Manual de usuario

Serie ProMA

Fecha: Diciembre 2022

Versión del documento: 2.0

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

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

Marca comercial

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

Descargo de responsabilidad

Este manual contiene información sobre la operación y mantenimiento del equipo ZKTeco. Los derechos de autor de todos los documentos, dibujos, etc. en relación con el equipo suministrado por ZKTeco pertenecen y son propiedad de ZKTeco. El contenido del presente no debe ser utilizado o compartido por el receptor con ningún tercero sin el permiso expreso por escrito de ZKTeco.

El contenido de este manual debe leerse en su totalidad antes de iniciar la operación y mantenimiento del equipo suministrado. Si alguno de los contenidos del manual parece confuso o incompleto, comuníquese con ZKTeco antes de iniciar la operación y el mantenimiento de dicho equipo.

Es un requisito previo esencial para la operación y el mantenimiento satisfactorios que el personal de operación y mantenimiento esté completamente familiarizado con el diseño y que dicho personal haya recibido una capacitación completa en la operación y el mantenimiento de la máquina/unidad/equipo. Es además esencial para la operación segura de la máquina/unidad/equipo que el personal haya leído, entendido y seguido las instrucciones de seguridad contenidas en el manual.

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

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

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

ZKTeco en ningún caso será responsable ante el usuario o cualquier tercero por daños incidentales, consecuentes, indirectos, especiales o ejemplares, incluidos, entre otros, pérdida de negocios, pérdida de ganancias, interrupción del negocio, pérdida de información comercial o cualquier pérdida pecuniaria, que surja de, en conexión con, o

relacionados con el uso de la información contenida en este manual o a la que se hace referencia en él, incluso si ZKTeco ha sido advertido de la posibilidad de tales daños.

Este manual y la información que contiene pueden incluir imprecisiones técnicas, de otro tipo o errores tipográficos. ZKTeco cambia periódicamente la información contenida en este documento que se incorporará en nuevas adiciones/enmiendas al manual. ZKTeco se reserva el derecho de agregar, eliminar, enmendar o modificar la información contenida en el manual de vez en cuando en forma de circulares, cartas, notas, etc. para una mejor operación y seguridad de la máquina/unidad/equipo. Dichas adiciones o enmiendas están destinadas a la mejora/ mejor funcionamiento de la máquina/unidad/equipo y tales enmiendas no darán derecho a reclamar compensación o daños en ninguna circunstancia.

ZKTeco no será responsable de ninguna manera (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 operación de la máquina/unidad/equipo más allá de los límites de tasa (iii) en caso de operación 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 últimos procedimientos de operación y documentos relevantes están disponibles enhttp://www.zkteco.com

Si hay algún problema relacionado con el producto, contáctenos.

Sede ZKTeco

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

Ciudad de Tangxia, Dongguan, China.

Teléfono + 86 769 - 82109991

Fax + 86 755 - 89602394

Para consultas relacionadas con negocios, por favor escríbanos a:sales@zkteco.com .

Para saber más sobre nuestras sucursales globales, visitewww.zkteco.com .

Sobre la empresa

ZKTeco es uno de los mayores fabricantes del mundo de lectores RFID y biométricos (huellas dactilares, faciales, venosos). Las ofertas de productos incluyen lectores y paneles de control de acceso, cámaras de reconocimiento facial de alcance cercano y lejano, controladores de acceso a ascensores/pisos, torniquetes, controladores de puerta con reconocimiento de matrículas (LPR) y productos de consumo que incluyen cerraduras de puerta con lector de rostro y huella dactilar que funcionan con batería. Nuestras soluciones de seguridad son multilingües y están localizadas en más de 18 idiomas diferentes. En las instalaciones de fabricación de última generación con certificación ISO9001 de 700 000 pies cuadrados de ZKTeco, controlamos la fabricación, el diseño del producto, el ensamblaje de componentes y la logística/envío, todo bajo un mismo techo.

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

Sobre el Manual

Este manual presenta las operaciones de la Serie ProMA.

