Manual de Usuario

F35

Fecha: Marzo 2026
Versión: 1.0

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 F35.

Todas las figuras mostradas son sólo para fines ilustrativos. Las figuras de este manual pueden no coincidir exactamente con los productos reales.

Convenciones del Documento

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

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

Símbolos

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

Contenido

1 MEDIDAS DE SEGURIDAD 9
2 SEGURIDAD ELÉCTRICA 10
3 SEGURIDAD EN EL FUNCIONAMIENTO 10
4 INSTRUCCIONES DE USO 11
4.1 POSICIÓN DE LOS DEDOS 11
4.2 INTERFAZ DE ESPERA 11
4.3 MODO DE VERIFICACIÓN 13
4.3.1 VERIFICACIÓN DE HUELLA DACTILAR 13
4.3.2 VERIFICACIÓN DE TARJETA 15
4.3.3 VERIFICACIÓN DE CONTRASEÑA 16
4.3.4 VERIFICACIÓN COMBINADA 17
5 RESUMEN 18
5.1 APARIENCIA 18
5.2 DESCRIPCIÓN DE LOS TERMINALES Y EL CABLEADO 19
5.2.1 DESCRIPCIÓN DE LOS TERMINALES 19
5.3 DESCRIPCIÓN DEL CABLEADO 20
5.3.1 CONEXIÓN DE ALIMENTACIÓN 20
5.3.2 SENSOR DE PUERTA, BOTÓN DE SALIDA, ALARMA Y CONEXIÓN AUXILIAR 20
5.3.3 CONEXIÓN DEL RELÉ DE BLOQUEO 20
5.3.4 CONEXIÓN WIEGAND 23
5.3.5 CONEXIÓN RS485 Y RS232 23
5.3.6 CONEXIÓN ETHERNET 24
6 INSTALACIÓN 25
6.1 ENTORNO DE INSTALACIÓN 25
6.2 INSTALACIÓN DEL DISPOSITIVO 25
7 MENÚ PRINCIPAL 26
8 GESTIÓN DE USUARIOS 27
8.1 REGISTRO DE NUEVOS USUARIOS 27
8.1.1 REGISTRAR UN ID DE USUARIO Y UN NOMBRE 27
8.1.2 ROL DEL USUARIO 28
8.1.3 REGISTRAR HUELLA DACTILAR 28
8.1.4 NÚMERO DE TARJETA 29
8.1.5 CONTRASEÑA 29
8.1.6 FUNCIÓN DE CONTROL DE ACCESO 30
8.2 TODOS LOS USUARIOS 30
8.2.1 EDITAR USUARIO 31
8.2.2 ELIMINAR USUARIO 31

8.3 ESTILO DE VISUALIZACIÓN....32
9 ROL DEL USUARIO....33
10 COMUNICACIÓN....35
10.1 ETHERNET....35
10.2 COMUNICACIÓN SERIE....36
10.3 CONEXIÓN PC....37
10.4 CONFIGURACIÓN DE WI-FI★....37
10.5 CONFIGURACIÓN DEL SERVIDOR EN LA NUBE....40
10.6 CONFIGURACIÓN WIEGAND....40
10.6.1 ENTRADA WIEGAND....41
10.6.2 SALIDA WIEGAND....43
10.7 DIAGNÓSTICO DE RED....44
11 CONFIGURACIÓN DEL SISTEMA....45
11.1 FECHA Y HORA....45
11.2 CONFIGURACIÓN DE REGISTROS DE ACCESO / ASISTENCIA....46
11.3 HUELLA DIGITAL....48
11.4 Parámetros DEL VIDEOPORTERO★....49
11.5 CONFIGURACIÓN ONVIF★....50
11.6 CONFIGURACIÓN DEL TIPO DE DISPOSITIVO....52
11.7 CONFIGURACIÓN DE SEGURIDAD....53
11.8 ACTUALIZAR FIRMWARE EN LÍNEA....54
11.9 RESTABLECIMIENTO DE FÁBRICA....54
12 PERSONALIZAR CONFIGURACIÓN....55
12.1 INTERFAZ DE USUARIO....55
12.2 VOZ....56
12.3 HORARIOS DE CAMPANAS....57
12.4 OPCIONES DE ESTADOS DE PERFORACIÓN....58
12.5 ASIGNACIONES DE TECLAS DE ACCESO RÁPIDO....59
13 GESTIÓN DE DATOS....62
14 CONTROL DE ACCESO....64
14.1 OPCIONES DE CONTROL DE ACCESO....65
14.2 CONFIGURACIÓN DE REGLAS DE TIEMPO / PROGRAMACIÓN HORARIA....68
14.3 DÍAS FESTIVOS....69
14.4 GRUPOS DE ACCESO....70
14.5 VERIFICACIÓN COMBINADA....71
14.6 CONFIGURACIÓN ANTIPASSBACK....72
14.7 CONFIGURACIÓN DE OPCIONES DE COACCIÓN....73
15 BÚSQUEDA DE ASISTENCIA....76

16 CONFIGURACIÓN DE IMPRESIÓN★ 77
16.1 CONFIGURACIÓN DEL CAMPO DE DATOS 77
16.2 CONFIGURACIÓN DE OPCIONES DE IMPRESIÓN 77
17 AUTOTEST 79
18 INFORMACIÓN DEL SISTEMA 80
19 CONECTAR AL SERVIDOR WEB 81
19.1 INICIAR SESIÓN EN EL SERVIDOR WEB 81
19.2 OLVIDÉ LA CONTRASEÑA 82
19.3 GESTIÓN DE USUARIOS 86
19.3.1 REGISTRO DE USUARIO 86
19.3.2 BÚSQUEDA DE USUARIOS 88
19.3.3 EDITAR USUARIO 88
19.3.4 ELIMINAR USUARIO 89
19.4 CONFIGURACIÓN AVANZADA 90
19.4.1 CONFIGURACIÓN DE COMUNICACIÓN 90
19.4.2 CONFIGURACIÓN DE CONEXIÓN 91
19.4.3 CONFIGURACIÓN DEL SERVICIO EN LA NUBE 91
19.4.4 CONFIGURACIÓN DE WI-FI★ 92
19.4.5 CONFIGURACIÓN DE LA FECHA 93
19.4.6 CONFIGURACIÓN DEL SISTEMA 94
19.4.7 INTERCOMUNICADOR DE VÍDEO★ 96
19.4.8 CONFIGURACIÓN SIP★ 96
19.4.9 CONFIGURACIÓN ONVIF★ 98
19.4.10 COMUNICACIÓN SERIE 99
19.4.11 CONFIGURACIÓN WIEGAND 100
19.4.12 OPCIONES DE CONTROL DE ACCESO 101
19.5 GESTIÓN DE DISPOSITIVOS 103
19.5.1 GESTIÓN DE DISPOSITIVOS 103
19.5.2 ACTUALIZACIÓN DE FIRMWARE 104
19.5.3 CAMBIAR CONTRASEÑA 105
19.5.4 REGISTRO DE OPERACIONES 105
19.5.5 DESCARGAR REGISTROS DE FIRMWARE 106
19.6 INFORMACIÓN DEL SISTEMA 107
20 CONECTAR AL SOFTWARE ZKBIO CVACCESS 108
20.1 CONFIGURAR LA DIRECCIÓN DE COMUNICACIÓN 108
20.2 AÑADIR DISPOSITIVO EN EL SOFTWARE 108
20.3 AÑADIR PERSONAL EN EL SOFTWARE Y REGISTRO DE HUELLAS DACTILARES EN LÍNEA 109
21 CONECTAR AL SOFTWARE ZKBIOTIME 8.0 111
21.1 CONFIGURAR LA DIRECCIÓN DE COMUNICACIÓN 111

21.2 AÑADIR DISPOSITIVO EN EL SOFTWARE....111
21.3 AÑADIR PERSONAL EN EL SOFTWARE Y REGISTRO DE HUELLAS DACTILARES EN LÍNEA....112
22 CONEXIÓN A LA APLICACIÓN ZSMART★ 114
22.1 AÑADIR DISPOSITIVO EN LA APLICACIÓN ZSMART 114
22.2 CONEXIÓN DEL VIDEOTELÉFONO....115
23 CONEXIÓN A SIP★ 116
23.1 USO DE LA RED DE ÁREA LOCAL....118
23.2 SERVIDOR SIP....120
24 CONEXIÓN AL TIMBRE INALÁMBRICO★ 122
24.1 CONECTAR EL TIMBRE INALÁMBRICO 122
24.2 DESVINCULAR EL TIMBRE INALÁMBRICO 122
24.3 CONFIGURACIÓN 123
APÉNDICE 1....124
POLÍTICA DE PRIVACIDAD 124
OPERACIÓN ECOLÓGICA 127

1 Medidas de Seguridad

Las siguientes instrucciones tienen por objeto garantizar que el usuario pueda utilizar el producto correctamente para evitar peligros o pérdidas materiales. Las siguientes precauciones tienen por objeto garantizar la seguridad delos usuarios y evitar cualquier daño. Léalas atentamente antes de la instalación.

El incumplimiento de las instrucciones podría provocar daños en el producto o lesiones físicas (incluso la muerte)

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. **Precauciones 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 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 derrama líquido o se cae algún objeto dentro del sistema.
   - Si el sistema se expone al agua o a condiciones climáticas adversas (lluvia, nieve, etc.).
   - Si el sistema no funciona con normalidad, según las instrucciones de funcionamiento.

Simplemente cambie los controles definidos en las instrucciones de funcionamiento. Un ajuste incorrecto de los controles puede provocar daños y requerir la intervención de un técnico cualificado para que el dispositivo vuelva a funcionar con normalidad.
No conecte varios dispositivos a un mismo adaptador de corriente, ya que la sobrecarga del adaptador puede provocar un sobrecalentamiento o un riesgo de incendio.

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

8. **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 funcionamiento correcto del dispositivo.

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. Evitan que las sobrecargas destruyan el sistema.

Se recomienda instalar los dispositivos en áreas con acceso limitado

2 Seguridad eléctrica

- Antes de conectar un cable externo al dispositivo, realice una conexión a tierra adecuada y configure la protección contra sobretensiones; de lo contrario, la electricidad estática dañará la placa base
- Asegúrese de que la alimentación esté desconectada antes de cablear, instalar o desmontar el dispositivo.
- Asegúrese de que la señal conectada al dispositivo sea una señal de corriente débil (interruptor); de lo contrario, los componentes del dispositivo se dañarán.
- Asegúrese de que se aplica el voltaje estándar vigente en su país o región. Si no está seguro del voltaje estándar recomendado, consulte a su compañía eléctrica local. Una incompatibilidad de voltaje puede provocar un cortocircuito o daños en el dispositivo.
- Para evitar interferencias, mantenga el dispositivo alejado de dispositivos con alta radiación electromagnética, como generadores (incluidos generadores eléctricos), radios, televisores (especialmente monitores CRT) o altavoces.

3 Seguridad de funcionamiento

- Si sale humo, olor o ruido del dispositivo, apáguelo inmediatamente, desenchufe el cable de alimentación y póngase en contacto con el centro de servicio técnico.
- El transporte y otras causas impredecibles pueden dañar el hardware del dispositivo. Compruebe si el dispositivo presenta daños graves antes de instalarlo.
- Si el dispositivo presenta defectos graves que no puede solucionar, póngase en contacto con su distribuidor lo antes posible.
- El polvo, la humedad y los cambios bruscos de temperatura pueden afectar a la vida útil del dispositivo. Se recomienda no mantener el dispositivo en tales condiciones.
- No mantenga el dispositivo en un lugar que vibre. Manipule el dispositivo con cuidado. No coloque objetos pesados sobre el dispositivo
- No aplique resina, alcohol, benceno, pesticidas ni otras sustancias volátiles que puedan dañar la carcasa del dispositivo. Limpie los accesorios del dispositivo con un paño suave o una pequeña cantidad de producto de limpieza.
- Si tiene alguna pregunta técnica sobre el uso, póngase en contacto con personal técnico certificado o con experiencia.

Nota:

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

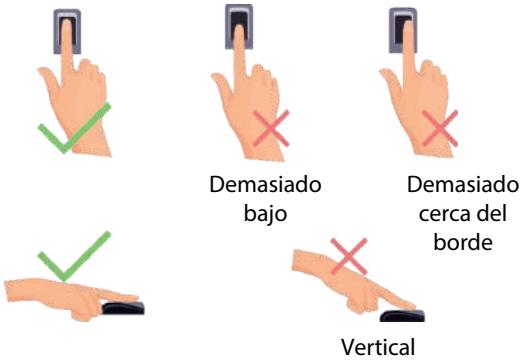
- El servicio de garantía no cubre daños accidentales, daños causados por un mal funcionamiento y daños debidos a la instalación o reparación independiente del producto por parte del usuario.

4 Instrucciones de uso

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

4.1 Posición de los dedos

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



Note: 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.

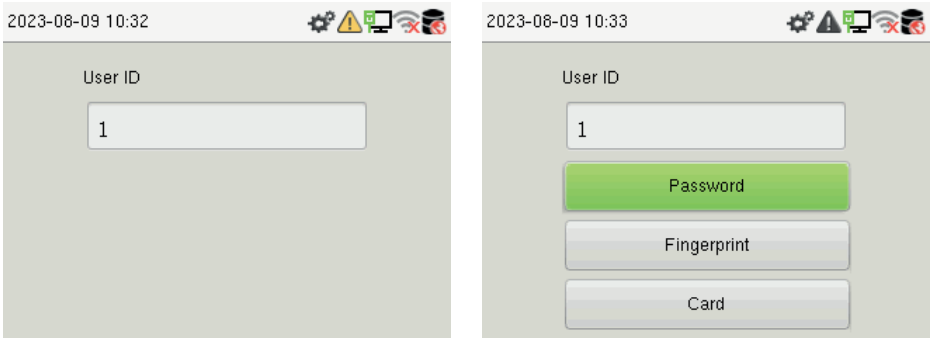
4.2 Interfaz de espera

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

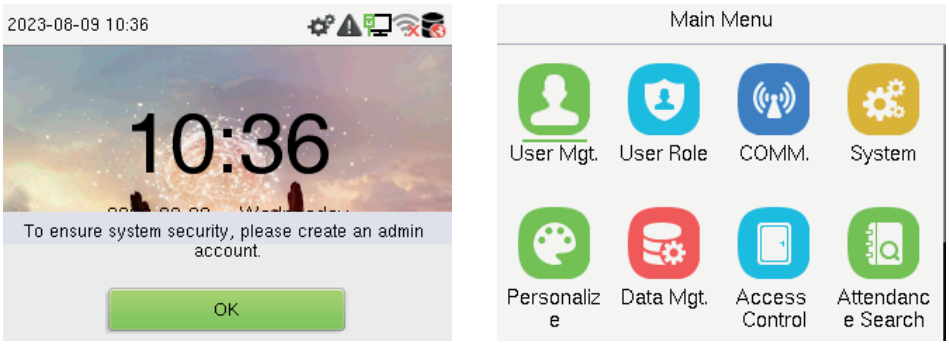




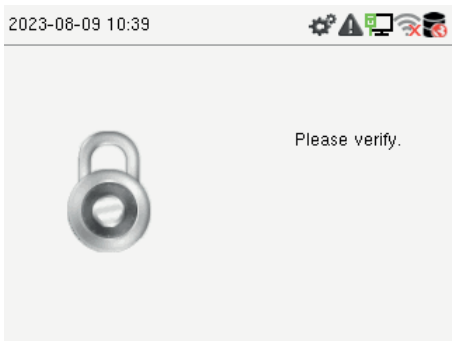
- Introduzca cualquier número para acceder a la interfaz de introducción del ID de usuario.



- Cuando no hay ningún superadministrador configurado en el dispositivo, pulse **M/OK** para ir al menú.

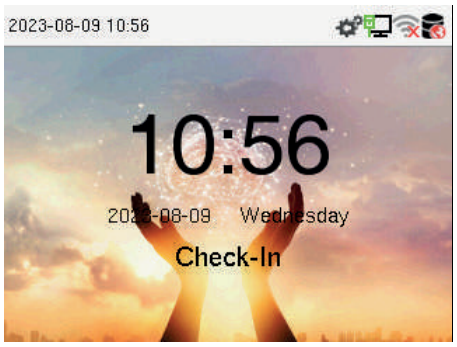


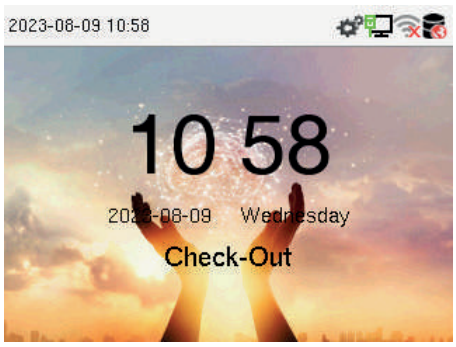
- Después de añadir un superadministrador en el dispositivo, se requiere la verificación del superadministrador antes de abrir las funciones del menú.



Nota: Por motivos de seguridad del dispositivo, se recomienda registrar un superadministrador la primera vez que se utiliza el dispositivo

- En la interfaz en espera, las opciones de estado de punzonado también se pueden mostrar y utilizar directamente. Las asignaciones de teclas de acceso directo en negrita y negras se mostrarán en la pantalla si pulsa la tecla de acceso directo correspondiente en el teclado táctil oculto, como se muestra en la imagen siguiente. Para conocer el método de funcionamiento específico, consulte «Asignaciones de teclas de acceso directo»





Note: Las opciones de estado de punzón están habilitadas de forma predeterminada cuando el tipo de dispositivo se configura como terminal de asistencia.

4.3 Modo de verificación

4.3.1 Verificación de huellas dactilares

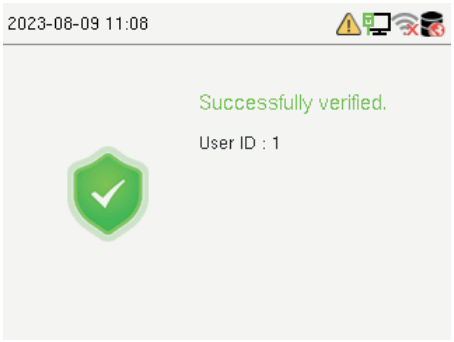
➢**1: N Modo de verificación de huellas dactilares**

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

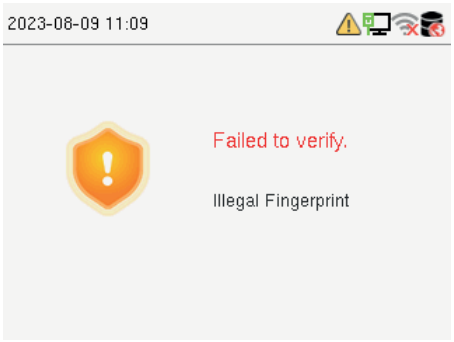
El modo de autenticación de huellas dactilares se activa cuando el usuario coloca el dedo en el escáner de huellas dactilares.

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

La verificación se ha realizado correctamente:



La verificación ha fallado:

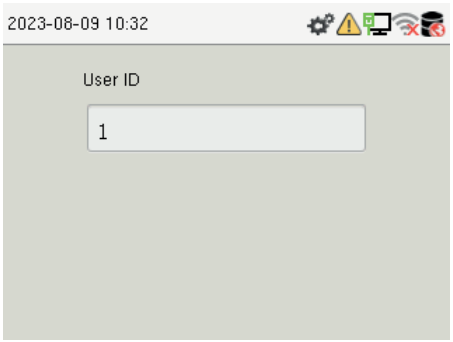


➢**1: 1 Modo de verificación de huellas dactilares**

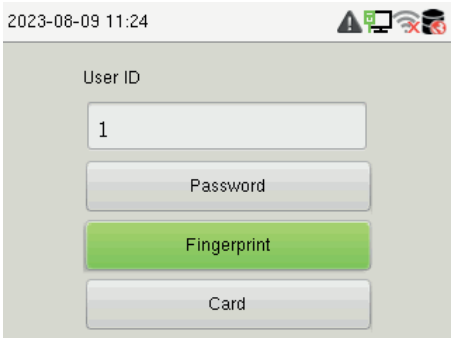
El dispositivo compara la huella dactilar actual con las huellas dactilares vinculadas al ID de usuario introducido a través del teclado virtual.

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

Introduzca el ID de usuario y pulse **M/OK** para entrar en el modo de verificación de huellas dactilares 1:1.

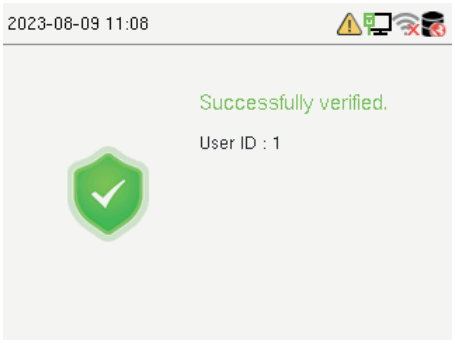


Si un empleado registra una contraseña y una tarjeta además de la huella dactilar, aparecerá la siguiente pantalla. Seleccione la huella dactilar para entrar en el modo de verificación de huellas dactilares

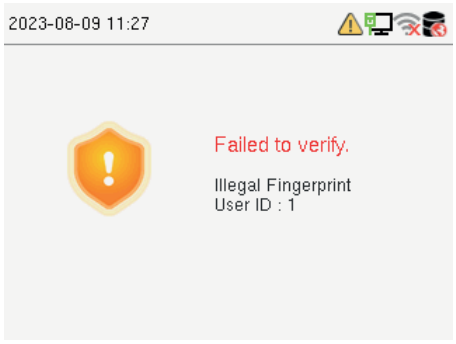


Presione la huella dactilar para verificar.

La verificación se ha realizado correctamente:



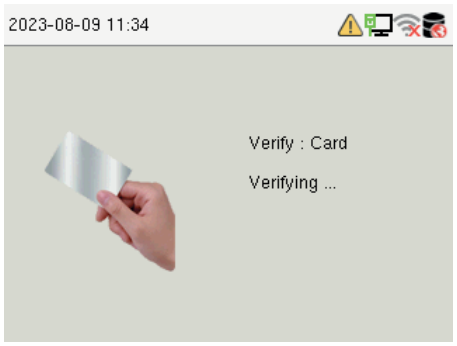
La verificación ha fallado:

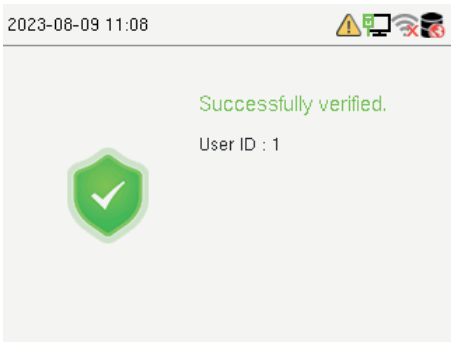


4.3.2 Verificación de la tarjeta

➢1: N Modo de verificación de tarjetas

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



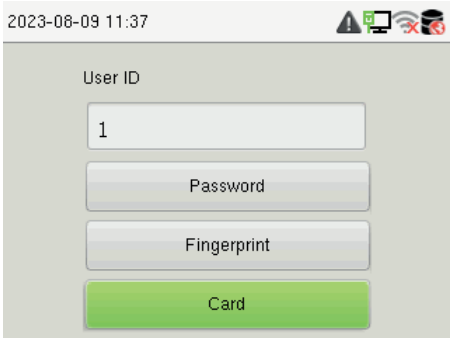


➢1:1 Modo de verificación de tarjetas

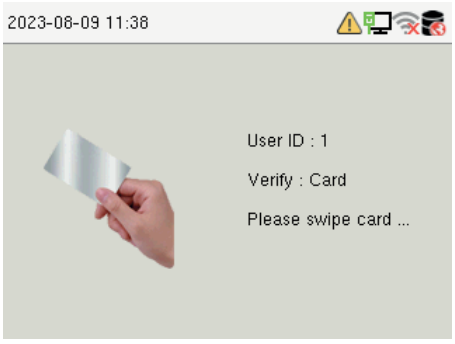
El modo de verificación de tarjetas 1:1 compara el número de tarjeta en el área de inducción de tarjetas con el número asociado al ID de usuario del empleado registrado en el dispositivo.

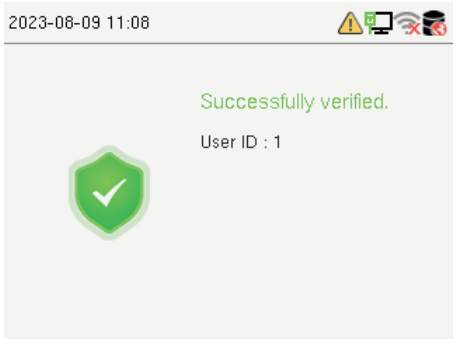
Introduzca el ID de usuario y pulse M/OK para entrar en el modo de verificación de tarjetas 1:1.





Si un empleado registra una huella dactilar y una contraseña además de la tarjeta, aparecerá la siguiente pantalla.
Seleccione la tarjeta para entrar en el modo de verificación de la tarjeta



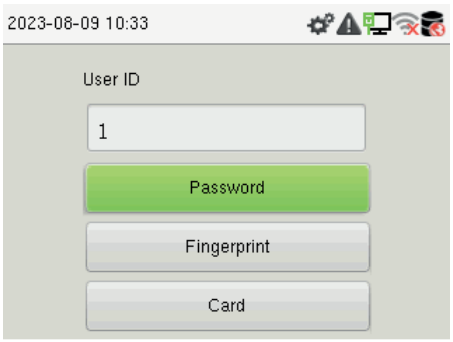


4.3.3 Verificación de contraseña

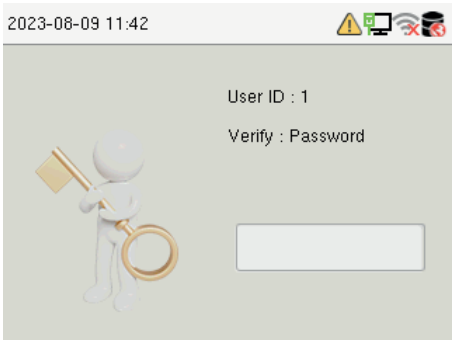
El dispositivo compara la contraseña introducida con la contraseña registrada y el ID de usuario.

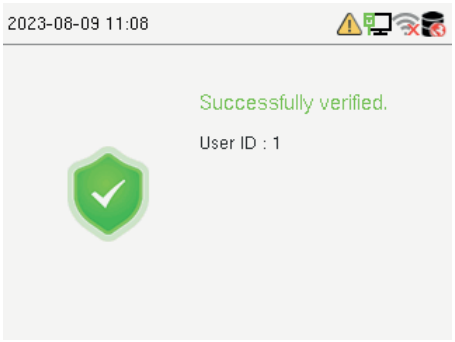
Introduzca el ID de usuario y pulse **M/OK** para entrar en el modo de verificación de contraseña 1:1. A continuación, introduzca el ID de usuario y pulse **M/OK**





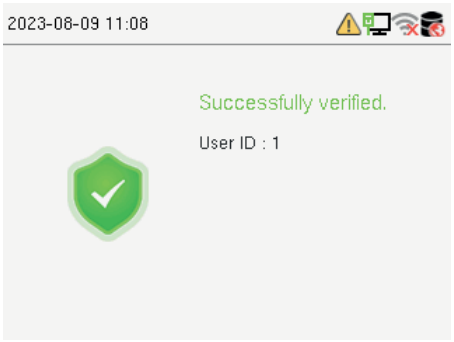
Si un empleado registra una huella dactilar y una tarjeta además de la contraseña, aparecerá la siguiente pantalla. Seleccione la contraseña para entrar en el modo de verificación de la tarjeta.



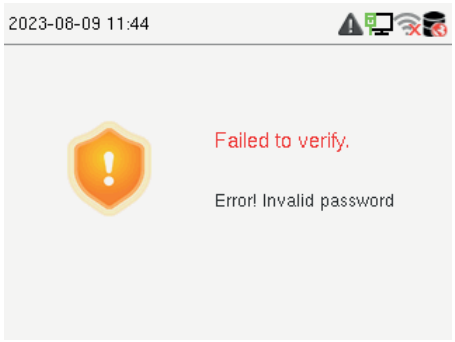


A continuación se muestran las pantallas que aparecen tras introducir una contraseña correcta y una contraseña incorrecta, respectivamente

La verificación se ha realizado correctamente:



Verificación fallida:

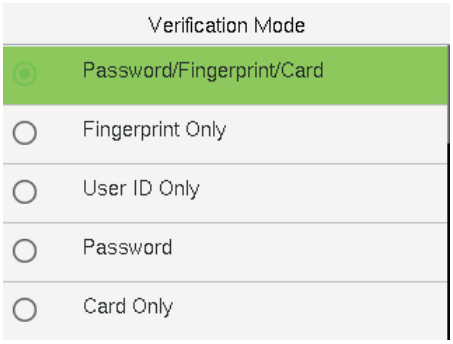


4.3.4 Verificación combinada

Este dispositivo le permite utilizar diferentes tipos de métodos de verificación para aumentar la seguridad. Hay un total de 15 combinaciones de verificación diferentes que se pueden implementar, como se indica a continuación:

Verificación combinada Símbolo Definición

Símbolo	Definición	Explicación
/	o	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 de configuración del modo de verificación combinada:

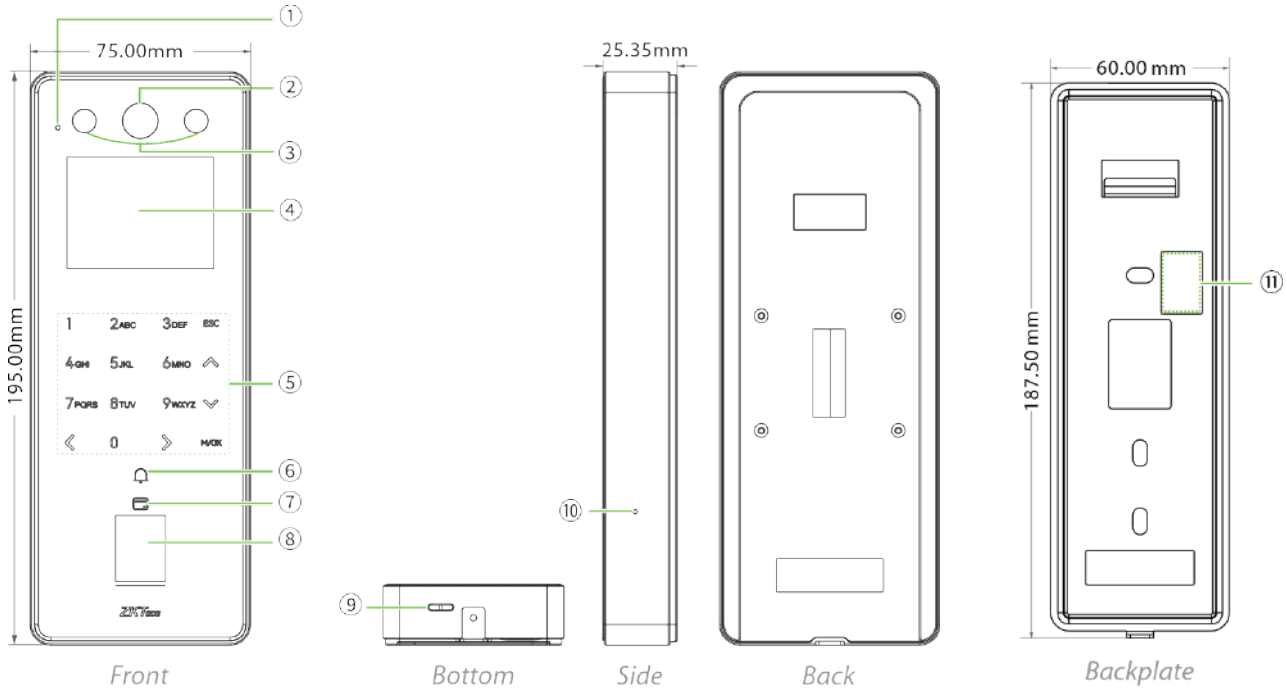
- La verificación combinada requiere que el personal registre todos los diferentes métodos de verificación. De lo contrario, los empleados no podrán verificar correctamente el proceso de verificación combinada.
- Por ejemplo, si un empleado solo se ha registrado con datos de contraseña, pero el modo de verificación del dispositivo está configurado en «Contraseña + Tarjeta», el empleado no podrá completar correctamente el procedimiento de verificación.

Motivo:

- Esto se debe a que el dispositivo compara la plantilla de contraseña de la persona con la plantilla de verificación registrada (tanto la tarjeta como la contraseña) almacenada previamente en ese ID de personal en el dispositivo.
- Sin embargo, dado que el empleado solo ha registrado su contraseña y no su tarjeta, el proceso de verificación no se completará con éxito y el dispositivo mostrará el mensaje «Verificación fallida».

5 Descripción general

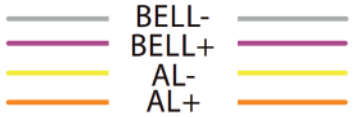
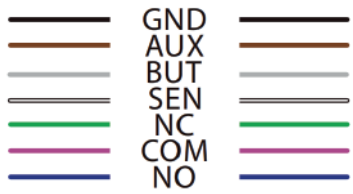
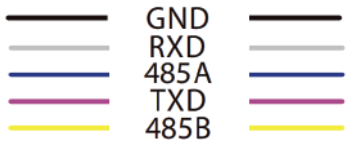
5.1 Apariencia



No.	Descripción
1	Micrófono
2	Cámara
3	Flash de infrarrojo cercano
4	Pantalla a color de 2,4 pulgadas
5	Teclado táctil oculto
6	Botón del timbre
7	Área de lectura de tarjetas
8	Sensor de huellas dactilares
9	Altavoz
10	Botón de reinicio
11	Interruptor magnético antisabotaje

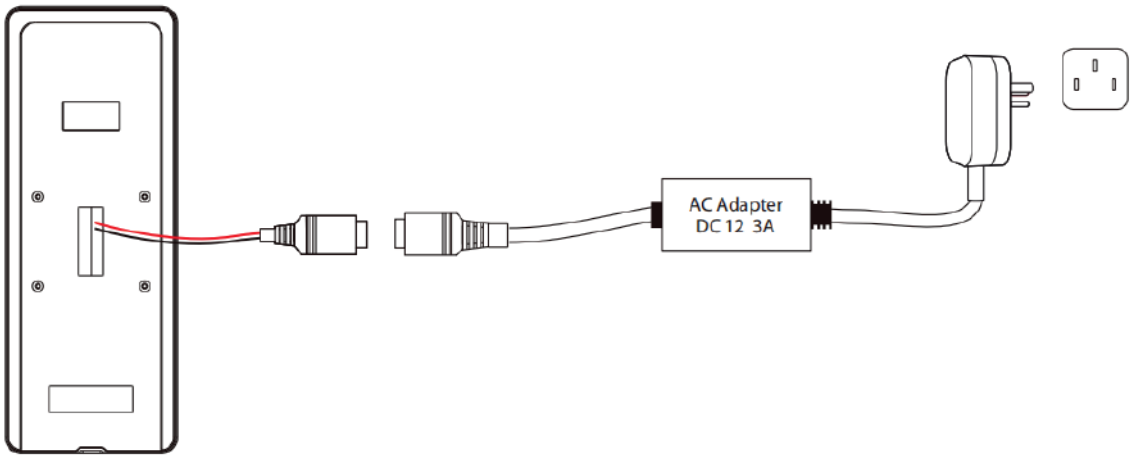
5.2 Descripción de los terminales y el cableado

5.2.1 Descripción de los terminales

Interfaz	Descripción	
	BELL-	Campana
	BELL+	
	AL-	Alarma
	AL+	
	GND	Sensor / Botón de salida / Entrada auxiliar
	AUX	
	BUT	
	SEN	
	NC	Lock
	COM	
	NO	
	INWD0	Wiegand
	INWD1	
	GND	
	12VOUT	
	WD1-OUT	
	WD0-OUT	
	GND	RS232 / RS485
	RXD	
	485A	
	TXD	
	485B	
	Entrada de alimentación de 12 V	
	Interfaz de red	

5.3 Descripción del cableado

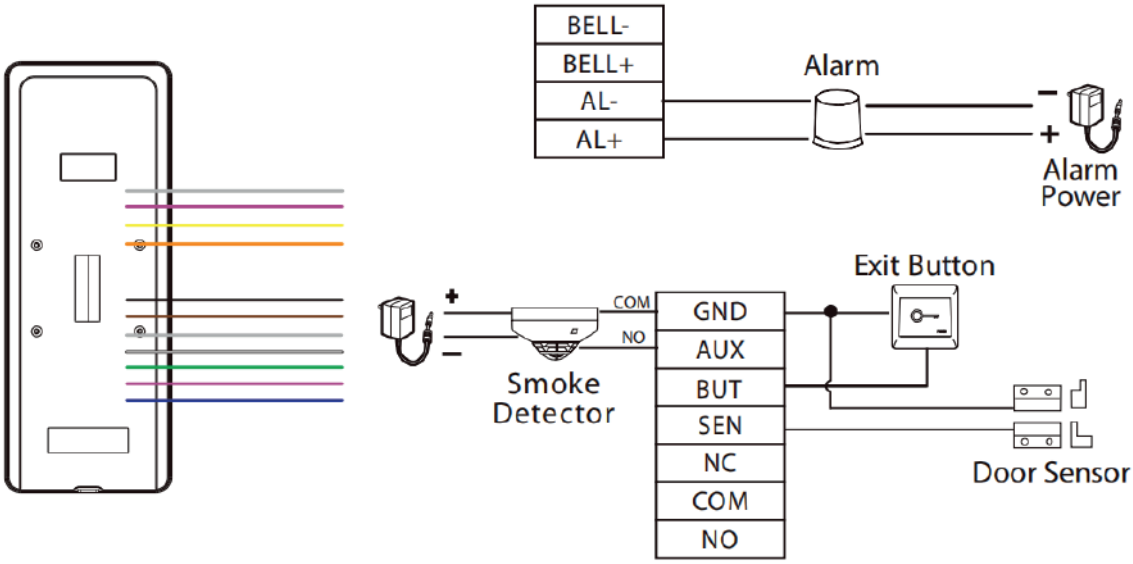
5.3.1 Conexión de alimentación



Fuente de alimentación recomendada

- 12 V y 3 A.
- Para compartir la alimentación del dispositivo con otros dispositivos, utilice una fuente de alimentación con una potencia nominal más alta

5.3.2 Conexión del sensor de puerta, botón de salida, alarma y auxiliar

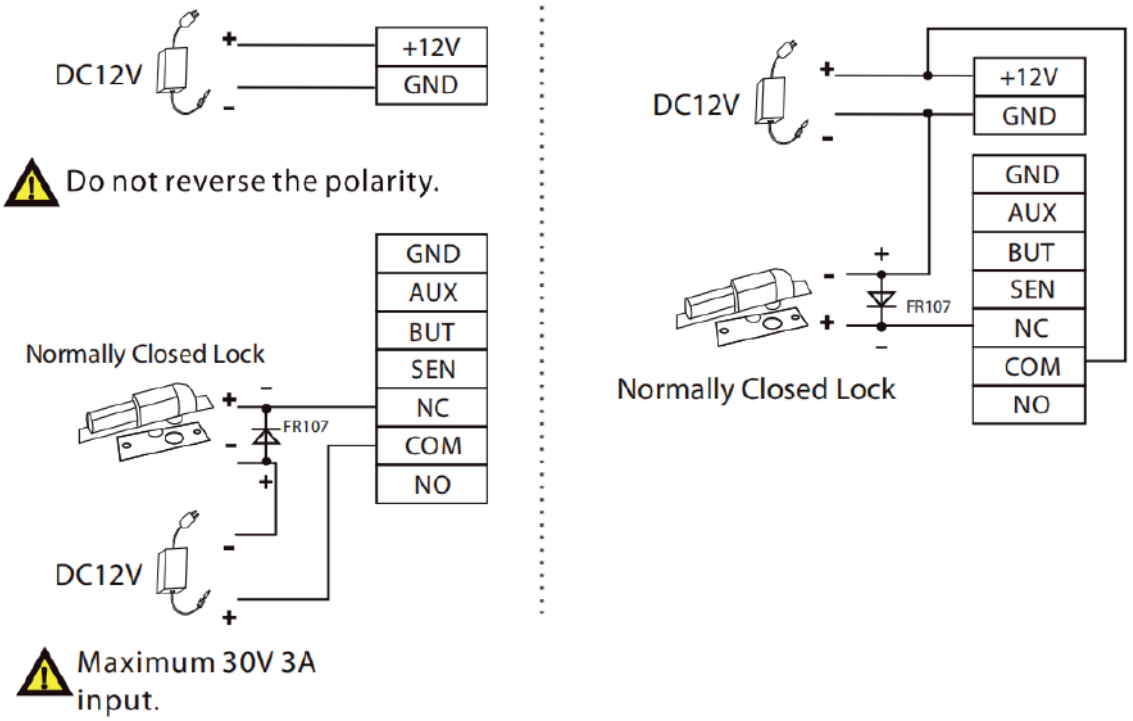


5.3.3 Conexión del relé de bloqueo

- **Método 1: conexión como dispositivo independiente**

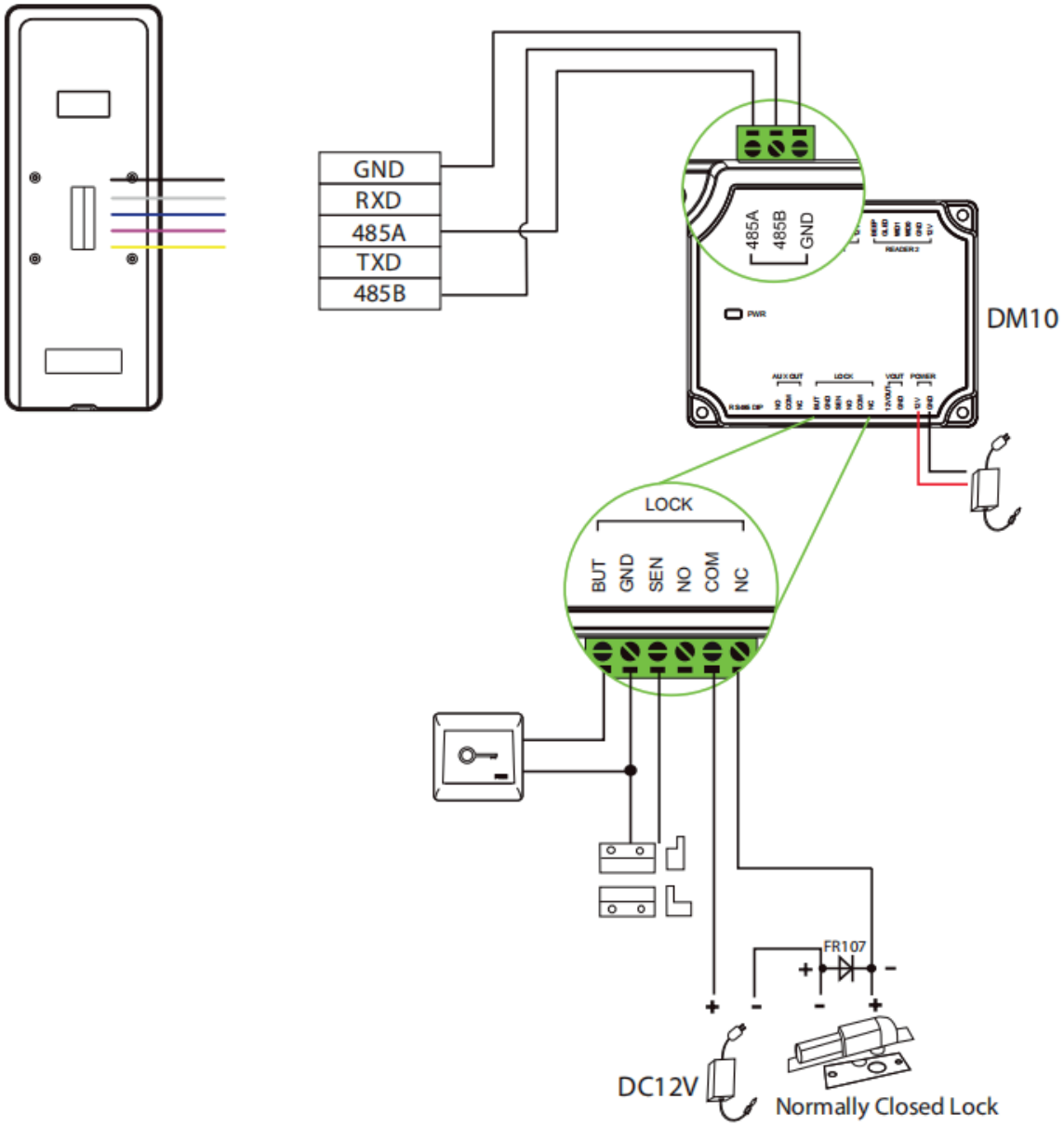
El sistema admite tanto cerraduras normalmente abiertas como cerraduras normalmente cerradas. La cerradura NO (normalmente abierta cuando está alimentada) se conecta a los terminales «NO1» y «COM1», y la cerradura NC (normalmente cerrada cuando está alimentada) se conecta a los terminales «NC1» y «COM1». La

alimentación se puede compartir con la cerradura o se puede utilizar por separado para la cerradura, como se muestra en el ejemplo con la cerradura NC a continuación:



- **Método 2: Conexión al DM10**

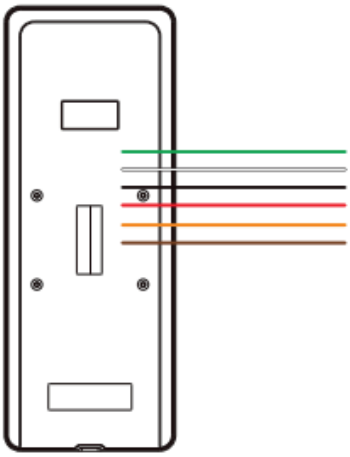
El DM10 se puede conectar al F35 con el cable RS485. La seguridad se puede mantener incluso si se ha perdido la conexión entre el F35 y el DM10 o si se ha cortado la alimentación del F35 debido a factores externos.

