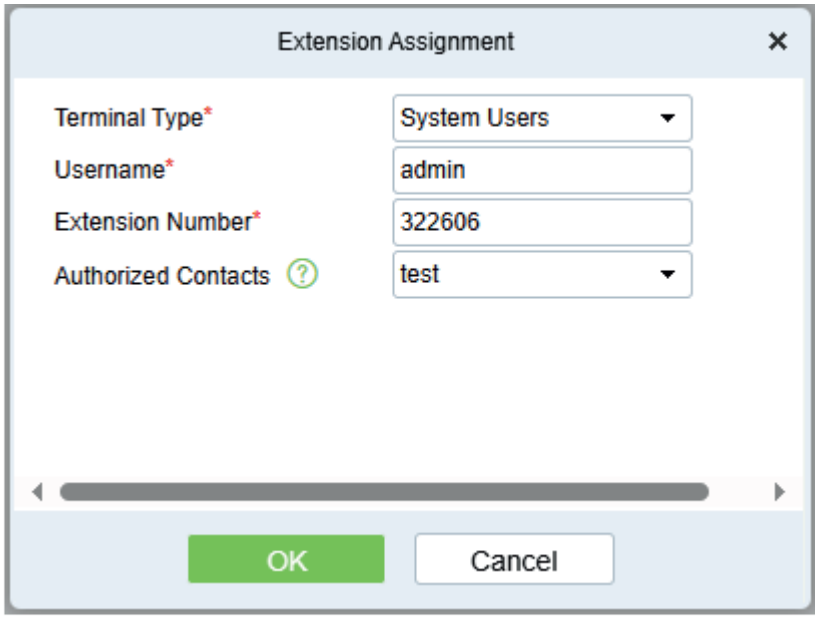






Asignación de cuentas de usuario del sistema (aplicación ZKBio Zexus)

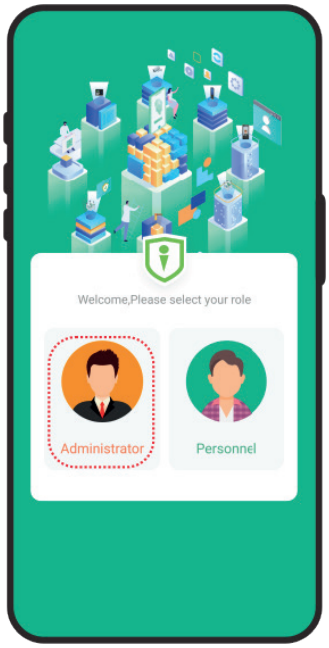
1. Seleccione el tipo de terminal como usuarios del sistema
2. Seleccione el usuario del sistema al que se le asignará una cuenta y el número de extensión. Seleccione los contactos autorizados para asignar la lista de contactos al administrador y, tras la asignación, el administrador podrá ver los contactos de la lista de contactos al iniciar sesión en la aplicación ZKBio Zexus.

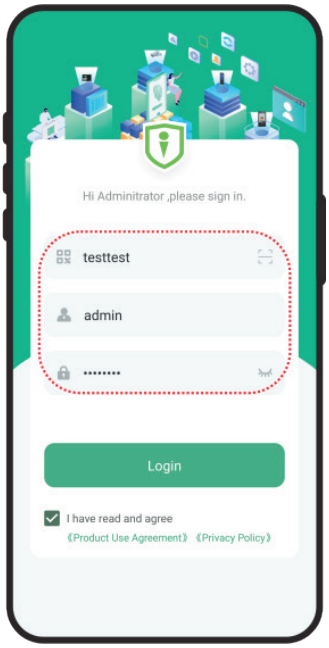


3. Después de una asignación exitosa, el administrador puede iniciar sesión en la aplicación. Seleccione el rol-Administrador, ingrese la información de la cuenta y haga clic en Iniciar sesión.

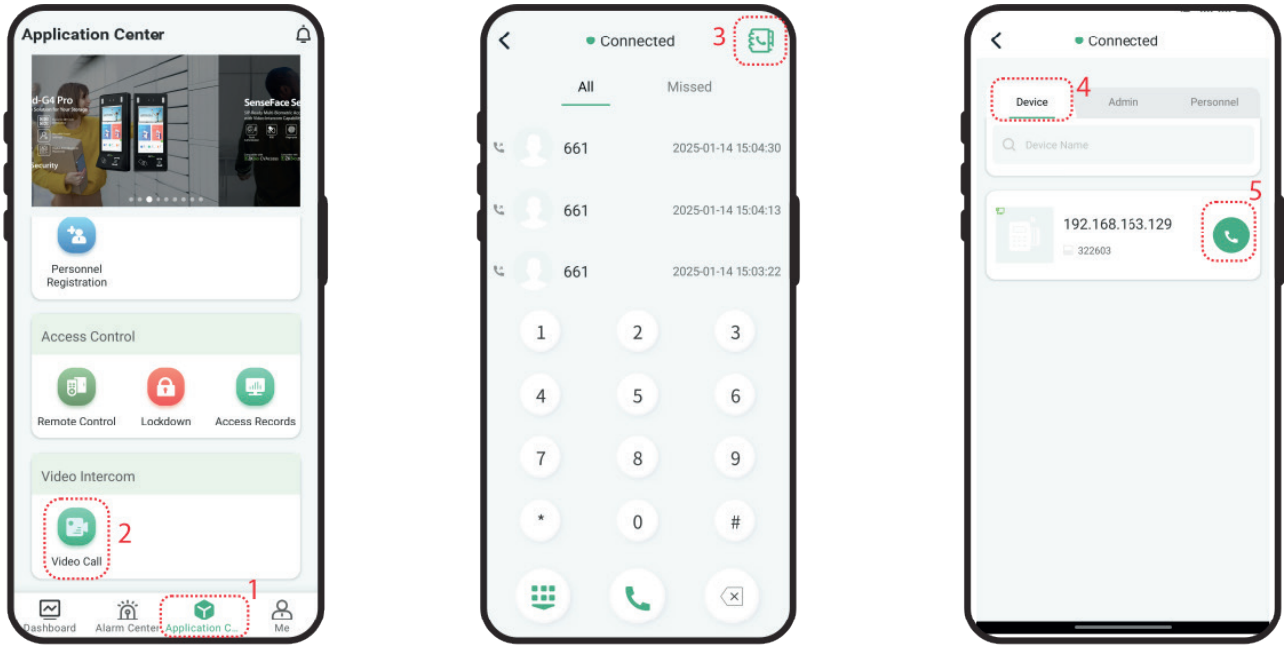
Nombre de la organización: Escanee el código de organización que obtuvo antes.

Cuenta y contraseña: La cuenta de administrador; La misma cuenta y contraseña que ZKBio CVSecurity





4. Haga clic en Centro de aplicaciones > videollamada para ingresar a la aplicación de videollamada, y el estado se mostrará como Conectado. Luego, puede ingresar directamente el número de extensión del dispositivo o hacer clic en el icono para buscar el dispositivo y llamarlo.



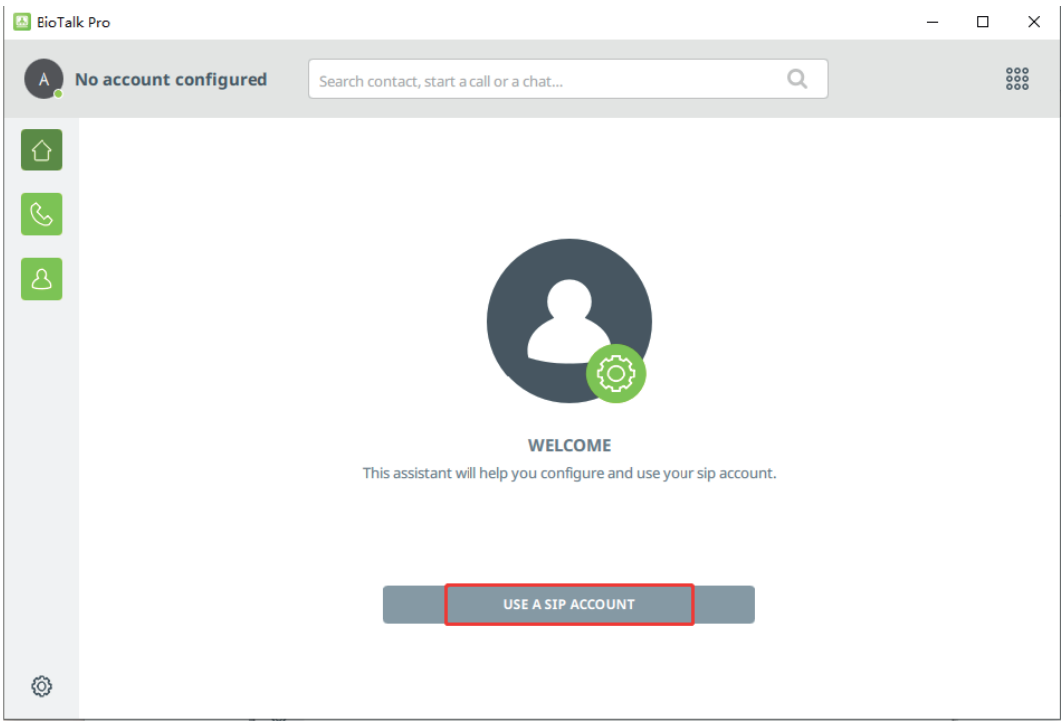
Para conocer los pasos completos de funcionamiento de la aplicación, consulte el Manual del usuario de la aplicación móvil ZKBio Zexus.