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

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

Convenciones de documentos

Las convenciones utilizadas en este manual se enumeran a continuación:

Convenciones de GUI

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

simbolos

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

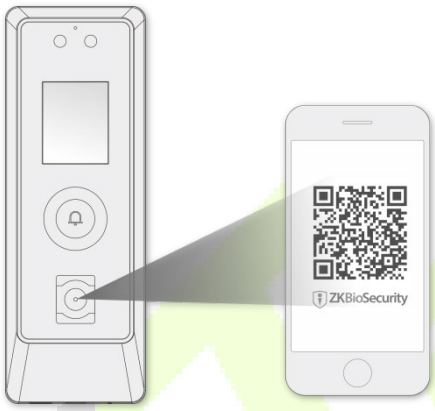
Tabla de contenido

1Instrucciones de uso

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

1.1¿Cómo escanear el código QR?

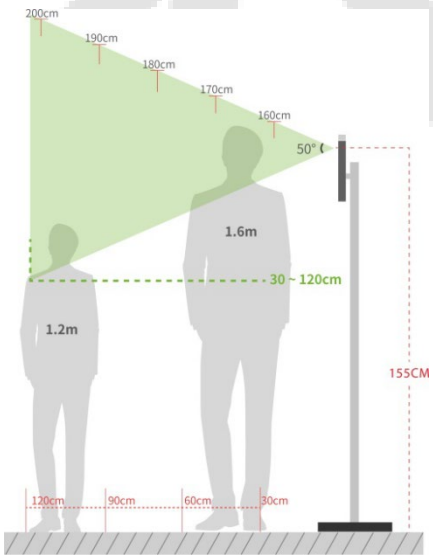
Abra la credencial móvil de la aplicación ZKBioSecurity y coloque la pantalla del teléfono en paralelo con el escáner de código QR del dispositivo.



Nota:Coloque su teléfono a una distancia de 15 a 50 cm del dispositivo (la distancia depende del tamaño de la pantalla del teléfono), no bloquee el escáner de código QR del dispositivo ni el código QR en la pantalla del teléfono.

1.2Posición de pie, postura y expresión facial

-La distancia recomendada



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

-Postura de pie y expresión facial recomendadas

Postura de pie

Expresión facial

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

1.3Registro de palmeras★

Coloque la palma de la mano en el área de recogida de la palma, de modo que la palma quede paralela al dispositivo.

Asegúrate de dejar espacio entre tus dedos.

Nota:

1.Coloque la palma de la mano a una distancia de entre 30 y 50 cm del dispositivo.

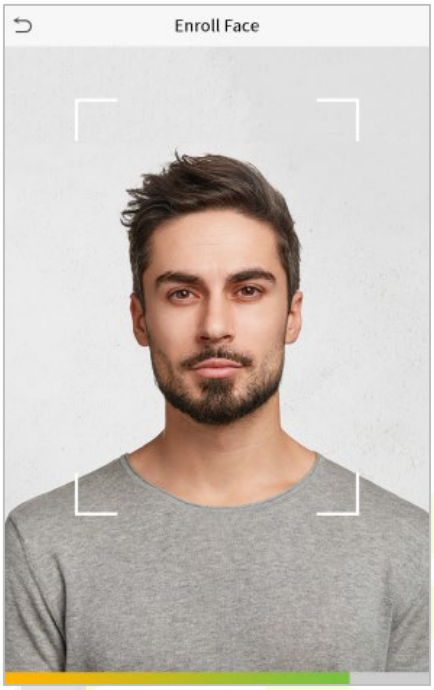
2.Coloque la palma de la mano en el área de recogida de la palma, de modo que la palma quede paralela al dispositivo.

3.Asegúrate de dejar espacio entre tus dedos.

4.Evite la luz solar directa cuando utilice la función Palm al aire libre. Según las pruebas de laboratorio, el efecto de reconocimiento de la palma de la mano es mejor cuando la intensidad de la luz no supera los 10 000 lux.