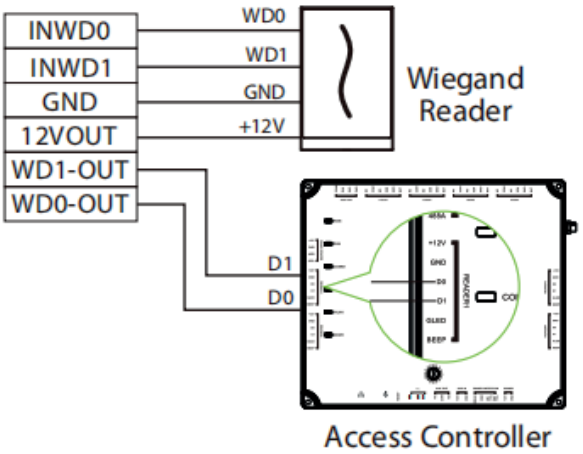


Nota:

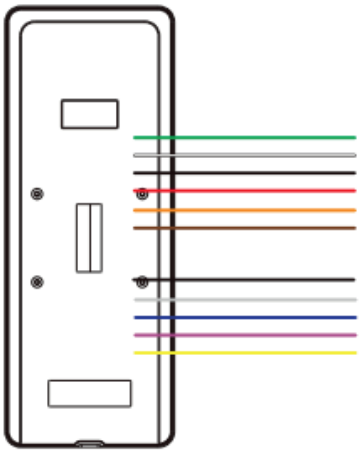
1) Para utilizar esta función, debe acceder al menú **([COMM.] > [Serial Comm] > [Serial Port])** y configurarla como **DM10**. Si la conexión entre F35 y DM10 se establece correctamente, aparecerá el icono en la esquina superior derecha de la interfaz de espera.
2) Los dos métodos de conexión del relé de bloqueo no se pueden utilizar simultáneamente, solo se puede seleccionar uno

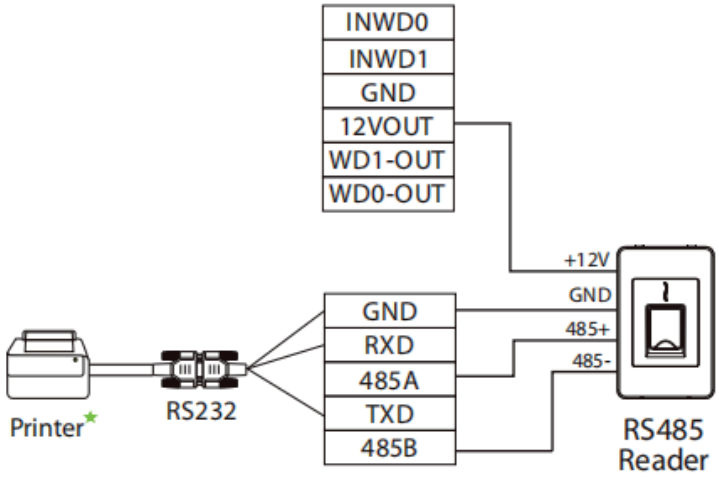
5.3.4 Conexión Wiegand





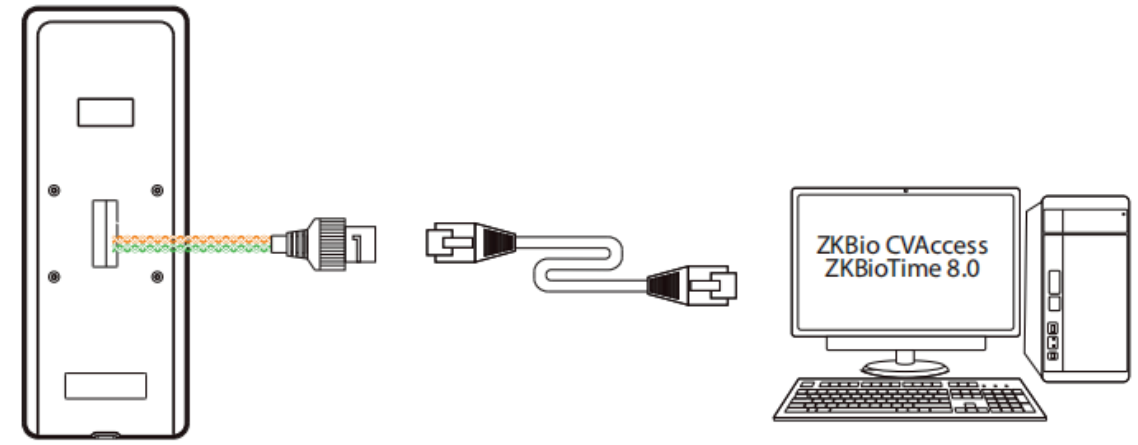
5.3.5 Conexión RS485 y RS232





5.3.6 Conexión Ethernet

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



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

6 Instalación

6.1 Entorno de instalación

Consulte las siguientes recomendaciones para la instalación.



KEEP DISTANCE



AVOID GLASS REFRACTION



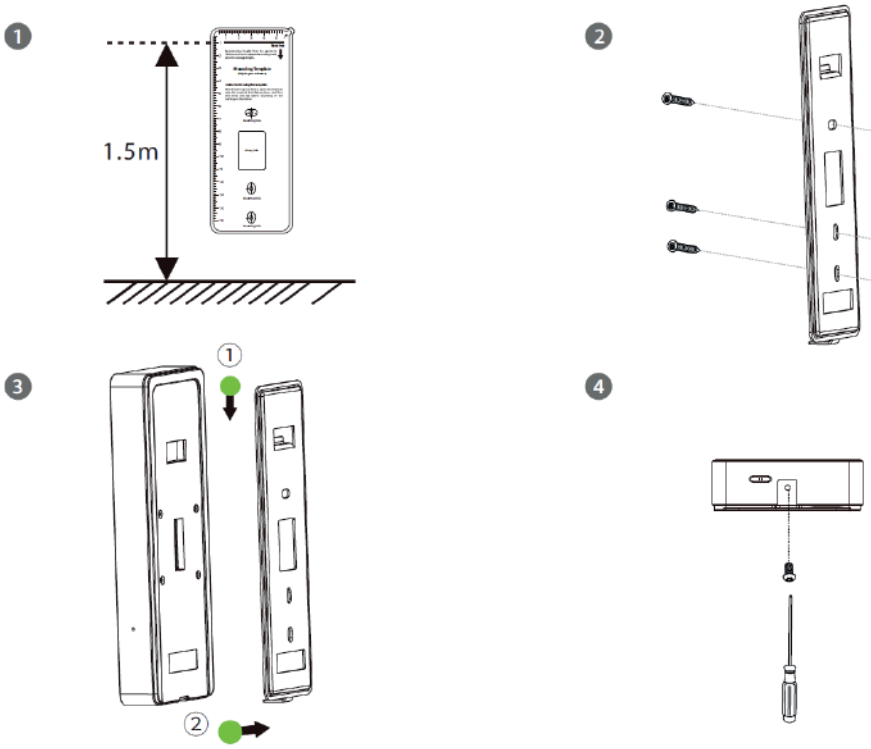
AVOID DIRECT SUNLIGHT AND EXPOSURE



AVOID USE OF ANY HEAT SOURCE NEAR THE DEVICE

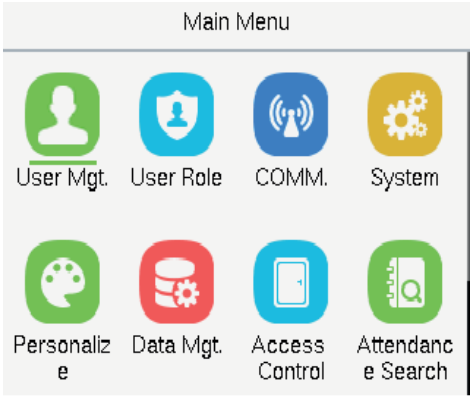
6.2 Instalación del dispositivo

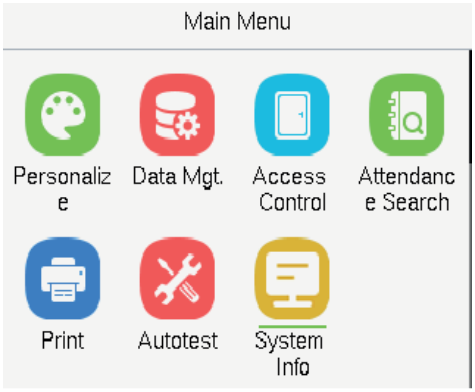
1. Pegue la plantilla de montaje adhesiva a la pared y taladre los agujeros según la plantilla de montaje adhesiva.
2. Fije la placa trasera a la pared con tornillos de montaje en pared.
3. Fije el dispositivo a la placa posterior.
4. Fije el dispositivo a la placa trasera con un tornillo de seguridad



7 Menú principal

Toque **M/OK** en la interfaz inicial para acceder al menú principal, como se muestra a continuación:





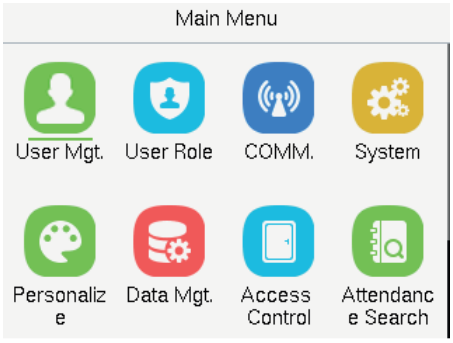
Descripción de la función

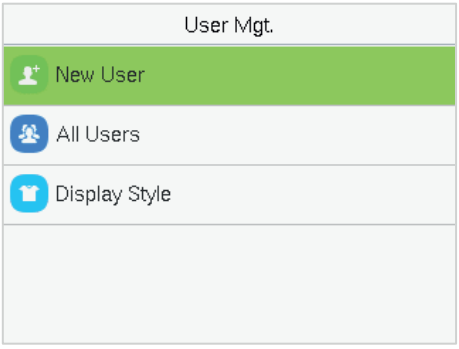
Menú	Descripción
Gestión de usuario	Para añadir, editar, ver y eliminar información de un usuario.
Rol de usuario	Para establecer el ámbito de permisos del rol personalizado y el registrador para los usuarios, por ejemplo, los derechos operativos del sistema.
COMM.	Para configurar los parámetros relevantes de red, comunicación serie, conexión a PC, Wi-Fi★, servidor en la nube, Wiegand y diagnóstico de red.
Sistema	Para configurar los parámetros relacionados con el sistema, incluyendo fecha y hora, configuración de registros de asistencia/acceso, huellas dactilares, parámetros de videoportero★, configuración ONVIF★, configuración del tipo de dispositivo, configuración de seguridad, actualización del firmware en línea y restablecimiento de la configuración de fábrica.
Personalizar	Para personalizar la configuración de la interfaz de usuario, la voz, los horarios de timbre, las opciones de estado de punzonado y la asignación de teclas de acceso directo..
Gestión de datos	Para eliminar los datos.
Control de acceso	Para configurar los parámetros de la cerradura y el dispositivo de control de acceso correspondiente, incluidas opciones como horarios, configuración de días festivos, grupos de acceso, verificación combinada, configuración antipassback y configuración de opciones de coacción
Búsqueda de asistencia	Para consultar los registros de eventos especificados.
Imprimir★	Para configurar la información y las funciones de impresión (si la impresora está conectada al dispositivo).
Autocompro-bación	Para comprobar automáticamente si cada módulo funciona correctamente, incluyendo la pantalla LCD, el audio, el micrófono, el teclado, el sensor de huellas dactilares, la cámara y el reloj en tiempo real.
Información del sistema	Para ver la Política de privacidad, la capacidad de datos y la información sobre el dispositivo y el firmware del dispositivo actual.

8 Gestión de usuarios

8.1 Registro de nuevos usuarios

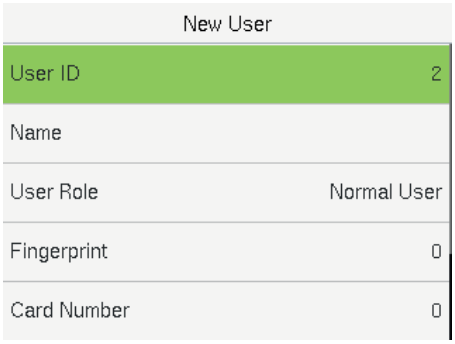
Cuando el dispositivo se encuentre en la interfaz inicial, pulse el botón **[M/OK] > Gestión de usuarios > Nuevo usuario.**





8.1.1 Registrar un ID de usuario y un nombre

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



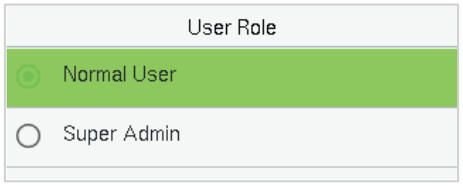
Nota:

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

8.1.2 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 posee todos los privilegios de administración del dispostivo.
- **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 verificaciones auténticas.
- **Roles definidos por el usuario:** Al usuario normal también se le pueden asignar roles personalizados con el rol definido por el usuario. Se le puede permitir al usuario acceder a varias opciones del menú según sea necesario.

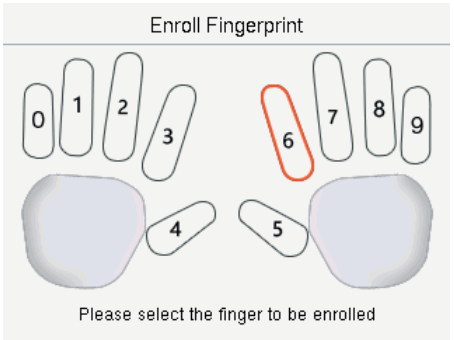


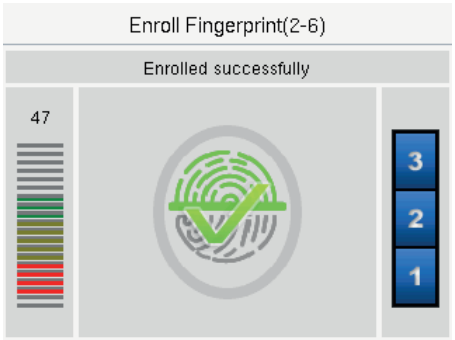
Nota: Si el rol de usuario seleccionado es el de superadministrador, el usuario deberá superar la autenticación de identidad para acceder al menú principal. La autenticación se basa en los métodos de autenticación que haya registrado el superadministrador.

8.1.3 Registrar huella dactilar

Toque **Huella digital** en la interfaz **Nuevo usuario** 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.
- El color verde indica que la huella dactilar se ha registrado correctamente.

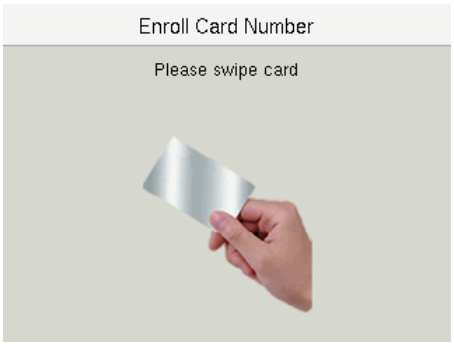


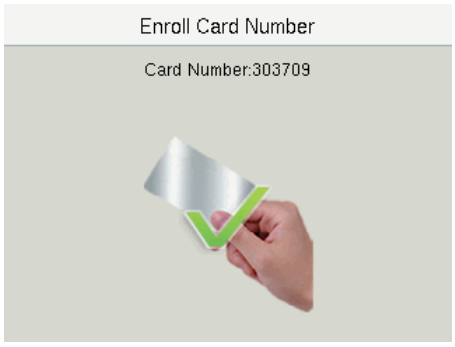


8.1.4 Número de tarjeta

Toque **Número de tarjeta** en la interfaz **Nuevo usuario** para acceder a la página de registro de la tarjeta.

- En la interfaz de la tarjeta, pase la tarjeta por debajo del área de lectura de tarjetas. El registro de la tarjeta se habrá realizado correctamente
- Si la tarjeta ya está registrada, aparecerá el mensaje **«Error. Tarjeta ya registrada».** La interfaz de registro tiene el siguiente aspecto:

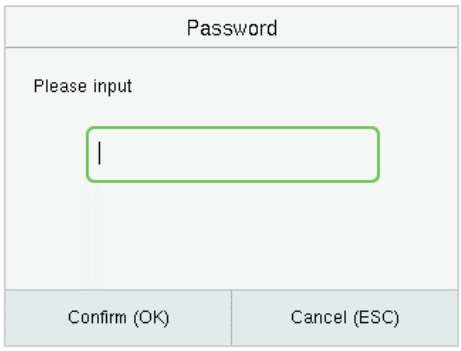


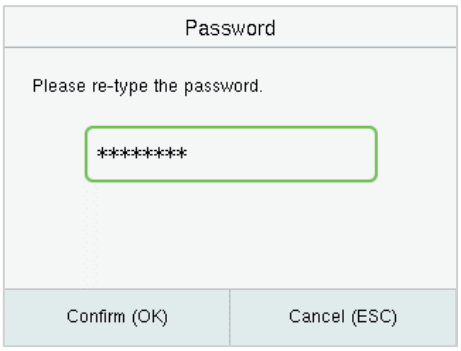


8.1.5 Contraseña

Toque Contraseña en la interfaz de 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 M/OK.
- Si la contraseña introducida de nuevo es diferente de la introducida inicialmente, el dispositivo mostrará el mensaje «¡Contraseña no coincidente!», y el usuario deberá volver a confirmar la contraseña.
- La contraseña puede contener de 6 a 8 dígitos de forma predeterminada.

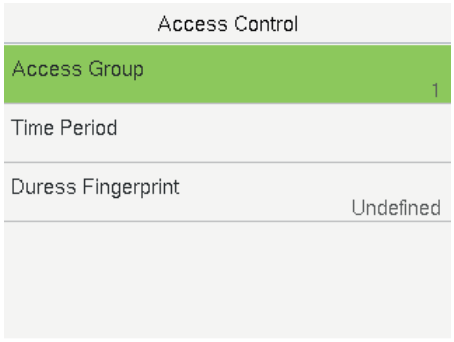




8.1.6 Función de control de acceso

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

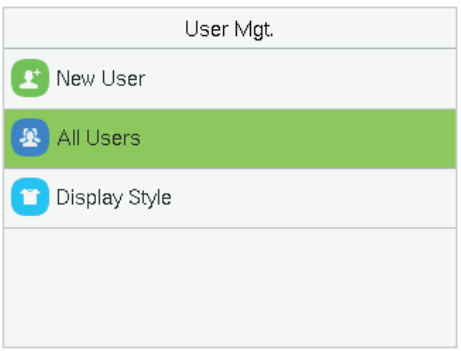
- Toque **Función de control de acceso > Grupo de acceso** para asignar a los usuarios registrados a diferentes grupos para una mejor gestión. Los nuevos usuarios pertenecen al Grupo 1 de forma predeterminada y pueden ser reasignados a otros Grupos. El dispositivo admite hasta 99 grupos de control de acceso..
- Toque **Período de tiempo** para seleccionar el tiempo que desea utilizar.
- El usuario puede especificar una o varias huellas dactilares que se hayan registrado como huellas dactilares de coacción. Al presionar el dedo correspondiente a la huella dactilar de coacción en el sensor y pasar la verificación, el sistema generará inmediatamente una alarma de coacción.

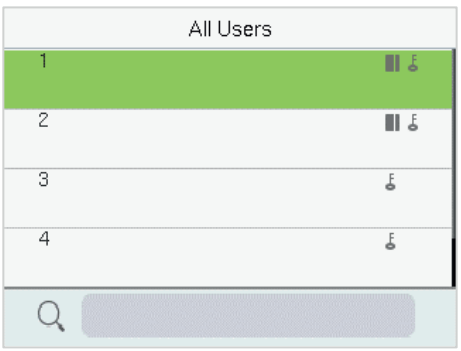


8.2 Todos los usuarios

Cuando el dispositivo se encuentre en la interfaz inicial, pulse el botón **[M/OK] > Gestión de usuarios > Todos los usuarios.**

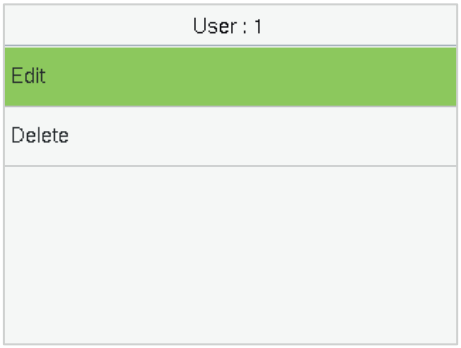
- En la interfaz **Todos los usuarios**, pulse la barra de búsqueda de la lista de usuarios para introducir la palabra clave de búsqueda requerida (la palabra clave puede ser el ID de usuario, el apellido o el nombre completo) y el sistema buscará la información relacionada con el usuario.

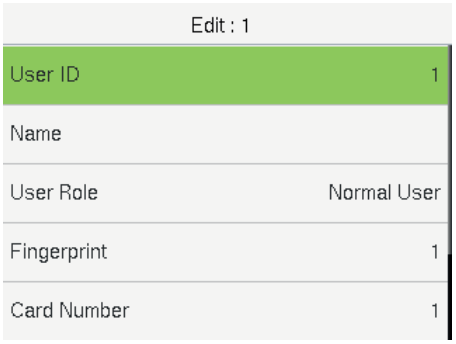




8.2.1 Editar usuario

En la interfaz **Todos los usuarios**, pulse sobre el usuario deseado en la lista y pulse **Editar** para modificar la información del usuario.





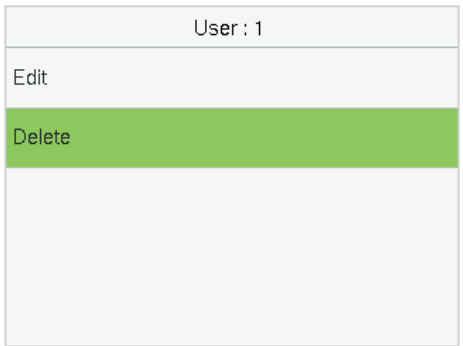
Nota: El proceso de edición de la información del usuario es el mismo que el de añadir un nuevo usuario, salvo que el ID de usuario no se puede modificar mientras se edita un usuario. El proceso detallado se describe en «Registro de usuarios»

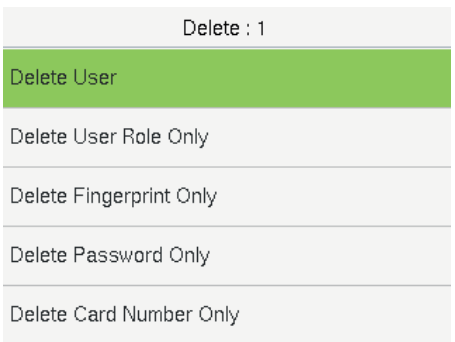
8.2.2 Eliminar usuario

En la interfaz **Todos los usuarios**, pulse el usuario deseado de la lista y pulse **Eliminar** para eliminar el usuario o la información específica del usuario del dispositivo. En la interfaz **Eliminar**, pulse la operación deseada y, a continuación, pulse **M/OK** para confirmar la eliminación

Operaciones de eliminación:

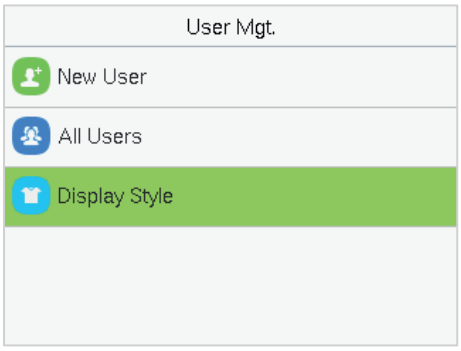
- **Eliminar usuario:** Elimina toda la información del usuario (elimina el usuario seleccionado en su totalidad) del dispositivo.
- **Eliminar solo el rol de usuario:** Elimina los privilegios de administrador del usuario y lo convierte en un usuario normal
- **Eliminar solo huella dactilar:** Elimina la información de huella dactilar del usuario seleccionado.
- **Eliminar solo contraseña:** Elimina la información de contraseña del usuario seleccionado.
- **Eliminar solo número de tarjeta:** Elimina la información de la tarjeta del usuario seleccionado.





8.3 Estilo de Visualización

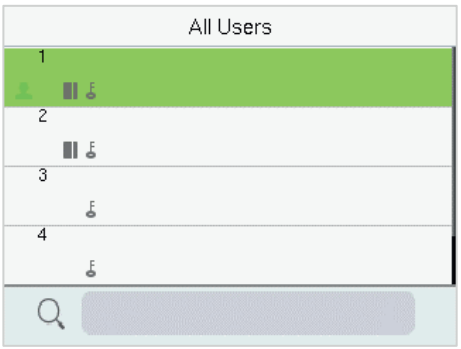
Cuando el dispositivo se encuentre en la interfaz inicial, pulse el botón **[M/OK] > Gestión de usuarios > Estilo de visualización**



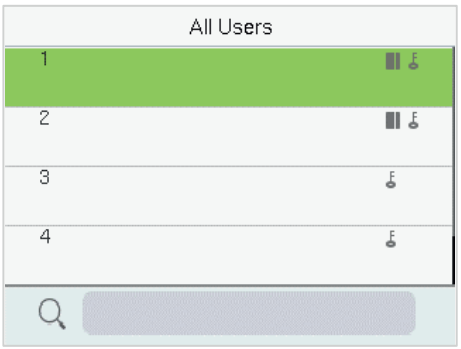


Todos los estilos de visualización se muestran a continuación:

Varias líneas:



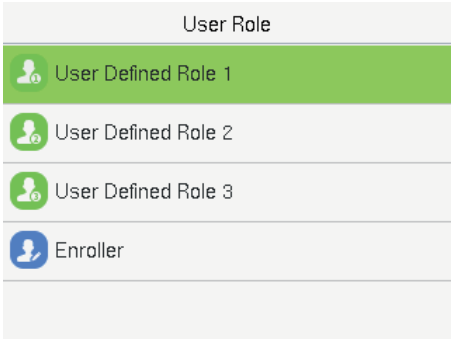
Línea mixta:



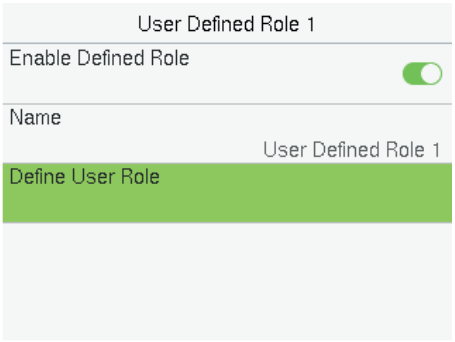
9 Función del usuario

La función de usuario le permite asignar permisos específicos a determinados usuarios en función de sus necesidades.

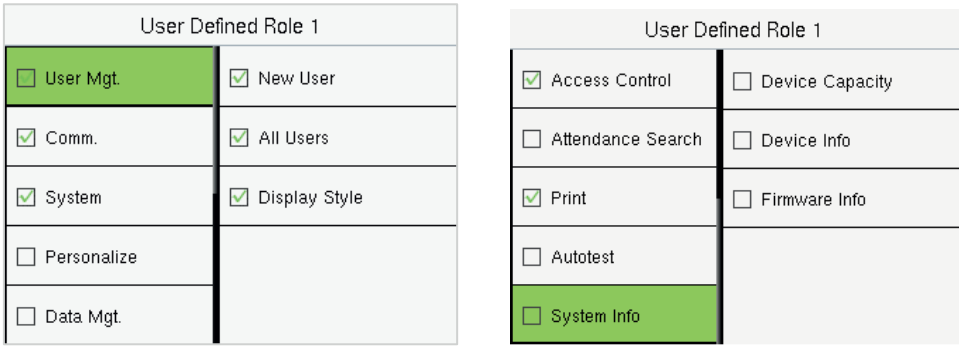
- Cuando el dispositivo se encuentra en la interfaz inicial, pulse el botón [M/OK] > Rol de usuario > Rol definido por el usuario para establecer los permisos definidos por el usuario.
- El ámbito de permisos del rol personalizado se puede configurar en 3 roles, es decir, el ámbito operativo personalizado de las funciones del menú del usuario.



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



- A continuación, seleccione Definir rol de usuario, seleccione los privilegios necesarios para el nuevo rol y pulse la tecla **M/OK.**
- Al asignar privilegios, los nombres de las funciones del menú principal se mostrarán a la izquierda y sus submenús se enumerarán a la derecha.
- Primero pulse el nombre de la función **del menú principal** requerida y, a continuación, seleccione los submenús requeridos de la lista.

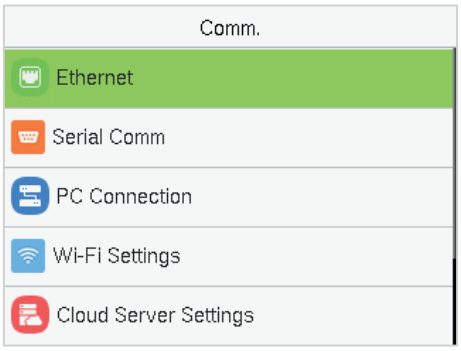


Nota: Si la función Rol de usuario está habilitada para el dispositivo, pulse **Gestión de usuarios > Nuevo usuario > Rol de usuario** para asignar los roles creados a los usuarios necesarios. Sin embargo, si no hay ningún superadministrador registrado en el dispositivo, este mostrará el mensaje **«¡Inscriba primero al superadministrador!»** al habilitar la función Rol de usuario

10 Comunicación

La configuración de comunicación se utiliza para establecer los parámetros de la red, la comunicación serie, la conexión al PC, el Wi-Fi★, el servidor en la nube, Wiegand y el diagnóstico de red.

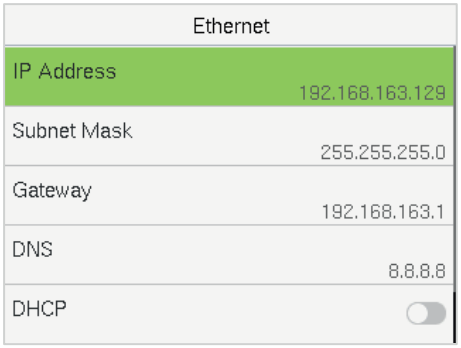
Cuando el dispositivo se encuentra en la interfaz inicial, pulse el botón **[M/OK] > COMM.**

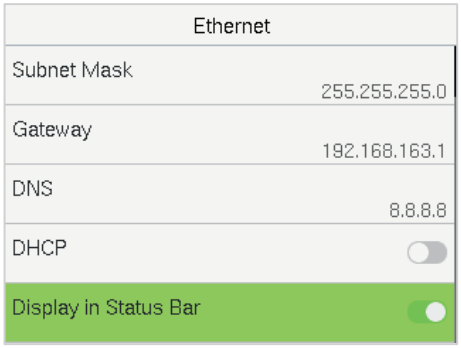


10.1 Ethernet

Cuando el dispositivo necesita comunicarse con un PC a través de Ethernet, es necesario configurar los ajustes de red y asegurarse de que el dispositivo y el PC se conectan al mismo segmento de red

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





Function Description:

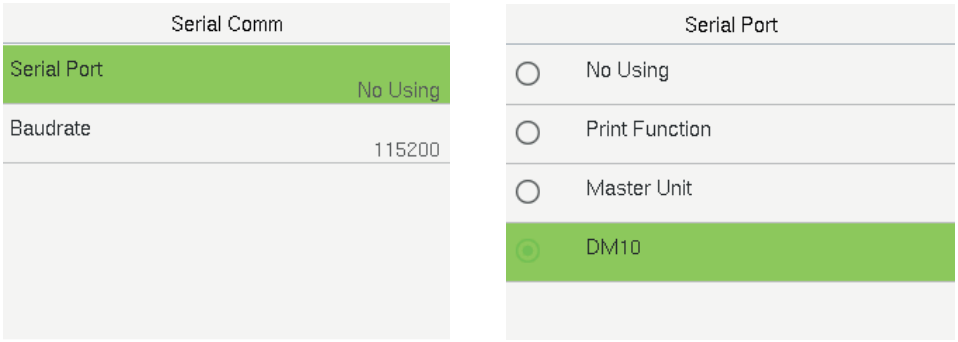
Nombre de la función	Descripción
Dirección IP	La dirección IP predeterminada es 192.168.1.201. Se puede modificar según la disponibilidad de la red.
Máscara de subred	La máscara de subred predeterminada es 255.255.255.0. Se puede modificar según la disponibilidad de la red.
Puerta de enlace	La dirección de la puerta de enlace predeterminada es 0.0.0.0. Se puede modificar según la disponibilidad de la red.

Nombre de la función	Descripción
DNS	La dirección DNS predeterminada es 0.0.0.0. Se puede modificar según la disponibilidad de la red.
DHCP	El Protocolo de configuración dinámica de host asigna dinámicamente direcciones IP a los clientes a través del servidor.
Display in Status Bar	Active o desactive esta opción para mostrar el icono de red en la barra de estado

10.2 Comunicación serie

La función de comunicación serie establece la comunicación con el dispositivo a través de un puerto serie (unidad maestra/DM10/función de impresión).

Toque **Comunicación serie** en la interfaz Configuración **de comunicación.**



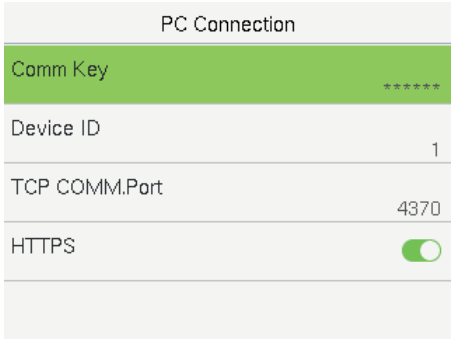
Descripción de la función

Nombre de la función	Descripción
Puerto serie	**No utilizar:** No hay comunicación con el dispositivo a través del puerto serie. **Unidad maestra:** cuando se utiliza RS485 como función de «unidad maestra», se puede conectar a un lector. **Función de impresión:** El dispositivo se puede conectar a la impresora cuando RS232 habilita la función de impresión. **DM10:** Cuando se utiliza RS485 como función de «DM10», se puede conectar a DM10 para controlar el relé de bloqueo. **(Nota:** al seleccionar DM10 o al cambiar de DM10 a otra opción, el dispositivo se reiniciará para que el cambio surta efecto).
Baudrate	Cuando el puerto serie se configura como **unidad maestra** o **DM10**, la velocidad de transmisión es de 115200 por defecto y no se puede modificar. Cuando el puerto serie se configura como **función de impresión**, hay 5 opciones de velocidad en baudios. Son: 115200 (predeterminada), 57600, 38400, 19200 y 9600. Cuanto mayor sea la velocidad en baudios, mayor será la velocidad de comunicación, pero también menor será la fiabilidad. Por lo tanto, se puede utilizar una velocidad de transmisión más alta cuando la distancia de comunicación es corta; cuando la distancia de comunicación es larga, es más fiable elegir una velocidad de transmisión más baja.

10.3 Conexión al PC

Comm Key facilita la mejora de la seguridad de los datos mediante la configuración de la comunicación entre el dispositivo y el PC. Una vez configurada Comm Key, se requiere una contraseña para conectar el dispositivo al software del PC.

Toque **Conexión con PC** en la interfaz de configuración **COMM.** para configurar los ajustes de comunicación



Descripción de la función

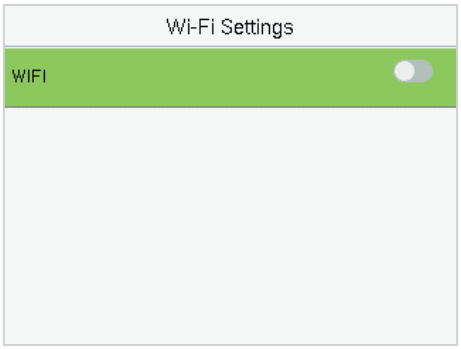
Nombre de la función	Descripción
Clave de comunicación	La contraseña predeterminada es 0 y se puede cambiar. La clave de comunicación puede contener de 1 a 6 dígitos.
ID del dispositivo	Es el número de identificación del dispositivo, que oscila entre 1 y 254.
Puerto de comunicación TCP	El valor predeterminado del puerto TCP COMM es 4370. Se puede modificar según la disponibilidad de la red
HTTPS	Basado en HTTP, el cifrado de la transmisión y la autenticación de identidad garantizan la seguridad del proceso de transmisión.

10.4 Configuración Wi-Fi★

El dispositivo proporciona un módulo Wi-Fi, que puede estar integrado en el módulo del dispositivo o conectarse externamente.

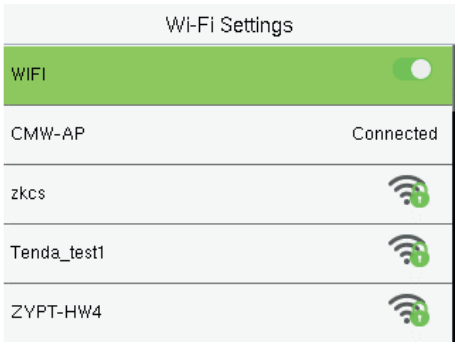
El módulo Wi-Fi permite la transmisión de datos a través de Wi-Fi (Wireless Fidelity) y establece un entorno de red inalámbrica. El Wi-Fi está habilitado de forma predeterminada en el dispositivo. Si no necesita utilizar la red Wi-Fi, puede desactivar el botón Wi-Fi.

Toque **Configuración de Wi-Fi** en la interfaz Configuración **de COMM.** para configurar los ajustes de Wi-Fi.

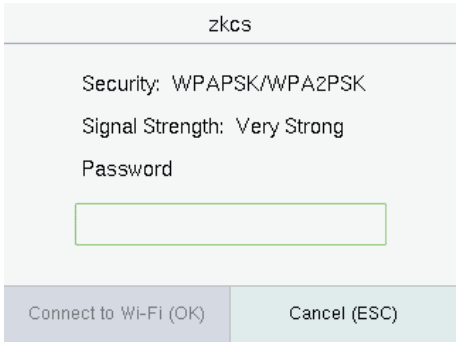


➢ **Búsqueda de la red Wi-Fi**

- El Wi-Fi está habilitado de forma predeterminada en el dispositivo. Active o desactive el Wi-Fi pulsando el botón «» (Activar/Desactivar Wi-Fi).
- Una vez activada la conexión Wi-Fi, el dispositivo buscará las redes Wi-Fi disponibles dentro del alcance de la red.
- Toque el nombre de la red Wi-Fi deseada en la lista disponible e introduzca la contraseña correcta en la interfaz de contraseña, luego toque **M/OK.**



Wi-Fi habilitado: pulse la red deseada en la lista de redes encontradas.



Toque el campo de contraseña para introducir la contraseña y toque M/OK.