20.2.6 Funcionalidad del cliente para PC

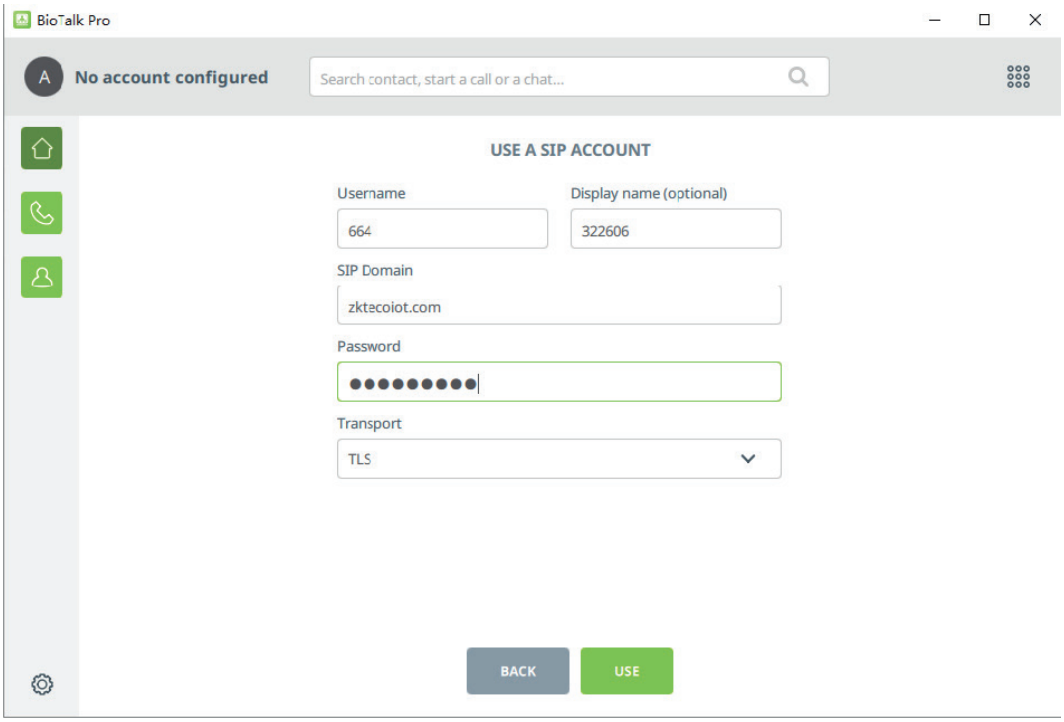
Para utilizar el cliente BioTalk Pro para PC, póngase en contacto con la persona adecuada para obtener un paquete de instalación.

Guía de operación

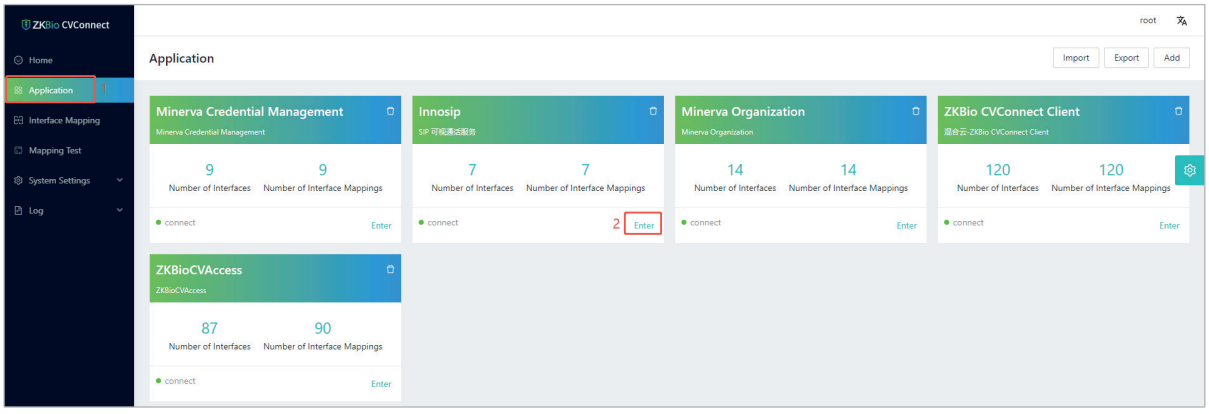
Paso 1: Configurar la cuenta SIP: Haga clic en el botón **USAR UNA CUENTA SIP.**

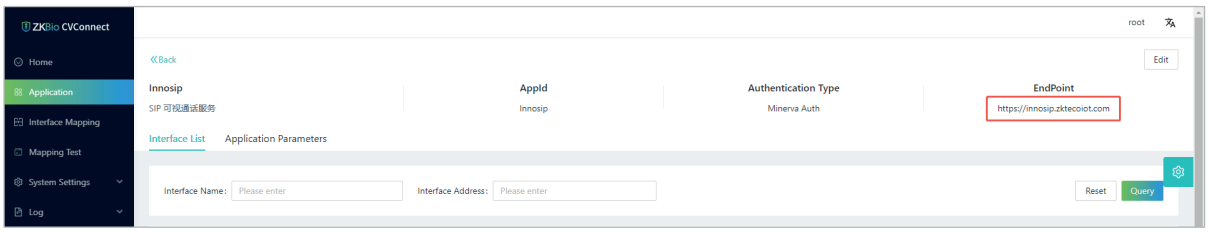


Paso 2: Complete la información de la cuenta SIP en orden y haga clic en **USAR.**



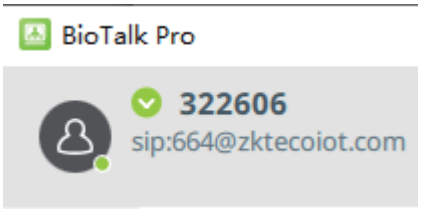
- **Nombre de usuario:** Introduzca la cuenta SIP. (Nota: Debe crear una nueva cuenta SIP para el cliente de PC en ZKBio CVSecurity, luego puede usar la cuenta para iniciar sesión en el cliente de PC)
- **Nombre para mostrar:** Es el número de extensión.
- **Dominio SIP:** El dominio del servidor SIP. (Vaya al cliente ZKBio CVConnect, haga clic en Aplicación > Innosip > Introduzca, la dirección del punto de conexión es "https://innosip.zktecoiot.com". Entonces 'zktecoiot.com' es el domian del servidor SIP real que debe ingresar en el cliente de PC)





- **Contraseña:** La contraseña de extensión de la cuenta SIP para el cliente de PC.
- **Transporte:** Protocolo de transporte, TLS de forma predeterminada.

Espere 1 minuto hasta que el estado muestre Conectado, como se muestra a continuación:

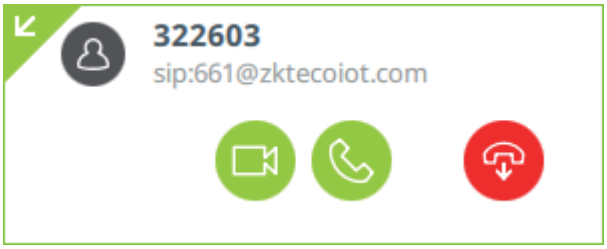


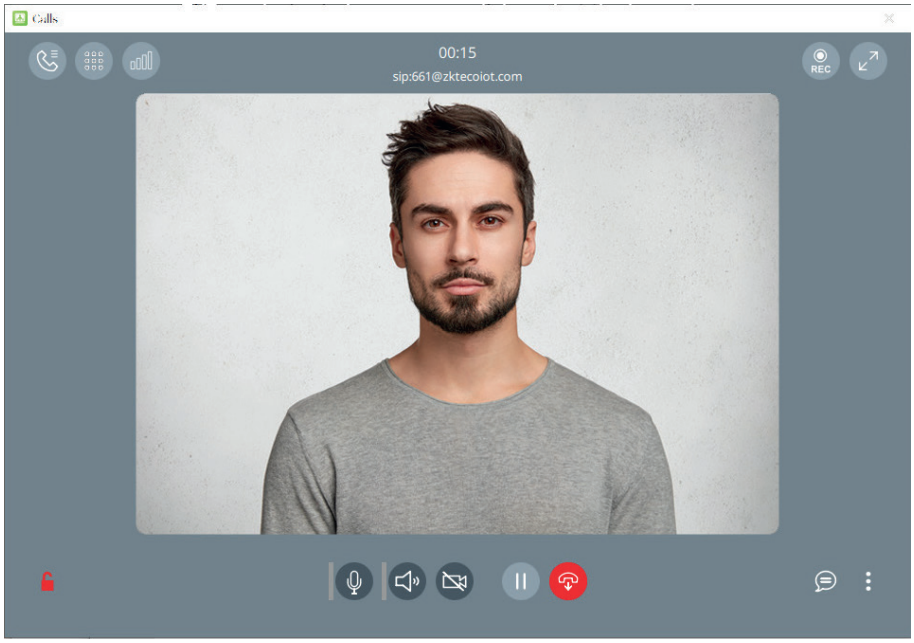
Nota: En el modo Cloud SIP, si es necesario marcar, el cliente PC debe marcar directamente la cuenta SIP de destino. Por ejemplo, si el número de extensión creado en ZKBio CVSecurity es 322603, la cuenta SIP generada correspondiente es 661, por lo que el cliente PC debe marcar 661 al realizar una llamada. Por lo tanto, se recomienda crear directamente un contacto en la libreta de direcciones con el número 661.

En este punto, ya puede empezar a utilizarlo con normalidad: el cliente de PC, el dispositivo y la aplicación pueden llamarse y responderse entre sí.

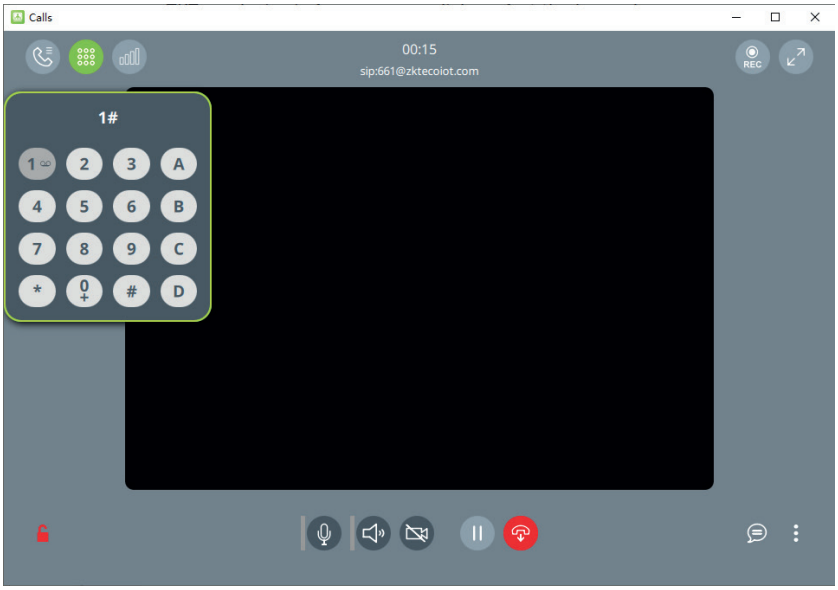
Cuando el cliente de PC reciba una llamada, aparecerá una alerta de ventana en la esquina inferior derecha del escritorio.

Haga clic en el icono para aceptarlo.





Puede abrir la puerta haciendo clic en el teclado e ingresando el valor DTMF del dispositivo, por ejemplo, el valor predeterminado del dispositivo ZKTeco es 1, por lo que puede hacer clic en 1 en el teclado.



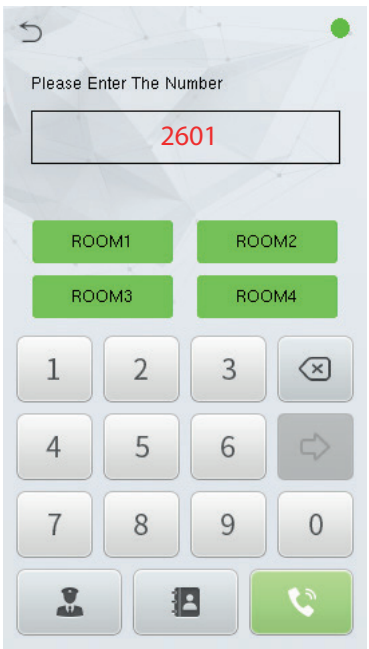
20.2.7 Hacer una llamada

Se pueden realizar llamadas bidireccionales entre el dispositivo, el monitor interior, la aplicación ZKBio Zexus y el cliente de PC (BioTalk Pro).

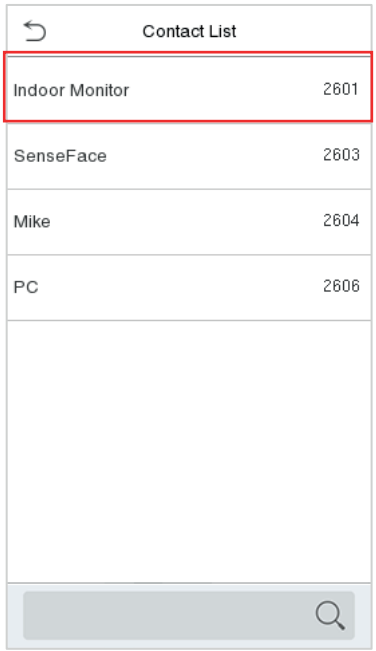
- **Llamada del dispositivo al monitor interior (VT07-B26L-W / VT07-B22L)**

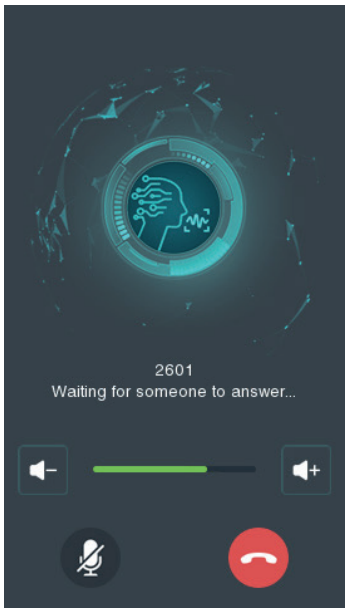
1. Añada el monitor interior al software ZKBio CVSecurity y, a continuación, asigne un número de extensión al monitor interior. (Los pasos de funcionamiento se pueden consultar en 20.2.2 Añadir dispositivo y 20.2.5 Asignación de números de extensión y cuentas SIP).

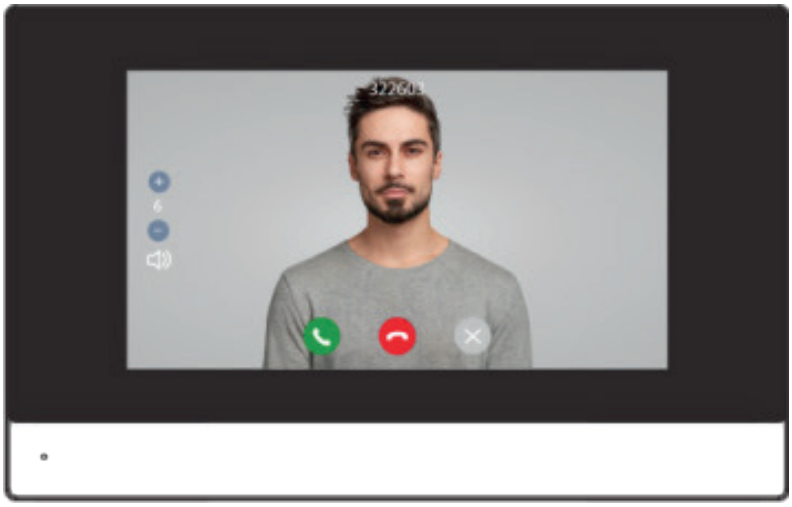
2. Haga clic en el icono del dispositivo e introduzca el número corto del monitor interior en la interfaz emergente del dispositivo. O haga clic en el icono de la página de llamadas para abrir la lista de contactos y buscar el monitor interior al que desea llamar.