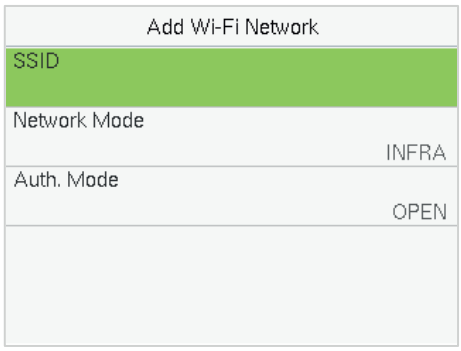
- Cuando la conexión Wi-Fi se haya establecido correctamente, la interfaz inicial mostrará el logotipo de Wi-Fi

➢ **Añadir una red Wi-Fi manualmente**

La red Wi-Fi también se puede añadir manualmente si la red Wi-Fi requerida no aparece en la lista.



Toque Añadir red Wi-Fi para añadir la red Wi-Fi manualmente

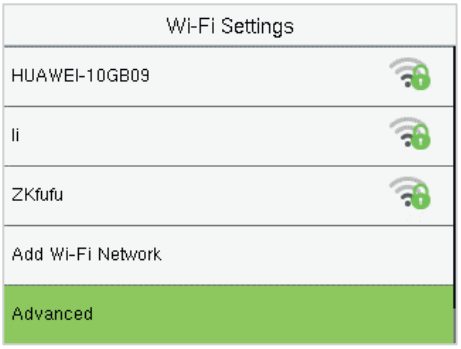


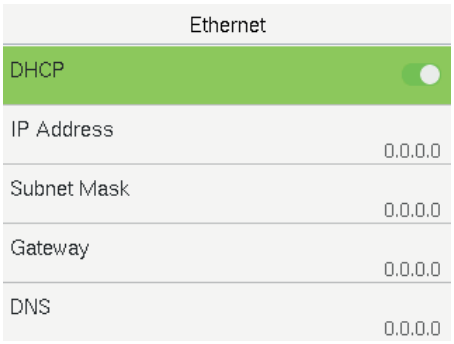
En esta interfaz, introduzca los parámetros de la red Wi-Fi. (La red añadida debe existir).

Nota: Después de añadir correctamente la red Wi-Fi de forma manual, siga el mismo proceso para buscar el nombre de la red Wi-Fi añadida.

➢ **Configuración avanzada**

En la interfaz de configuración de Wi-Fi, pulsa en Avanzado para configurar los parámetros pertinentes según sea necesario.



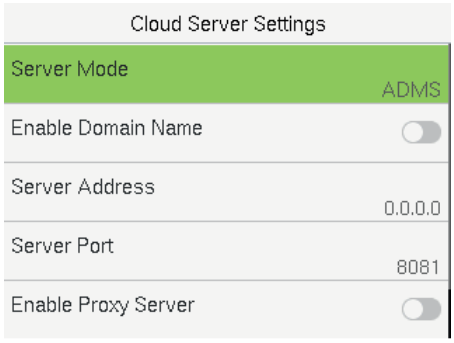


Descripción de la función

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

10.5 Configuración del servidor en la nube

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



Descripción de la función

Function Name		Description
Habilitar Nombre de dominio	**Server Address**	Una vez activado este modo, se utilizará el modo de nombre de dominio «http://...», como http://www.XYZ.com, donde «XYZ» denota el nombre de dominio.
Desactivar nombre de dominio	**Server Address**	La dirección IP del servidor ADMS.
	Server Port	Puerto utilizado por el servidor ADMS.
Habilitar servidor proxy		La dirección IP y el número de puerto del servidor proxy se configuran manualmente cuando se habilita el proxy

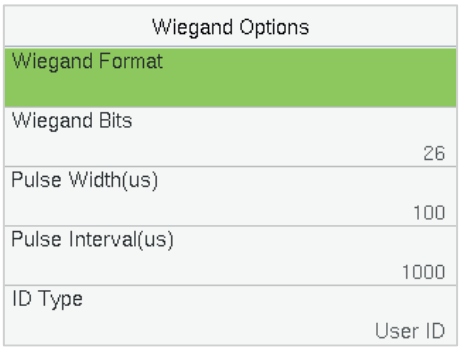
10.6 Configuración Wiegand

Se utiliza para configurar los parámetros de entrada y salida Wiegand.

Toque **Configuración Wiegand** en la interfaz Configuración **COMM.** para configurar los parámetros de entrada y salida Wiegand



10.6.1 Entrada Wiegand



Descripción de la función

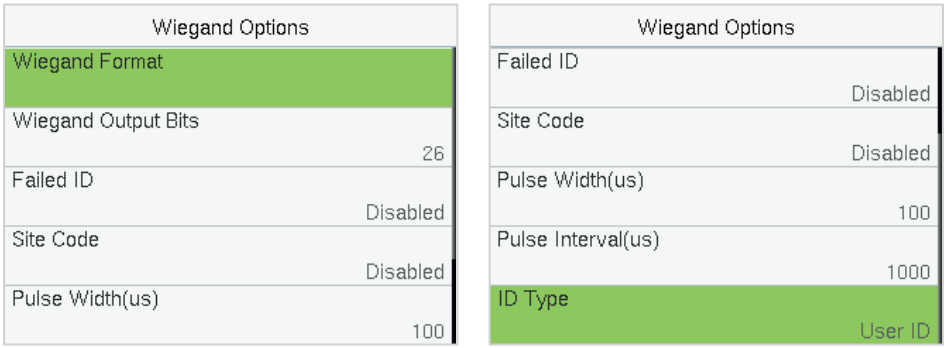
Nombre de la función	Descripción
Formato Wiegand	Su valor puede ser de 26 bits, 34 bits, 36 bits, 37 bits, 50 bits y 64 bits.
Bits Wiegand	El número de bits de los datos Wiegand.
Ancho de pulso (us)	El valor del ancho de pulso enviado por Wiegand es de 100 microsegundos por defecto, que se puede ajustar dentro del rango de 20 a 400 microsegundos.
Intervalo de pulso (us)	El valor predeterminado es 1000 microsegundos y se puede ajustar dentro del rango de 200 a 20 000 microsegundos.
Tipo de ID	Seleccione entre el ID de usuario y el número de tarjeta.

Descripción de varios formatos Wiegand comunes:

Formato Wiegand	Descripción
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 bit1 es el bit de paridad par de los bits 2 a13, mientras que el bit 26 es el bit de paridad impar de los bits 14 a 25. Los bits del 2.ºal 9.ºson los códigos de sitio, mientras que los bits del 10.ºal 25.ºson los números de tarjeta
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El primer bit es el bit de paridad par de los bits 2º a17º, mientras que el bit 34º es el bit de paridad impar de los bits18º a 33º. Los bits 2º a 25º son los números de la tarjeta.

Formato Wiegand	Descripción
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El bit 1 es el bit de paridad par de los bits 2 a17, mientras que el bit 34 es el bit de paridad impar de los bits 18 a 33. Los bits del 2.º al 9.º son los códigos de sitio, mientras que losbits del 10.º al 25.º son los números de tarjeta
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El bit 1es el bit de paridad impar de los bits 2 a18, mientras que el bit36 es el bit de paridad par de los bits 19 a 35. Los bits 2 a 17 son los códigos de dispositivo. Los bits del 18.ºal 33.ºson los números de tarjeta, y los bits del 34.º al 35.ºson los códigos de fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consta de 36 bits de código binario. El bit1 es el bit de paridad par de los bits 2 a18, mientras que el bit 36 es el bit de paridad impar de los bits 19 a 35. Los bits del 2.º al 19.º son los códigos de dispositivo, y losbits del 20.º al 35.º son los números de tarjeta.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE Consta de 37 bits de código binario. El primerbit es el bit de paridad impar de los bits 2º a18º, mientras que el bit 37º es el bit de paridad par de los bits19º a 36º. Los bits 2º a 4ºson los códigos del fabricante. Los bits del quinto al decimosexto son los códigos de sitio, y los bits del vigésimo primeroal trigésimo sexto son los números de tarjeta.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consta de 37 bits de código binario. El bit1es 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 2 a 4 son los códigos de fabricante. Los bits del quintoal decimocuarto son los códigos de dispositivo, los deldecimoquintoal vigésimo son los códigos de sitio y los del vigésimo primeroal trigésimo sextoson los números de tarjeta.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 50 bits de código binario. El bit 1 es el bit de paridad par de los bits 2 a 25, mientras que el bit 50 es el bit de paridad impar de los bits 26 a 49. Los bits del 2.º al 17.º son los códigos de sitio, y los bits del 18.º al 49.ºson los números de tarjeta.
«C» indica el número de tarjeta; **«E»** indica el bit de paridad par; **«O»** indica el bit de paridad impar. **«F»** indica el código de instalación; **«M»** indica el código de fabricante; **«P»** indica el bit de paridad; y **«S»** indica el código de sitio.	

10.6.2 Salida Wiegand



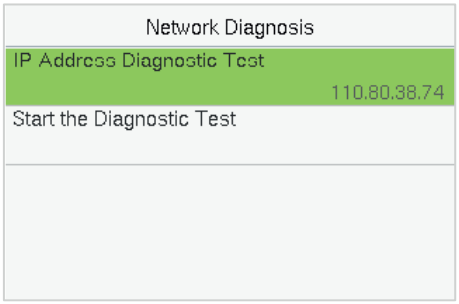
Descripción de la función

Nombre de la función	Descripción
Formato Wiegand	Su valor puede ser de 26 bits, 34 bits, 36 bits, 37 bits, 50 bits y 64 bits.
Bits de salida Wiegand	Después de seleccionar el formato Wiegand requerido, seleccione los dígitos de bits de salida correspondientes del formato Wiegand.
ID fallida	Si la verificación falla, el sistema enviará el ID fallido al dispositivo y sustituirá el número de tarjeta o el ID personal por uno nuevo.
Código de sitio	Es similar al ID del dispositivo. La diferencia es que un código de sitio se puede configurar manualmente y se puede repetir en un dispositivo diferente. El valor válido oscila entre 0 y 256 de forma predeterminada.
Ancho de pulso (us)	La anchura del tiempo representa los cambios en la cantidad de carga eléctrica con una capacitancia de alta frecuencia regular dentro de un tiempo especificado.
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.

10.7 Diagnóstico de red

Ayuda a configurar los parámetros de diagnóstico de red.

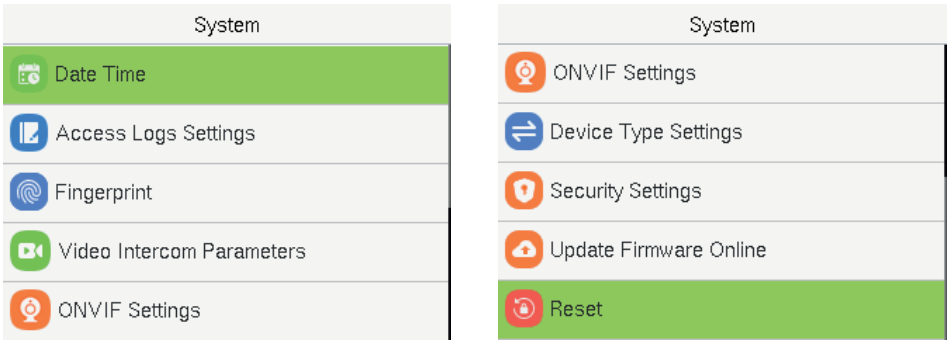
Toque **Diagnóstico de red** en la interfaz Configuración **de comunicación**. Introduzca la dirección IP que necesita ser diagnosticada y toque **Iniciar la prueba de diagnóstico** para comprobar si la red puede conectarse al dispositivo



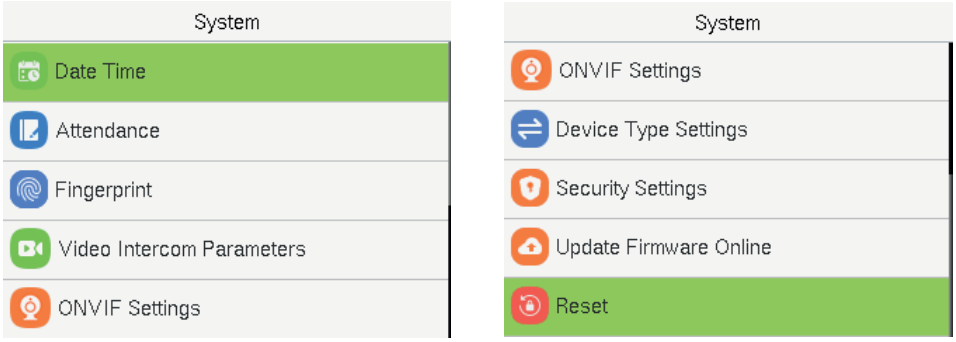
11 Configuración del sistema

Ayuda a configurar los parámetros del sistema relacionados para optimizar la accesibilidad del dispositivo. Cuando el dispositivo se encuentre en la interfaz inicial, pulse el botón **[M/OK] > Sistema.**

Terminal de control de acceso:

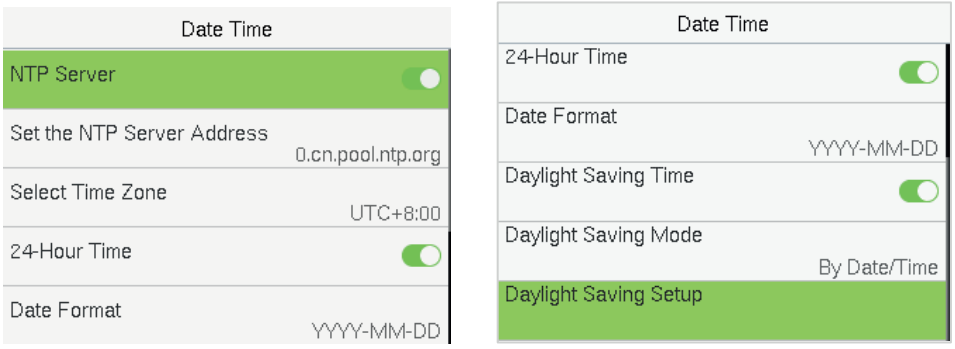


Terminal de control de asistencia:



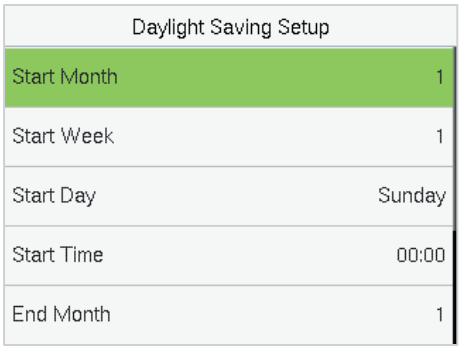
11.1 Fecha y hora

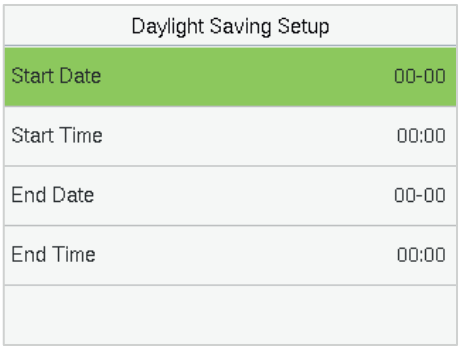
Toque **Fecha y hora** en la interfaz **del sistema** para configurar la fecha y la hora.



- Toque **Servidor NTP** para habilitar la sincronización automática de la hora según la dirección del servicio que introduzca.
- Toque **Fecha y hora manuales** para configurar manualmente la fecha y la hora y, a continuación, toque **Confirmar** y guardar

- Toque **Seleccionar zona horaria** para seleccionar manualmente la zona horaria en la que se encuentra el dispositivo.
- Active o desactive este formato tocando Hora de 24 horas. Si está activado, seleccione **Formato de fecha** para configurar la fecha.
- Toque «**Hora de verano**» para activar o desactivar la función. Si está activada, toque «**Modo de hora de verano**» para seleccionar un modo de hora de verano y, a continuación, toque «C**onfiguración de hora de verano**» para establecer el hora.





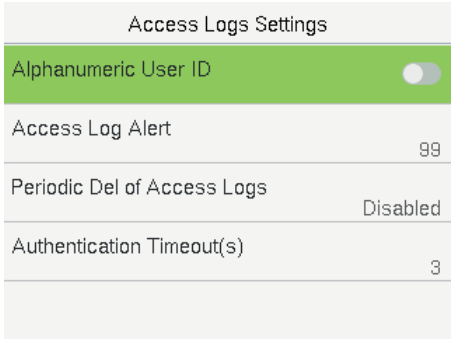
- Al restaurar los ajustes de fábrica, se pueden restaurar la hora (24 horas) y el formato de fecha (AAAA-MM-DD), pero no se pueden restaurar la fecha y la hora del dispositivo

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

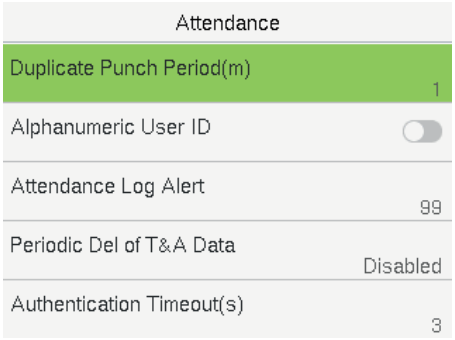
11.2 Configuración de registros de acceso / Asistencia

Toque Configuración de registros de acceso/Asistencia en la interfaz del sistema.

Terminal de control de acceso:



Terminal de control de asistencia:



Descripción de las funciones del terminal de control de acceso:

Nombre de la función	Descripción
ID de usuario alfanumérico	Habilitar/deshabilitar el alfanumérico como ID de usuario.
Alerta de registro de acceso	Cuando el espacio de registro del acceso de asistencia alcanza el valor umbral máximo, el dispositivo muestra automáticamente la advertencia de espacio de memoria. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999.
Eliminación periódica de registros deacceso	Cuando los registros de acceso alcanzan su capacidad máxima, el dispositivo elimina automáticamente un conjunto de registros de acceso antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 999
Tiempo de espera de autenticación	El tiempo que tarda en aparecer un mensaje de verificación correcta. Valor válido: de 1 a 9 segundos.

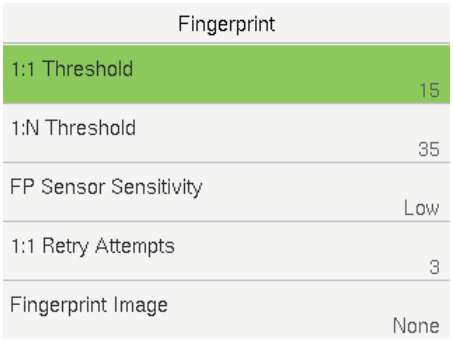
Descripción de la función del terminal de control de asistencia:

Nombre de la función	Descripción
Período de duplicado de fichaje (m)	Dentro de un periodo de tiempo establecido (unidad: minutos), no se reservará el registro de asistencia duplicado (el valor oscila entre 1 y 999999 minutos).
ID de usuario alfanumérico	Habilitar/deshabilitar el alfanumérico como ID de usuario.

Nombre de la función	Descripción
Alerta de registro de asistencia	Cuando el espacio de registro de asistencia alcanza el valor máximo, el dispositivo muestra automáticamente una advertencia de espacio de memoria. Los usuarios pueden desactivar la función o establecer un valor válido entre1 y 9999.
Eliminación periódica de datos de control de asistencia	Cuando los registros de asistencia alcanzan su capacidad máxima de almacenamiento, el dispositivo elimina automáticamente un conjunto de registros de asistencia antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 999
Tiempo de espera de autenticación	El tiempo que tarda en mostrarse un mensaje de verificación correcta. Valor válido: de 1 a 9 segundos.

11.3 Huella dactilar

Toque **Huella digital** en la interfaz **del sistema** para ir a la configuración de los parámetros de huella digital.



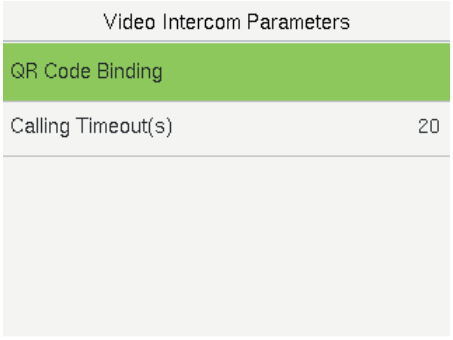
Descripción de la función

Nombre de la función	Descripción
Valor umbral 1:1	Con el método de verificación 1:1, la verificación solo se considerará satisfactoria cuando la similitud entre los datos de huella dactilar adquiridos y la plantilla de huella dactilar asociada al ID de usuario introducido y registrado en el dispositivo sea superior al valor establecido.
Valor umbral 1:N	Con el método de verificación 1:N, la verificación solo se considerará satisfactoria cuando la similitud entre los datos de huellas dactilares adquiridos y las plantillas de huellas dactilares registradas en el dispositivo sea superior al valor establecido.

Nombre de la función	Descripción
Sensibilidad del sensor FP	Para establecer la sensibilidad de la adquisición de huellas dactilares. Se recomienda utilizar el nivel predeterminado «Medio». Cuando el ambiente es seco, lo que ralentiza la detección 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».
Número de reintentos 1:1	En la verificación 1:1, los usuarios pueden olvidar la huella dactilar registrada o presionar el dedo de forma incorrecta. Para reducir el proceso de volver a introducir el ID de usuario, se permite reintentar.
Imagen de la huella dactilar	Para configurar si se muestra la imagen de la huella dactilar en la pantalla durante el registro o la verificación de la huella dactilar. 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 coincidencia:** para mostrar la imagen de la huella dactilar en la pantalla solo durante la verificación. **Mostrar siempre:** para mostrar la imagen de la huella dactilar en la pantalla durante el registro y la verificación **Ninguna:** no mostrar la imagen de la huella dactilar.

11.4 Parámetros del videoportero★

Toque **Parámetros del videoportero** en la interfaz **del sistema.**



Descripción de la función

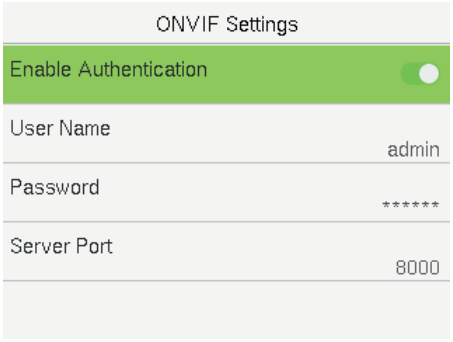
Nombre de la función	Descripción
Vinculación del código QR	Utilice el cliente de la aplicación ZSmart para escanear el código QR y conectar y vincular el dispositivo.
Tiempo de espera de llamada(s)	Si la llamada no se responde en un tiempo determinado, se sale a la interfaz principal.

Para obtener más información, consulte 22. Conexión a la aplicación ZSmart.

11.5 Configuración ONVIF★

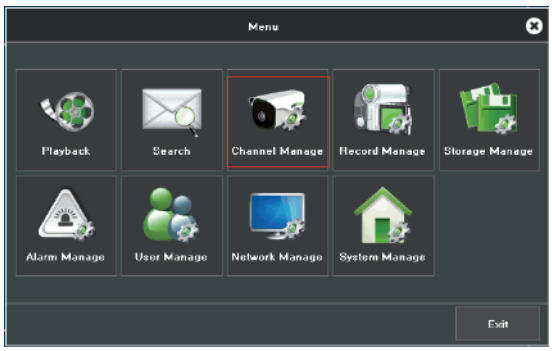
Nota: Esta función debe utilizarse con el grabador de vídeo en red (NVR).

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

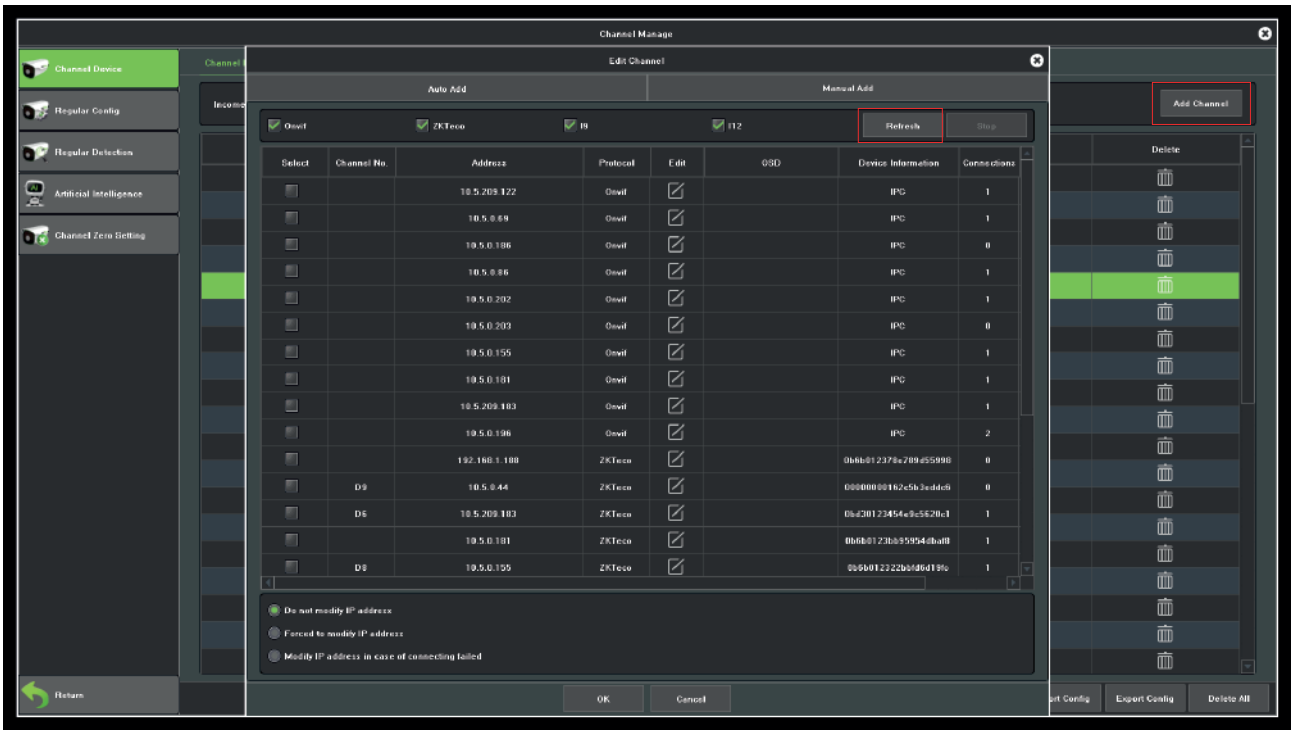


Nombre de la función	Descripción
Habilitar autenticación	Habilitar/Deshabilitar la función de autenticación. Cuando está deshabilitada, no es necesario introducir el nombre de usuario y la contraseña al añadir el dispositivo al NVR.
Nombre de usuario	Establezca el nombre de usuario. El valor predeterminado es admin.
Contraseña	Configure la contraseña. El valor predeterminado es admin.
Puerto del servidor	El valor predeterminado es 8000 y no se puede modificar.

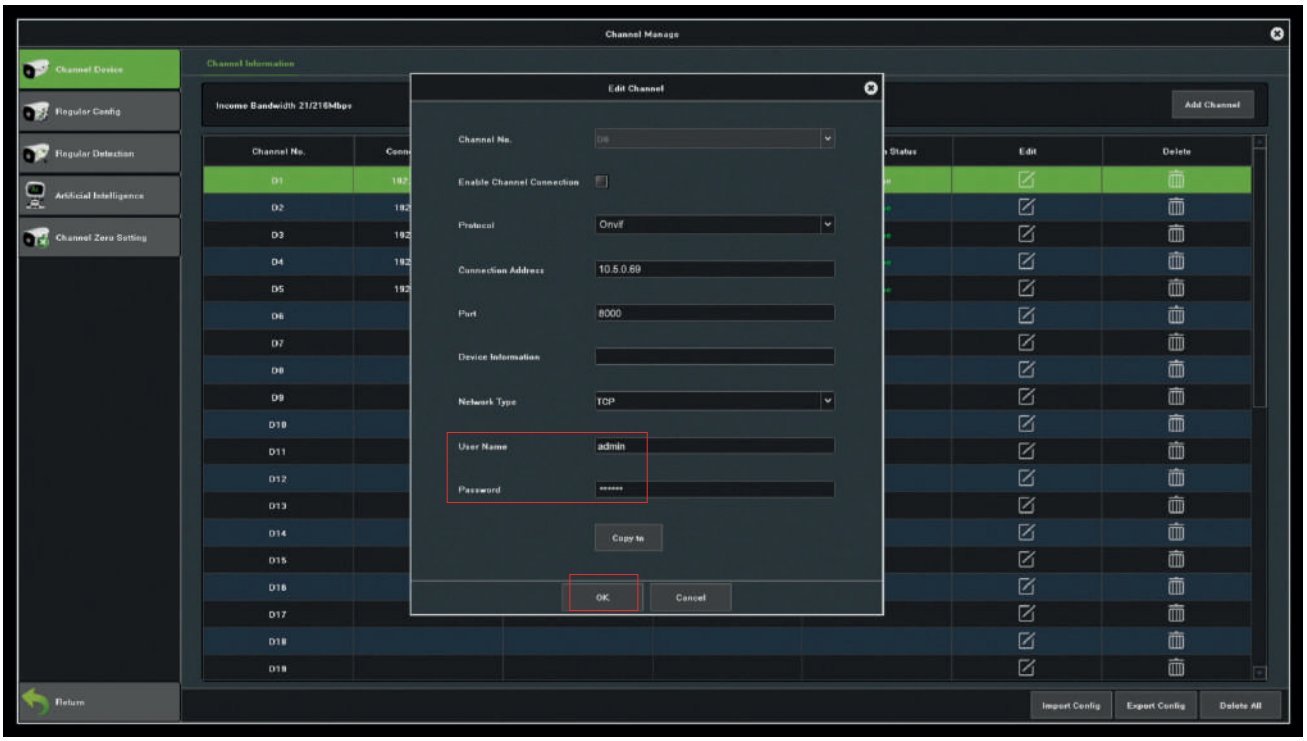
3. En el sistema NVR, haga clic en **[Inicio] > [Menú]** y aparecerá el menú principal.



4. Haga clic en **[Administrar canales] > [Añadir canal] > [Actualizar]** para buscar el dispositivo.

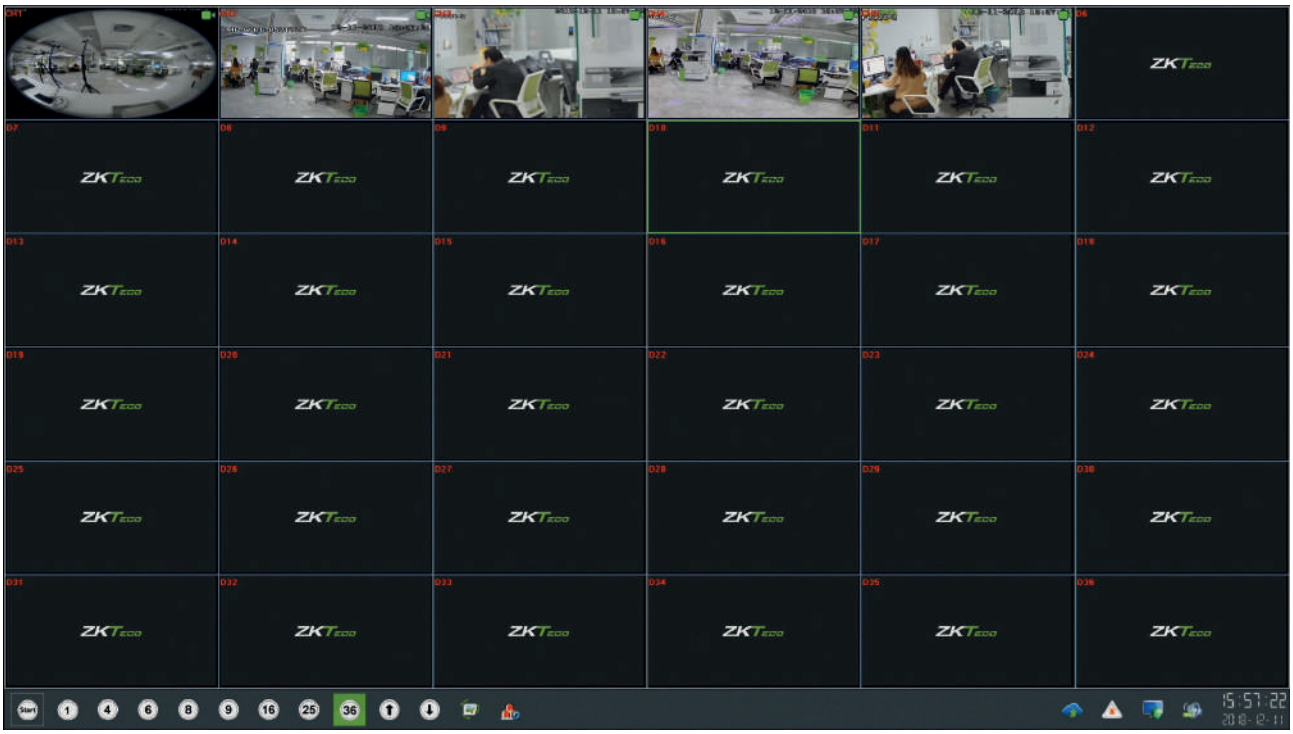


5. Seleccione la casilla de verificación del dispositivo que desea añadir y edite los parámetros en el campo de texto correspondiente, luego haga clic en **Aceptar** para añadirlo a la lista de conexiones.



Nota: El nombre de usuario y la contraseña se configuran en los **ajustes ONVIF** del dispositivo.

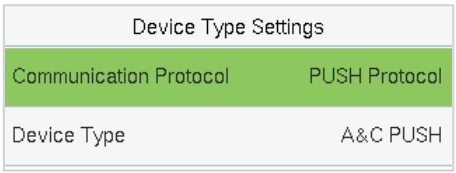
6. Una vez añadido correctamente, la imagen de vídeo obtenida del dispositivo se puede ver en tiempo real.



Para obtener más información, consulte el *manual del usuario del NVR*.

11.6 Configuración del tipo de dispositivo

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

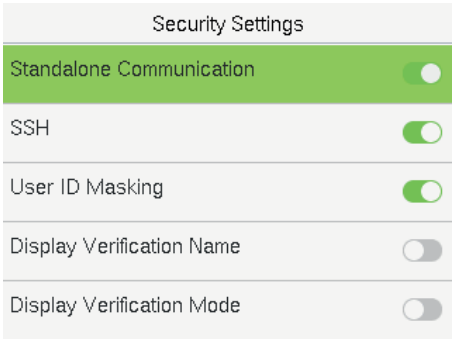


Nombre de la función	Descripción
Protocolo de comunicación	Configure el protocolo PUSH.
Tipo de dispositivo	Configure el dispositivo como terminal de control de acceso o terminal de asistencia.

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

11.7 Configuración de seguridad

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

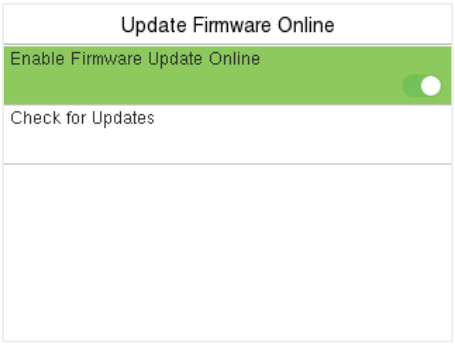


Descripción de la función

Nombre de la función	Descripción
Comunicación independiente	Para evitar no poder utilizar el dispositivo cuando esté desconectado, puede descargar previamente el software C/S (como ZKAccess 3.5) en su ordenador para utilizarlo sin conexión.
SSH	SSH se utiliza para acceder al fondo del dispositivo con fines de mantenimiento.
Enmascaramiento del ID de usuario	Cuando se habilita y, a continuación, se compara y verifica correctamente al usuario, el ID de usuario del resultado de la verificación mostrado se sustituirá por un * para lograr una protección segura de los datos privados confidenciales.
Mostrar nombre de verificación	Establezca si se mostrará el nombre de usuario en la interfaz de resultados de verificación.
Mostrar modo de verificación	Establezca si se muestra el modo de verificación en la interfaz de resultados de verificación

11.8 Actualizar firmware en línea

Toque **Actualizar firmware en línea** en la interfaz del sistema.



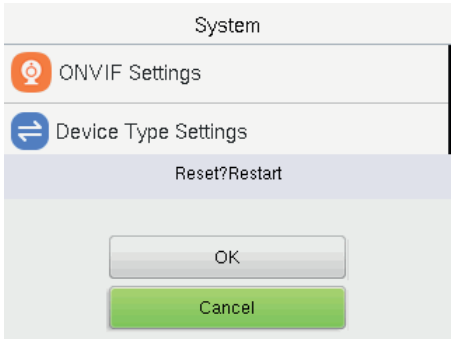
La función Actualizar firmware en línea está habilitada de forma predeterminada. Pulse **Buscar actualizaciones.** Pueden darse los tres casos siguientes:

- Si la consulta falla, la interfaz mostrará el mensaje «Consulta fallida»..
- Si la versión del firmware del dispositivo es la más reciente, aparecerá el mensaje «La versión actual del firmware ya es la más reciente».
- Si la versión del firmware del dispositivo no es la más reciente, se mostrarán el número de versión y el registro de cambios de la última versión. Los usuarios pueden elegir si desean actualizar a la última versión del firmware.

11.9 Restablecimiento de fábrica

La función 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).

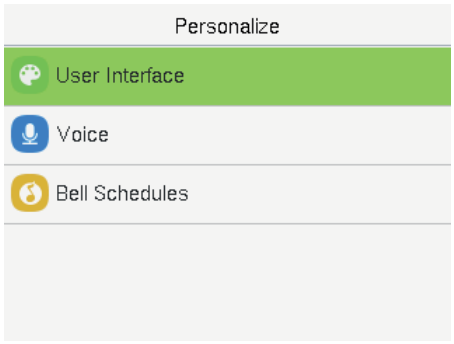
Toque **Restablecer** en la interfaz **del sistema** y, a continuación, toque **Aceptar** para restaurar la configuración predeterminada de fábrica



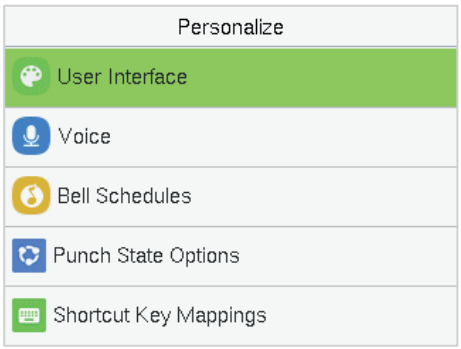
12 Personalizar ajustes

Cuando el dispositivo se encuentre en la interfaz inicial, pulse el botón **[M/OK] > Personalizar** para personalizar la configuración de la interfaz, la voz, la campana, las opciones de estado de punzonado y las asignaciones de teclas de acceso directo.

Terminal de control de acceso:

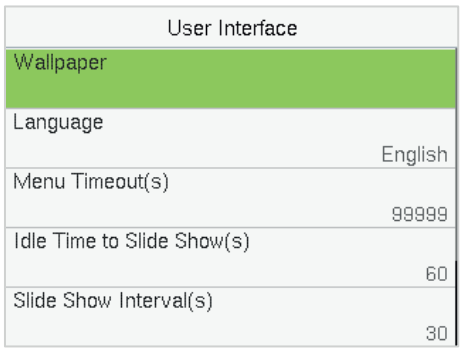


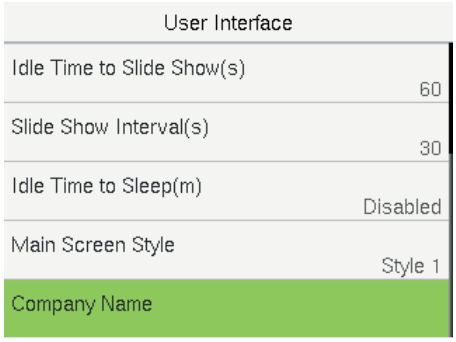
Terminal de control de asistencia:



12.1 Interfaz de usuario

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



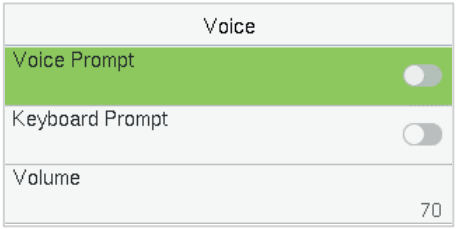


Descripción de la función

Nombre de la función	Descripción
Fondo de Pantalla	Ayuda a seleccionar el fondo de pantalla de la pantalla principal según las preferencias del usuario.
Idioma	Ayuda a seleccionar el idioma del dispositivo
Tiempo de espera del menú (s)	Cuando no se realiza ninguna operación y el tiempo excede el valor establecido, el dispositivo vuelve automáticamente a la interfaz inicial. La función se puede desactivar o establecer el valor requerido entre 60 y 99999 segundos.
Tiempo de inactividad para presentación de diapositivas (s)	Cuando no se realiza ninguna operación y el tiempo supera el valor establecido, se muestra una presentación de diapositivas. Esta función se puede desactivar o se puede configurar entre 3 y 999 segundos.
Intervalo(s) de presentación de diapositivas	Es el intervalo de tiempo para cambiar entre diferentes imágenes de la presentación. Esta función se puede desactivar o configurar entre 3 y 999 segundos.
Tiempo de inactividad (m)	Si el modo de suspensión está activado y no se realiza ninguna operación en el dispositivo, éste entrará en modo de espera. Esta función se puede desactivar o establecer un valor entre 1 y 999 minutos.
Estilo de pantalla principal	El estilo de la pantalla principal se puede seleccionar según la preferencia del usuario.
Nombre de empresa	Introduzca aquí el nombre de la empresa. Cuando la opción de nombre de la empresa está activada en la configuración de información de impresión, se imprime el nombre de la empresa.

12.2 Voz

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

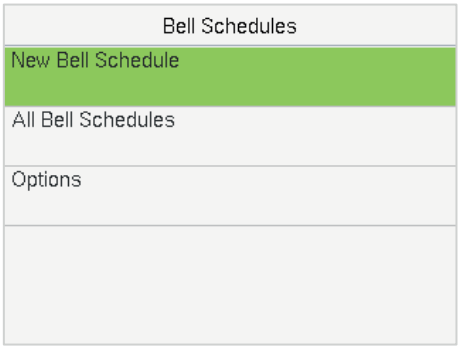


Descripción de la función

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

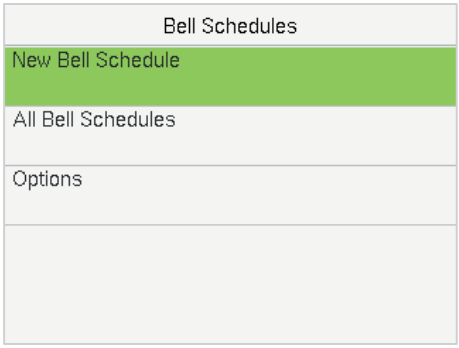
12.3 Horarios de timbre

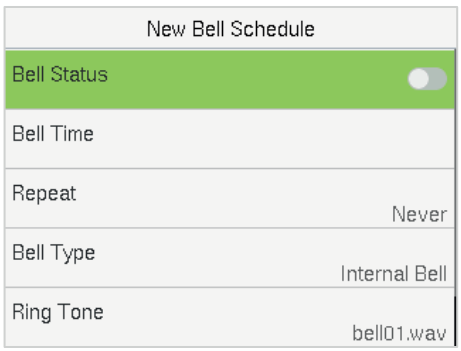
Toque **Horarios de timbre** en la interfaz **Personalizar** para configurar los ajustes de timbre



➢ **Nuevo horario de timbre:**

Toque **Nuevo horario** de timbre en la interfaz **Horario de timbre** para agregar 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 campana	Una vez establecido el tiempo requerido, el dispositivo se activa automáticamente para hacer sonar la campana durante ese tiempo.

Nombre de la función	Descripción
Repetir	Establezca el número necesario de recuentos para repetir la campana programada.
Tipo de campana	Seleccione el tipo de timbre: Timbre interno, Timbre externo o Timbre interno y externo.
Tono de llamada	Seleccione un tono de llamada
Retardo(s) de campana interna	Establezca el tiempo de repetición de la alarma interna. Los valores válidos oscilan entre 1 y 999 segundos

- **Todos los horarios de campana:**

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

- **Editar la campana programada:**

En la interfaz **Todos los horarios de timbre**, seleccione el horario deseado y luego **Editar** para editarlo. El método de edición es el mismo que para agregar un nuevo horario

- **Eliminar un horario de timbre:**

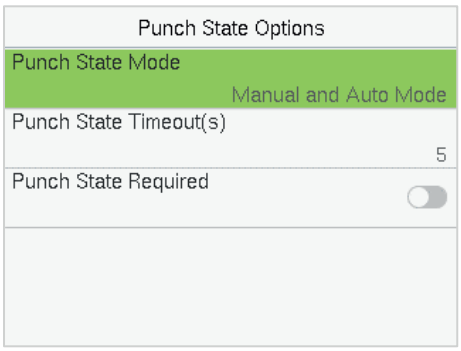
En la interfaz **Todos los horarios** de timbre , toque el horario de timbre requerido, toque **Eliminar** y luego toque **Sí** para eliminar la campana seleccionada.

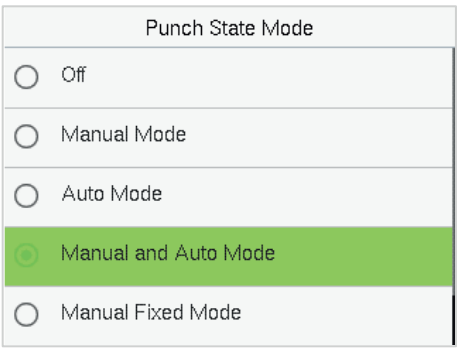
- **Opciones:**

Toque **Opciones** en la interfaz de **Programación de timbre** para configurar el terminal de salida de timbre externo NC1 o NC2, que se puede desactivar.

12.4 Opciones de estados de asistencia

Toque **Opciones de estados de asistencia** en la interfaz **Personalizar** para configurar los ajustes del estado de asistencia





Descripción de la función

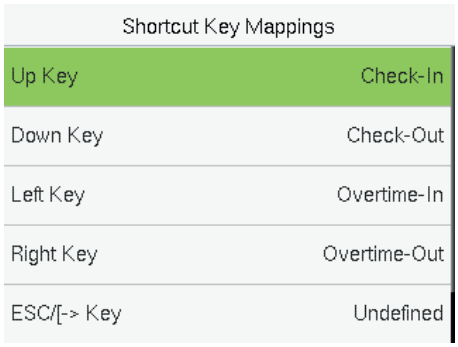
Nombre de la función	Descripción
Modo de estado de asistencia	**Desactivado:** Desactiva la función de estado de asistencia. Por lo tanto, la tecla de estado de fichaje configurada en el menú Asignaciones de teclas de acceso directo dejará de ser válida.

Nombre de la función	Descripción
	Modo manual: Cambie la tecla de estado de asistencia manualmente, y la tecla de estado de asistencia desaparecerá después del tiempo de espera del estado de asistencia. **Modo automático:** La tecla de estado de registro cambiará automáticamente a un estado de registro específico de acuerdo con el cronograma de tiempo predefinido que se puede configurar en las asignaciones de teclas de acceso directo **Modo manual y automático:** La interfaz principal mostrará la tecla para cambiar automáticamente el estado de asistencia. Sin embargo, los usuarios podrán seleccionar el estado de asistencia manual. Tras el tiempo límite, la tecla para cambiar manualmente al estado de asistencia se convertirá en la tecla para cambiar automáticamente. **Modo fijo manual:** Después de que la tecla de estado de asistencia se configura manualmente en un estado de asistencia particular, la función permanecerá sin cambios hasta que se cambie manualmente nuevamente **Modo Fijo:** Solo se mostrará la tecla de estado de fichaje fijada manualmente. Los usuarios no pueden cambiar el estado pulsando ninguna otra tecla
Tiempo(s) de espera del estado de asistencia	Es el tiempo que se muestra el estado del fichaje. El valor oscila entre 5 y 999 segundos
Estado de asistencia requerido	Seleccione si es necesario seleccionar un estado de asistencia después de la verificación. **ENCENDIDO:** El estado de asistencia debe seleccionarse después de la verificación. **APAGADO:** No es necesario seleccionar el estado de asistencia después de la verificación.

12.5 Asignaciones de teclas de acceso directo

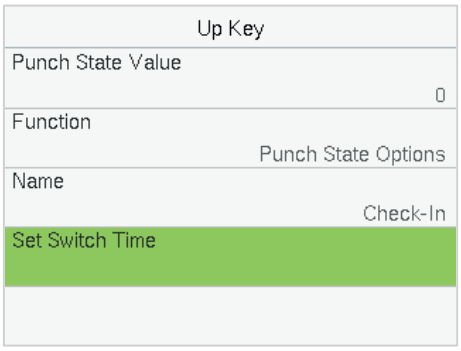
Los usuarios pueden definir atajos de teclado para el estado de asistencia y las teclas de función, que se mostrarán en la interfaz principal. De esta manera, al pulsar los atajos de teclado en la interfaz principal, se mostrará directamente el estado de asistencia o la interfaz de función correspondiente.

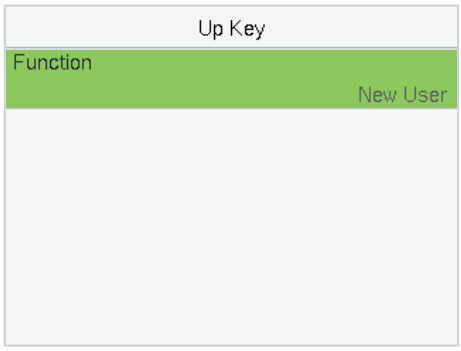
Toque **Asignaciones de teclas de acceso directo** en la interfaz **Personalizar** para configurar las teclas de acceso directo necesarias



- En la interfaz de asignaciones de teclas de acceso directo , toque la tecla de acceso directo requerida para configurar los ajustes de la tecla de acceso directo

- En la interfaz de la tecla de acceso directo (por ejemplo, "Tecla arriba"), toque la función para configurar el proceso funcional la tecla de acceso directo, ya sea como tecla de estado de asistencia o tecla de función.
- Si la tecla de acceso directo está definida como una tecla de función (como Nuevo usuario, Todos los usuarios, etc.), la configuración se completa como se muestra en la imagen a continuación

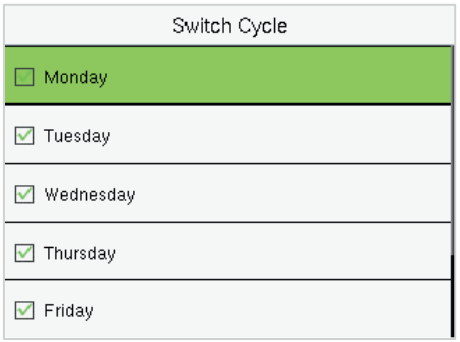


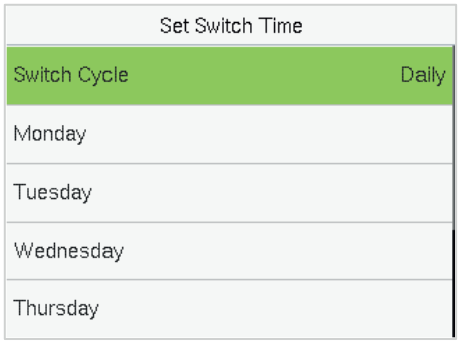


- Si la tecla de acceso directo se configura como una tecla de estado de registro (como registrar entrada, registrar salida, etc.), entonces es necesario configurar el valor del estado de registro (valor válido de 0 a 250), nombre.

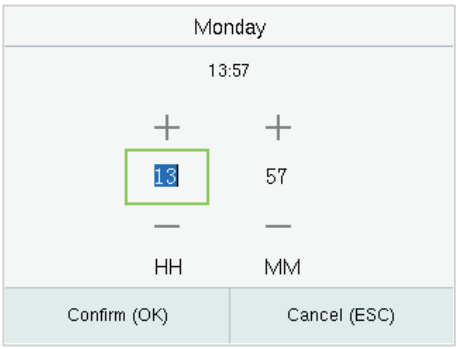
➢ **Establecer la hora del cambio**

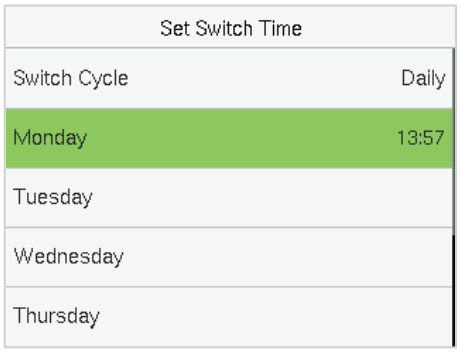
- El tiempo de cambio se establece de acuerdo con las opciones de estado de asistencia.
- Cuando el modo de estado de asistencia se establece en modo automático, se debe configurar el tiempo de cambio
- En la interfaz de teclas de acceso directo , toque Establecer hora de cambio para configurar la hora de cambio
- En la interfaz Ciclo de cambio , seleccione el ciclo de cambio (lunes, martes, etc.) como se muestra en la Imagen a continuación.





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

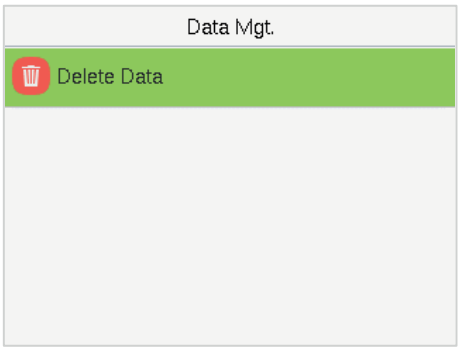




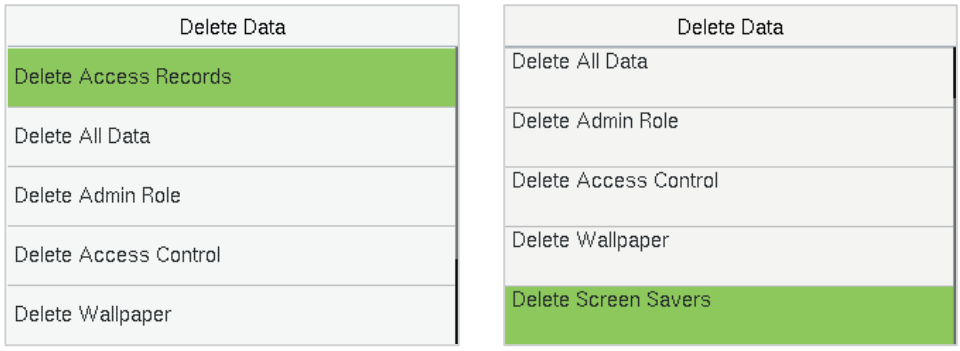
Nota: Cuando la función se establece en Indefinido, el dispositivo no habilitará la tecla de estado de asistencia.

13 Gestión de datos

Cuando el dispositivo esté en la interfaz inicial, presione el botón **[M/OK] > Administración de datos** para administrar los datos relevantes en el dispositivo.



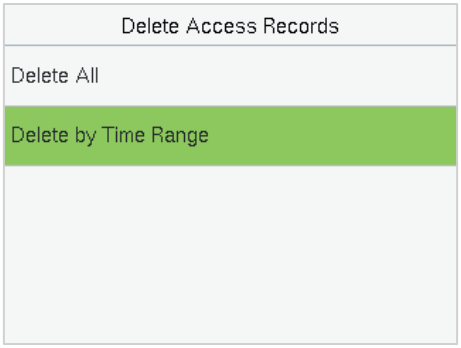
Toque **Eliminar datos** en la interfaz de **Administración de datos** para eliminar los datos requeridos.

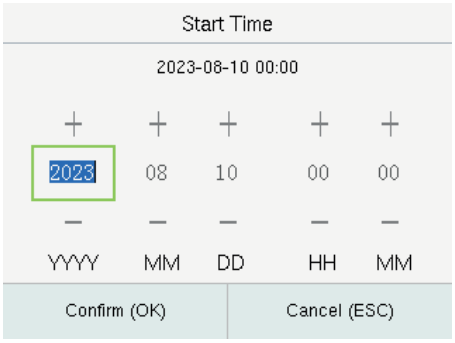


Descripción de la función

Nombre de la función	Descripción
Eliminar registros de acceso Datos de asistencia	Para eliminar los registros de acceso y datos de asistencia de forma condicional
Eliminar todos los datos	Para eliminar la información y acceder a los registros y datos de asistencia de todos los usuarios registrados
Eliminar rol de administrador	Para eliminar todos los privilegios de administrador.
Eliminar el control de acceso	Para eliminar todos los datos de acceso.
Eliminar fondo de pantalla	Para eliminar todos los fondos de pantalla del dispositivo.
Eliminar protectores de pantalla	Para eliminar todos los protectores de pantalla del dispositivo.
Eliminar lista de contact	Para eliminar toda la lista de contactos del videoportero en el dispositivo.

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

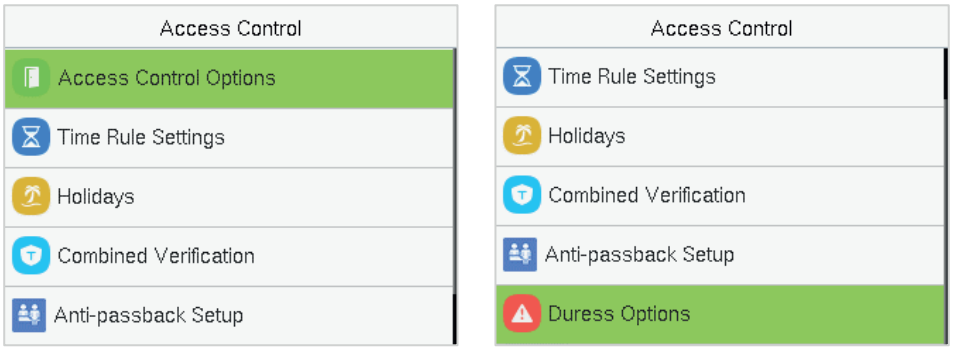




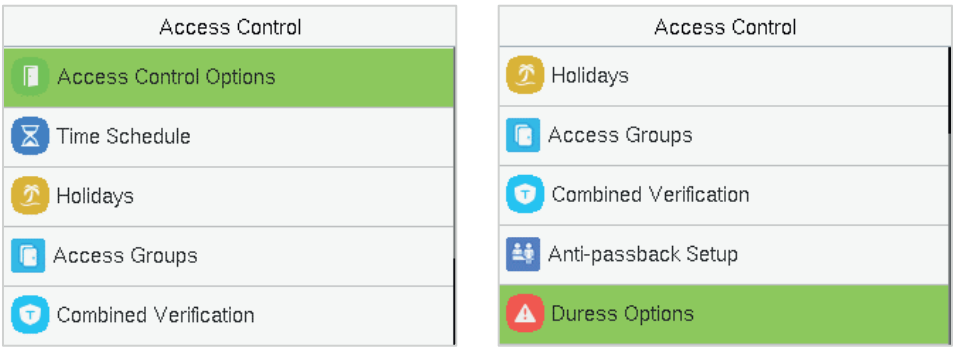
14 Control de acceso

Cuando el dispositivo esté en la interfaz inicial, presione el botón **[M/OK] > Control de acceso** para configurar el cronograma de apertura de puertas, el control de cerraduras y configurar otros parámetros relacionados con el control de acceso.

Terminal de control de acceso:



Terminal de control de asistencia:



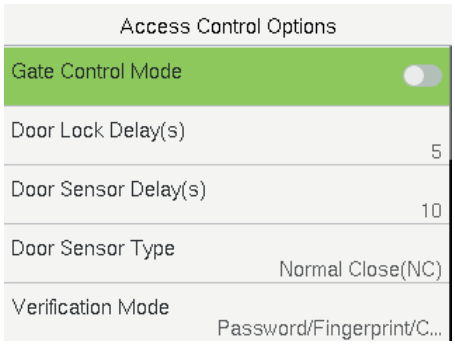
Para acceder, el usuario registrado deberá cumplir las siguientes condiciones:

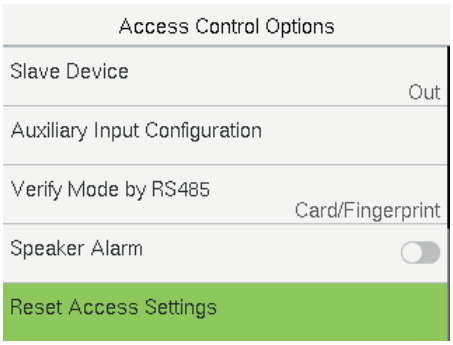
1. La hora actual de desbloqueo de la puerta en cuestión debe estar comprendida dentro de cualquier zona horaria válida del periodo de tiempo del usuario.
2. El grupo de usuarios correspondiente debe estar ya configurado en la combinación de desbloqueo de la puerta (y si hay otros grupos configurados en la misma combinación de acceso, entonces también se requiere la verificación de los miembros de esos grupos para desbloquear la puerta).
3. En la configuración predeterminada, los nuevos usuarios se asignan al primer grupo con la zona horaria del grupo predeterminada, donde el combo de acceso es "1" y está configurado en estado de desbloqueo por defecto.

14.1 Opciones de control de acceso

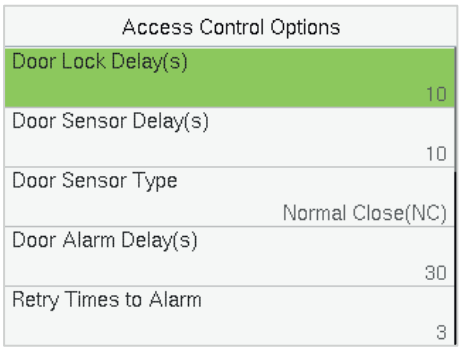
Toque **Opciones de control de acceso** en la interfaz de **Control de acceso** para configurar los parámetros del bloqueo de control de la terminal y el equipo relacionado

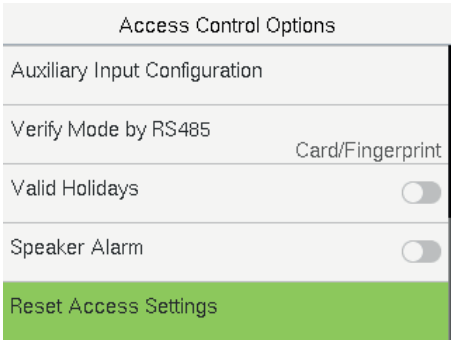
Terminal de control de acceso:





Terminal de control de asistencia:





Descripción de la función del terminal de control de acceso:

Nombre de la función	Descripción
Modo de control de puerta	Alterna entre el interruptor ON o OFF para entrar en el modo de control de puerta o no. Cuando se configura en ENCENDIDO, la interfaz elimina las opciones Retraso de bloqueo de puerta, Retraso de sensor de puerta y Tipo de sensor de puerta.
Retardo(s) de bloqueo de puerta	El tiempo que el dispositivo controla la cerradura eléctrica para que esté en estado de desbloqueo. Valor válido: 1~99 segundos.
Retardo(s) del sensor de puerta	Si la puerta no está bloqueada y se deja abierta durante un período determinado (retardo del sensor de puerta), se activará una alarma. El valor válido del retardo del sensor de puerta varía entre 1 y 255 segundos.

Nombre de la función	Descripción
Tipo de sensor de puerta	Hay tres tipos de sensores: **Ninguno, Normalmente abierto y Normalmente cerrado.** **Ninguno:** significa que el sensor de la puerta no está en uso. **Normalmente abierto:** significa que la puerta siempre se deja abierta cuando hay energía eléctrica encendida. **Normalmente cerrado:** significa que la puerta siempre queda cerrada cuando hay energía eléctrica encendida
Modo de verificación	El modo de verificación admitido incluye Contraseña/Huella dactilar/Tarjeta, 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).
Período de tiempo disponible de la puerta	Establece el tiempo para que la puerta sea accesible solo durante ese período.
Período de tiempo abierto normal	Es el período de tiempo programado para el modo "Normalmente Abierto" para que la puerta esté siempre abierta durante este período.
Dispositivo Maestro	Al configurar los dispositivos maestro y esclavo, puede establecer el estado del maestro como **Salida o Entrada.** **Salida:** A record of verification on the master device is a check-out record. **Entrada:** Un registro de verificación en el dispositivo maestro es un registro de entrada.
Dispositivo Esclavo	Al configurar los dispositivos maestro y esclavo, puede establecer el estado del esclavo como **Salida o Entrada** **Salida:** Un registro de verificación en el dispositivo maestro es un registro de salida. **Entrada:** Un registro de verificación en el dispositivo esclavo es un registro de entrada.
Configuración de la entrada auxiliar	Establece el 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	Cuando se activa la función de lector RS485, se utiliza este método de verificación tanto si el dispositivo se utiliza como maestro como si se utiliza como esclavo.
Alarma con altavoz	Transmite una alarma sonora o una alarma de desmontaje desde el panel local. Cuando la puerta se cierra o la verificación se realiza con éxito, el sistema cancela la alarma desde el panel local.

Nombre de la función	Descripción
Restablecer configuración de acceso	Los parámetros de reinicio del control de acceso incluyen el retraso del bloqueo de la puerta, el retraso del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el período de tiempo disponible de la puerta, el período de tiempo de apertura normal, el dispositivo maestro y la alarma. Sin embargo, los datos de control de acceso borrados en Gestión de datos quedan excluidos

Descripción de la Función del Terminal de Control de Asistencia

Nombre de la función	Descripción
Retardo(s) de bloqueo de puerta	El tiempo que el dispositivo controla la cerradura eléctrica para que esté en estado de desbloqueo. Valor válido: 0 a 10 segundos.
Retardo(s) del sensor de puerta	Si la puerta no está bloqueada y se deja abierta durante un período determinado (retardo del sensor de puerta), se activará una alarma. El valor válido del retardo del sensor de puerta varía entre 1 y 255 segundos.
Tipo de sensor de puerta	Hay tres tipos de sensores: Ninguno, Normalmente abierto y Normalmente cerrado. **Ninguno:** Significa que el sensor de la puerta no está en uso. **Normalmente abierto (NO):** Significa que la puerta siempre se deja abierta cuando hay energía eléctrica encendida. **Normalmente cerrado (NC):** significa que la puerta siempre queda cerrada cuando hay energía eléctrica encendida.
Retardo(s) de alarma de puerta	Cuando el número de verificaciones fallidas alcance el valor establecido (el valor varía de 1 a 9 veces), se activará la alarma. Si el valor establecido es Ninguno, la alarma no se activará tras una verificación fallida.
Veces de reintento para la alarma	Cuando el número de verificaciones fallidas alcance el valor establecido (el valor varía de 1 a 9 veces), se activará la alarma. Si el valor establecido es Ninguno, la alarma no se activará tras una verificación fallida
Período de tiempo abierto normal	Es el período de tiempo programado para el modo "Cierre normal" para que la puerta esté siempre cerrada durante este período
Configuración de entrada auxiliar	Es el período de tiempo programado para el modo "Normalmente Abierto" para que la puerta esté siempre abierta durate este período
Configuración de entrada auxiliar	Establece el 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.

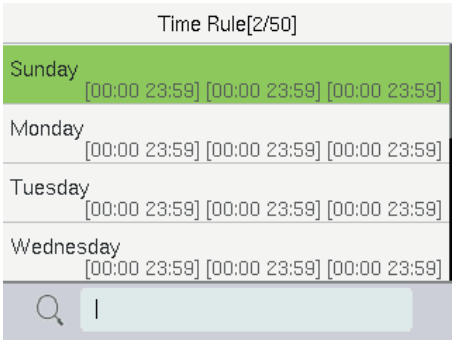
Nombre de la función	Descripción
Modo de verificación por RS485	Cuando la función de lector RS485 está activada, la verificación Este método se utiliza cuando el dispositivo se utiliza como maestro o esclavo.
Días festivos válidos	Para configurar si los ajustes del Período de Cierre Normal o del Período de Apertura Normal son válidos durante el período de vacaciones establecido. Seleccione [ON] para habilitar el período de NC o NO establecido durante las vacaciones.
Alarma con altavoz	Transmite una alarma sonora o alarma de desmontaje desde el local. Cuando la puerta se cierra o la verificación es exitosa, el sistema cancela la alarma del local.
Restablecer configuración de acceso	Los parámetros de restablecimiento del control de acceso incluyen el retardo de bloqueo de la puerta, el retardo del sensor de la puerta, el tipo de sensor de la puerta, el retardo de la alarma de la puerta, el tiempo de cierre normal, el tiempo de apertura normal y la alarma. Sin embargo, se excluyen los datos de control de acceso borrados en la Gestión de Datos.

14.2 Configuración de reglas de tiempo / Programación de tiempo

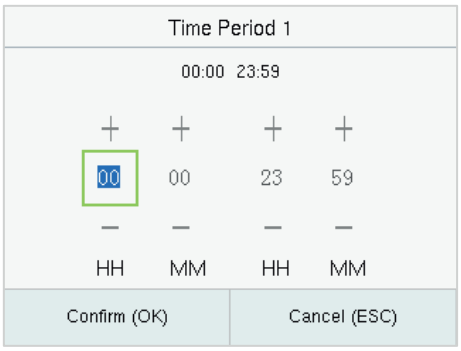
Toque Configuración de reglas de tiempo/Programación de tiempo en la interfaz de Control de acceso para configurar los ajustes de tiempo.

- 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 es "OR". Por lo tanto, cuando la hora de verificación cae dentro de cualquiera de estos períodos, la verificación es válida.
- El formato de zona horaria de cada período de tiempo es HH MM HH MM, que es preciso en 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 pantalla de selección de la zona horaria, pulsa el día correspondiente (es decir, lunes, martes, etc.) para ajustar la hora.



Especifique la hora de inicio y finalización y luego toque **M/OK.**

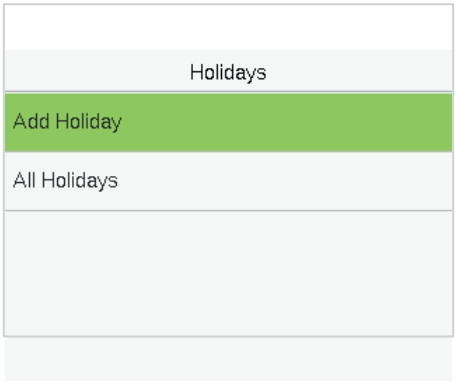
Nota:

1. La puerta es inaccesible durante todo el día cuando la hora de finalización ocurre antes de la hora de inicio (por ejemplo, 23:57 a 23:56)
2. Es el intervalo de tiempo para el acceso válido cuando la hora de finalización ocurre después de la hora de inicio (por ejemplo, 08:00 hasta 23:59).
3. La puerta es accesible durante todo el día cuando la hora de finalización ocurre después de la hora de inicio (por ejemplo, la hora de inicio es 00:00 y la hora de finalización es 23:59).
4. La zona horaria predeterminada 1 indica que la puerta está abierta todo el día.

14.3 Días festivos

Cuando hay un día festivo, es posible que necesites un horario de acceso diferente; sin embargo, modificar el horario de acceso de cada persona una por una lleva mucho tiempo. Por eso, se puede configurar un horario de acceso para días festivos que se aplique a todos los trabajadores, de modo que el usuario pueda abrir la puerta durante esos días.

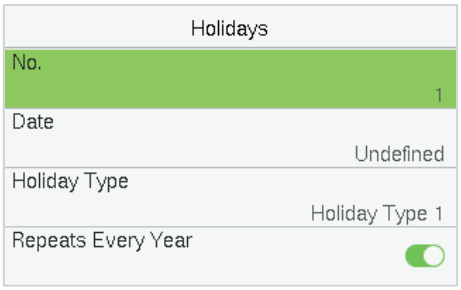
Toque Vacaciones en la interfaz de Control de acceso para configurar el acceso durante las vacaciones.



➢ **Agregar un nuevo día festivo:**

Toque Agregar feriado en la interfaz de Feriados y configure los parámetros de feriados.

Terminal de control de acceso:



Terminal de control de asistencia:



➢ **Editar un día festivo**

En la interfaz de **Días Festivos** , seleccione el elemento de día festivo que desee modificar. Pulse **Editar** para modificar los parámetros de los días festivos.

➢ **Eliminar un día festivo:**

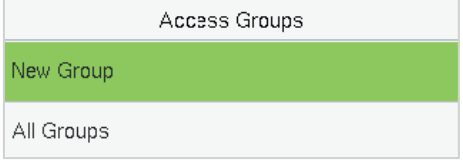
En la pantalla **Días festivos**, selecciona el día festivo que deseas eliminar y pulsa **Eliminar**. Pulsa M/Aceptar para confirmar la eliminación. Una vez eliminado, este día festivo ya no aparecerá en la pantalla Todos los días festivos.

14.4 Grupos de acceso

La agrupación es para administrar usuarios en grupos, solo para terminal de control de asistencia.

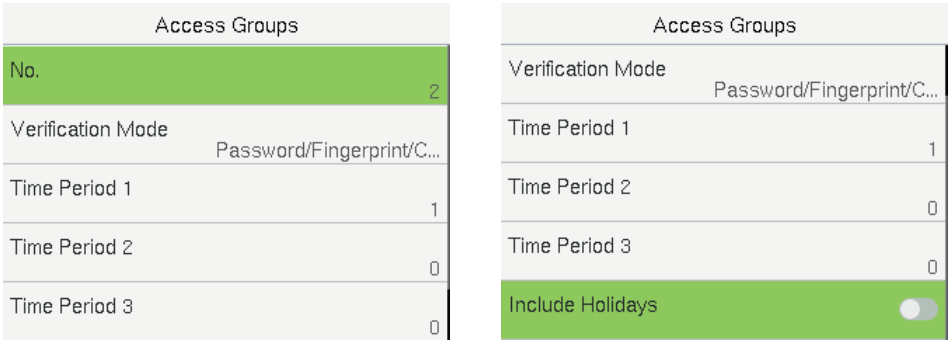
La zona horaria predeterminada para los miembros del grupo es la del grupo, mientras que los usuarios pueden configurar su propia zona horaria. Cuando el modo de verificación de grupo y el de usuario se superponen, este último tiene prioridad. Cada grupo puede configurar un máximo de tres zonas horarias; siempre que una de ellas sea válida, el grupo se puede verificar correctamente. El usuario recién registrado se asigna al Grupo deacceso 1 por defecto, pero puede asignarse a otro grupo de acceso.

Toque Grupos de acceso en la interfaz de Control de acceso



➢ **Agregar un nuevo día festivo:**

Toque **Nuevo grupo** en la interfaz de Grupo de acceso



Note:

1. El sistema tiene un grupo de acceso predeterminado numerado 1, que no se puede eliminar pero sí modificar
2. Un número no se puede modificar nuevamente después de haberlo establecido.
3. Cuando se establece que el día festivo es válido, el personal de un grupo solo puede abrir la puerta cuando el horario del grupo coincide con el horario del día festivo.
4. Cuando el día festivo se establece como inválido, el tiempo de control de acceso del personal de este grupo no se ve afectado por los días festivos.

➢ **Editar grupo:**

En la interfaz «Todos los grupos», pulsa para seleccionar el elemento del grupo de acceso que deseas modificar. Pulsa «Editar» para modificar los parámetros del grupo.

➢ **Eliminar un grupo:**

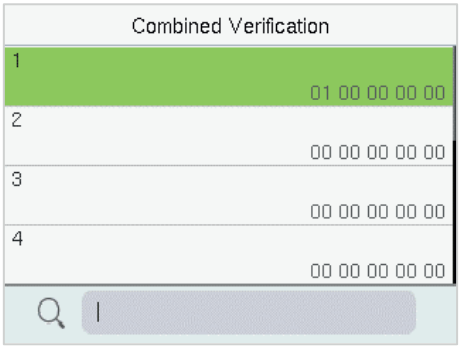
En la pantalla «Todos los grupos», selecciona el grupo de acceso que deseas eliminar y pulsa «Eliminar». Pulsa «M/Aceptar» para confirmar la eliminación. Una vez eliminado, este grupo ya no aparecerá en la pantalla «Todos los grupos».

14.5 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 para abrir una puerta, el intervalo del número combinado N es $0 \leq N \leq 5$, y los N miembros pueden pertenecer todos a un mismo 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 desea configurar, toque las flechas hacia arriba y hacia abajo para ingresar el número de combinación y luego toque M/OK.

Por ejemplo:

- Si la combinación de desbloqueo de puerta 1 está configurada como (01 03 05 06 08), esto indica que dicha combinación está compuesta por 5 personas y que todas ellas pertenecen a 5 grupos: Grupo AC 1, Grupo AC 3, Grupo AC 5, Grupo AC 6 y Grupo AC 8, respectivamente.
- Si la combinación de desbloqueo de puerta 2 está configurada como (02 02 04 04 07), indica que la combinación de desbloqueo 2 está compuesta por 5 personas: las dos primeras pertenecen al grupo de aire acondicionado 2, las dos siguientes al grupo de aire acondicionado 4 y la última al grupo de aire acondicionado 7.
- Si la combinación de desbloqueo de puerta 3 está configurada como (09 09 09 09 09), indica que hay 5 personas en esta combinación; todas pertenecen al grupo 9 de aire acondicionado
- Si la combinación de desbloqueo de puerta 4 está configurada como (03 05 08 00 00), indica que la combinación de desbloqueo 4 está compuesta por solo tres personas: la primera persona pertenece al grupo de aire acondicionado 3, la segunda al grupo de aire acondicionado 5 y la tercera al grupo de aire acondicionado 8

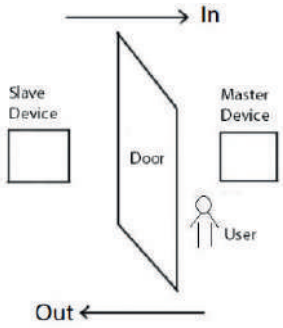
Nota: Para eliminar la combinación de desbloqueo de puerta, configure todas las combinaciones de desbloqueo de puerta en 0.

14.6 Configuración anti-passback

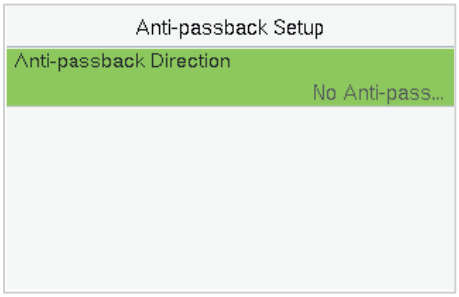
Un usuario podría ser seguido por otra persona para entrar sin verificación, lo que podría provocar una vulneración de seguridad. Para evitar estas situaciones, se desarrolló la opción Anti Passback. Una vez activada, el registro de entrada y salida debe realizarse alternativamente para abrir la puerta y así representar un patrón consistente

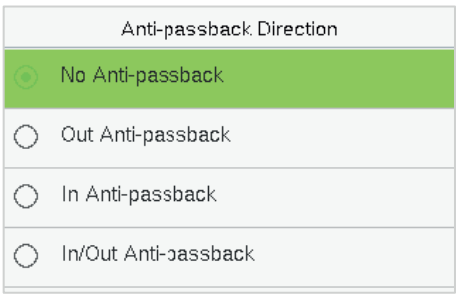
Esta función requiere que dos dispositivos funcionen juntos:

Un dispositivo se instala en el lado interior de la puerta (dispositivo maestro) y el otro se instala en el lado interior de la puerta (dispositivo maestro). El lado exterior de la puerta (dispositivo esclavo). Ambos dispositivos se comunican mediante la señal Wiegand. El formato Wiegand y el tipo de salida (ID de usuario/Número de tarjeta) adoptados por el dispositivo maestro y el dispositivo esclavo deben ser consistentes.



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





Descripción de la función:

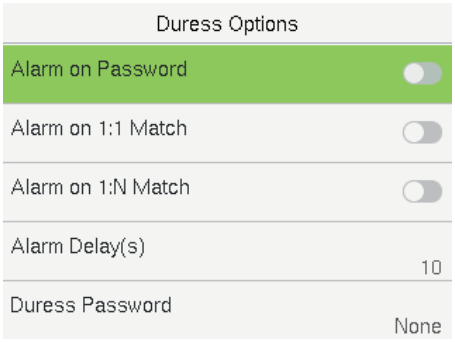
Nombre de la función	Descripción
Dirección Anti-passback	**Sin función anti-passback:** La función anti-passback está desactivada, lo que significa que la puerta se puede desbloquear tras una verificación satisfactoria realizada tanto desde el dispositivo maestro como desde el dispositivo esclavo. Con esta opción, no se guarda el estado de asistencia. **Anti passback de salida:** El usuario solo puede salir si el último registro es de entrada; de lo contrario, se activa una alarma. Sin embargo, el usuario puede entrar libremente. **En el modo Anti-Passback:** el usuario solo puede volver a registrarse si el último registro es de salida; de lo contrario, se activa una alarma. Sin embargo, el usuario puede salir libremente. **Anti passback de entrada/salida:** en este caso, un usuario puede realizar el check in solo si el último registro es un check out o el usuario puede realizar el check out solo si el último registro es un check in, de lo contrario se activa la alarma.

14.7 Configuración de opciones de coacción

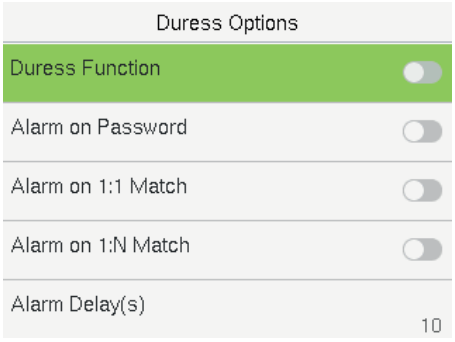
Una vez que un usuario activa la función de verificación de coacción con uno o más métodos de autenticación específicos, y cuando se encuentra bajo coacción y se autentica mediante verificación de coacción, el dispositivo desbloquea la puerta como de costumbre. Simultáneamente, se envía una señal para activar la alarma

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

Terminal de control de acceso:



Terminal de control de asistencia:



Descripción de la función del terminal de control de acceso:

Nombre de la función	Descripción
Alarma por contraseña	Cuando un usuario utiliza el método de verificación de contraseña, se generará una señal de alarma, de lo contrario no habrá señal de alarma
Alarma en el partido 1:1	Cuando un usuario utiliza el método de verificación 1:1, se generará una señal de alarma; de lo contrario, no habrá ninguna señal de alarma
Alarma en partido 1:N	Cuando un usuario utiliza el método de verificación 1:N, se generará una señal de alarma; de lo contrario, no habrá ninguna señal de alarma
Retardo de alarma(s)	La señal de alarma no se transmitirá hasta que transcurra el tiempo de retardo de alarma. El valor varía de 1 a 999 segundos.
Contraseña de emergencia	Establezca la contraseña de coacción de 6 dígitos. Cuando el usuario la ingrese para verificación, se generará una señal de alarma

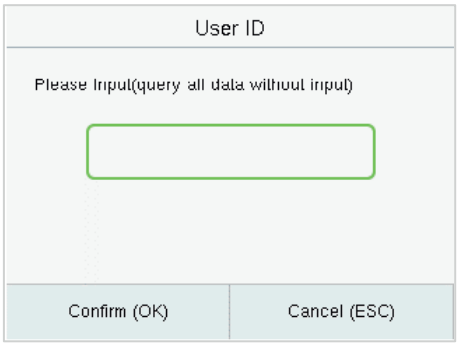
Descripción de la función del terminal de control de asistencia:

Function Name	Description
Función de coacción	Habilitar/Deshabilitar la función de coacción
Alarma por contraseña	En el estado [ON] , se activará la alarma cuando un usuario use el método de verificación de contraseña. En el estado [OFF] , no se activará ninguna señal de alarma.
Alarma por coincidencia 1:1	Cuando un usuario utiliza el método de verificación 1:1, se generará una señal de alarma; de lo contrario, no habrá ninguna señal de alarma
Alarma por coincidencia 1:N	Cuando un usuario utiliza el método de verificación 1:N, se generará una señal de alarma; de lo contrario, no habrá ninguna señal de alarma.
Retardo de alarma (s)	La señal de alarma no se transmitirá hasta que transcurra el tiempo de retardo de alarma. El valor varía de 1 a 999 segundos.

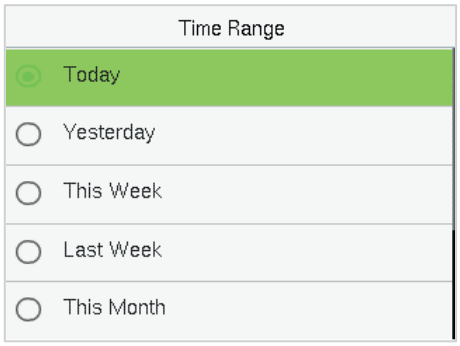
15 Búsqueda de asistencia

Una vez verificada la identidad de un usuario, los datos de acceso y asistencia se guardan en el dispositivo. Esta función permite a los usuarios consultar sus registros de eventos.