o

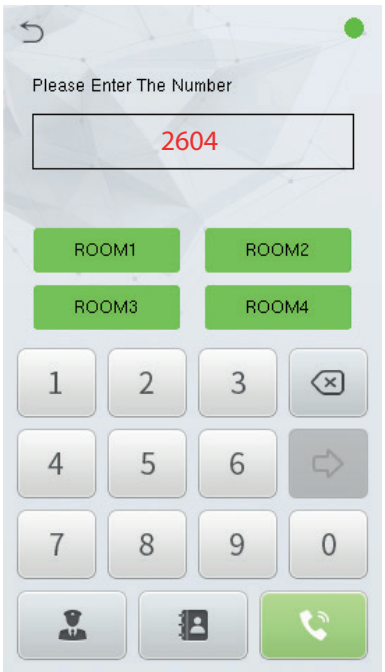




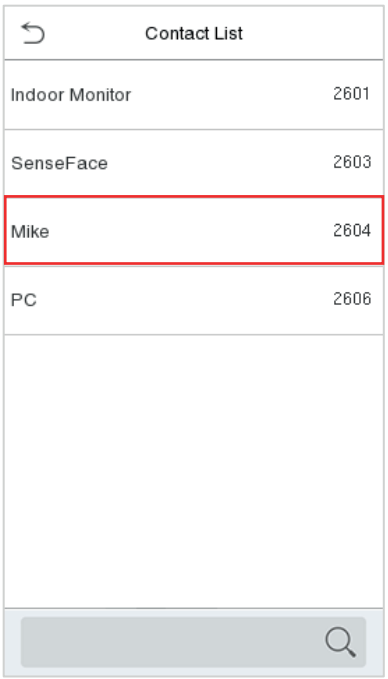


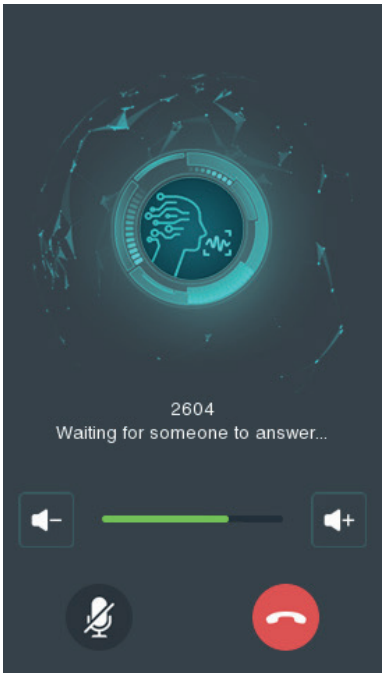
- **Dispositivo Llamar al teléfono (aplicación ZKBio Zexus)**

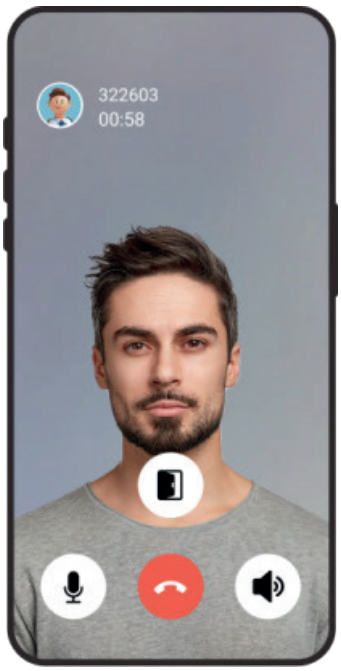
1. En el software ZKBio CVSecurity, asigne un número de extensión al personal. (Los pasos de la operación se pueden consultar en 20.2.5 Asignación de números de extensión y cuentas SIP).
2. Haga clic en el icono del dispositivo e introduzca el número corto del empleado en la interfaz emergente del dispositivo. O haga clic en el icono de la página de llamadas para abrir la lista de contactos y buscar al empleado al que desea llamar.



o



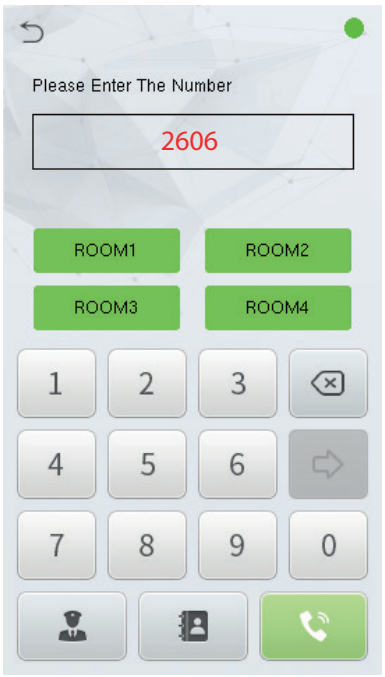




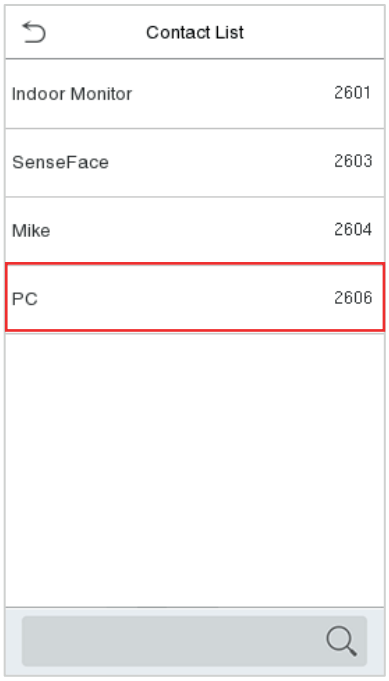
Llamada del dispositivo al cliente de PC (BioTalk Pro)

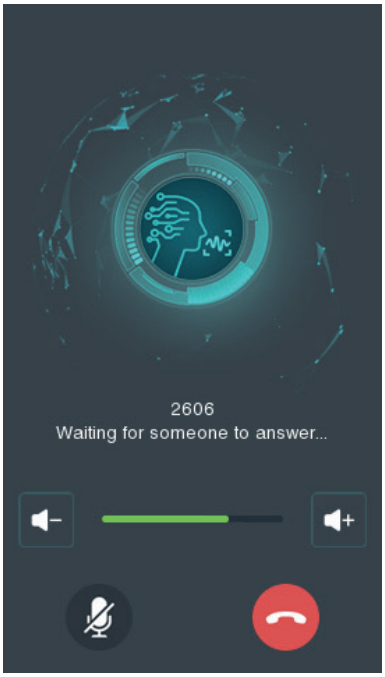
1. Instale el software BioTalk Pro y configure la cuenta SIP. (Los pasos de operación se pueden consultar en 20.2.6 Funcionalidad del cliente PC).

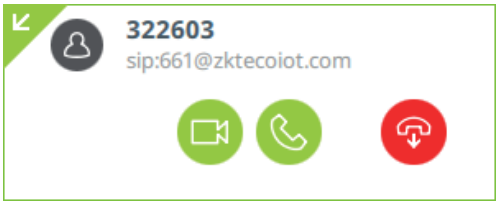
2. Haga clic en el icono del dispositivo e introduzca el número corto del cliente PC en la interfaz emergente del dispositivo. O haga clic en el icono de la página de llamadas para abrir la lista de contactos y buscar el cliente PC al que desea llamar.

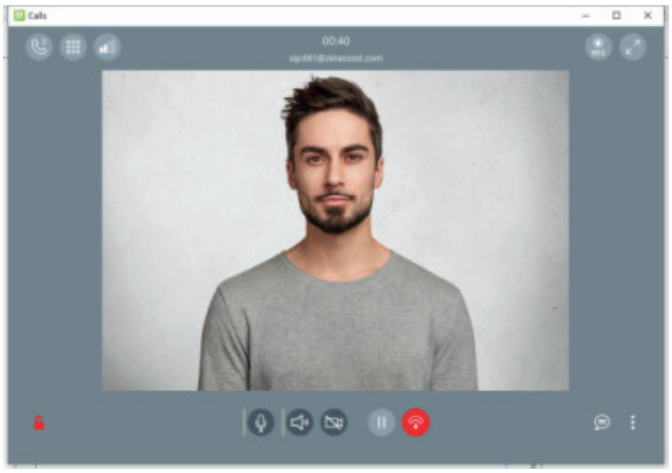


o



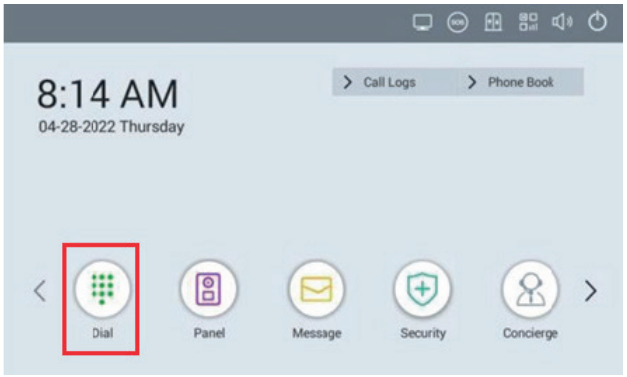


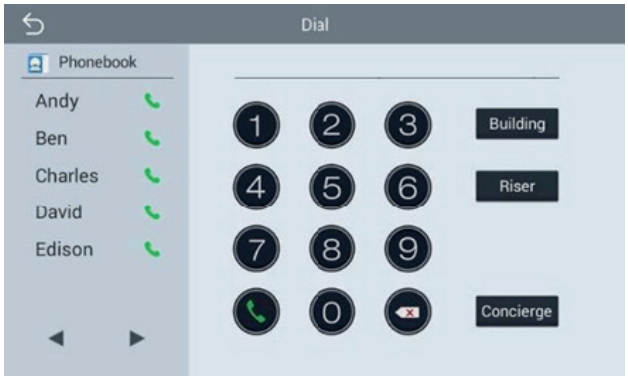




- **Llamada de monitor interior**

Haga clic en el icono Marcar, luego ingrese la cuenta SIP para realizar una llamada.