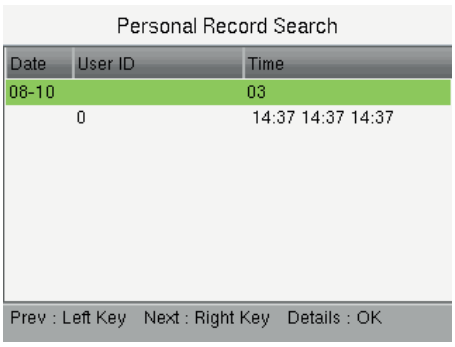
Cuando el dispositivo esté en la interfaz inicial, presione el botón **[M/OK] > Búsqueda de asistencia** para buscar los registros de eventos requeridos.



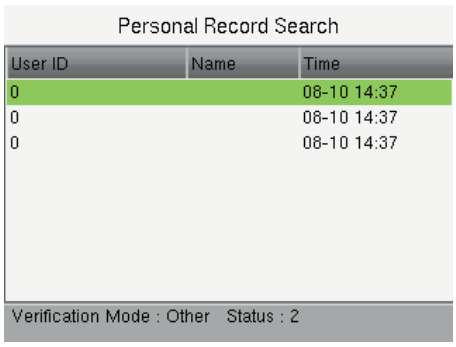
1. Introduce el ID de usuario que deseas buscar y pulsa M/OK. Si deseas buscar registros de todos los usuarios, pulsa M/OK sin introducir ningún ID de usuario.



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



3. Una vez finalizada la búsqueda de registros, pulsa sobre el registro resaltado en verde para ver sus detalles.

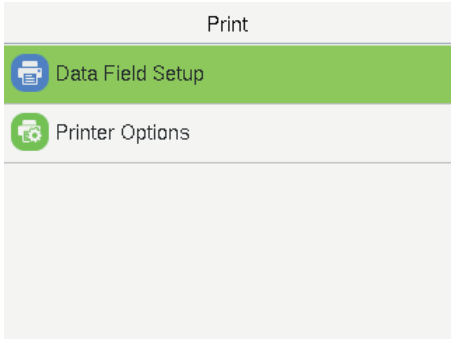


4. La figura muestra los detalles del registro seleccionado.

16 Configuración de impresión★

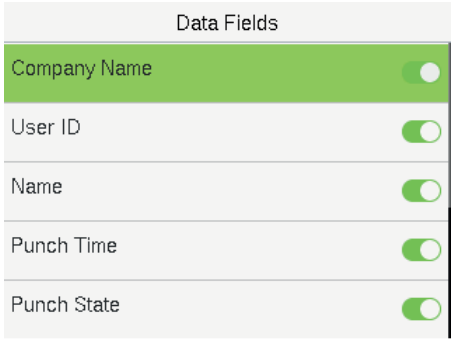
Los dispositivos con función de impresión pueden imprimir registros de asistencia cuando hay una impresora conectada.

Cuando el dispositivo esté en la interfaz inicial, presione el botón **[M/OK] > Imprimir**



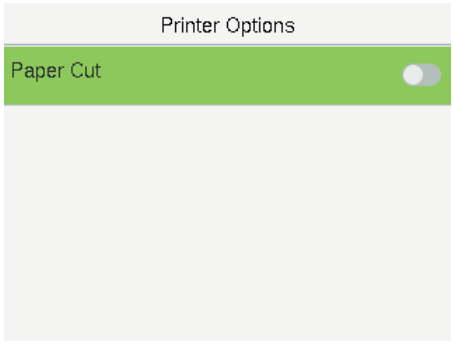
16.1 Configuración de campos de datos

Selecciona «Configuración de campos de datos» en la interfaz de impresión. Utiliza el botón de alternancia para activar o desactivar los campos que se deben imprimir.



16.2 Configuración de opciones de impresión

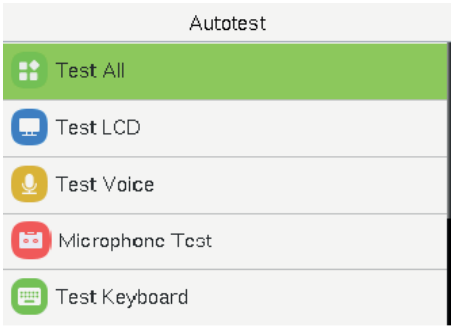
Seleccione las opciones de impresora en la interfaz de impresión. Utilice el botón de alternancia para activar o desactivar la función de corte de papel.



Observaciones: Para activar la función de corte de papel , es necesario conectar el dispositivo a una impresora con función de corte de papel, para que la impresora corte el papel según la información de impresión seleccionada durante la impresión.

17 Autoprueba

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

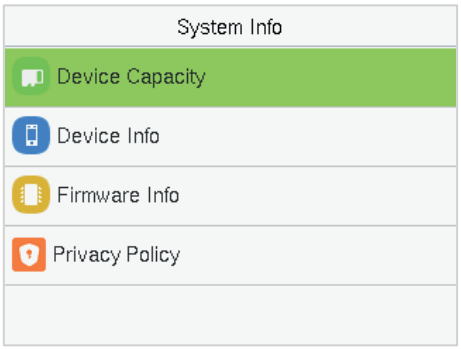


Descripción de la función

Nombre de la función	Descripción
Probar todo	Para probar automáticamente si la pantalla LCD, la voz, el micrófono, la huella digital, la cámara y el reloj en tiempo real (RTC) están normales
Prueba LCD	Para probar automáticamente el efecto de visualización de la pantalla LCD mostrando colores completos, blanco puro y negro puro para verificar si la pantalla muestra los 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	Para probar si el micrófono funciona correctamente, hable a través del micrófono
Prueba de teclado	El terminal comprueba si todas las teclas del teclado funcionan correctamente. Pulse cualquier tecla en la interfaz de prueba de teclado para comprobar si coincide con la tecla mostrada en la pantalla. Las teclas se muestran en gris oscuro antes de pulsarlas y se vuelven azules después. Pulse ESC para salir de la prueba.
Prueba del sensor de huellas dactilares	Para probar el sensor de huellas dactilares, presione el dedo sobre el escáner para comprobar si la imagen es nítida. Al presionar el dedo sobre el escáner, la imagen se mostrará en la pantalla.
Probar cámara	Para probar si la cámara funciona correctamente.
Reloj de prueba RTC	Para probar el RTC, el dispositivo comprueba si el reloj funciona con normalidad y precisión con un cronómetro. Toque la pantalla para iniciar el conteo y vuelva a tocarla para detenerlo.

18 Información del sistema

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



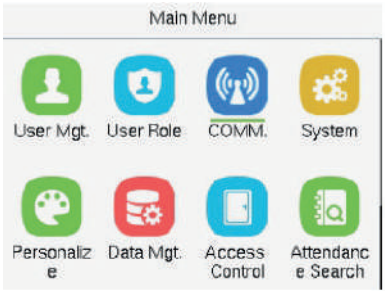
Descripción de la función

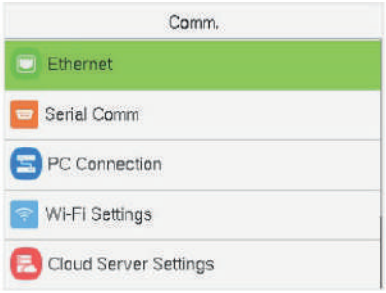
Nombre de la función	Descripción
Capacidad del dispositivo	Muestra el almacenamiento de usuarios, huellas dactilares, tarjetas y contraseñas, administradores y registros del dispositivo actual.
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la dirección MAC, el algoritmo de huella digital, la información de la plataforma, la versión de MCU y el fabricante.
Información del firmware	Muestra la versión del firmware y otra información de la versión del dispositivo.
Política de privacidad	Mostrar la política de privacidad del dispositivo.

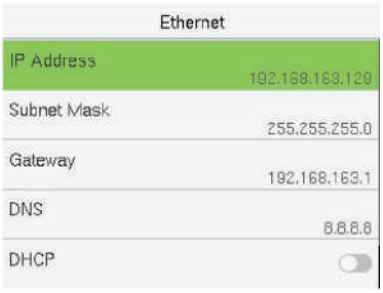
19 Conectarse al servidor web

19.1 Iniciar sesión en el servidor web

De acuerdo al inicio de sesión de red configurado , permite al servidor web ver de forma remota la información del dispositivo (hardware, software, capacidad y datos, etc.), configurar el sistema (comunicación, control de acceso y funciones del sistema, etc.), agregar usuarios y actualizar el sistema



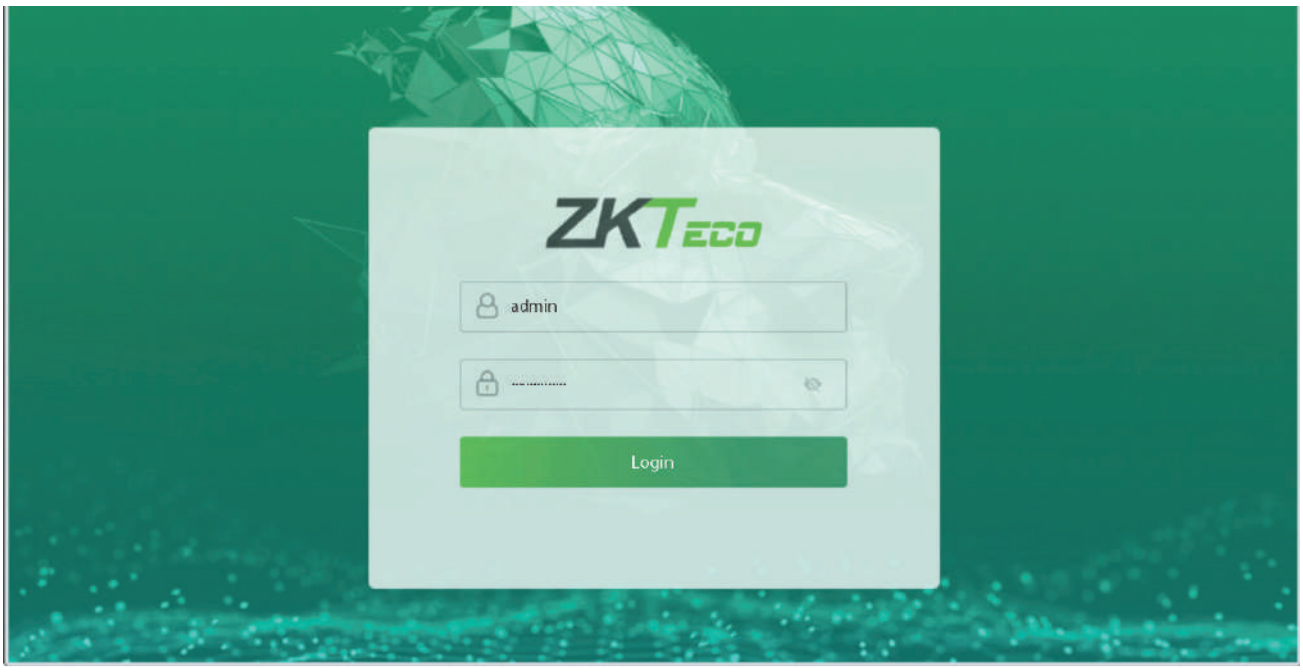




1. Abre un navegador e introduce la dirección para iniciar sesión en el servidor web; la dirección es **https://:1443.** Por ejemplo: **https://192.168.1.201:1443.**



2. Ingrese la cuenta y contraseña del servidor web, la cuenta predeterminada es: **admin, contraseña: admin@123.**



Nota:

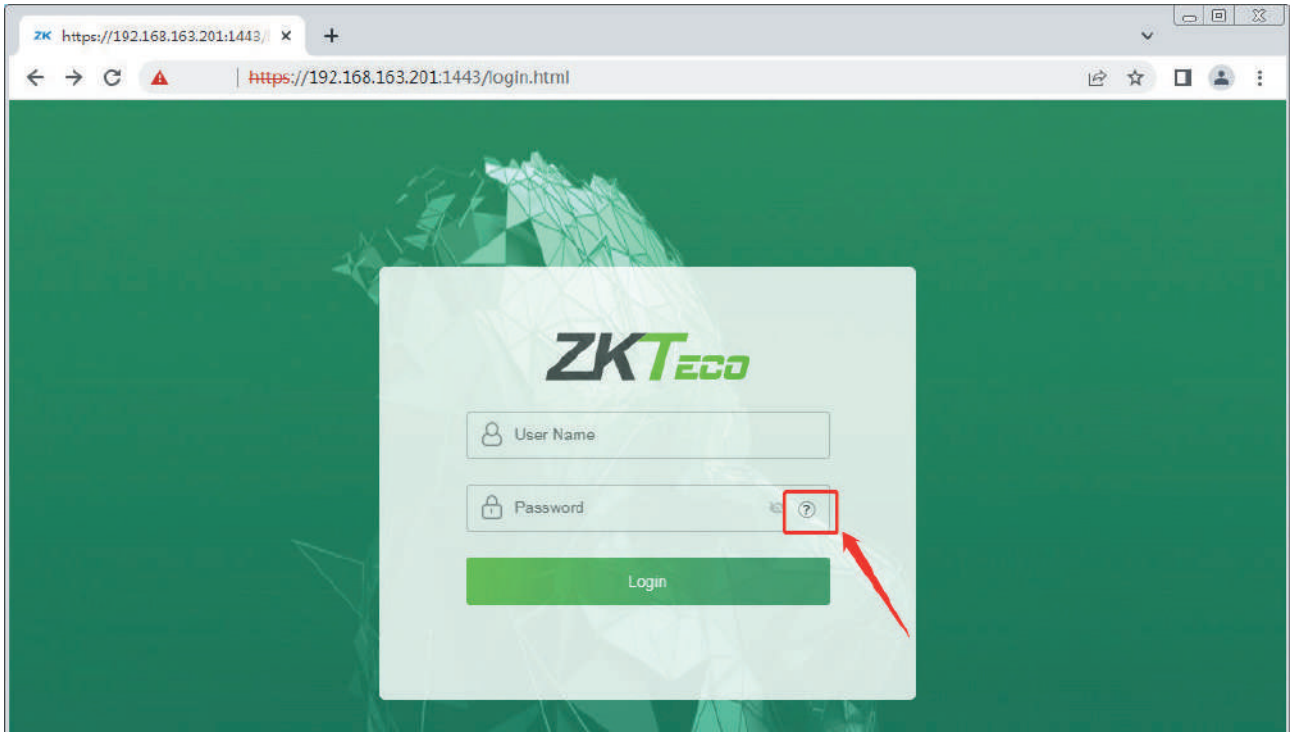
1. Tras iniciar sesión por primera vez, se recomienda a los usuarios que cambien su contraseña original; consulte la sección «Cambiar contraseña».
2. Para poder recuperar la contraseña fácilmente, regístrese primero como superadministrador; consulte el apartado 8.1 «Registro de usuarios».

19.2 Olvidé mi contraseña

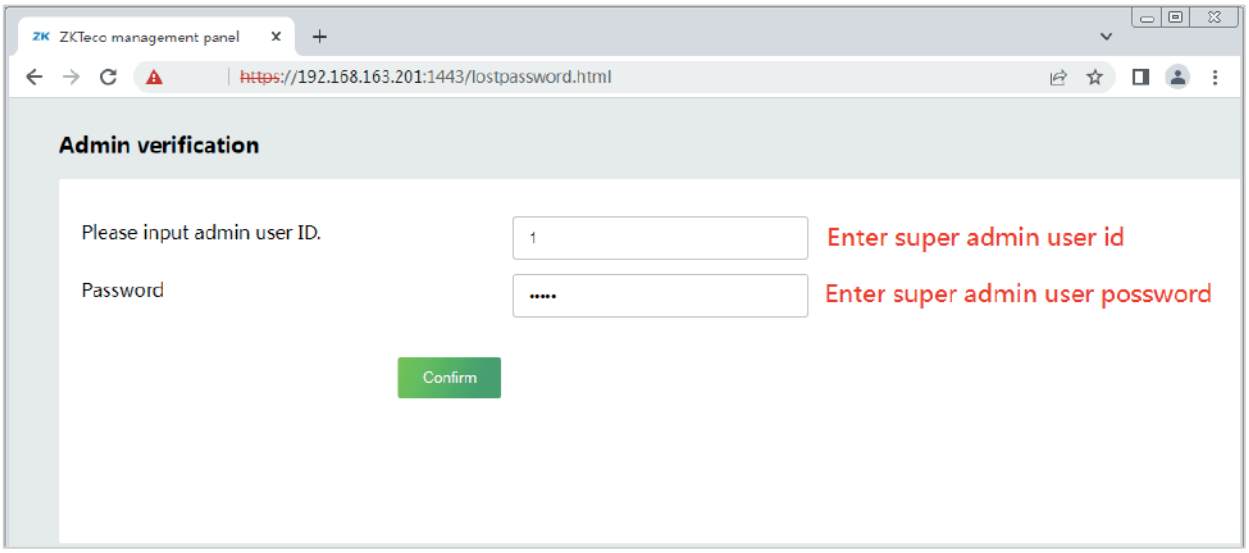
- **Método 1 (Cuando hay un superadministrador):**

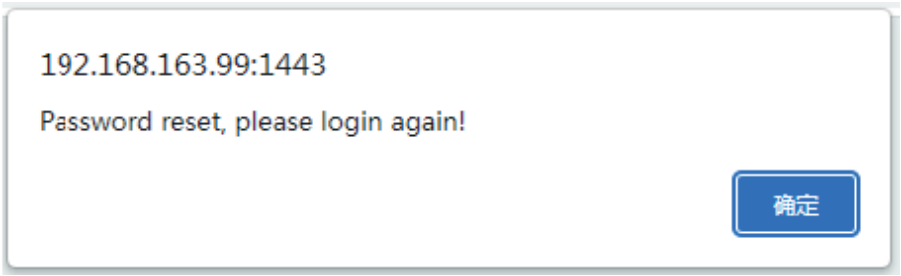
Si olvidó la contraseña del servidor web, el superadministrador registrado puede restablecerla . Los pasos detallados son los siguientes:

1. Haga clic en el icono en la interfaz de inicio de sesión.

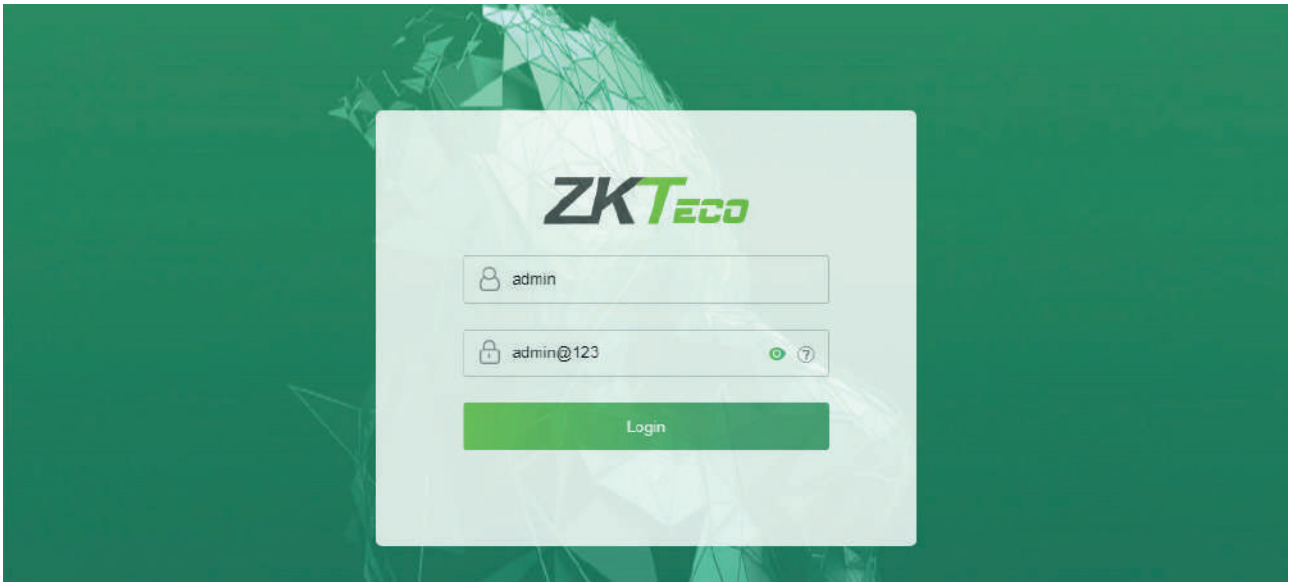


2. En la página emergente, ingrese la información relevante del usuario superadministrador según se le solicite.

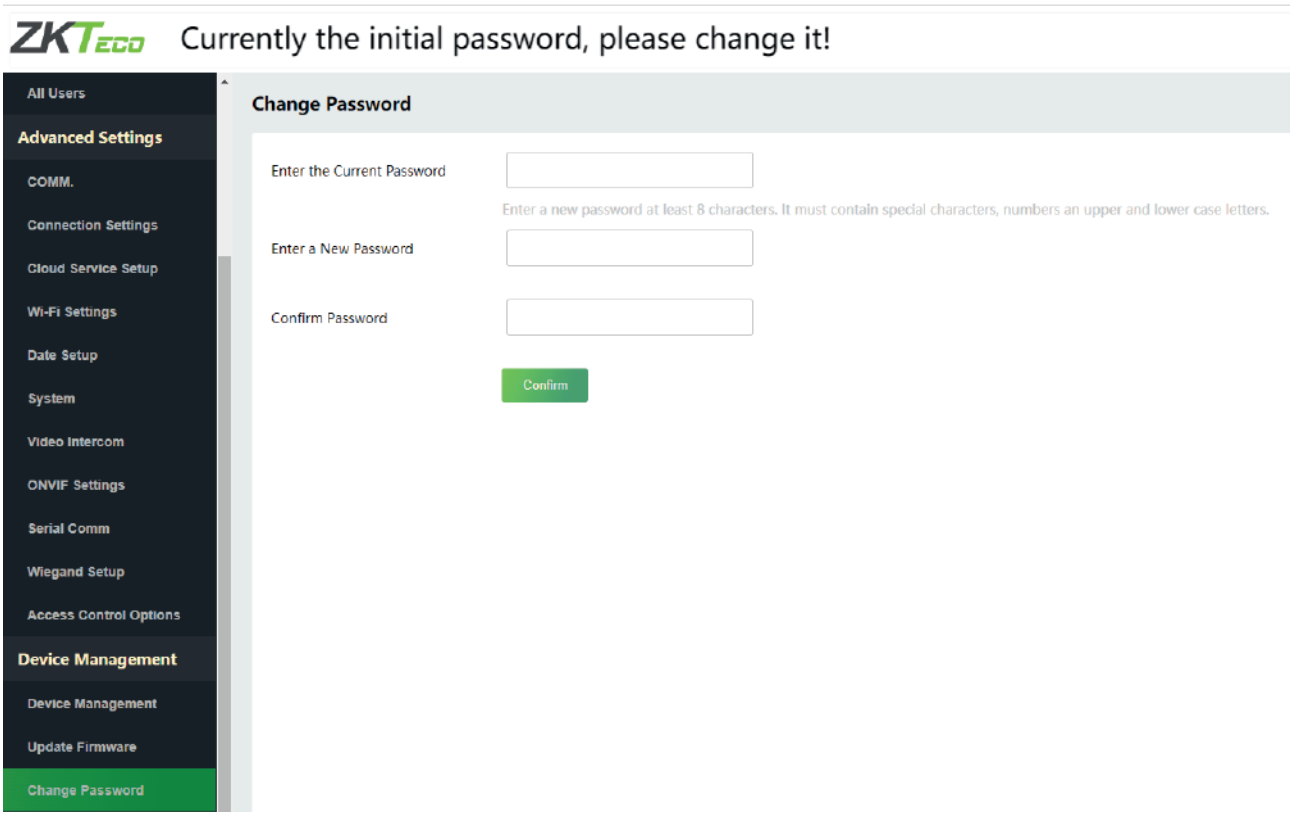




3. Después de un restablecimiento exitoso, ingrese la cuenta y contraseña predeterminadas (cuenta: admin, contraseña: admin@123) en la interfaz de inicio de sesión para iniciar sesión.



4. Por razones de seguridad, cambie su contraseña después de iniciar sesión correctamente.

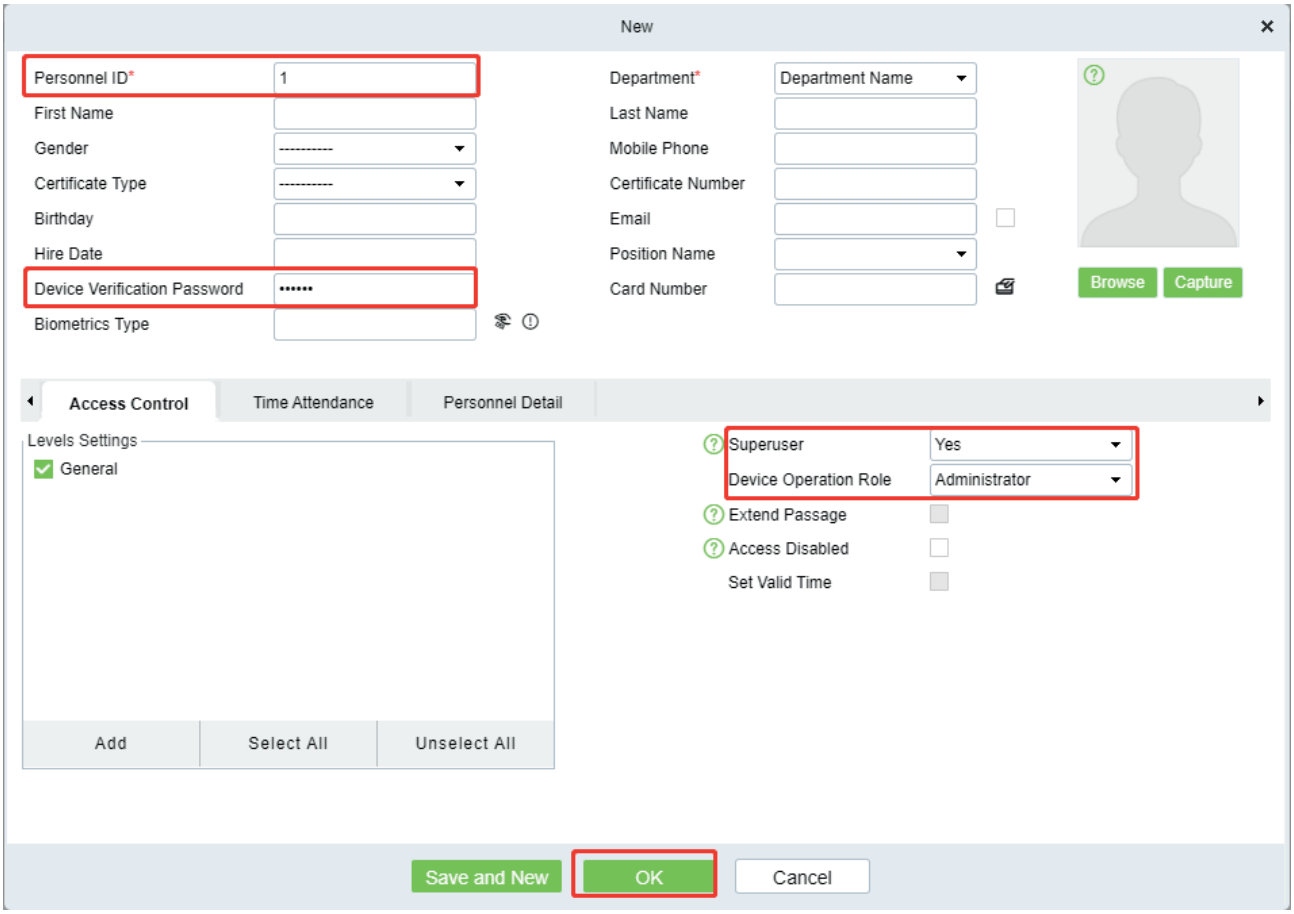


Nota: El superadministrador debe existir.

- **Método 2 (cuando no hay un superadministrador):**

Si la red del dispositivo es normal y se ha conectado ZKBio CVAccess / ZKBioTime 8.0, puede restablecer la contraseña enviando la cuenta de superadministrador y la contraseña desde el servidor.

1. Haga clic en «Personal» > «Persona» > «Nuevo» en el servidor ZKBio CVAccess / ZKBioTime 8.0; introduzca los datos del superadministrador y asigne el rol de superadministrador en la nueva interfaz según sea necesario.



2. Después de registrar la información del superadministrador, haga clic en Aceptar.

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

Nota: Para otras operaciones específicas, consulte el Manual del usuario de ZKBio CVAccess o el Manual del usuario de ZKBioTime 8.0.

4. Una vez completada la sincronización de datos, puede restablecer la contraseña con el superadministrador recién registrado. Los pasos a seguir son los mismos que en el método 1.

- **Método 3:**

Si el dispositivo no ha registrado un superadministrador y no puede conectarse al servidor, comuníquese con nuestros técnicos de posventa para que lo ayuden a recuperar la contraseña.

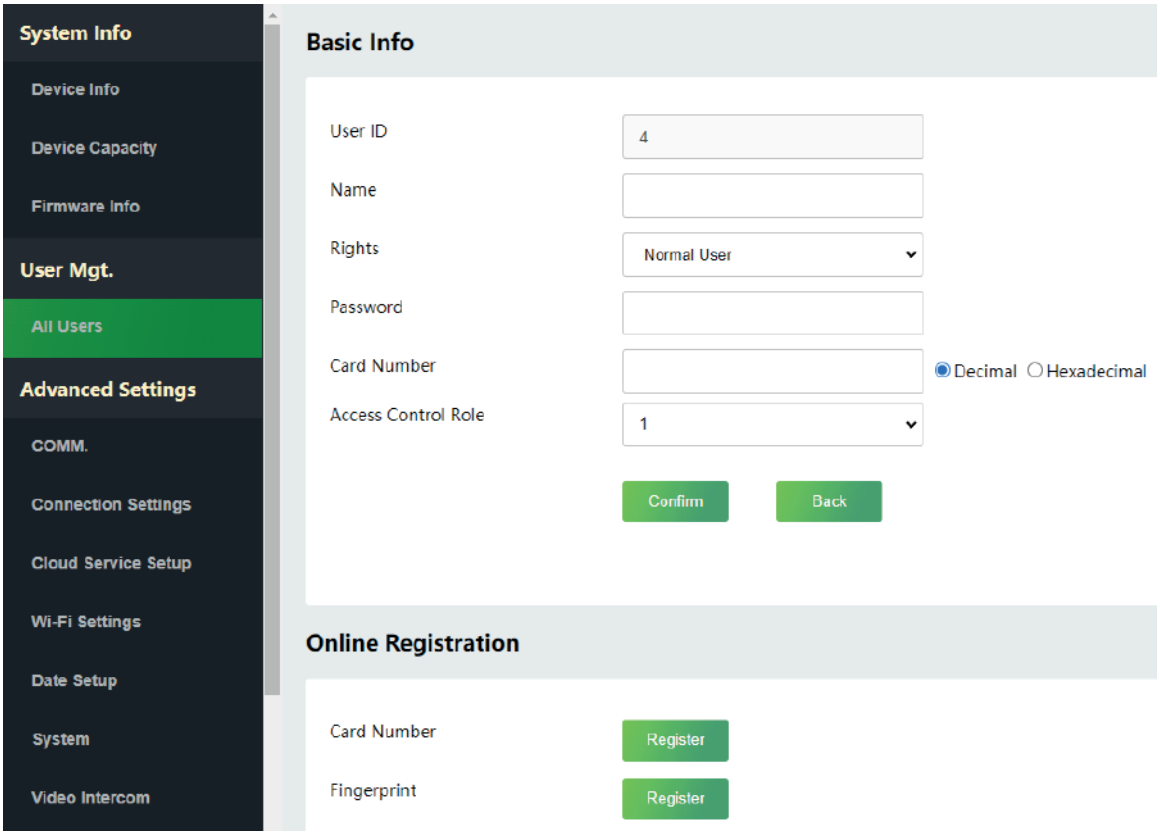
19.3 Gestión de usuarios

19.3.1 Registro de usuario

- **Información básica**

Haga clic en Todos los usuarios > Nuevo usuario en el servidor web.

En esta interfaz, puede introducir el ID de usuario, el nombre, los derechos, la contraseña, el número de tarjeta y la función de control de acceso del nuevo usuario; haga clic en «Confirmar» para guardar los datos.



Nombre de la función	Descripción
ID de usuario	El ID de usuario puede contener de 1 a 14 caracteres de forma predeterminada.
Nombre	Un nombre puede tener hasta 63 caracteres.
Derechos	Establezca el rol del usuario como Usuario normal o Superadministrador. • **Superadministrador:** El superadministrador tiene todos los privilegios de administración en el servidor web. • **Usuario normal:** Si el superadministrador ya está registrado en el servidor web, los usuarios normales no tendrán privilegios para administrar el sistema y solo podrán acceder a los procesos de autenticación.
Contraseña	Establecer la contraseña de registro del usuario.

Nombre de la función	Descripción
Número de tarjeta	Seleccione el tipo de número de tarjeta e ingréselo manualmente, luego de registrar el número de tarjeta del usuario, el usuario puede deslizar la tarjeta para verificación.
Rol de control de acceso	El rol de control de acceso establece el privilegio de acceso a la puerta para cada usuario. Los nuevos usuarios se añadirán al Grupo 1 de forma predeterminada, y este puede reasignarse a otros grupos según sea necesario. El sistema admite hasta 10 grupos de control de acceso

Nota:

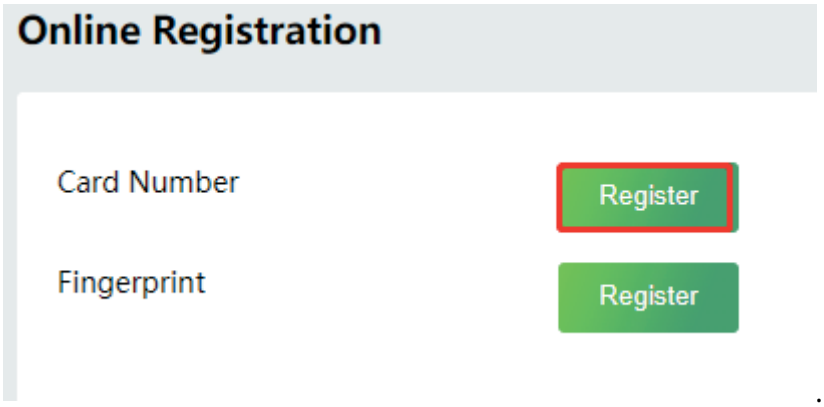
1. Durante el registro inicial, puedes modificar tu ID; una vez completado el registro, ya no podrás modificar el ID registrado.
2. Si aparece el mensaje «¡Error al registrarse!», debes elegir otro nombre de usuario, ya que el que has introducido ya existe.

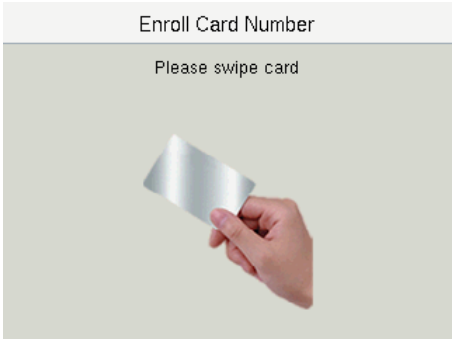
- **Registro en línea**

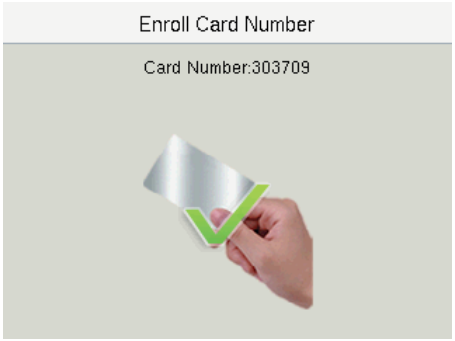
En esta interfaz, puede registrar el número de tarjeta y la huella dactilar del usuario. El modo de verificación solo se puede registrar tras confirmar la información básica.

➢ **Número de tarjeta de registro**

En la interfaz actual, detrás de la barra de número de tarjeta, haga clic en "Registrar". El dispositivo mostrará la interfaz de registro del número de tarjeta en tiempo real. Deslice la tarjeta por debajo del área de lectura. El registro se habrá realizado correctamente.

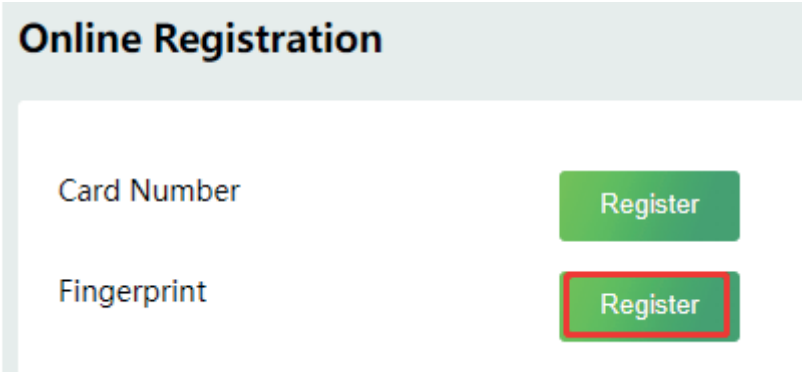


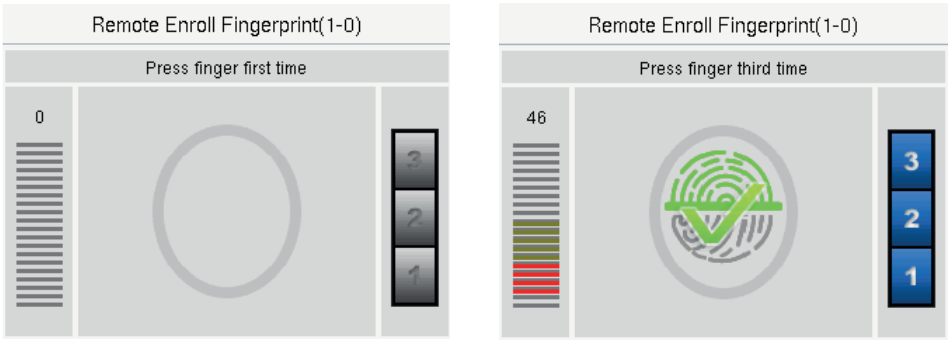




➢ Registrar huella dactilar

En la interfaz actual, detrás de la barra de huellas dactilares, haga clic en Registrar y el dispositivo mostrará la interfaz de registro de huellas dactilares en tiempo real, presione su dedo sobre el sensor de huellas dactilares del dispositivo y siga las instrucciones para completar el registro.

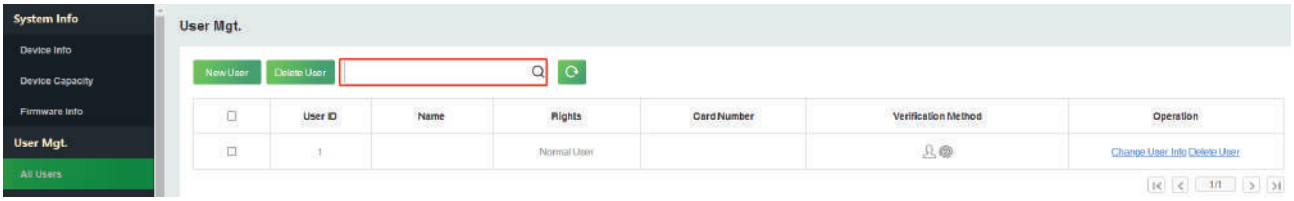




Para la operación de prensado de huellas dactilares, consulte Posicionamiento de dedos.