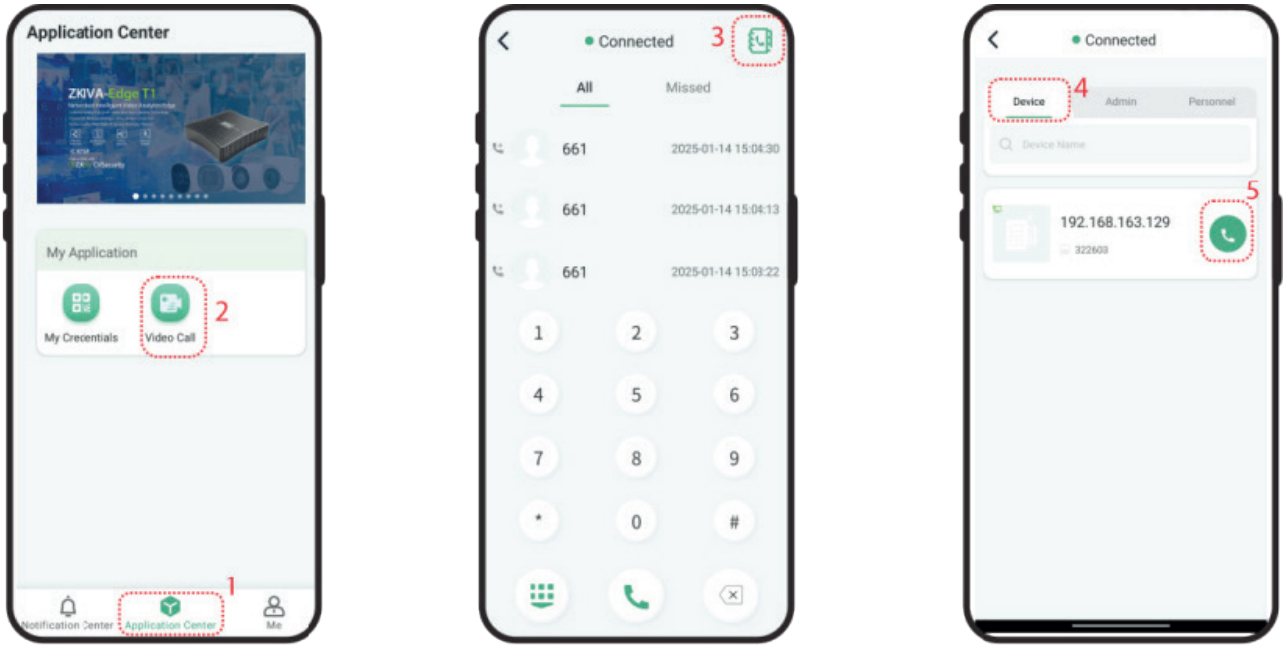


Nota: El monitor interior no es compatible con la asignación de la lista de contactos en ZKBio CVSecurity.

- **Llamada telefónica**

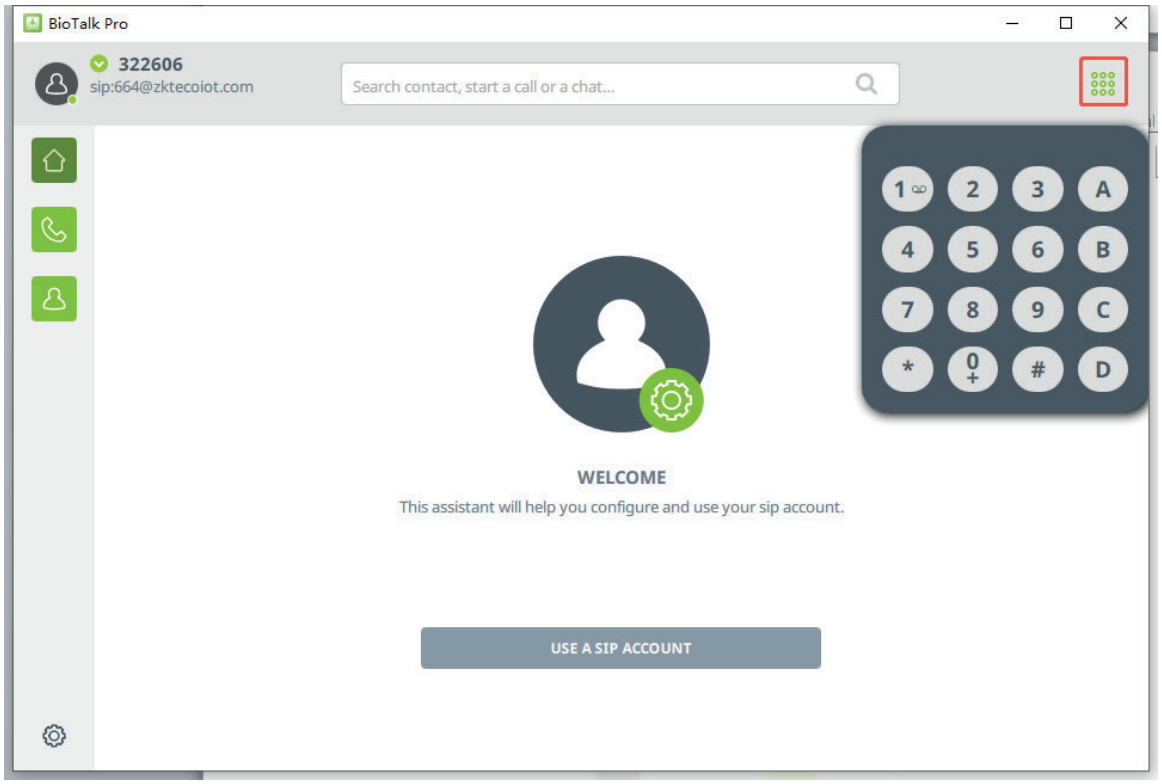
Inicie sesión en la aplicación ZKBio Zexus, haga clic en Centro de aplicaciones > Videollamada para acceder a la aplicación de videollamadas.

A continuación, puede introducir directamente el número de extensión o hacer clic en el icono para buscar a la persona a la que desea llamar.

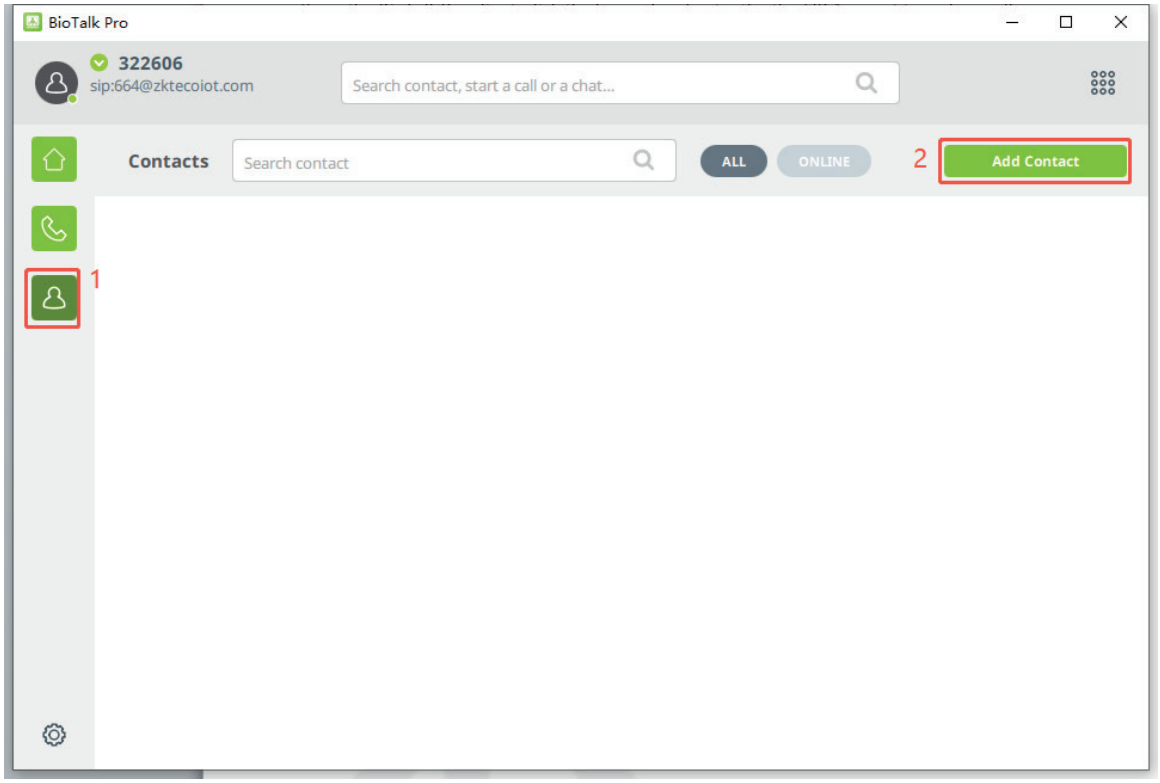


Cliente PC (BioTalk Pro) Llamada

Abra el cliente BioTalk Pro, haga clic en el teclado e ingrese la cuenta SIP para realizar una llamada.



Puede hacer clic en el botón > Agregar contacto para agregar la lista de contactos manualmente.


BioTalk Pro
322606
sip:664@zktecoiot.com
Search contact, start a call or a chat...
Contacts
Search contact
ALL
ONLINE
2
Add Contact
1

21. Conexión a la aplicación móvil ZKBio Zlink

Las páginas de la aplicación móvil pueden variar según la versión, y el documento es solo para referencia.

Cambie el protocolo de comunicación del dispositivo al protocolo BEST, luego el dispositivo puede ser administrado por ZKBio Zlink, consulte la configuración del tipo de dispositivo 8.5

- **Descargue la aplicación móvil ZKBio Zlink**

Busque la aplicación móvil "ZKBio Zlink" en iOS App Store o Google Play Store. O escanee el código QR a continuación para instalar la aplicación.

Apple App Store

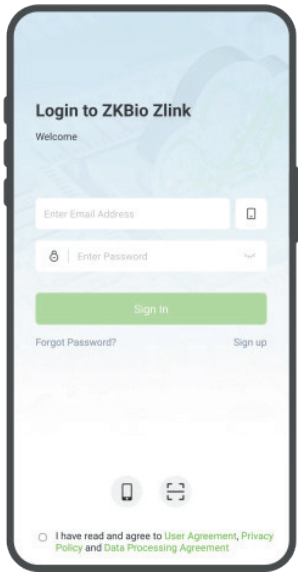
Google Play Store

Download on the App Store

GET IT ON Google Play

21.1 Inicie sesión en la aplicación móvil

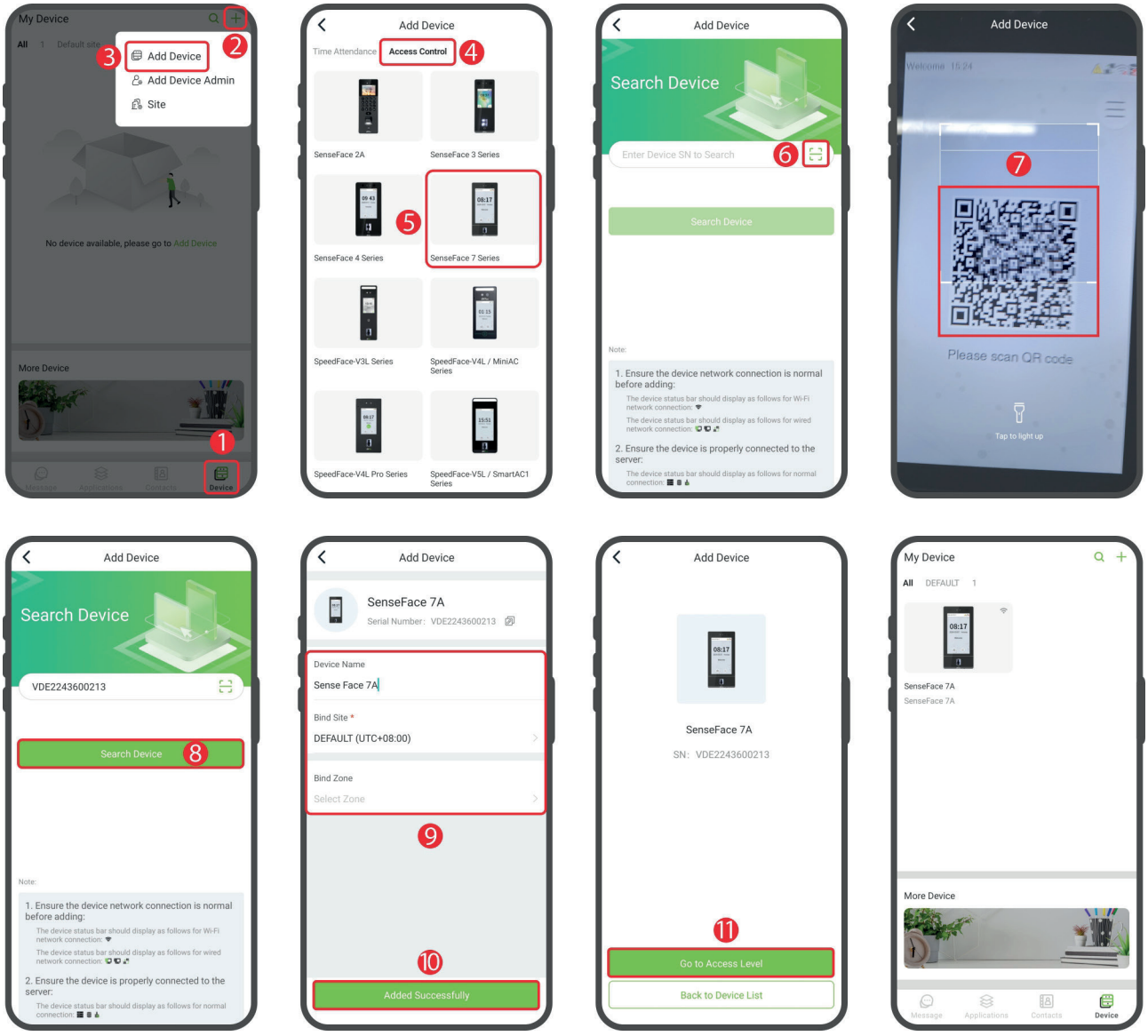
Ingrese su cuenta registrada y contraseña, marque "He leído y acepto el Acuerdo de usuario, la Política de privacidad y el Acuerdo de procesamiento de datos" y haga clic en Iniciar sesión para iniciar sesión en la aplicación móvil.



Nota: *Para obtener más operaciones, consulte el manual de usuario de la aplicación ZKBio Zlink.*

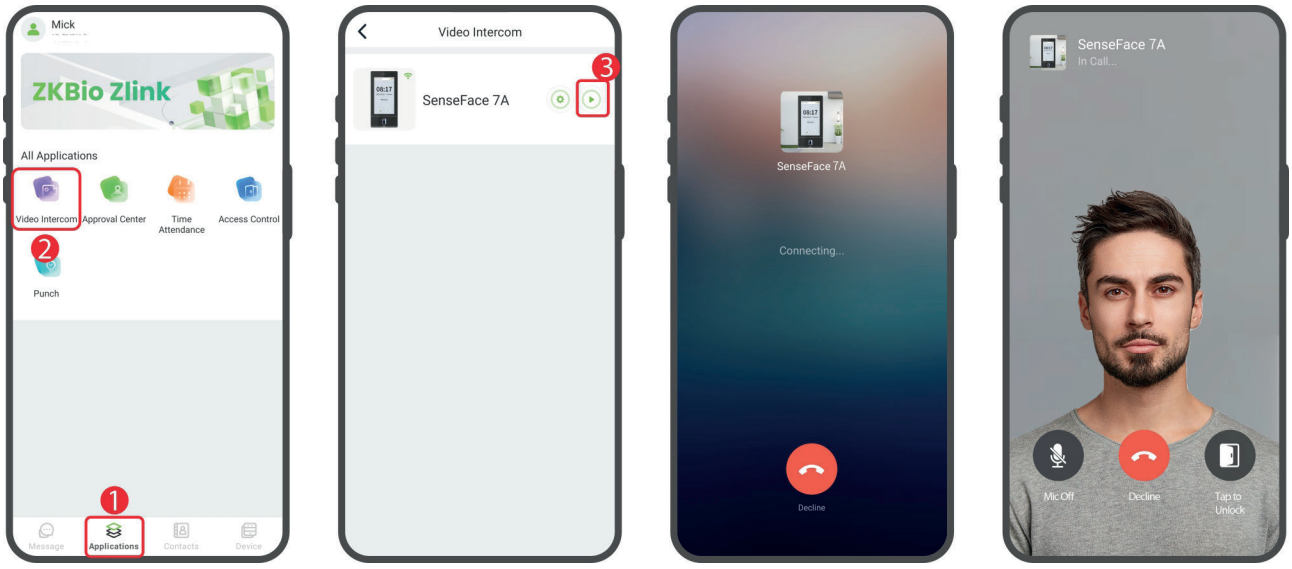
21.2 Agregar dispositivo en la aplicación móvil