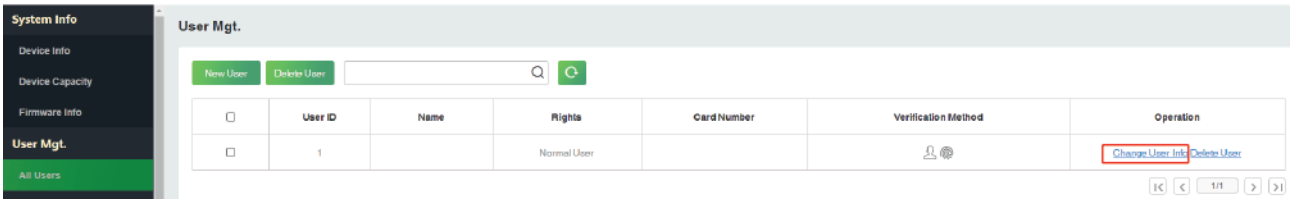
19.3.2 Búsqueda de usuarios

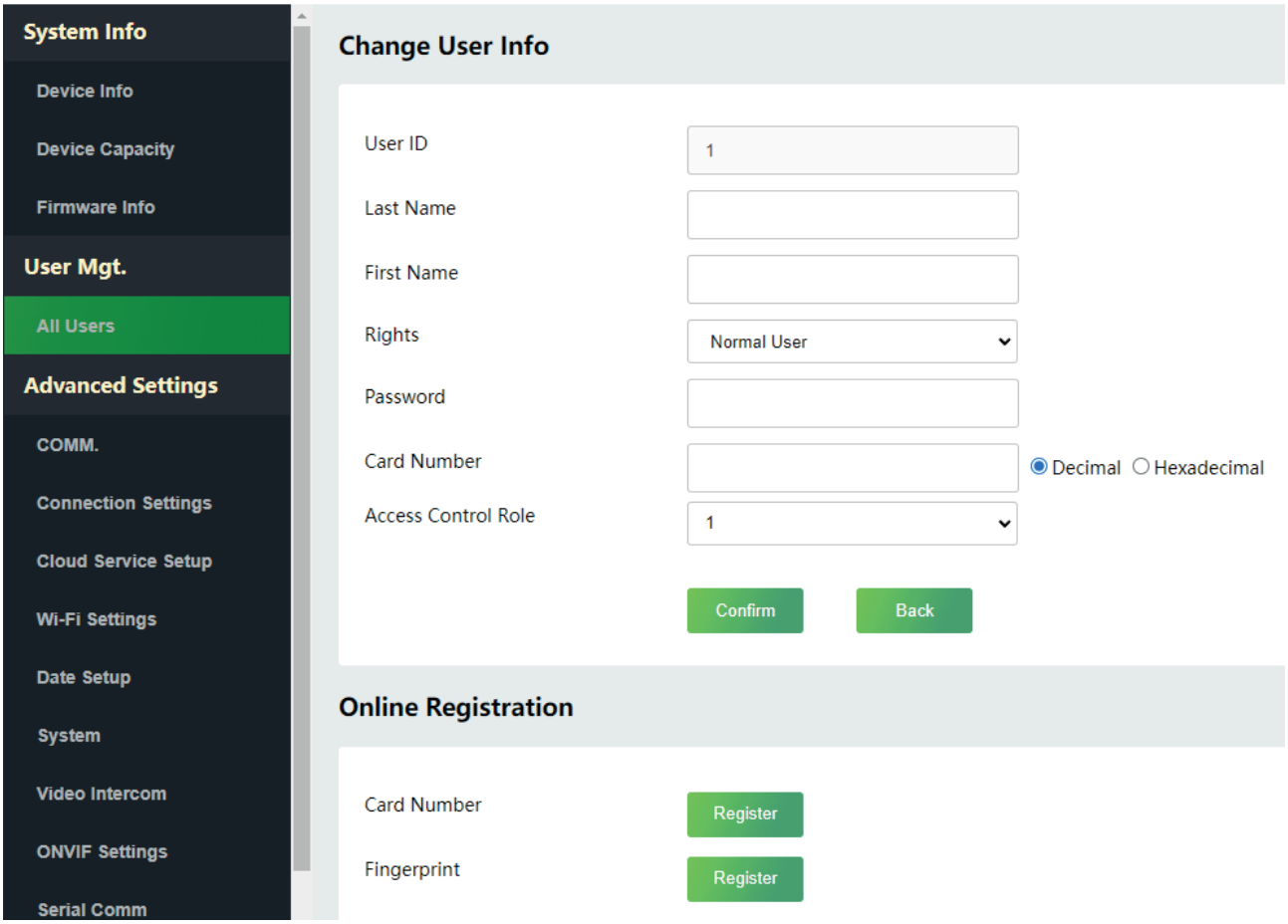
Haga clic en Todos los usuarios en el servidor web, haga clic en la barra de búsqueda para ingresar la palabra clave de recuperación requerida (donde la palabra clave puede ser el ID de usuario, el apellido o el nombre completo) y el sistema buscará la información del usuario relacionada



19.3.3 Editar usuario

En la interfaz Todos los usuarios , seleccione el usuario requerido de la lista y haga clic en Cambiar información del usuario para editar la información del usuario

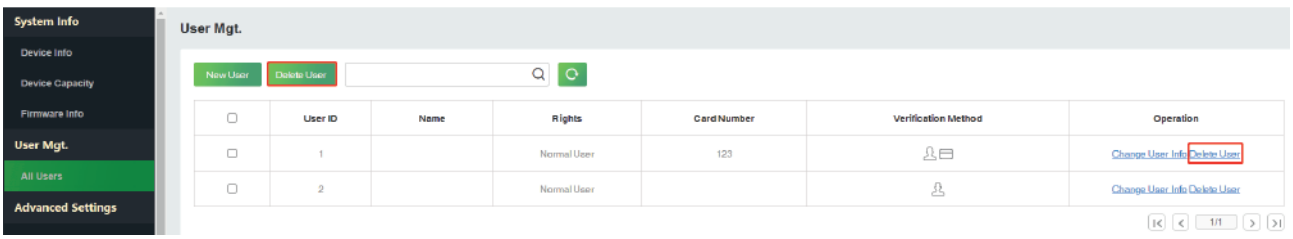




Nota: El proceso para editar la información del usuario es el mismo que el de añadir un nuevo usuario, salvo que no se puede modificar el ID de usuario. Para obtener información detallada sobre el proceso, consulte el apartado 19.3.1 «Registro de usuarios».

19.3.4 Eliminar usuario

En la interfaz «Todos los usuarios», selecciona el usuario deseado de la lista y haz clic en «Eliminar usuario» para borrarlo. Aquí puedes elegir entre la eliminación individual y la eliminación por lotes.

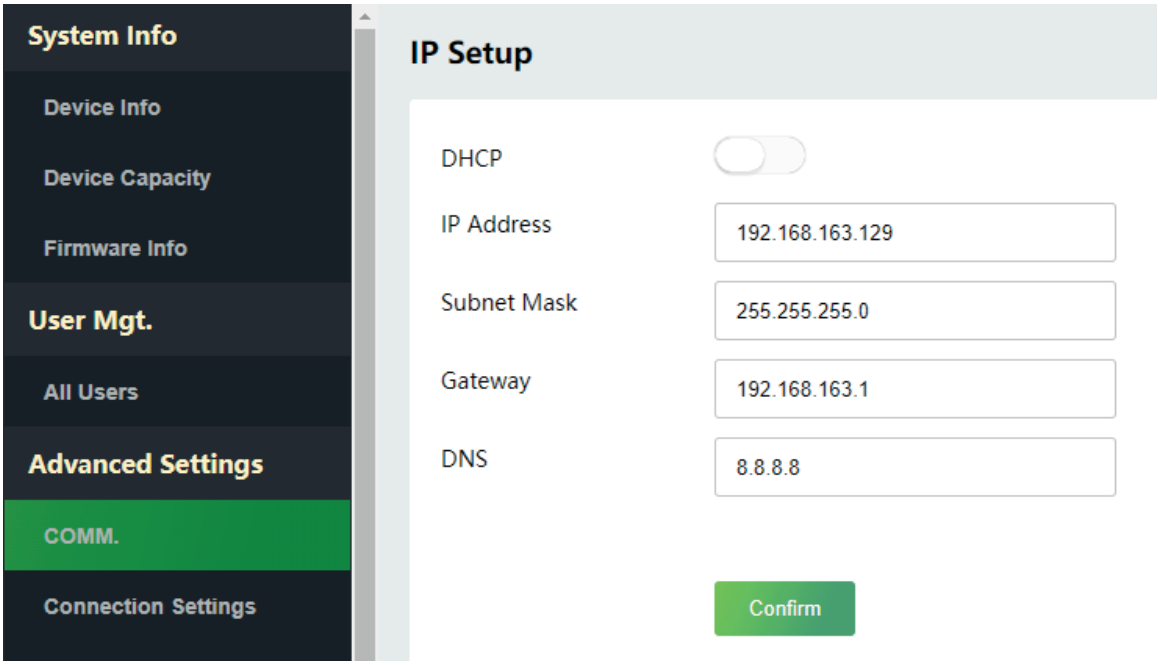


19.4 Configuración avanzada

19.4.1 Configuración de comunicación

Haga clic en COMM. en el servidor web

Cambie la dirección IP del dispositivo según sea necesario, haga clic en Confirmar para guardar y el dispositivo sincronizará automáticamente la información IP

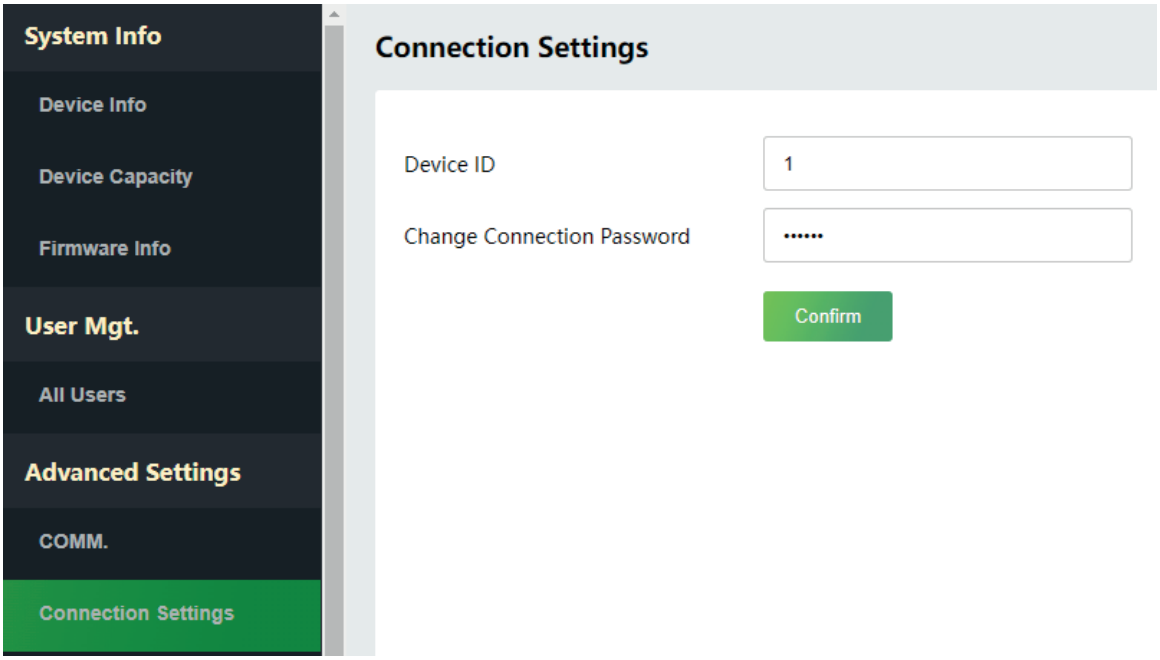


Nombre de la función	Descripción
DHCP	Seleccione si desea obtener la dirección IP automáticamente.
Dirección IP	La dirección IP predeterminada es 192.168.1.201. Puede modificarse según la disponibilidad de la red.
Máscara de subred	La máscara de subred predeterminada es 255.255.255.0. Puede modificarse según la disponibilidad de la red.
Gateway	La dirección de la puerta de enlace predeterminada es 0.0.0.0. Puede modificarse según la disponibilidad de la red.
DNS	La dirección DNS predeterminada es 0.0.0.0. Puede modificarse según la disponibilidad de la red.

Nota: Una vez modificada la dirección IP del dispositivo, deberá cerrar sesión en el servidor web actual y volver a iniciar sesión con la dirección IP que acaba de cambiar para conectarse al dispositivo. Para obtener información de inicio de sesión en el servidor web, consulte "Iniciar sesión en el servidor web"

19.4.2 Configuración de conexión

Haga clic en Configuración de conexión en el servidor web.

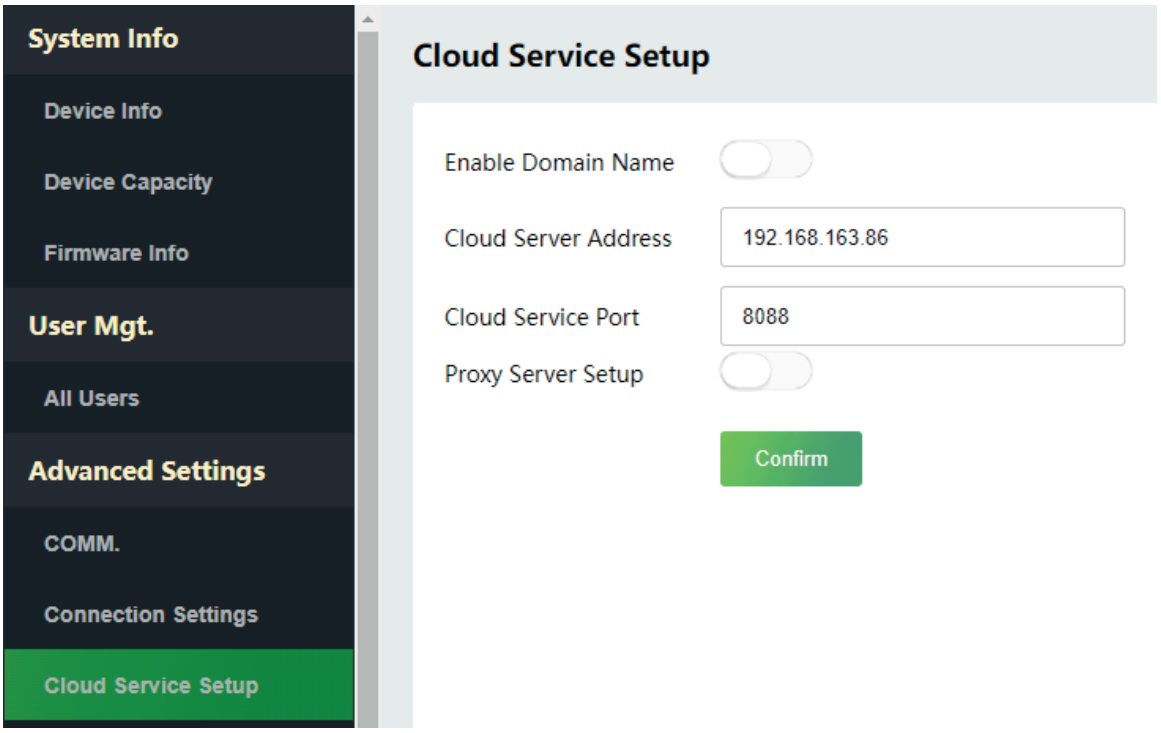


Nombre de la función	Descripción
ID del dispositivo	Es el número de identificación del dispositivo, que oscila entre 0 y 255.
Cambiar la contraseña de conexión	La contraseña de conexión debe tener 6 dígitos

19.4.3 Configuración del servicio en la nube

Haga clic en Configuración del servicio en la nube en el servidor web.

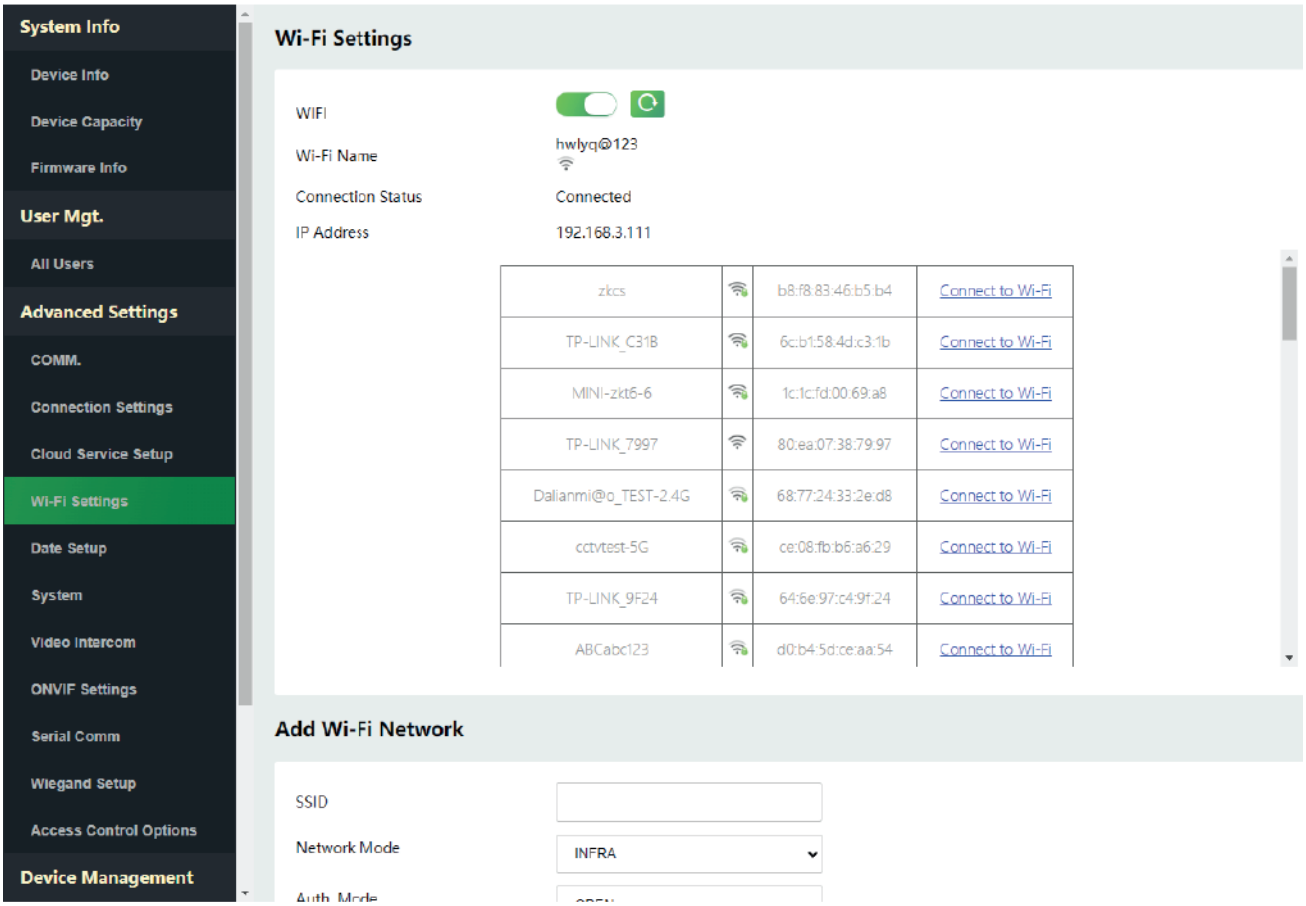
Se utilizó la configuración del servidor en la nube para conectarse al software ZKBio CVAccess y ZKBioTime 8.0; consulte el apartado 12.1 «Configuración de la dirección de comunicación».



Nombre de la función		Descripción
Habilitar nombre de dominio	**Dirección del servidor en la nube**	Una vez habilitada esta función, se utilizará el modo de nombre de dominio "http://...", como por ejemplo http://www.XYZ.com, mientras que "XYZ" denota el nombre de dominio (cuando este modo está activado)
Deshabilitar nombre de dominio	**Dirección del servidor en la nube**	Dirección IP del servidor ADMS.
	Puerto del servidor en la nube	Puerto utilizado por el servidor ADMS.
Configuración del servidor proxy		Cuando elige habilitar el proxy, debe configurar la dirección IP y el número de puerto del servidor proxy.

19.4.4 Configuración de Wi Fi★

El dispositivo es compatible con el módulo Wi Fi integrado en el hardware para permitir la transmisión de datos vía Wi Fi y establecer un entorno de red inalámbrica. El Wi Fi está desactivado por defecto. El usuario debe habilitar y configurar los parámetros correspondientes en el servidor web.

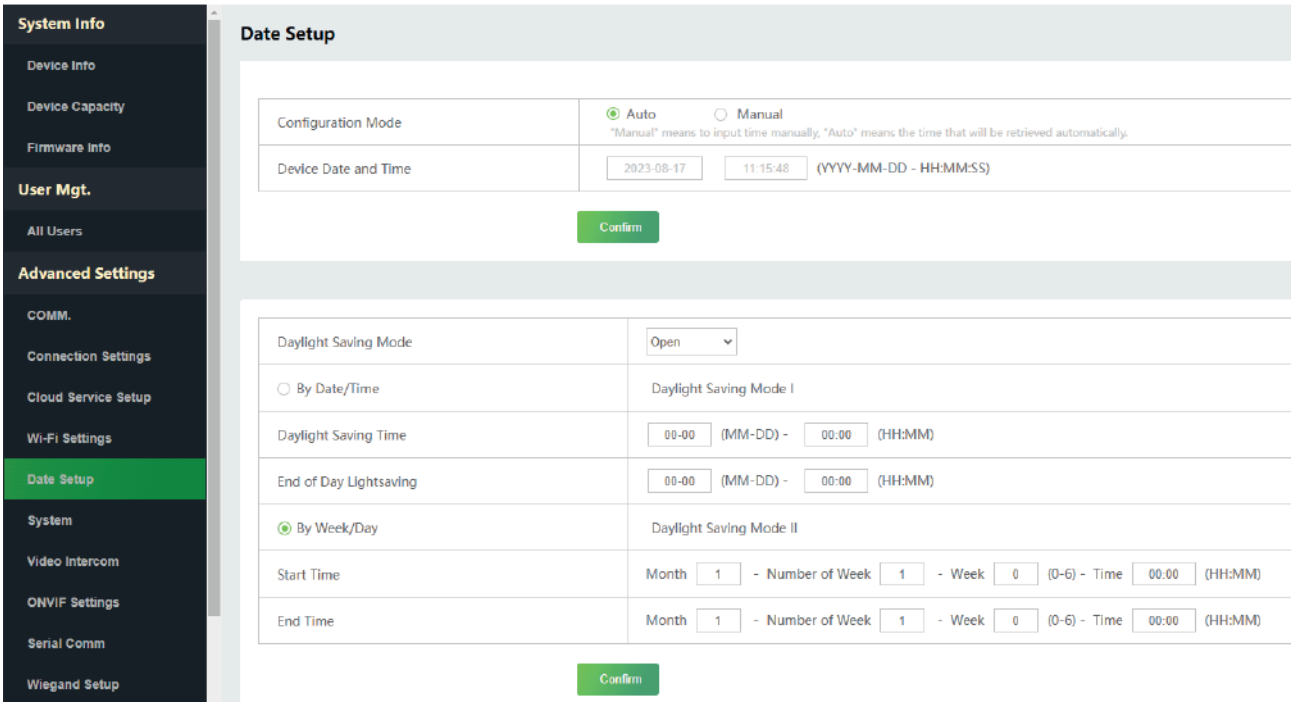


- Haga clic en el botón para habilitar la función Wi Fi.
- Cuando la conexión Wi Fi está habilitada, el dispositivo buscará la conexión Wi Fi disponible dentro del alcance de la red
- Haga clic en Conectar a Wi Fi después del nombre de Wi Fi requerido de la lista disponible e ingrese la contraseña correcta, luego haga clic en[Confirmar].
- Después de la verificación exitosa, el estado de la conexión mostrará "Conectado".

19.4.5 Configuración de fecha

Haga clic en Configurar fecha en el servidor web

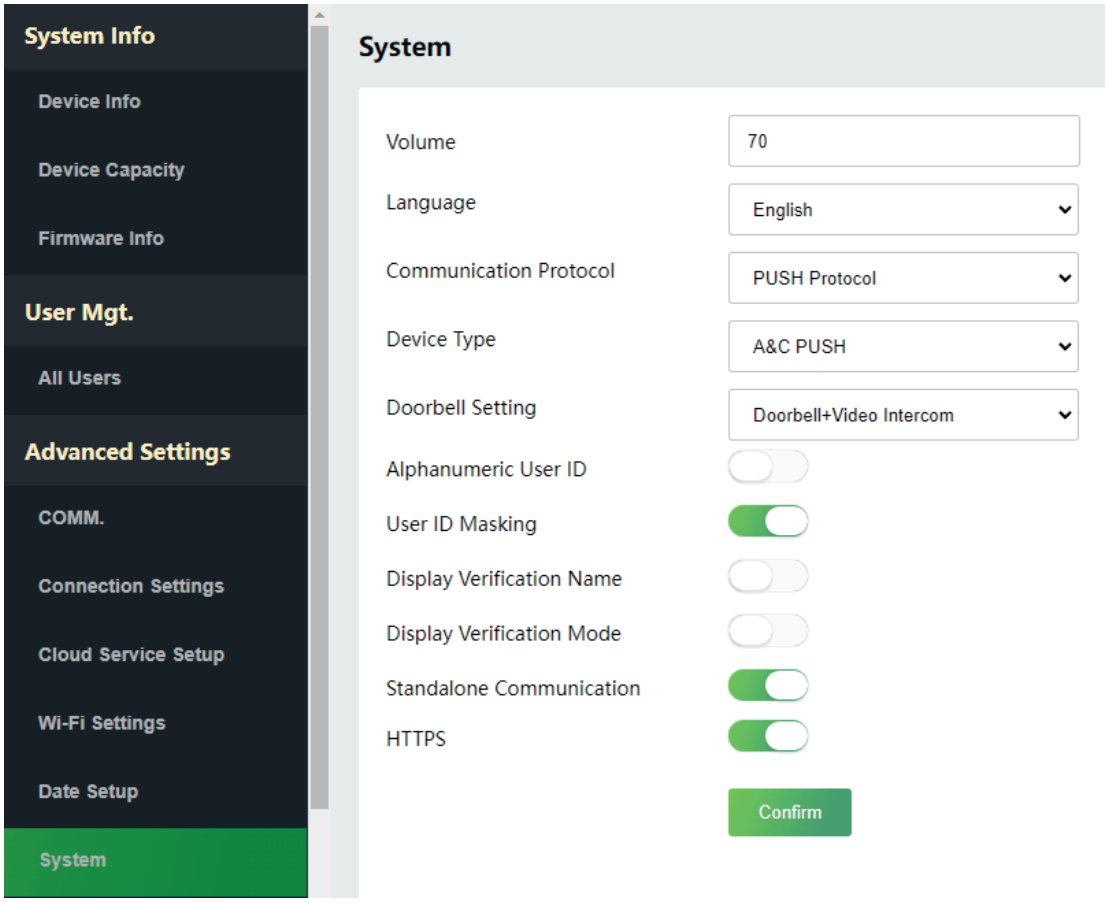
- Haga clic en Manual para configurar manualmente la fecha y la hora y haga clic en Confirmar para guardar.
- Selecciona la función «Activar o desactivar el horario de verano». Si la activas, configura la fecha de inicio y la fecha de finalización del horario de verano.



19.4.6 Configuración del sistema

Haga clic en Sistema en el servidor web.

Ayuda a establecer parámetros del sistema relacionados para optimizar la accesibilidad del dispositivo.



Nombre de la función	Descripción
Volumen	Ajuste el volumen del dispositivo, que puede configurarse entre 0 y 100.
Período de duplicación de marcajes (m)	Durante un periodo de tiempo determinado (unidad: minutos), el registro de asistencia duplicado no se conservará (el valor oscila entre 1 y 999 999 minutos).
Idioma	Selecciona el idioma del servidor web y del dispositivo.
Protocolo de comunicación	Configura el protocolo de comunicación del dispositivo.
Tipo de dispositivo	Configure el dispositivo como terminal de control de acceso o terminal de control de asistencia. ***Nota:*** Tras cambiar el tipo de dispositivo, este borrará todos los datos y se reiniciará, y algunas funciones se ajustarán en consecuencia.
Configuración del timbre	**Solo timbre:** Cuando el usuario pulsa el botón del timbre, solo suena el timbre. **Solo videoportero:** Cuando el usuario pulsa el botón del timbre, el dispositivo solo realiza una llamada. **Timbre + videoportero:** Cuando el usuario pulsa el botón del timbre, suena el timbre y el dispositivo realiza una llamada al mismo tiempo.
Identificación de usuario alfanumérica	Activar/desactivar el uso de caracteres alfanuméricos como ID de usuario.
Ocultación del ID de usuario	Cuando esta opción esté activada y el usuario haya sido comparado y verificado correctamente, el ID de usuario que aparece en el resultado de la verificación se sustituirá por un * para garantizar la protección de los datos personales confidenciales.
Visualización del nombre de verificación	Establece si se muestra el nombre de usuario en la interfaz de resultados de la verificación.
Modo de verificación de visualización	Establece si se muestra el modo de verificación en la interfaz de resultados de verificación.
Comunicación autónoma	Para evitar no poder utilizarlo cuando el dispositivo esté desconectado, puede descargar previamente el software cliente-servidor (como ZKAccess 3.5) en su ordenador para poder utilizarlo sin conexión.
HTTPS	Basándose en el protocolo HTTP, el cifrado de la transmisión y la autenticación de identidad garantizan la seguridad del proceso de transmisión.

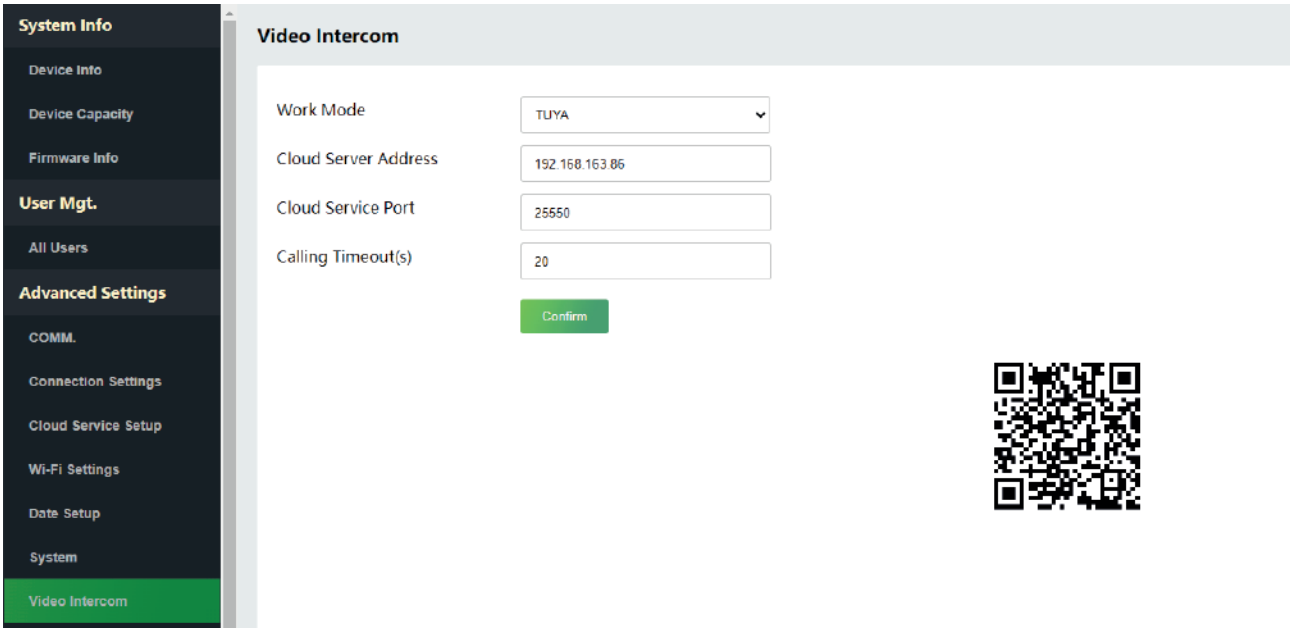
Nota:

1. Después de seleccionar el idioma y hacer clic en Confirmar, el dispositivo se reiniciará automáticamente y mostrará el idioma cambiado.
2. Luego, el servidor web no mostrará el idioma cambiado hasta que el dispositivo se reinicie e inicie sesión nuevamente.

19.4.7 Videoportero★

Haga clic en Video Intercomunicador en el servidor web

La función de intercomunicador de video es compatible con WAN, WAN es adecuada para teléfonos móviles.

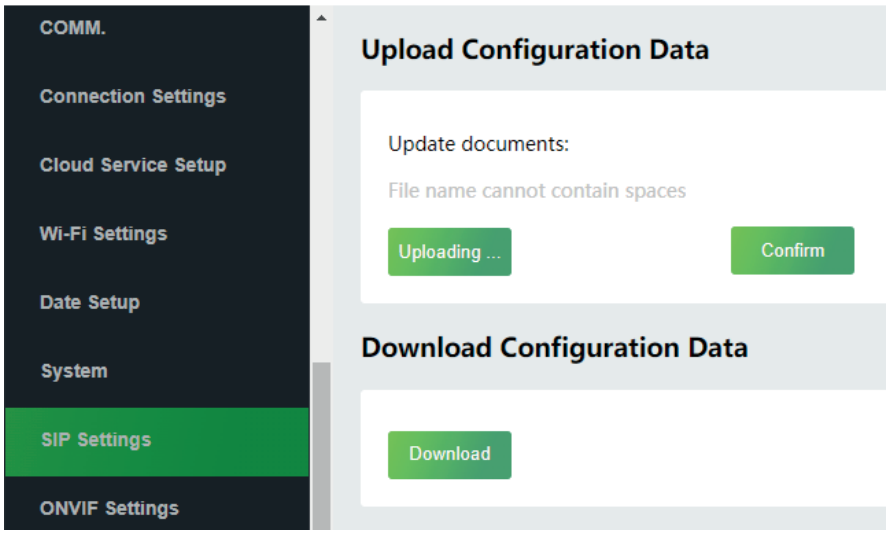


Para obtener más detalles, consulte 22. Conexión a la aplicación ZSmart.

19.4.8 Configuración SIP★

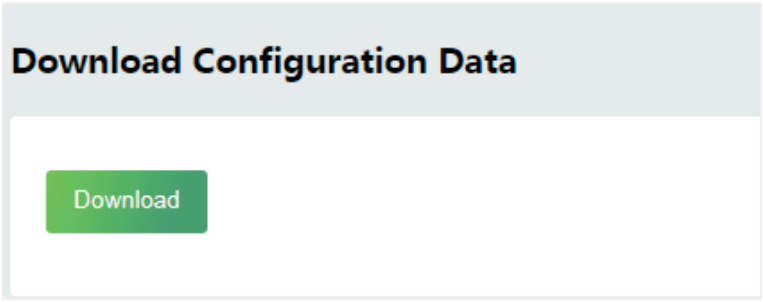
Nota: Esta función debe utilizarse con la estación interior.

Haz clic en **«Configuración SIP»** en el servidor web.



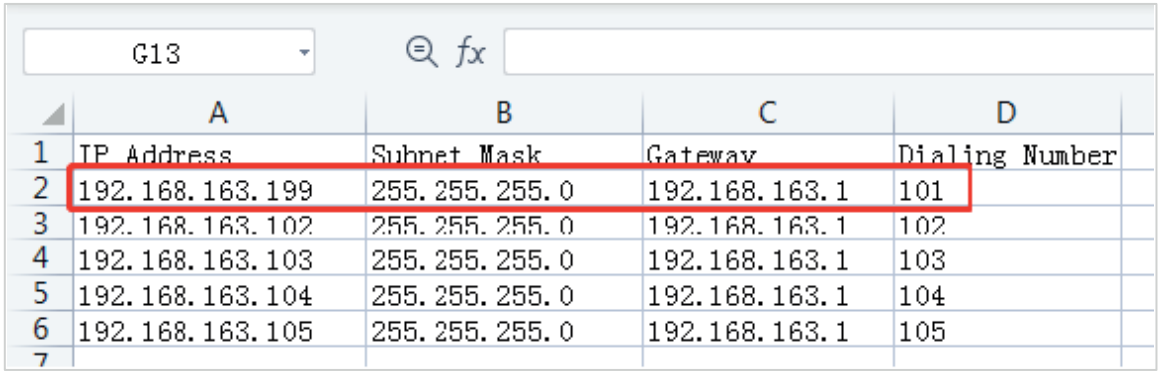
- **Descargar datos de configuración**

1. Haga clic en Descargar para descargar el archivo.



2. Abre el archivo descargado y modifica manualmente la dirección de comunicación y el número de dispositivo de la estación interior.

   Dirección IP/Máscara de subred/Puerta de enlace: deben coincidir con los de la estación interior a la que se va a conectar.
   Número de marcación: personaliza el número de la estación interior; puedes introducir el valor en F35 para llamar rápidamente a la estación interior y utilizar el videoportero.



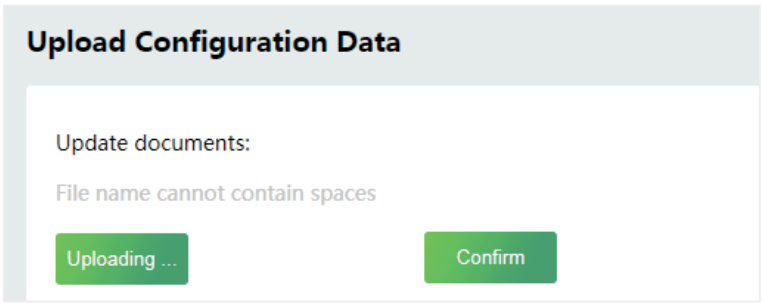
G13 fx

	A	B	C	D
1	IP Address	Subnet Mask	Gateway	Dialing Number
2	192.168.163.199	255.255.255.0	192.168.163.1	101
3	192.168.163.102	255.255.255.0	192.168.163.1	102
4	192.168.163.103	255.255.255.0	192.168.163.1	103
5	192.168.163.104	255.255.255.0	192.168.163.1	104
6	192.168.163.105	255.255.255.0	192.168.163.1	105



- **Cargar datos de configuración**

1. Una vez configurado y guardado el formulario, haga clic en Cargando... para cargar el formulario de configuración.



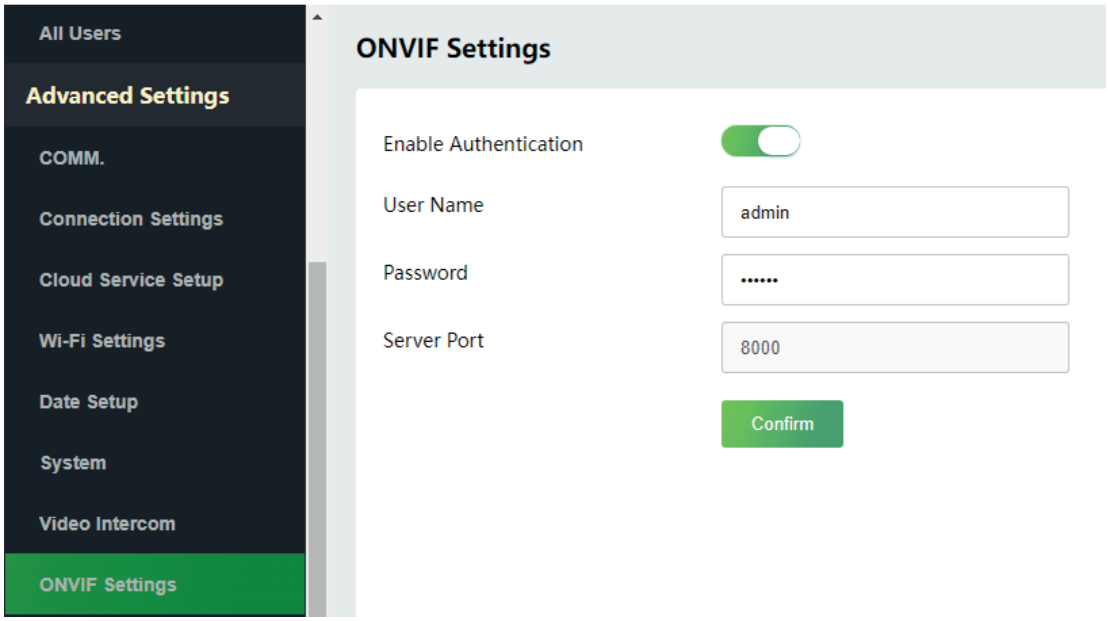
2. Haga clic en Confirmar para sincronizar los parámetros con F35.

Para obtener más detalles, consulte 23. Conexión a SIP

19.4.9 Configuración ONVIF★

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

Haga clic en **Configuración ONVIF** en el servidor web.

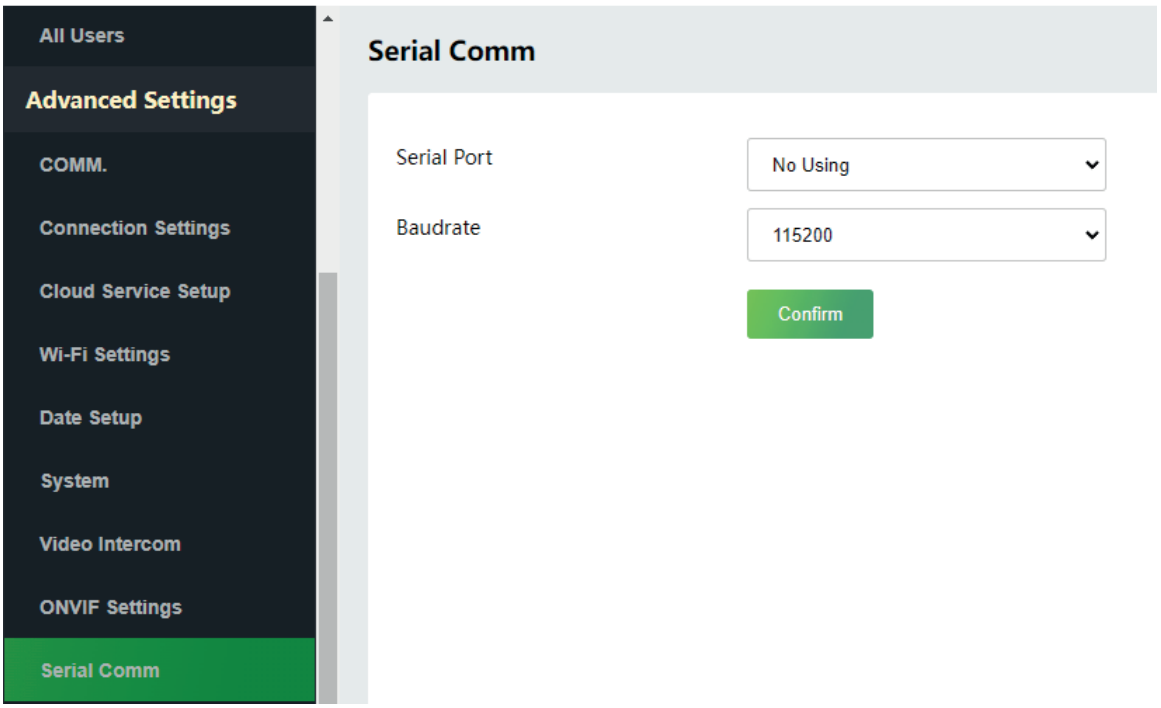


Nombre de la Función	Descripción
Habilitar autenticación	Habilite o deshabilite la función de autenticación. Si está deshabilitada, no es necesario ingresar el nombre de usuario ni la contraseña al agregar el dispositivo al NVR.
Nombre de usuario	Establezca el nombre de usuario. El predeterminado es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

Para obtener más detalles, consulte 11.5 Configuración de ONVIF.

19.4.10 Comunicación en serie

Haga clic en Comunicación serial en el servidor web.