1. Acceda a la aplicación móvil ZKBio Zlink y haga clic en [Dispositivo] > icono + > [Agregar dispositivo] > [AccessControl] > [SenseFace 7 Series]
2. Haga clic en el icono para escanear el código QR en el dispositivo. El número de serie del dispositivo se mostrará en la barra. A continuación, haga clic en [Buscar dispositivo].
3. Introduzca el nombre del dispositivo y especifique el dispositivo en un sitio y una zona. Haga clic en [Agregado correctamente] para completar la adición. Al mismo tiempo, el dispositivo indica por voz "El dispositivo se ha agregado correctamente", lo que indica que la adición se ha completado
4. Una vez agregado con éxito, el dispositivo se muestra en la lista de la interfaz del dispositivo. A continuación, puede configurar los niveles de acceso y la función de videoportero según sea necesario



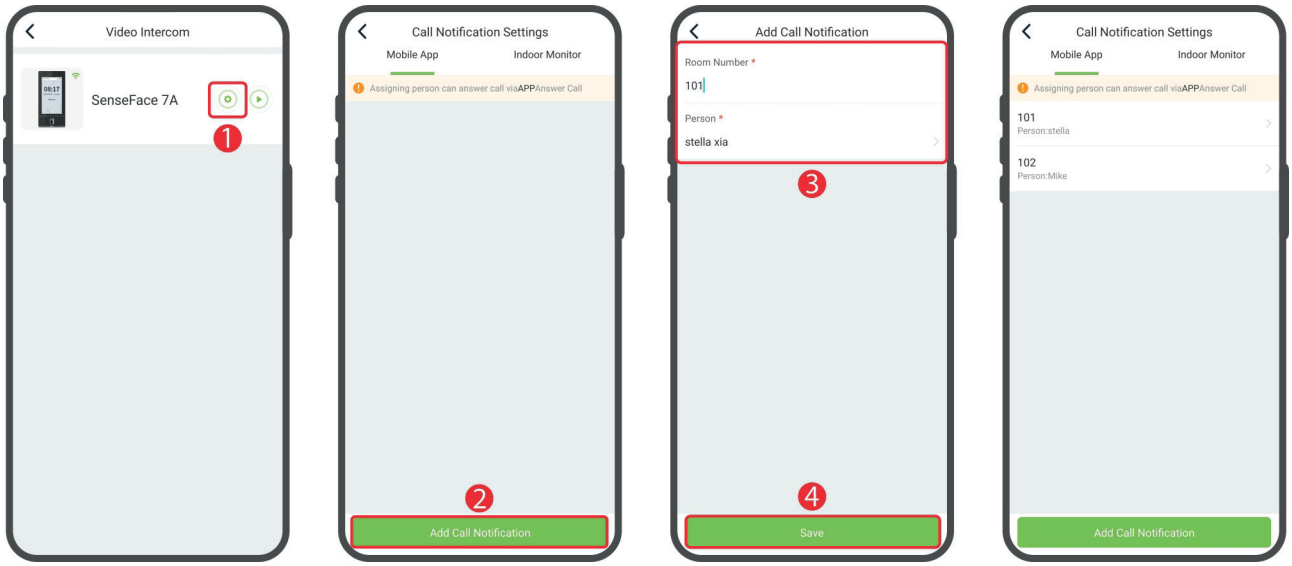
21.2.1 Videoportero

1. Haga clic en [Aplicaciones] > [Videoportero] > icono para llamar al dispositivo. Haga clic en el icono Tocar para desbloquear para abrir la puerta de forma remota.

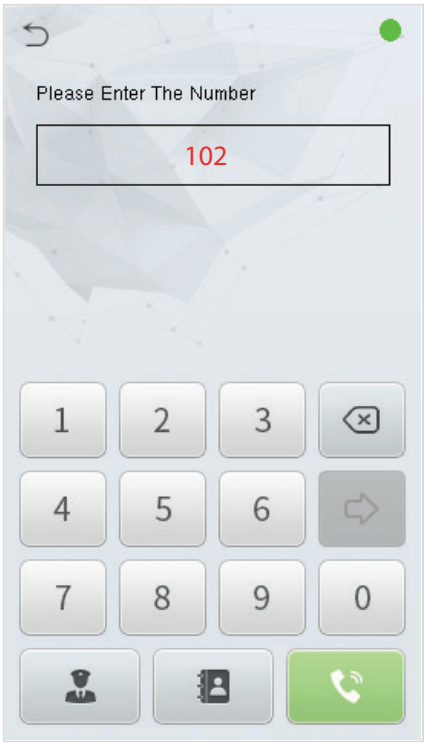


2. Haga clic en el icono > [Añadir notificación de llamada] para asignar a la persona que puede responder a la llamada a través de la aplicación.

- **Número de habitación:** Personalice el número de la persona.
- **Persona:** Se puede seleccionar una o varias personas. Si se seleccionan varias personas, todas ellas recibirán la llamada cuando el dispositivo marque el número..

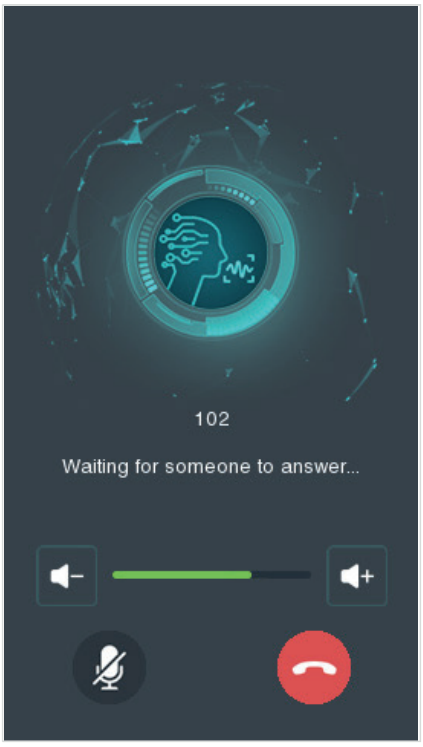


3. Una vez completada la configuración, puede pulsar la tecla del dispositivo e introducir el número de la persona en la interfaz emergente del dispositivo para llamarla


Please Enter The Number
102
1
2
3
4
5
6
7
8
9
0

or


Contact List
101
stella xia
101
102
Mike
102
103
104
105


102
Waiting for someone to answer...


SenseFace 4A
In Call...
Mic Off
Decline
Tap to Unlock

22. Conexión al portal web ZKBio Zlink

Las páginas del portal web pueden variar en función de la versión, y el documento es solo de referencia

Cambie el protocolo de comunicación del dispositivo al protocolo BEST, luego el dispositivo puede ser administrado por ZKBio Zlink, consulte la configuración del tipo de dispositivo 8.5

Los usuarios pueden usar la cuenta creada para acceder al portal web ZKBio Zlink para conectar dispositivos, agregar nuevo personal, registrar el método de verificación del personal registrado, sincronizar el personal con los dispositivos y consultar registros.