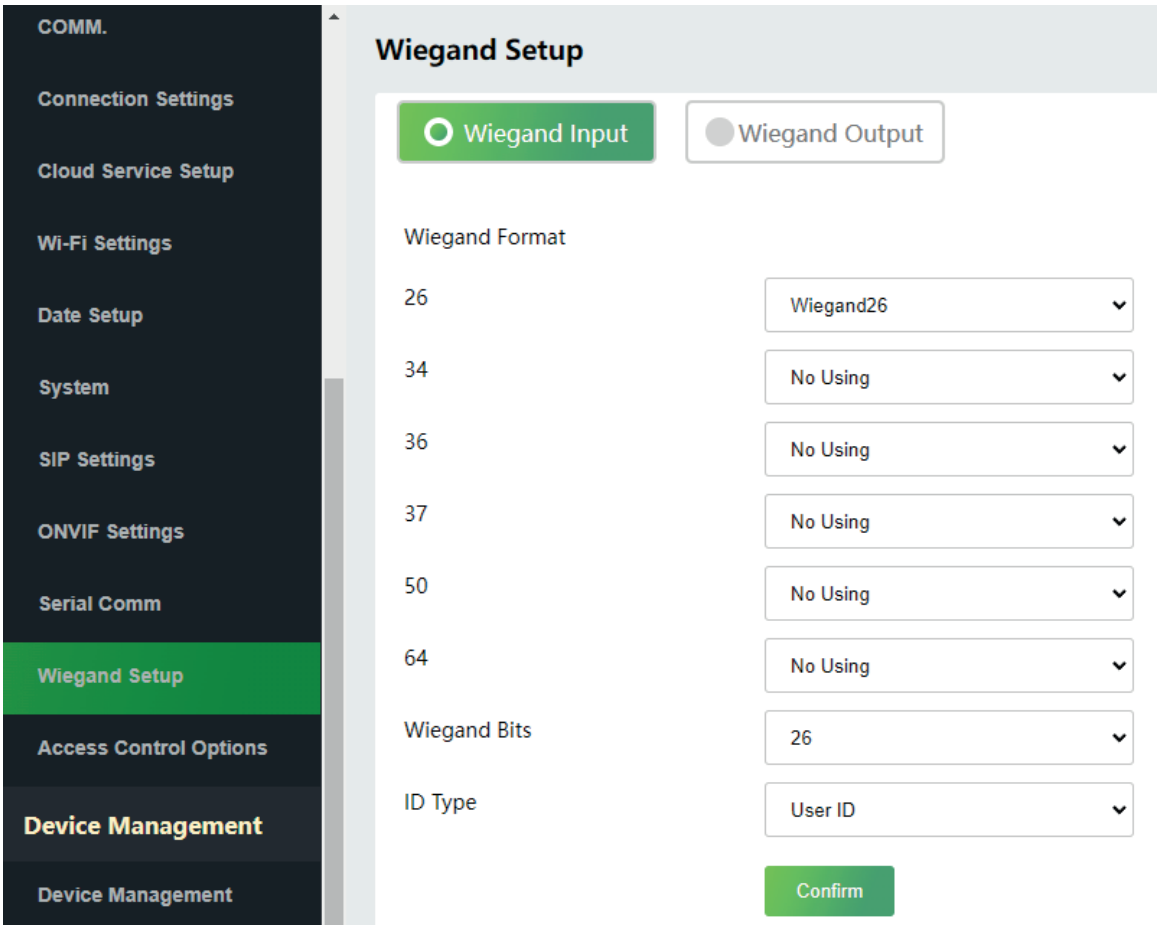


Nombre de la función	Descripción
Puerto serie	**No Usar:** No hay comunicación con el dispositivo a través del puerto serie. **Unidad maestra:** Cuando se utiliza RS485 como función de "Unidad maestra", se puede conectar a un lector. **Función de impresión:** El dispositivo se puede conectar a la impresora cuando la interfaz RS232 activa la función de impresión. **DM10:** Cuando se utiliza RS485 como función de «DM10», se puede conectar al DM10 para controlar el relé de bloqueo. (**Note:** Al seleccionar DM10 o cambiar de DM10 a otra opción, el dispositivo se reiniciará para tener efecto.)
Velocidad de transmisión	Hay cuatro opciones de velocidad en baudios para la comunicación de datos con la PC: 115200 (predeterminado), 57600, 38400 y 19200. Cuanto mayor sea la tasa de baudios, más rápida será la velocidad de comunicación, pero también menos confiable. Por lo tanto, se puede utilizar una tasa de transmisión en baudios más alta cuando la distancia de comunicación es corta; cuando la distancia de comunicación es larga, elegir una tasa de transmisión en baudios más baja es más confiable.

19.4.11 Configuración de Wiegand

Haga clic en Configuración Wiegand en el servidor web.

Se utiliza para configurar los parámetros de entrada y salida Wiegand.



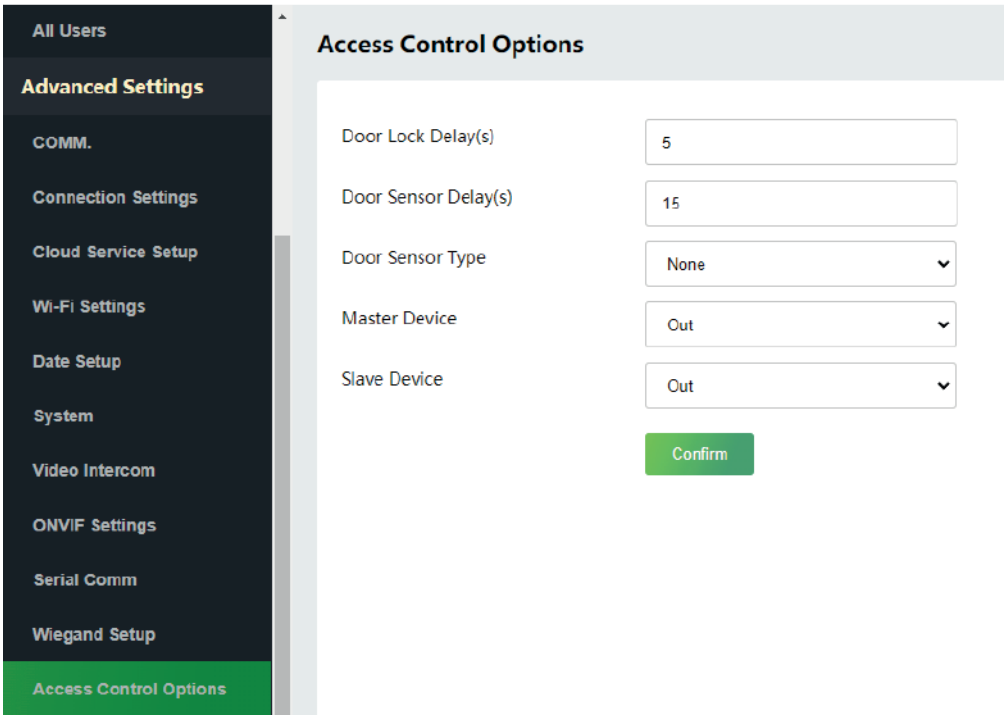
Nombre de la Función	Descripción
Formato Wiegand	Su valor puede ser de 26 bits, 34 bits, 36 bits, 37 bits, 50 bits o 64 bits.
Wiegand Bits	El número de bits de los datos Wiegand
Tipo de identificación	Seleccione entre el ID de usuario y el número de tarjeta

19.4.12 Opciones de control de acceso

Haga clic en **Opciones de control de acceso** en el servidor web.

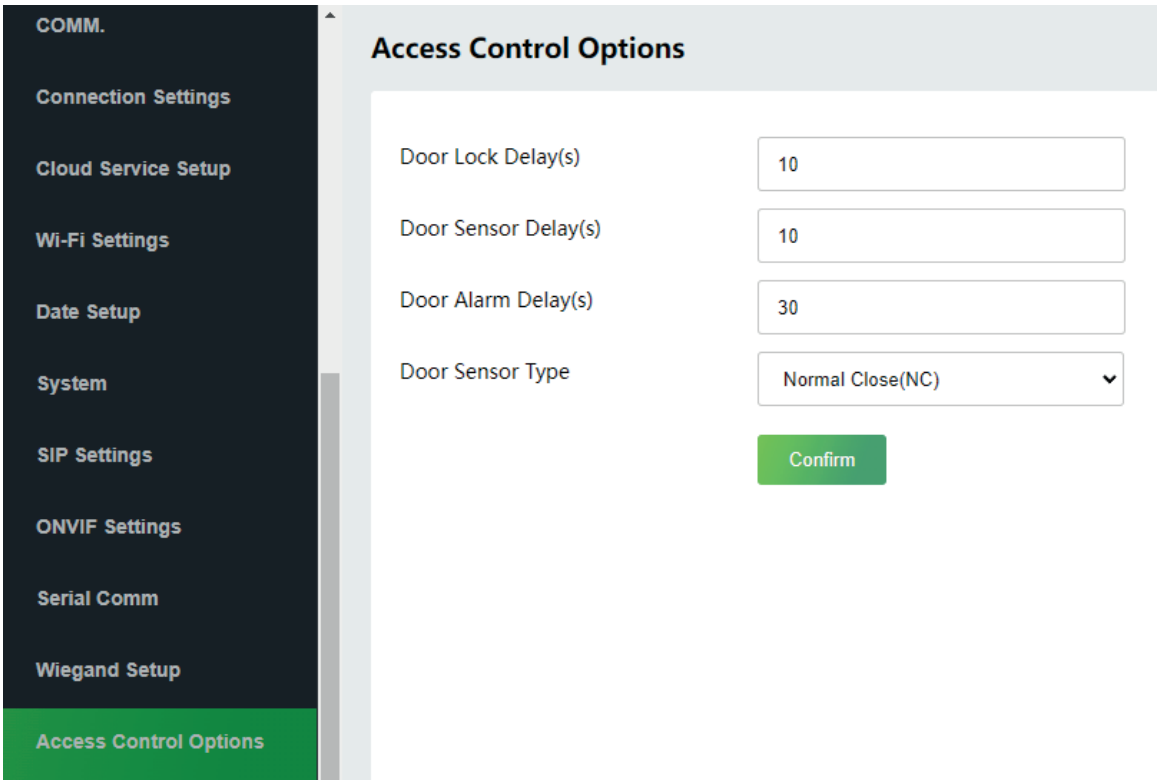
En la interfaz de Control de Acceso para configurar los parámetros del bloqueo de control del terminal y equipos relacionados.

Terminal de control de acceso:



Function Name	Description
Retardo(s) del cierre de la puerta	El tiempo que el dispositivo controla la cerradura eléctrica para que esté en estado de desbloqueo. Valor válido: 1~99 segundos; 0 segundos representa la desactivación de la función.
Retardo(s) del sensor de la puerta	ISi la puerta no está bloqueada y se deja abierta durante un período determinado (retardo del sensor de puerta), se activará una alarma. El valor válido del retardo del sensor de puerta varía entre 1 y 255 segundos
Tipo de sensor de la puerta	Hay tres tipos de sensores: Ninguno, Normalmente abierto y Normalmente cerrado. Ninguno: significa que el sensor de la puerta no está en uso Normalmente abierto: significa que la puerta siempre se deja abierta cuando hay energía eléctrica encendida. Normalmente cerrado: significa que la puerta siempre queda cerrada cuando hay energía eléctrica encendida.
Dispositivo maestro	Al configurar los dispositivos maestro y esclavo, puede establecer el estado del maestro como Fuera o Dentro. **Salida:** Un registro de verificación en el dispositivo maestro es un registro de salida**. Entrada:** Un registro de verificación en el dispositivo maestro es un registro de entrada.
Dispositivo esclavo	Al configurar los dispositivos maestro y esclavo, puede establecer el estado del esclavo como Fuera o Dentro. **Salida:** Un registro de verificación en el dispositivo esclavo es un registro de salida. **Entrada:** Un registro de verificación en el dispositivo esclavo es un registro de entrada

Terminal de asistencia:

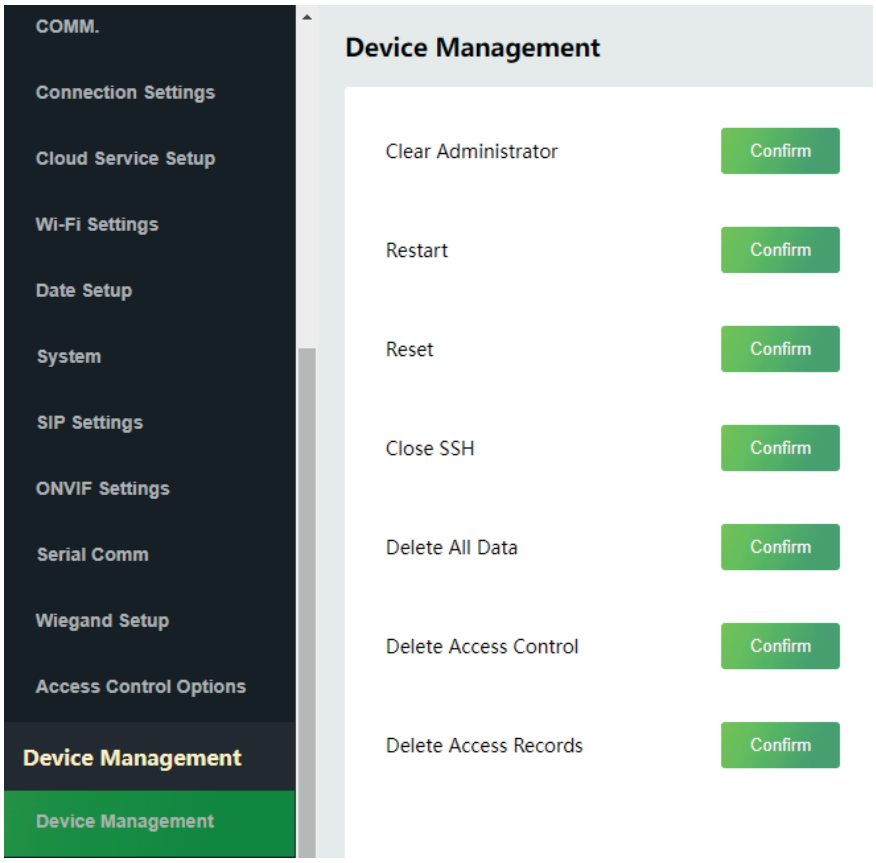


Nombre de la función	Descripción
Retraso(s) del bloqueo de la puerta	El tiempo que el dispositivo controla la cerradura eléctrica para que esté en estado de desbloqueo. Valor válido: 1~255 segundos; 0 segundos representa la desactivación de la función.
Retraso(s) del sensor de la puerta	Si la puerta no está bloqueada y se deja abierta durante un período determinado (retardo del sensor de puerta), se activará una alarma. El valor válido del retardo del sensor de puerta varía entre 1 y 255 segundos.
Retraso(s) de la alarma de la puerta	Cuando el estado del sensor de la puerta es inconsistente con el del tipo de sensor de la puerta, se activará la alarma después de un período de tiempo; este período de tiempo es el Retardo de alarma de puerta (el valor varía de 1 a 999 segundos)
Tipo de sensor de la puerta	Hay tres tipos de sensores: **Ninguno, Normalmente abierto y Normalmente cerrado. Ninguno:** significa que el sensor de la puerta no está en uso. **Normalmente abierto:** significa que la puerta permanece siempre abierta cuando hay corriente eléctrica. **Normalmente cerrado:** significa que la puerta permanece siempre cerrada cuando hay corriente eléctrica.

19.5 Administración de dispositivos

19.5.1 Gestión de dispositivos

Haga clic en Administración de dispositivos en el servidor web.



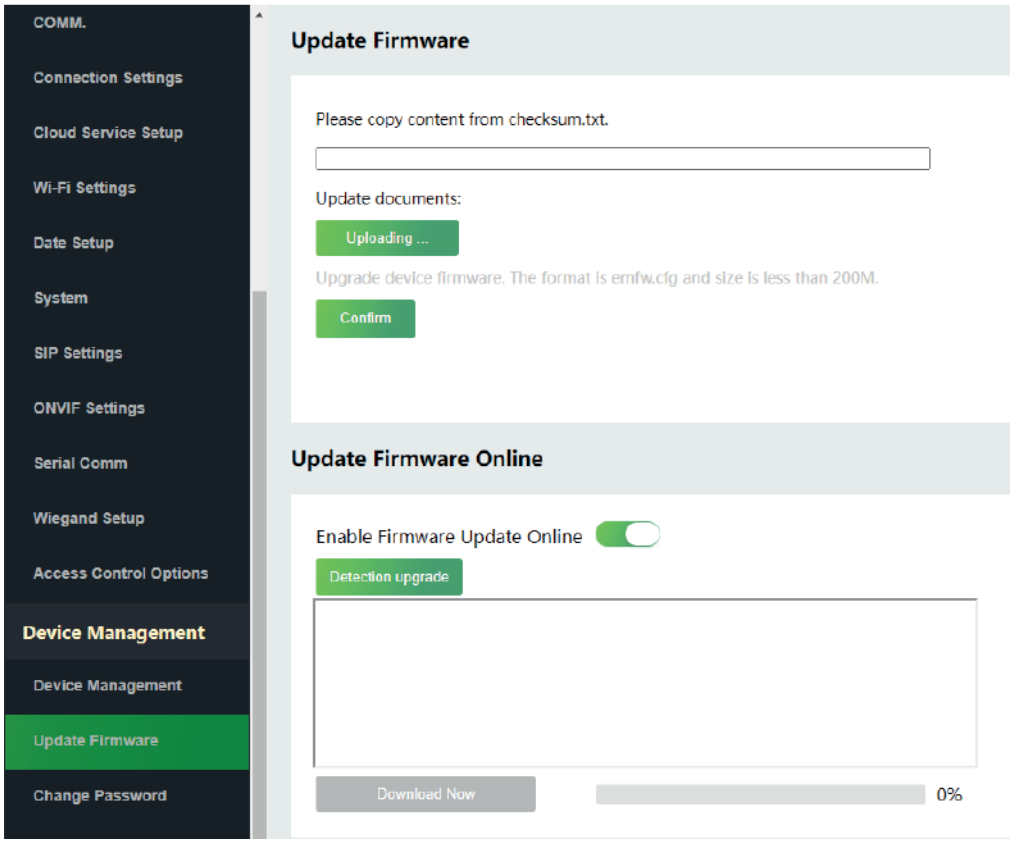
Nombre de la función	Descripción
Borrar administrador	Elija si desea cambiar el superadministrador a un usuario normal.
Reanudar	Elija si desea reiniciar el dispositivo.
Reiniciar	La función Restablecer restaura la configuración del dispositivo, como la comunicación y la configuración del sistema, a la configuración predeterminada de fábrica (esta función no borra los datos del usuario registrado). ***Nota:*** Después del reinicio, la IP del dispositivo se restaura a la original 192.168.1.201, consulte 19.4.1 Configuración de comunicación para modificarla.
Cerrar SSH	SSH se utiliza para ingresar al fondo del dispositivo para mantenimiento, elija si desea cerrar SSH.

Nombre de la función	Descripción
Eliminar todos los datos	Para eliminar la información y los registros de asistencia/acceso de todos los usuarios registrados.
Eliminar control de acceso	Para eliminar todos los datos de acceso
Eliminar registros de acceso/asistencia	Para eliminar todos los registros de acceso/asistencia.

19.5.2 Actualizar firmware

Haga clic en Actualizar firmware en el servidor web.

Seleccione un archivo de actualización y haga clic en Confirmar para completar la operación de actualización del firmware



Nota: Si necesita el archivo de actualización, póngase en contacto con nuestro servicio de asistencia técnica. En circunstancias normales, no se recomienda actualizar el firmware.

También puedes optar por actualizar el firmware en línea. Al hacer clic en «Detectar actualización», pueden darse los tres casos siguientes:

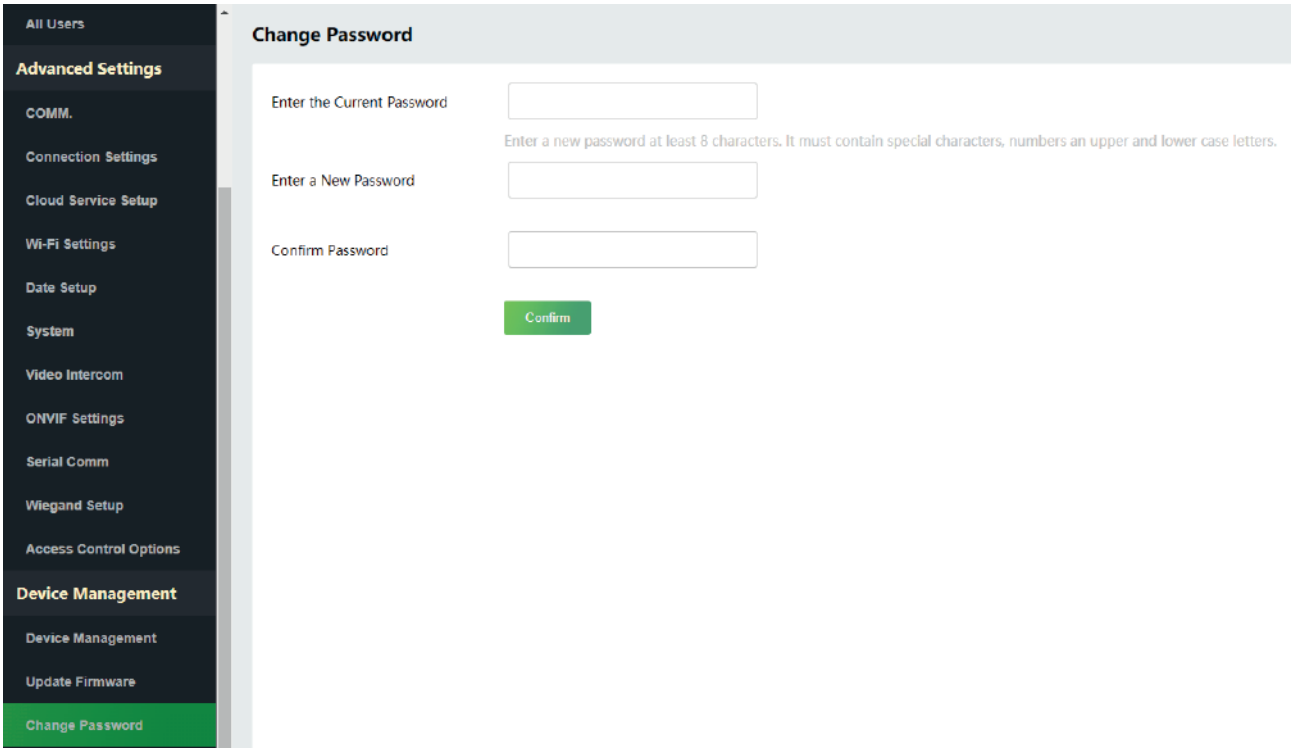
- Si la consulta falla, la interfaz indicará "Consulta fallida".

- Si la versión del firmware del dispositivo es la más reciente, aparecerá un mensaje indicando que la versión actual ya es la más reciente.
- Si la versión del firmware del dispositivo no es la más reciente, se mostrarán el número de versión y el registro de cambios de la última versión. Los usuarios pueden decidir si desean actualizar a la última versión del firmware.

19.5.3 Cambiar contraseña

Haga clic en Cambiar contraseña en el servidor web.

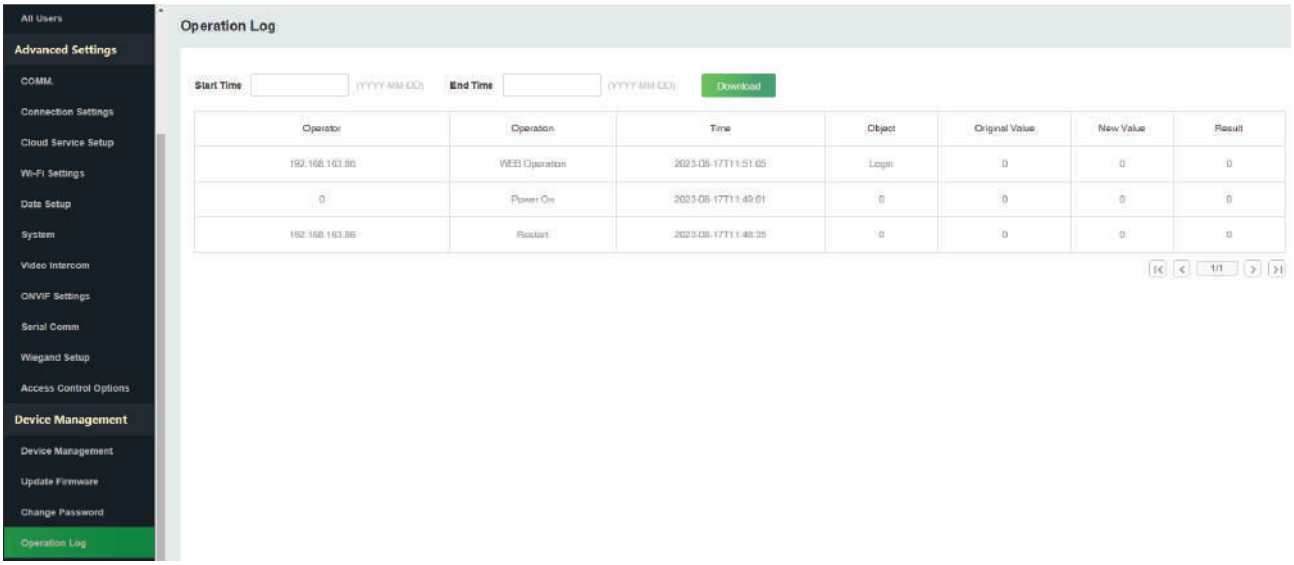
En esta interfaz, puede cambiar la contraseña del servidor web.



19.5.4 Registro de operaciones

Haga clic en Registro de operaciones en el servidor web.

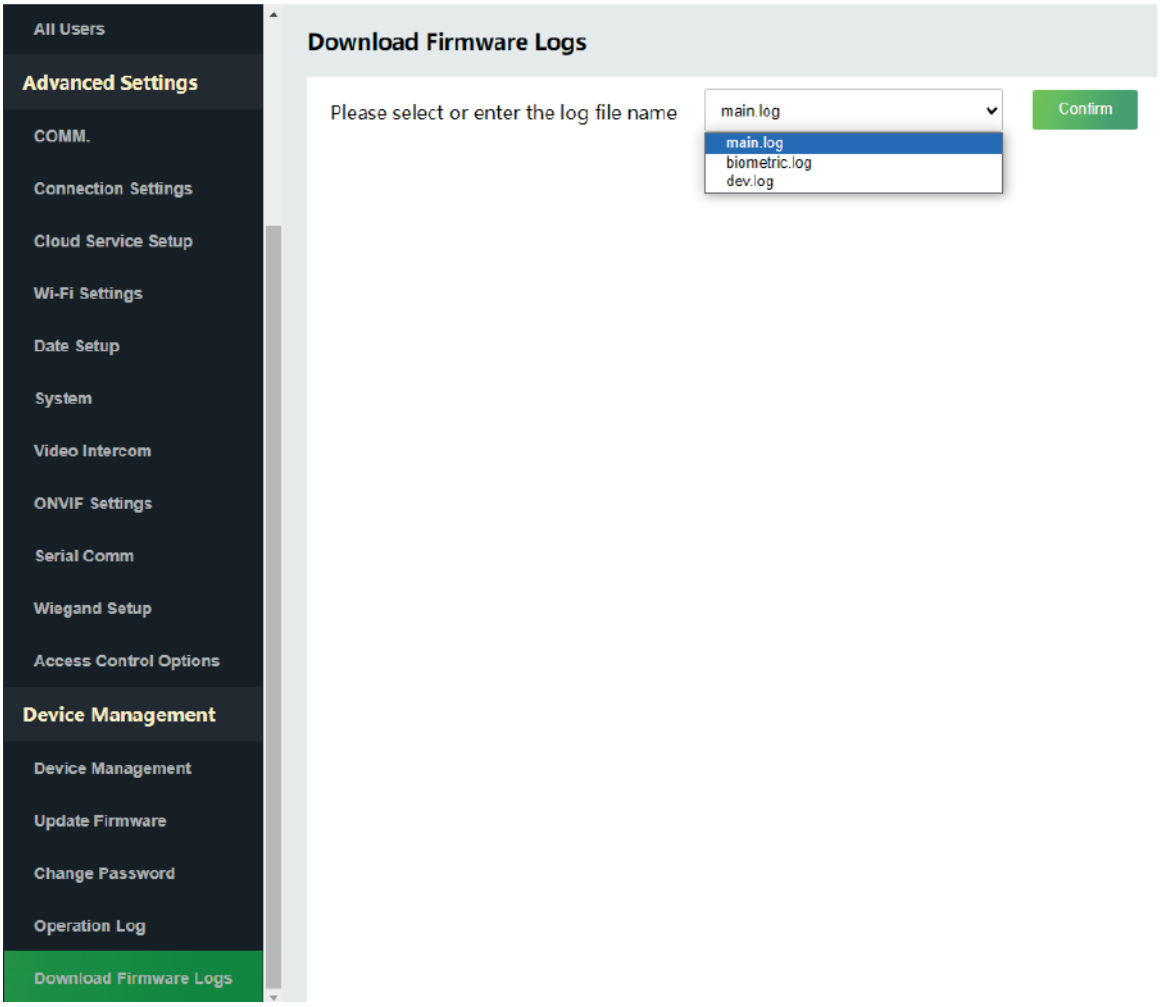
Se guardan todos los registros de operaciones del usuario en el dispositivo o servidor web. Los usuarios pueden buscar y descargar estos registros por fecha y hora.



19.5.5 Descargar registros de firmware

Haga clic en Descargar registros de firmware en el servidor web

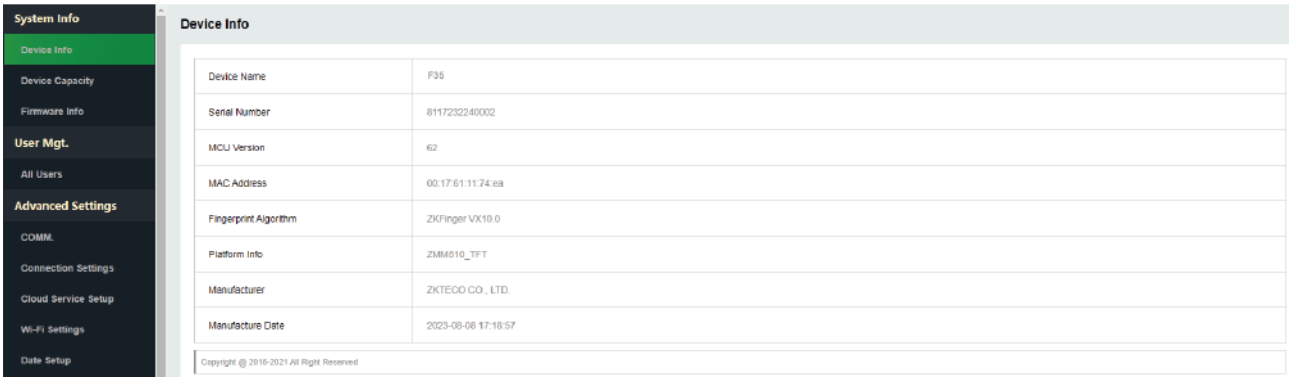
En esta interfaz, puede seleccionar descargar el registro principal, biométrico o de desarrollo.

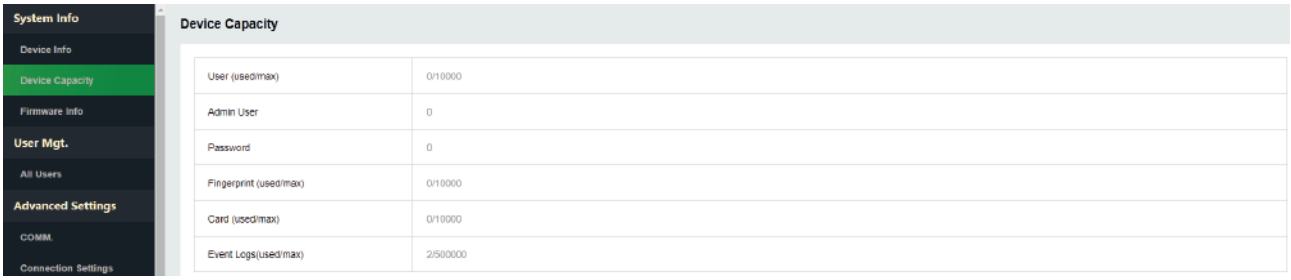


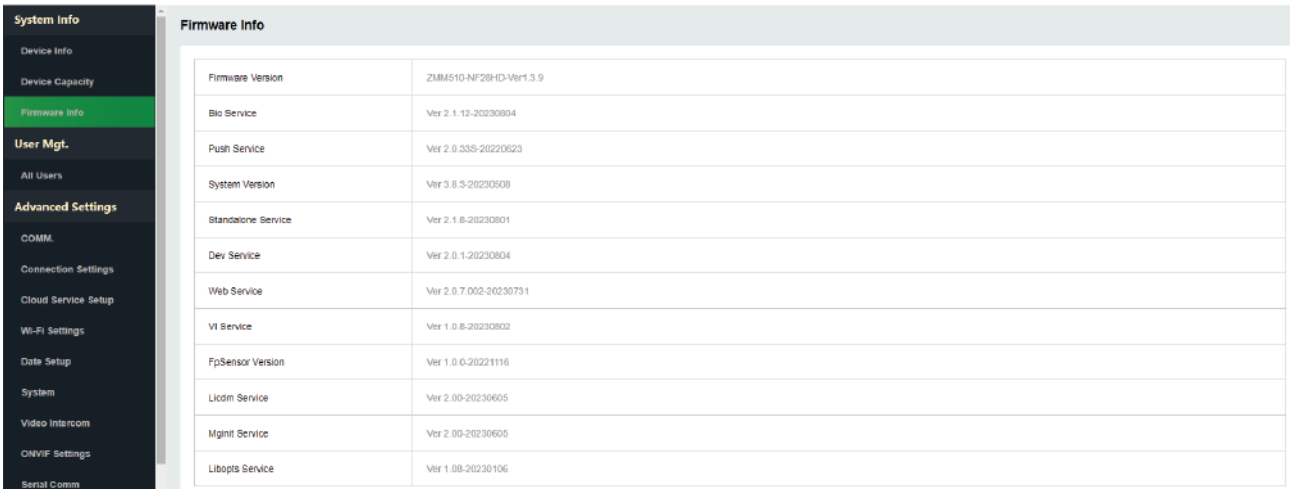
19.6 Información del sistema

Haga clic en Información del sistema en el servidor web

En esta interfaz, puede ver la capacidad de datos, el dispositivo y la información del firmware del dispositivo actual





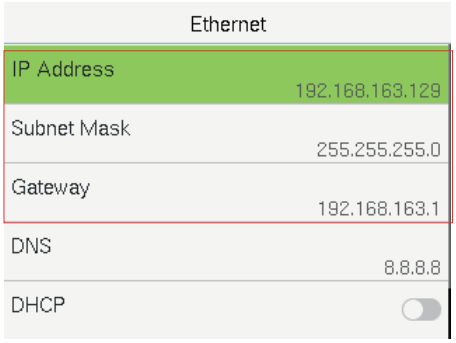


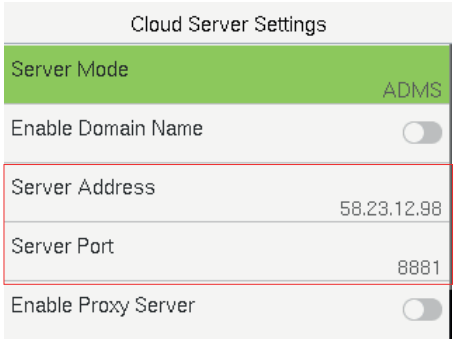
Nombre de la función	Descripción
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la versión de MCU, la dirección MAC y la huella digital. Información de la versión del algoritmo, información de la plataforma y del fabricante.
Capacidad del dispositivo	Muestra el almacenamiento de usuario, la contraseña, la huella digital, el almacenamiento de la tarjeta, los administradores y los registros de eventos del dispositivo actual.
Información sobre el firmware	Muestra la versión del firmware y otra información de la versión del dispositivo

20 Conéctese al software ZKBio CVAccess

20.1 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 poder comunicarse con el servidor ZKBio CVAccess)
2. En el menú principal, haz clic en COMUNICACIONES > Configuración del servidor en la nube para configurar la dirección y el puerto del servidor. Dirección del servidor: configura la dirección IP del servidor ZKBio CVAccess. Puerto del servidor: configura el puerto del servidor ZKBio CVAccess.

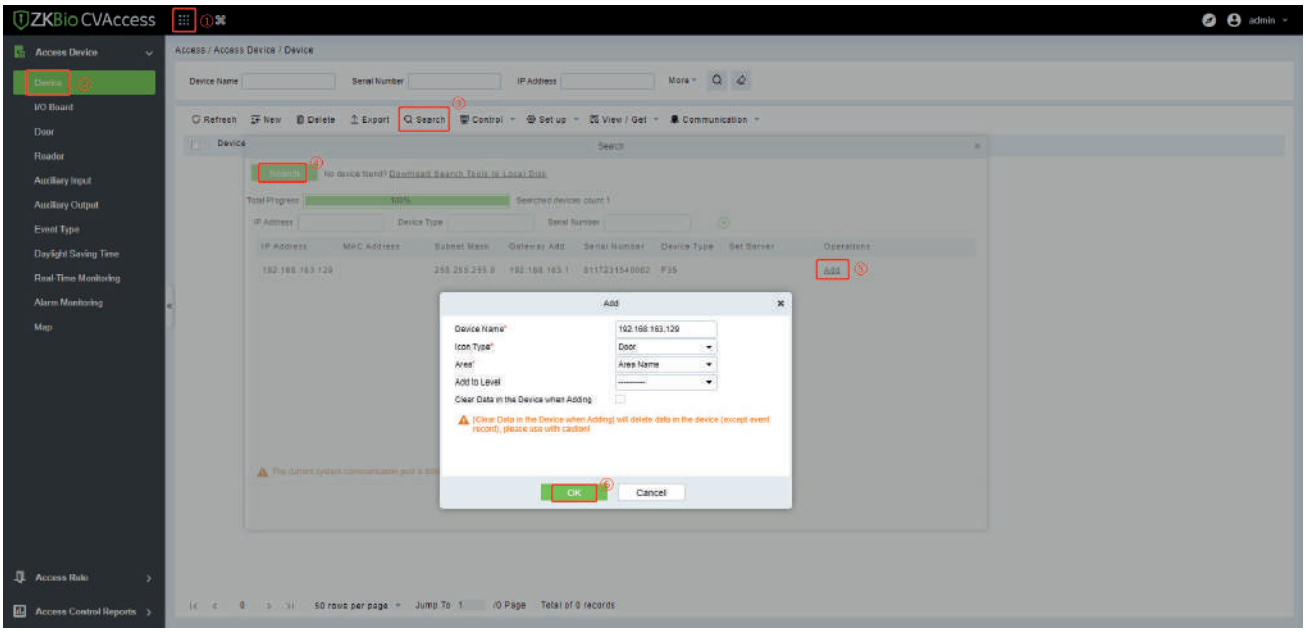




20.2 Agregar dispositivo en el software

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

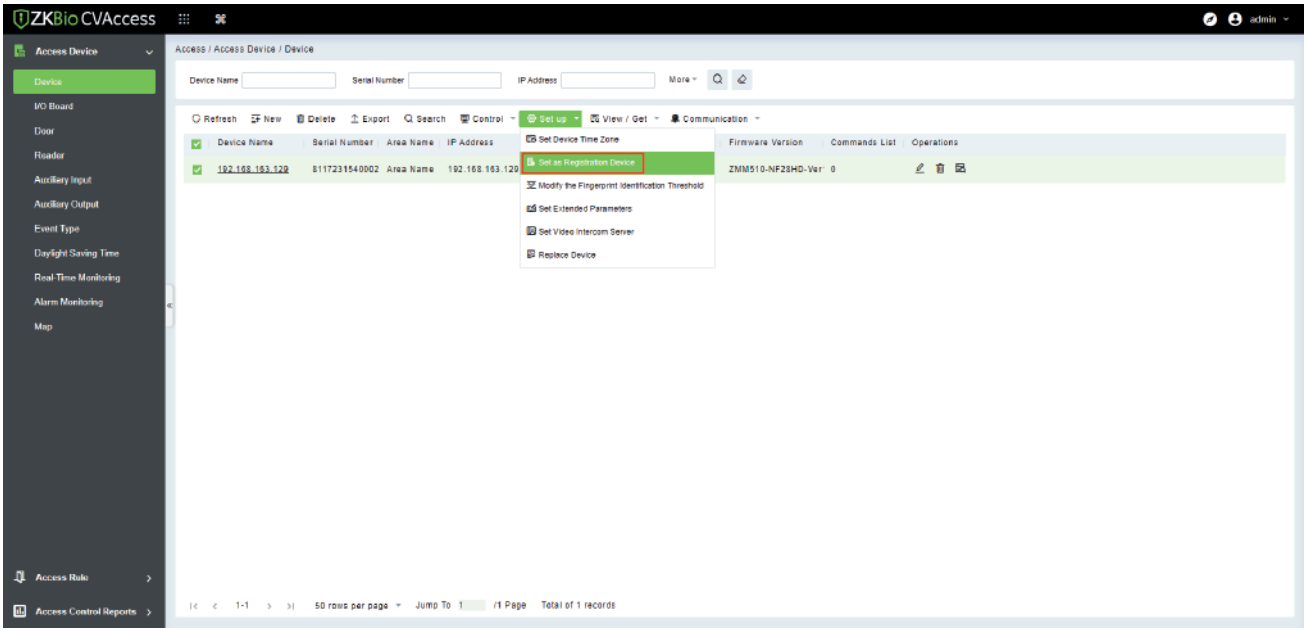
1. Haga clic en **Acceso > Dispositivo > Buscar > Buscar** para abrir la interfaz de búsqueda en el software.
2. Haga clic en **Buscar** y aparecerá el mensaje **[Buscando……]**
3. Después de la búsqueda, se mostrará la lista y el número total de controladores de acceso



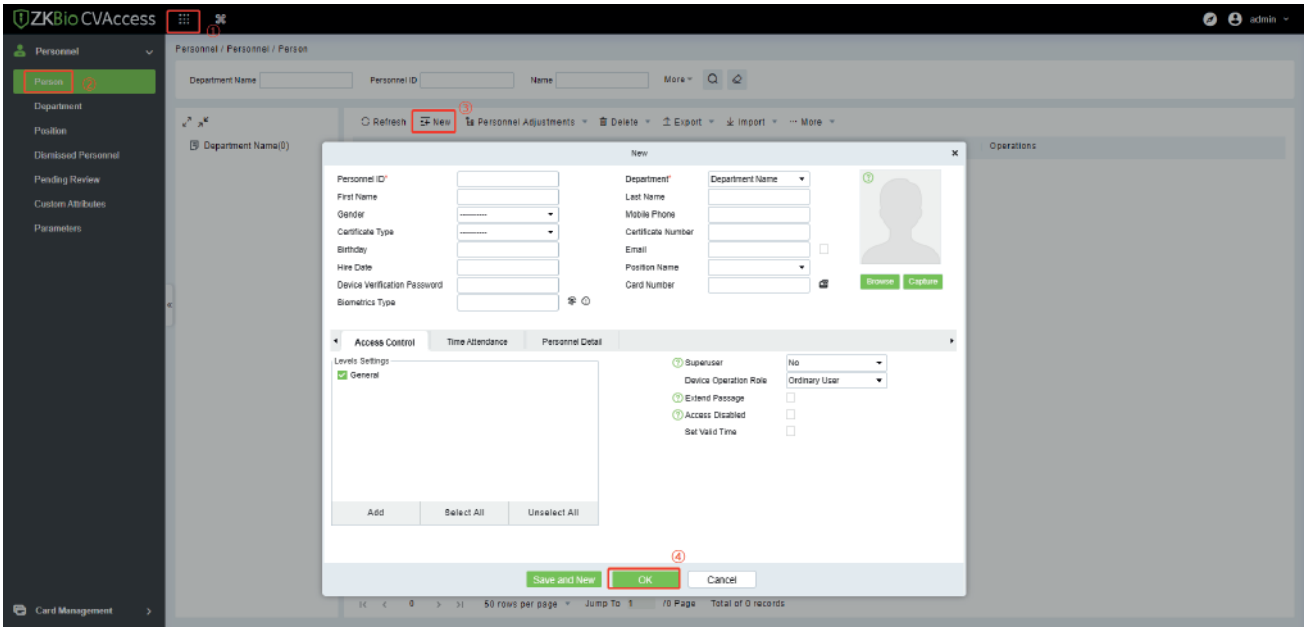
4. Haz clic en [Añadir] en la columna «Operación»; se abrirá una nueva ventana. Selecciona el tipo de icono, el área y «Añadir al nivel» en cada menú desplegable y haz clic en [Aceptar] para añadir el dispositivo.
5. Una vez que la adición se haya realizado correctamente, el dispositivo se mostrará en la lista de dispositivo

20.3 Añadir personal en el software y registro de huellas dactilares en línea

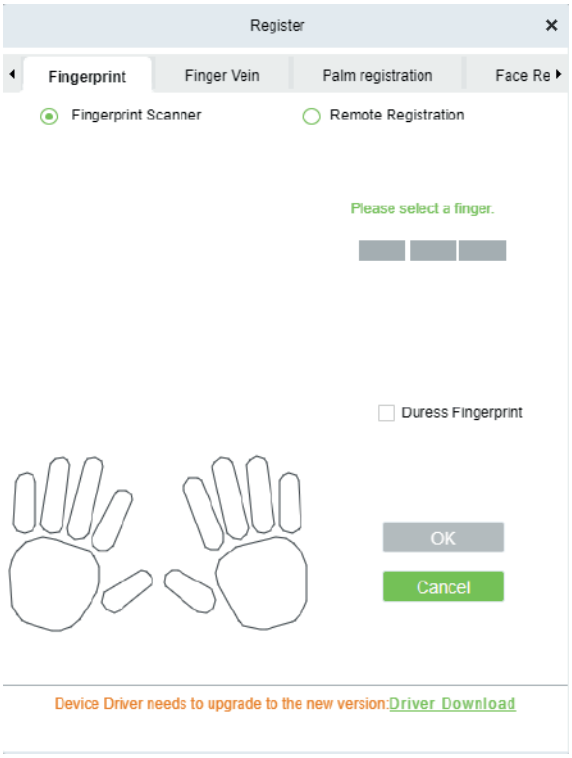
1. En la lista de dispositivos, seleccione el dispositivo y haga clic en Configurar > Establecer como dispositivo de registro



2. Haga clic en Personal > Persona > Nuevo



3. Rellene todos los campos obligatorios del usuario y haga clic 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 haga clic en Confirmar.