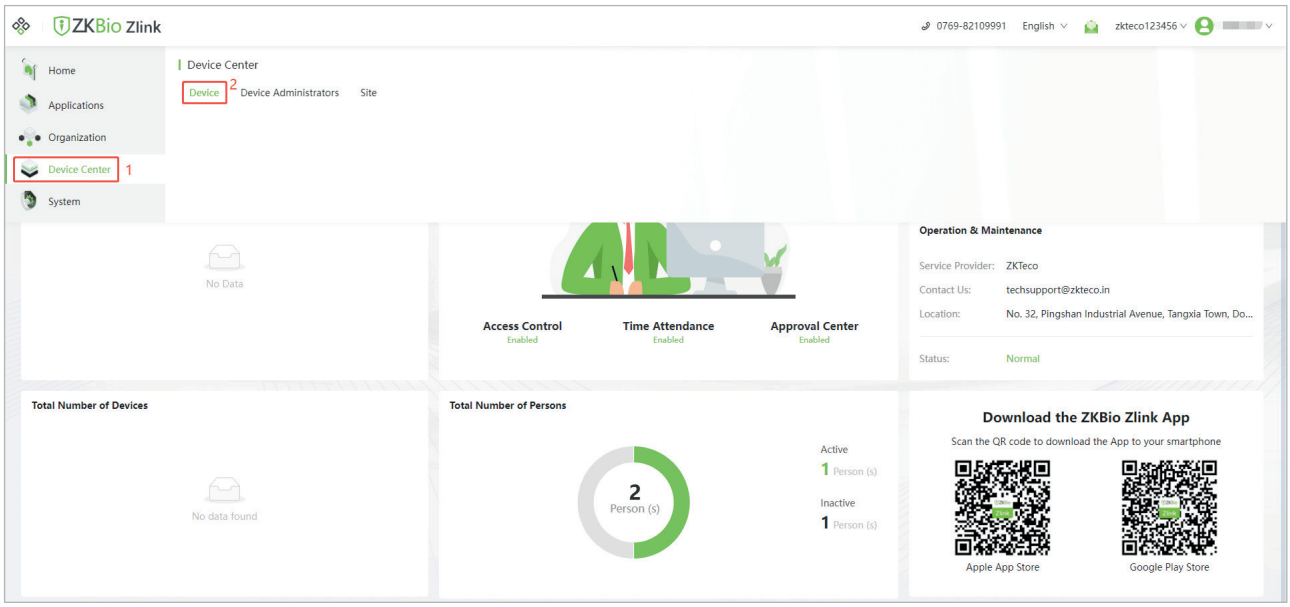
22.1 Inicie sesión en el portal web

1. Abra el navegador recomendado e ingrese la dirección IP para acceder al portal web ZKBio Zlink: http://zlink.minervaiot.com.
2. Ingrese a su cuenta registrada en la pantalla de inicio de sesión, marque "He leído y acepto el Acuerdo de usuario y la Política de privacidad y el Acuerdo de procesamiento de datos" y haga clic en [Iniciar sesión] para iniciar sesión.

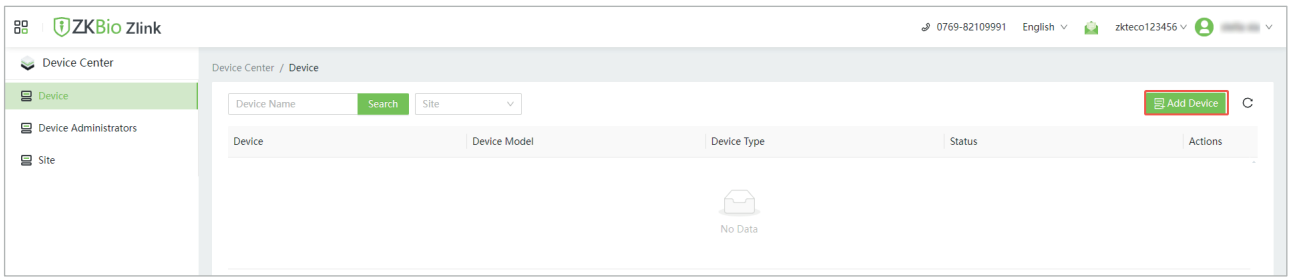


22.2 Agregar dispositivo en el portal web

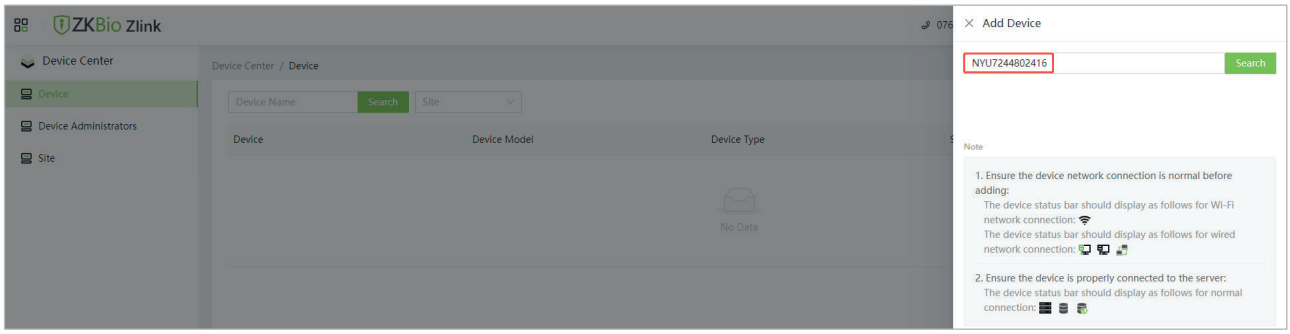
1. Haga clic en el icono de la esquina superior izquierda y seleccione [Centro de dispositivos] > [Dispositivo] para acceder a la interfaz de configuración del dispositivo.



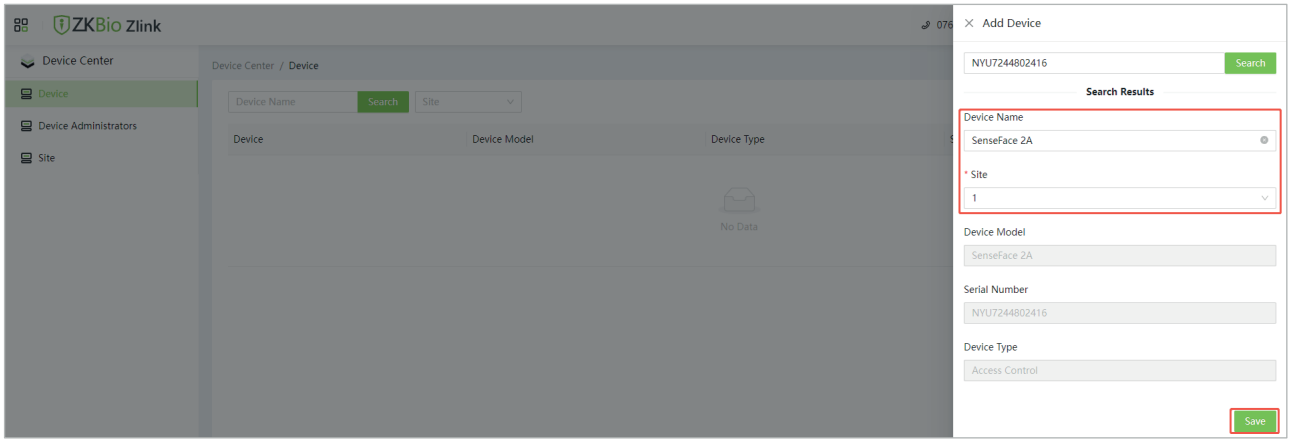
2. A continuación, haga clic en [Añadir dispositivo] para entrar en la interfaz Añadir dispositivo.



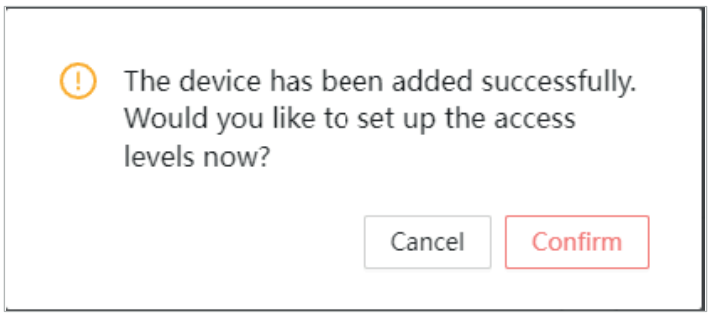
3. Introduzca el número de serie y haga clic en [Buscar].

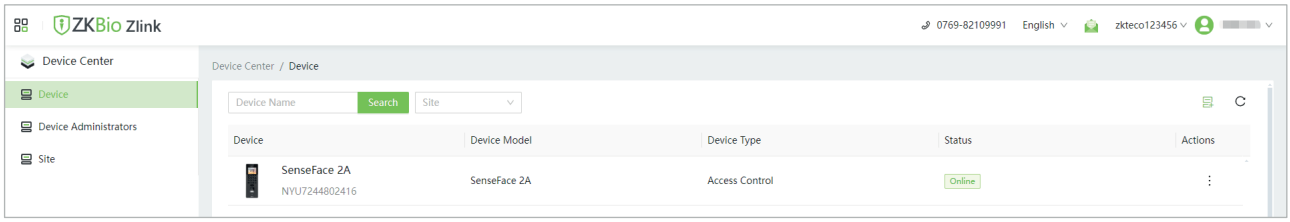


4. A continuación, introduzca el nombre del dispositivo y especifique el dispositivo en un sitio. Seleccione Sitio en el menú desplegable. Haga clic en [Guardar] para completar la adición



5. Una vez agregado el dispositivo, aparecerá el siguiente mensaje. Haga clic en Confirmar, ingresará directamente a la interfaz de configuración del nivel de acceso. Haga clic en Cancelar, el dispositivo se mostrará en la lista de dispositivos. Luego puede configurar los niveles de acceso según sea necesario





Nota: *: Espere un momento para que el estado del dispositivo cambie de "Sin conexión" a "En línea".*

Para obtener más información, consulte el Manual del usuario correspondiente.

Apéndice 1

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.