6. Seleccione el dedo que desea registrar y presione el dedo sobre el sensor de huellas dactilares del dispositivo. tres veces. Si la huella dactilar se registra correctamente, el dispositivo mostrará el mensaje "Registro exitoso".

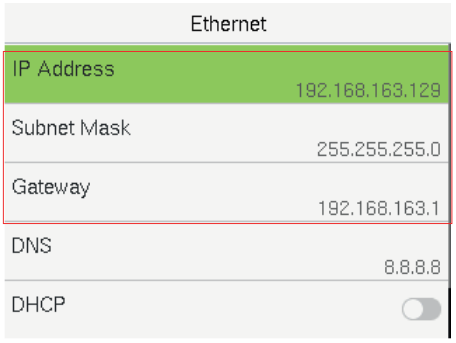
7. Si desea registrar una huella dactilar de emergencia, puede hacer clic en «Huella dactilar de emergencia» antes de registrar la huella.
   - Huella dactilar de emergencia: en cualquier caso, se activa una alarma de emergencia cuando una huella dactilar coincide con una huella dactilar de emergencia.
8. Haga clic en Aceptar para guardar el usuario.
9. Haga clic en Acceso > Dispositivo > Control > Sincronizar todos los datos con los dispositivos para sincronizar todos los datos con el dispositivo, incluidos los nuevos usuarios.

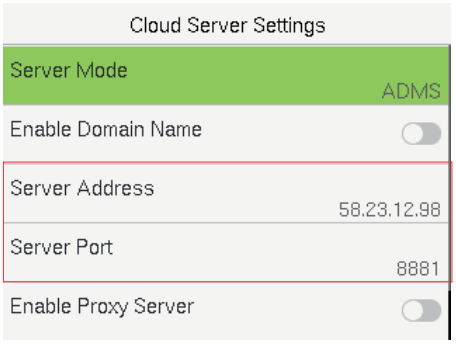
Nota: Para otras operaciones específicas, consulte el Manual de usuario de ZKBio CVAccess.

21 Conéctese al software ZKBioTime 8.0.

21.1 Establecer la dirección de comunicación

1. Pulse COMM. > Ethernet en el menú principal para configurar la dirección IP y la puerta de enlace del dispositivo (***Nota:*** La dirección IP debe poder comunicarse con el servidor ZKBioTime 8.0, preferiblemente en el mismo segmento de red que la dirección del servidor)
2. En el menú principal, haga clic en COM. > Configuración del servidor en la nube para establecer la dirección y el puerto del servidor: **Dirección del servidor:** Establezca la dirección IP del servidor ZKBioTime 8.0. **Puerto del servidor:** Configure el puerto del servidor como en el servidor ZKBioTime 8.0.

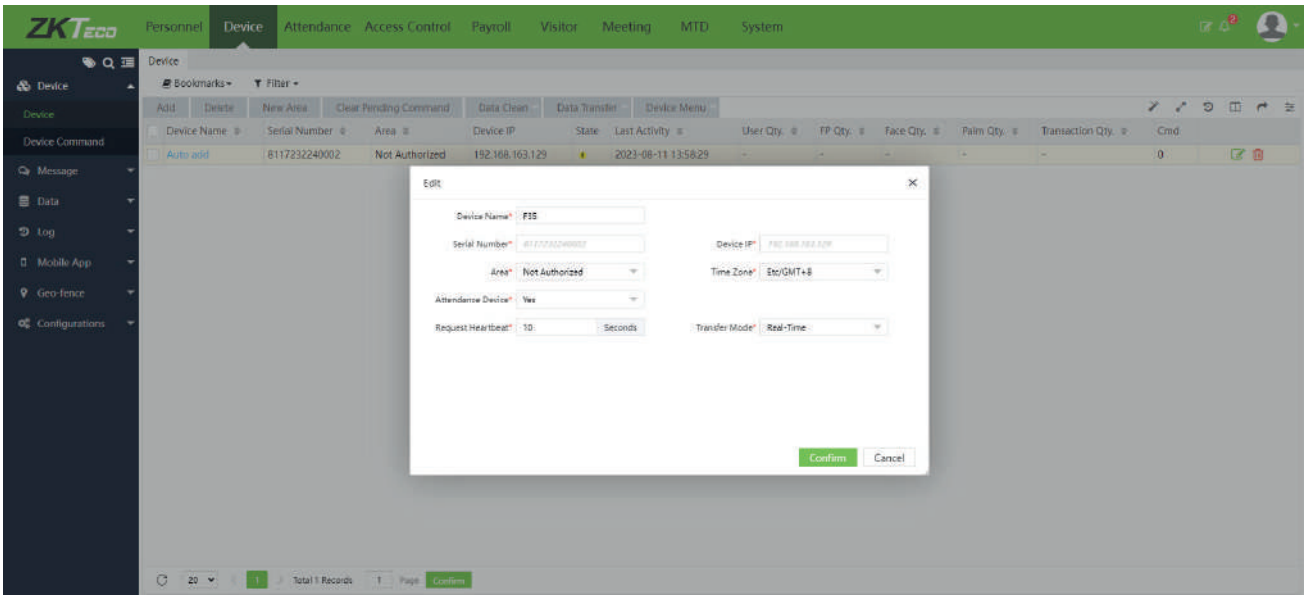




21.2 Agregar dispositivo en el software

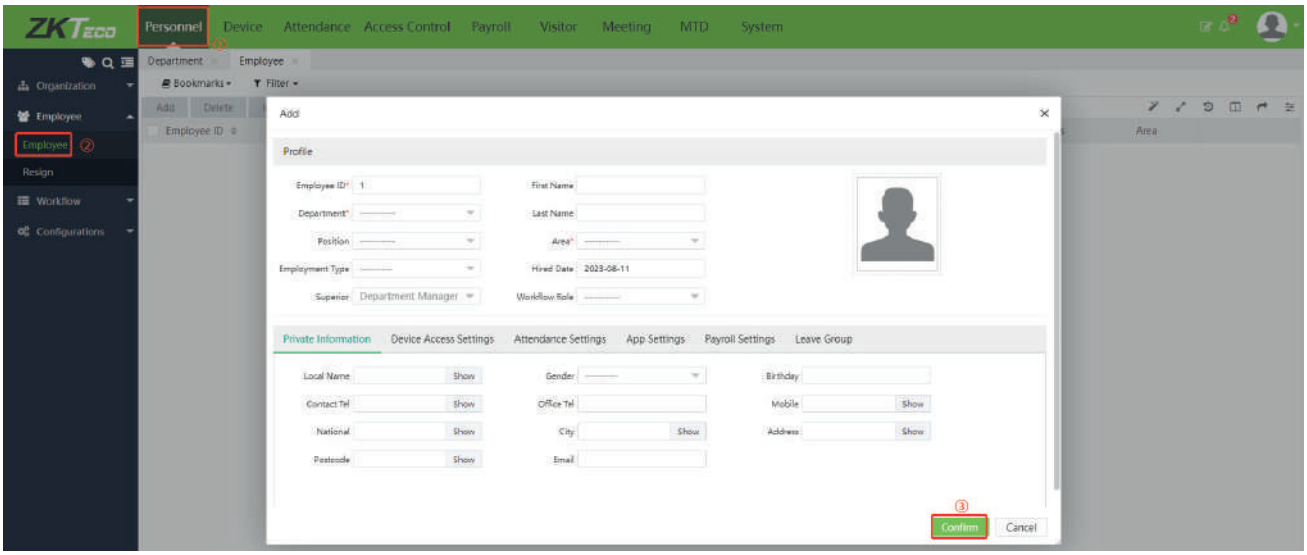
Tras configurar el dispositivo, este se añadirá automáticamente al software. Abra el software ZKBioTime y seleccione [Módulo de dispositivo] > [Dispositivo] > [Dispositivo], haga clic en el dispositivo de la lista y cambie el nombre y el área del dispositivo.

Nota: Los dispositivos añadidos automáticamente deben asignarse a áreas personalizadas para que puedan comunicarse con el software.

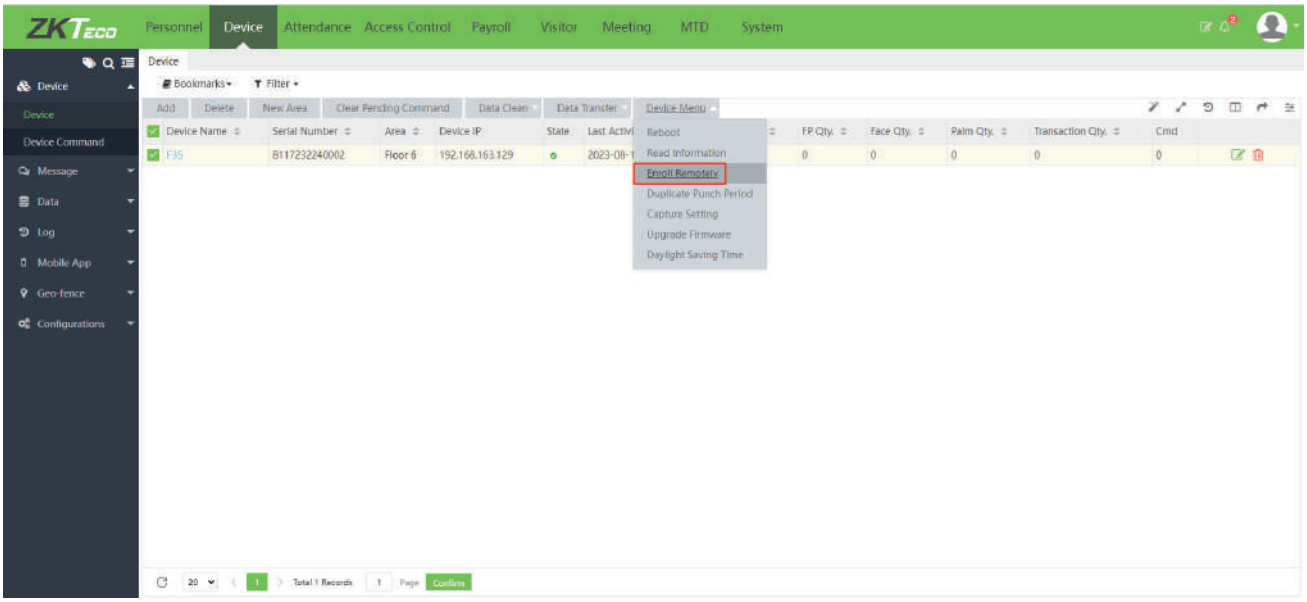


21.3 Añadir personal en el software y registro de huellas dactilares en línea

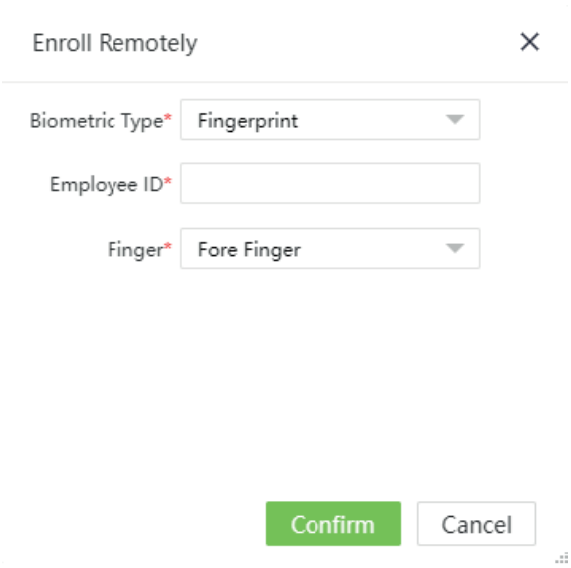
1. Haga clic en **Personal > Empleado > Agregar**



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 del dispositivo > Inscribir de forma remota



4. Introduzca el ID de empleado, seleccione la huella dactilar que desea registrar y presione el sensor de huellas dactilares del dispositivo tres veces. Si la huella se registra correctamente, el dispositivo mostrará el mensaje "Registro exitoso"



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

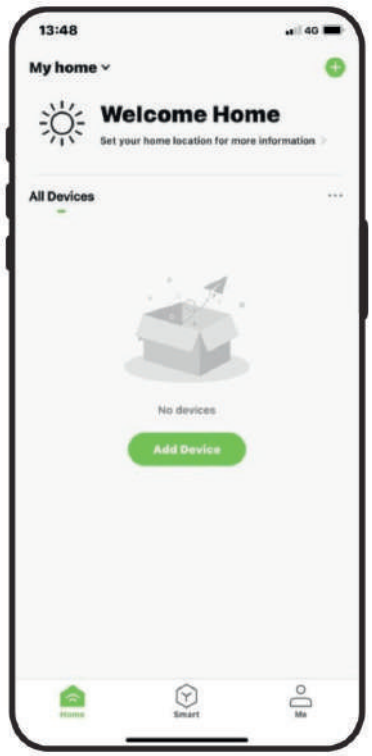
Nota: Para otras operaciones específicas, consulte el manual de usuario de ZKBioTime 8.0.

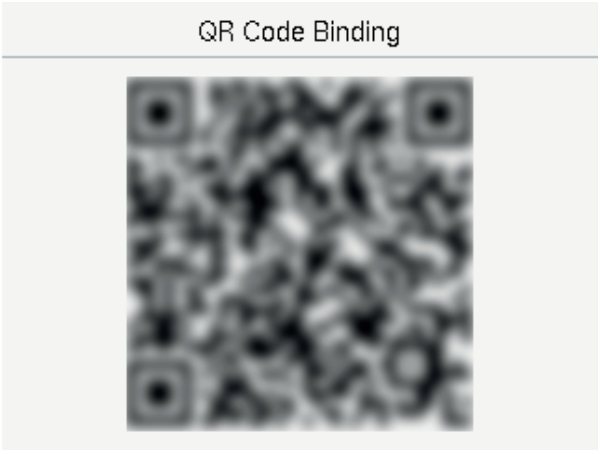
22 Conexión a la aplicación ZSmat★

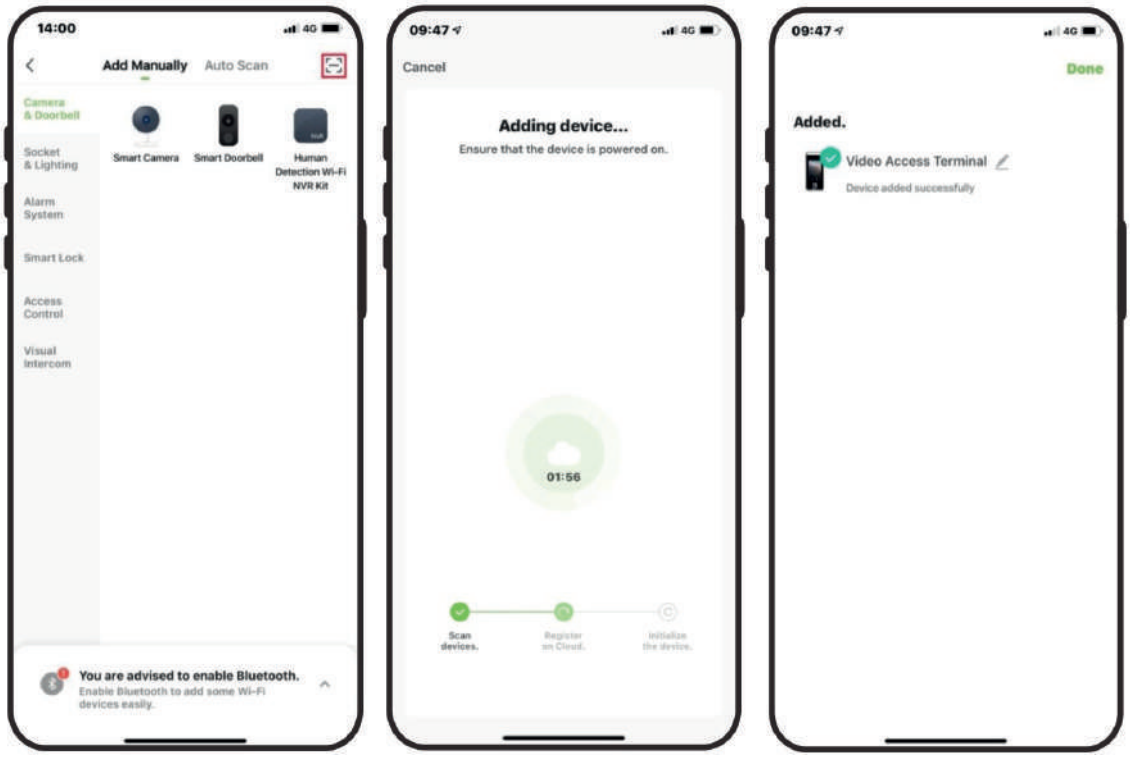
22.1 Añadir un dispositivo en la aplicación ZSmart

Una vez descargada e instalada la aplicación ZSmart en tu teléfono, empieza por crear una cuenta de usuario utilizando tu dirección de correo electrónico. Una vez completada la creación de la cuenta de usuario, inicia sesión en la aplicación. A continuación, pulsa el icono Add Device o situado en la esquina superior derecha de la pantalla para iniciar el proceso de añadir un dispositivo. El proceso paso a paso es el siguiente:

1. Haz clic en Agregar dispositivo en la página de inicio.
2. En el dispositivo, pulse [M/OK] > Sistema > Parámetros del videoportero > Vinculación de código QR para mostrar el código QR del dispositivo.
3. Haga clic en el icono en la esquina superior derecha.

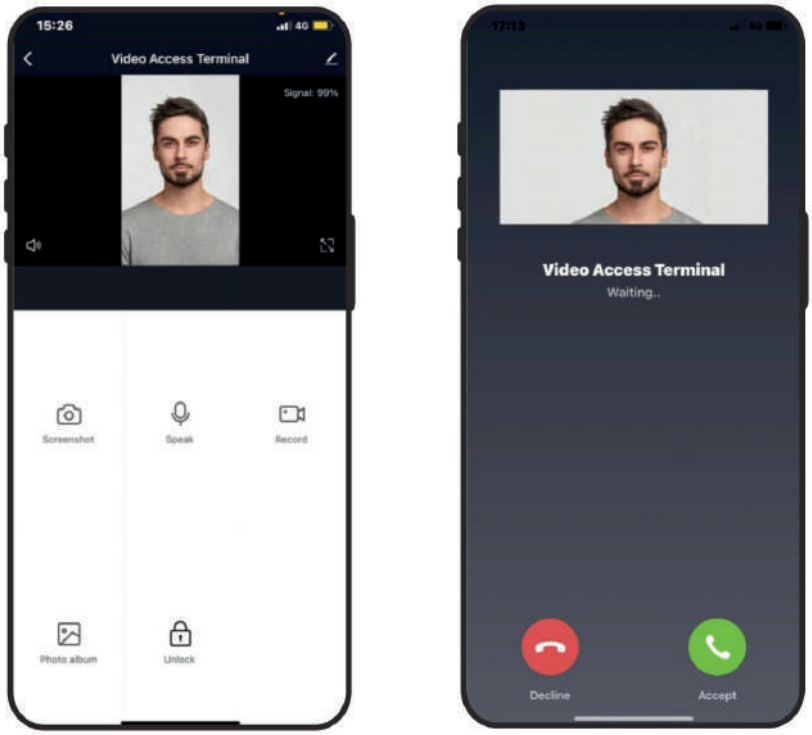






22.2 Conexión de videoteléfono

Los visitantes pulsan el icono del dispositivo para realizar una llamada y, a continuación, el teléfono sonará. El usuario puede aceptar o rechazar la llamada. Una vez que el usuario acepte la llamada, se abrirá la interfaz del videoportero. Introduzca la contraseña para abrir la puerta.



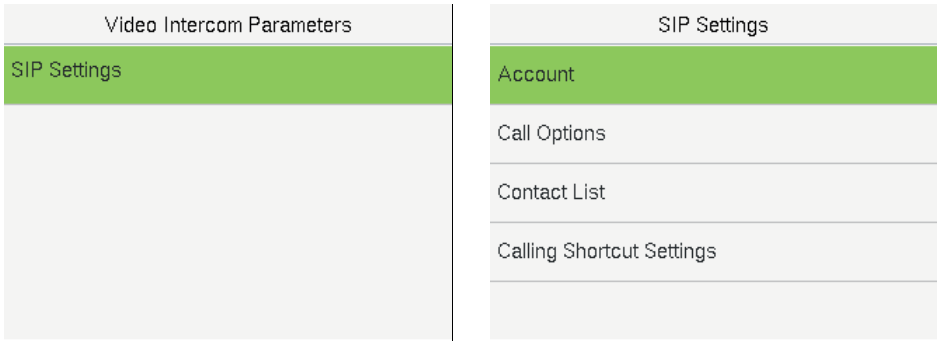
Parámetro	Descripción
Captura de pantalla	Haz clic para tomar una captura de pantalla
Hablar	Al hacer clic en el icono, este se vuelve azul y en ese momento puedes hablar con el dispositivo.
Registro	Haz clic para grabar un vídeo.
Álbum de fotos	Visualiza y elimina capturas de pantalla y vídeos grabados
Desbloquear	Haz clic para abrir la puerta de forma remota. El registro de desbloqueo se guarda en Yo > Centro de mensajes.

Nota: Para otras operaciones específicas, consulte el manual de usuario de la aplicación ZSmart

23 Conectando a SIP★

En el dispositivo, pulse **[M/OK] > Sistema > Parámetros del videoportero > Configuración SIP** para acceder a la configuración de los parámetros de monitorización

Nota: Esta función debe utilizarse con la estación interior.



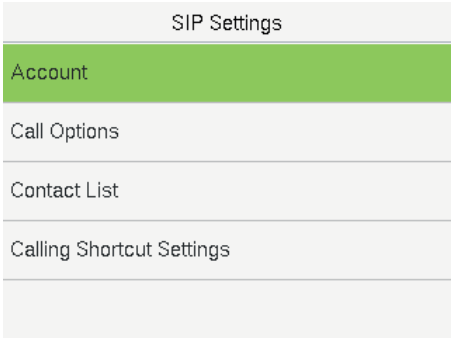
Descripción de la función

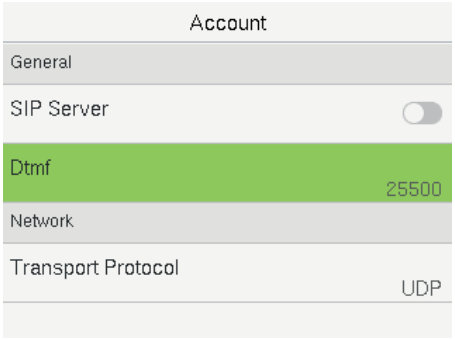
Nombre de la función		Descripción
Cuenta	**Servidor SIP**	Seleccione si desea habilitar el servidor SIP. Al habilitarlo, deberá configurar la dirección del servidor, el puerto del servidor, el nombre de usuario, el nombre de usuario y la contraseña. (Nota: Cada vez que se active o desactive, el dispositivo se reiniciará para que los cambios surtan efecto).
	Habilitar nombre de dominio	Seleccione si desea habilitar el modo de nombre de dominio.
	Dirección del servidor	Introduzca la dirección del servidor.
	Puerto del servidor	Introduzca el puerto del servidor.
	Nombre de inicio de sesión	Ingrese el nombre de usuario del servidor.
	Nombre de usuario	Introduzca el nombre de usuario del servidor.
	Contraseña	Introduzca la contraseña del servidor.
	DTMF	El valor debe configurarse igual que el valor DTMF en la estación interior.
	Protocolo de transporte	Establezca el protocolo de transporte entre F35 y la estación interior.
Opciones de llamada	**Retraso(s) de llamada**	Establezca la hora de la llamada; el valor válido es de 30 a 60 segundos.
	Retraso(s) de conversación	Configure el tiempo de intercomunicación; el valor válido es de 60 a 120 segundos.
	Cifrado	Está desactivada de forma predeterminada.
Lista de contactos	Cuando el servidor SIP está desactivado, aquí se pueden añadir el número de dispositivo y la dirección de llamada de las estaciones interiores.	
Configuración de accesos directos de llamadas	**Modo de llamada**	Cuando el servidor SIP está activado, se encuentra por defecto en modo estándar y no se puede modificar; cuando el servidor SIP está desactivado, se puede configurar en modo estándar o en modo de llamada directa. En el modo de llamada directa, el usuario puede llamar a varias estaciones interiores al mismo tiempo.
	En el dispositivo se pueden definir tres teclas de acceso directo: admin, ROOM1 y ROOM2. Puede configurar una tecla de acceso directo para llamar rápidamente a la estación interior sin tener que introducir la dirección IP ni el número de habitación de la unidad interior cada vez	

El F35 y la estación interior para lograr videoportero tienen dos modos, respectivamente, LAN y Servidor SIP.

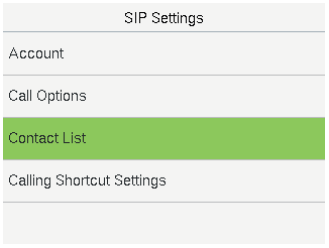
23.1 Uso de la red de área local

1. Configure la estación interior en el mismo segmento de red que el dispositivo.
2. En la interfaz de configuración SIP, haz clic en Cuenta > DTMF para establecer el valor igual al valor de DTMF de la estación interior.

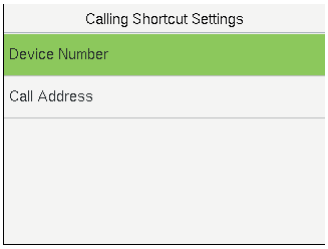




3. En la interfaz de Configuración SIP , haga clic en Lista de contactos > Agregar para añadir la estación interior conectada.



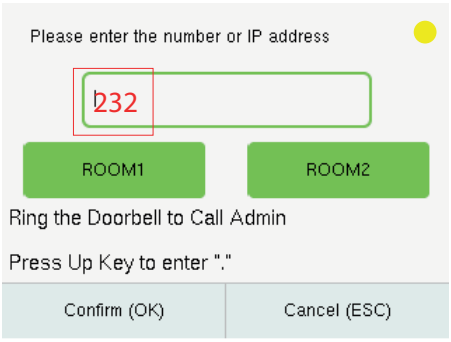


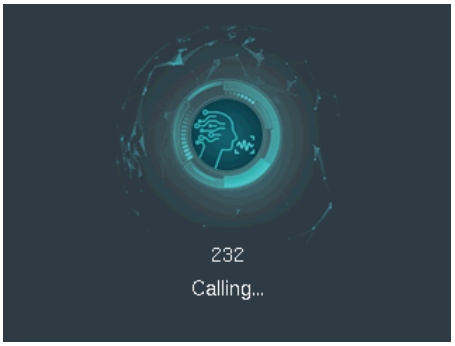


Número de dispositivo: Personalice el número de la estación interior. Puede introducir este número en el dispositivo para llamar rápidamente a la estación interior para el videoportero.

Dirección de llamada: Es la dirección IP de la estación interior.

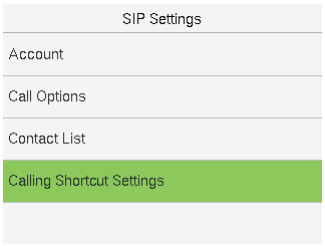
4. Para activar la función de videoportero, pulse el icono del F35 e introduzca la dirección IP o el número de dispositivo de la estación interior en la interfaz correspondiente

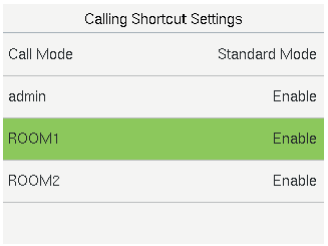


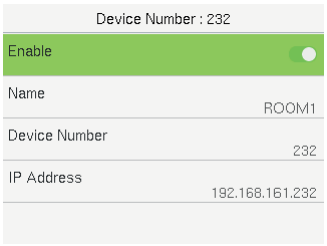


- **Personaliza las teclas de acceso directo para realizar llamadas**

1. En la interfaz de Configuración SIP , haga clic en Configuración de accesos directos de llamada para definir las teclas de acceso directo.

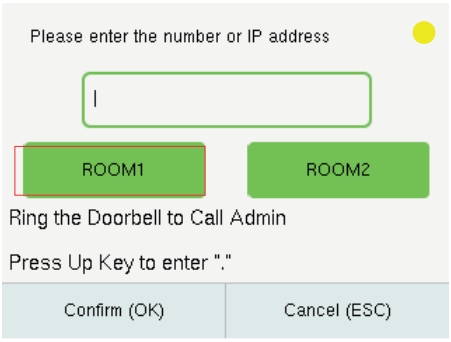


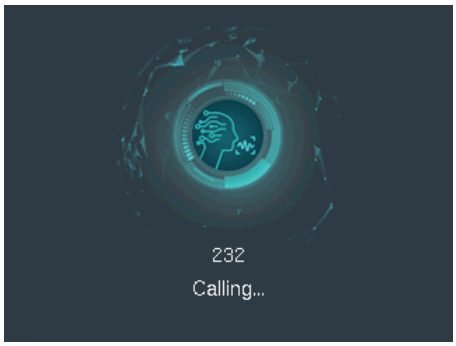




Nombre: Personaliza el nombre de las teclas de acceso directo
Número de dispositivo: Es el número de dispositivo que se configuró en el menú Lista de contactos.
Dirección IP: Una vez configurado el número del dispositivo, se mostrará automáticamente.

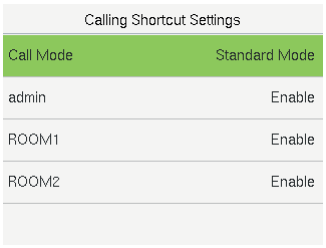
2. A continuación, puedes pulsar el icono del F35 y pulsar las teclas de acceso rápido de llamada para llamar a la estación interior.

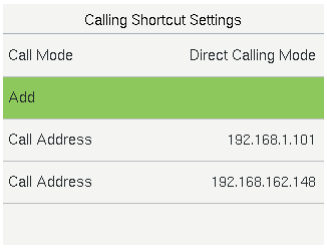


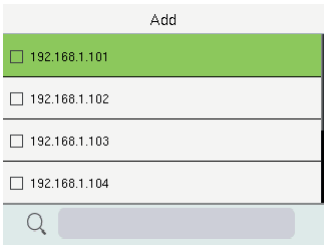


- **Llamada directa**

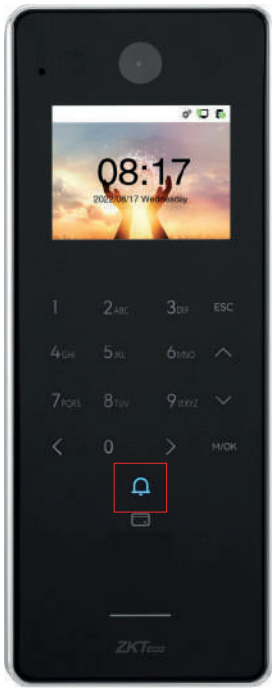
1. En la interfaz de configuración de SIP, haz clic en «Configuración de accesos directos de llamada» > «Modo de llamada» > «Modo de llamada directa» > «Añadir». Selecciona las direcciones IP de los teléfonos fijos a los que quieras llamar; a continuación, estos aparecerán en la lista.

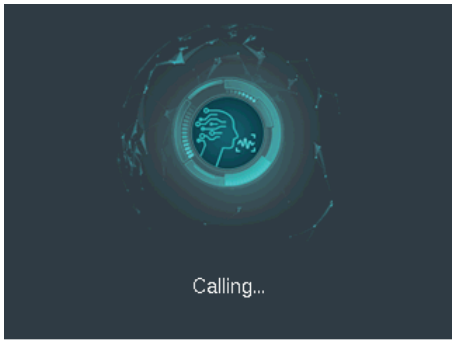






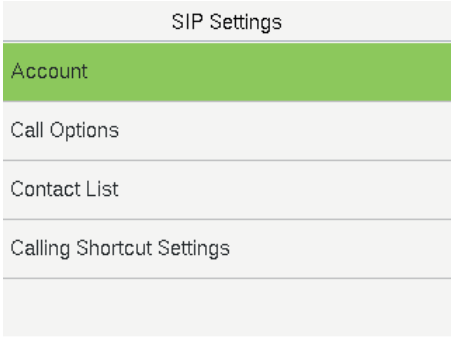
2. A continuación, puedes pulsar el icono del F35 para llamar a todas las estaciones interiores a la vez.

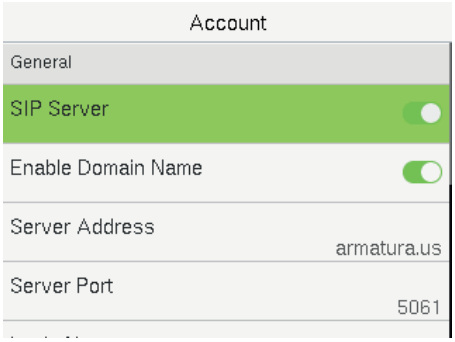




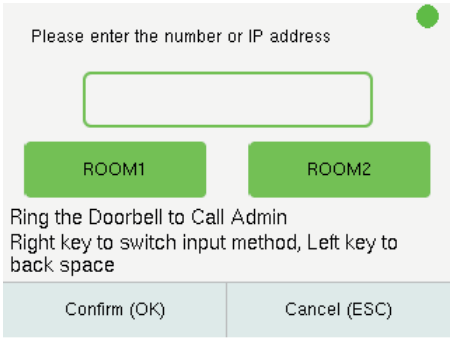
23.2 Servidor SIP

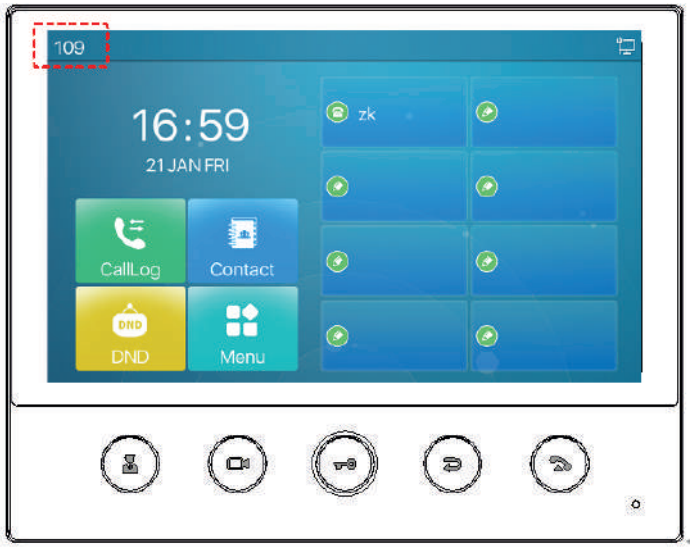
1. En la interfaz de Configuración SIP , haga clic en Cuenta > Servidor SIP para habilitarlo, ingrese los parámetros relacionados con el servidor, como se muestra a continuación:

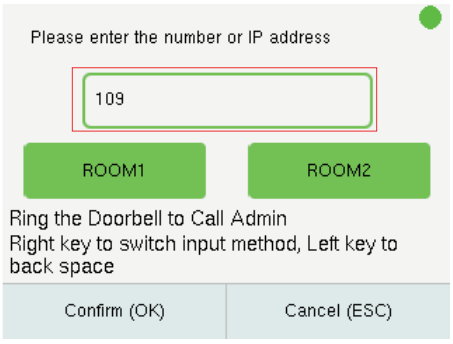


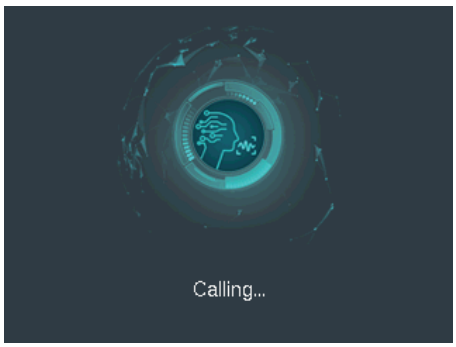


2. Tras configurar correctamente el SIP, el punto amarillo en la esquina superior derecha de la página de llamadas se volverá verde, lo que indica que el F35 está conectado al servidor. A continuación, podrá iniciar una llamada al nombre de cuenta de la estación interior.
   Nota: Los clientes crean su propio servidor SIP.









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

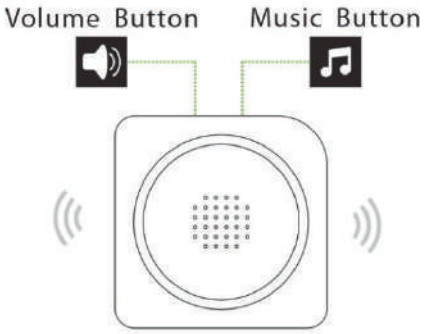
24 Conexión al timbre inalámbrico★

Nota: Esta función debe utilizarse con el timbre inalámbrico.

24.1 Conecte el timbre inalámbrico

1. En primer lugar, enciende el timbre inalámbrico. A continuación, mantén pulsado el botón de música durante 1,5 segundos hasta que el indicador empiece a parpadear. El parpadeo del indicador indica que el timbre se encuentra ahora en modo de emparejamiento. Si el timbre inalámbrico suena y el indicador parpadea, la conexión se ha establecido correctamente y, a continuación, puedes hacer clic en el icono del dispositivo para finalizar el proceso.





2. Tras un emparejamiento exitoso, haga clic en el icono del dispositivo sonará el timbre inalámbrico.

Nota:

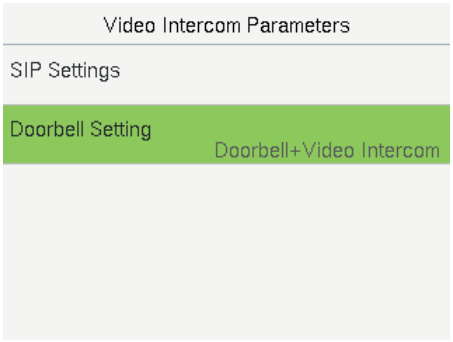
1) Para utilizar esta función, debe acceder al menú ([Sistema] > [Parámetros del videoportero] > [Configuración del timbre]) y configurarlo como Solo timbre o Timbre + Videoportero.
2) Cada F35 solo admite un timbre inalámbrico
3) El timbre inalámbrico debe ser comprado por los propios clientes

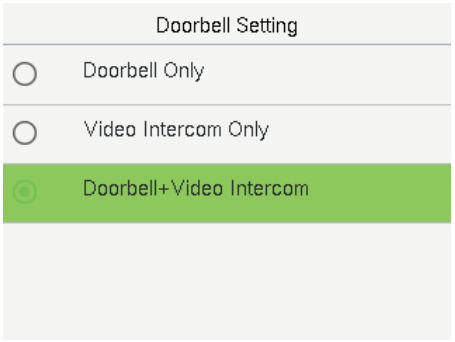
24.2 Desvinculación del timbre inalámbrico

Apaga primero el timbre inalámbrico y, a continuación, vuelve a colocar las pilas mientras mantienes pulsado el botón de música hasta que se encienda el indicador, lo que significa que el proceso de desvinculación se ha realizado correctamente.

24.3 Configuración

En el dispositivo, pulse **[M/OK] > Sistema > Parámetros del videoportero > Configuración del timbre** para configurar el timbre.





Descripción de la función:

Nombre de la función	Descripción
Configuración del timbre	**Solo timbre:** Cuando el usuario pulsa el botón del timbre, solo suena el timbre **Solo videoportero:** Cuando el usuario pulsa el botón del timbre, solo el dispositivo realiza la llamada**.** **Timbre + videoportero:** Cuando el usuario pulsa el botón del timbre, este suena y, al mismo tiempo, el dispositivo realiza una llamada.

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.