1.4Registro de rostros

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



Método correcto de registro y autenticación de rostros

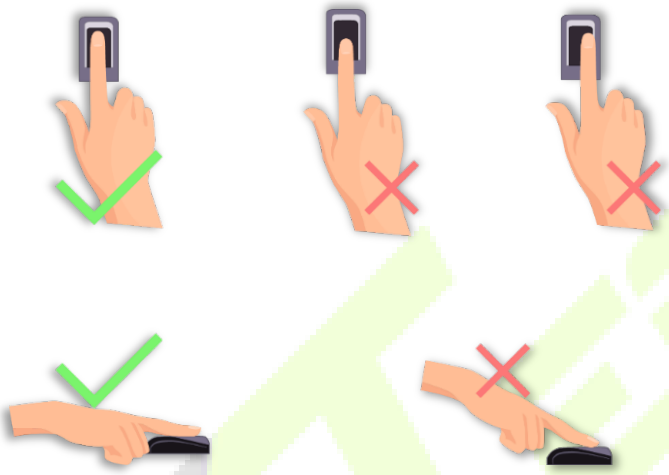
- **Recomendación para registrar una cara**
  - Al registrar una cara, mantenga una distancia de 40 cm a 80 cm entre el dispositivo y la cara.
  - Tenga cuidado de no cambiar su expresión facial. (Cara sonriente, cara demacrada, guiño, etc.)
  - Si no sigue las instrucciones en pantalla, el registro de rostros puede demorar más o fallar.
  - Tenga cuidado de no cubrir los ojos o las cejas. No use
  - sombreros, máscaras, anteojos de sol o anteojos.
  - Tenga cuidado de no mostrar dos caras en la pantalla. Registre una persona a la vez.
  - Se recomienda que un usuario que lleve gafas registre ambas caras con y sin gafas.
- **Recomendación para autenticar un rostro**
  - Asegúrese de que la cara aparezca dentro de la guía que se muestra en la pantalla del dispositivo. Si
  - se han cambiado las gafas, la autenticación puede fallar. Si se ha registrado el rostro sin anteojos, autentique aún más el rostro sin anteojos. Si se ha registrado el rostro con anteojos, autenticar el rostro con los anteojos usados anteriormente.

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

1.5Colocación de los dedos★

Dedos recomendados: dedos índice, medio o anular.

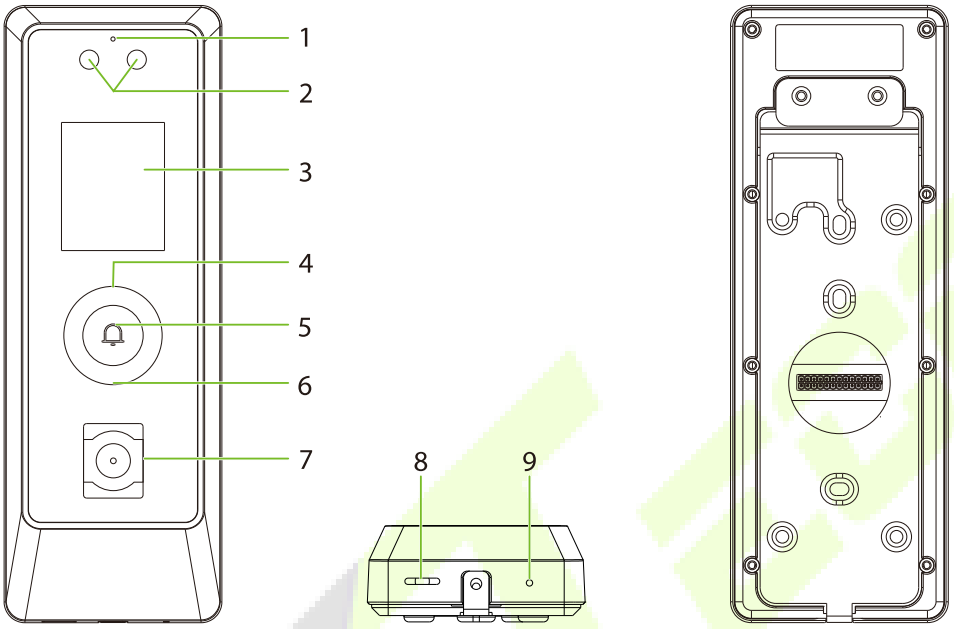
Evite usar el pulgar o el dedo meñique, ya que son difíciles de tocar con precisión en el lector de huellas dactilares.



Nota:Utilice el método correcto cuando presione con los dedos el lector de huellas dactilares para el registro y la identificación.

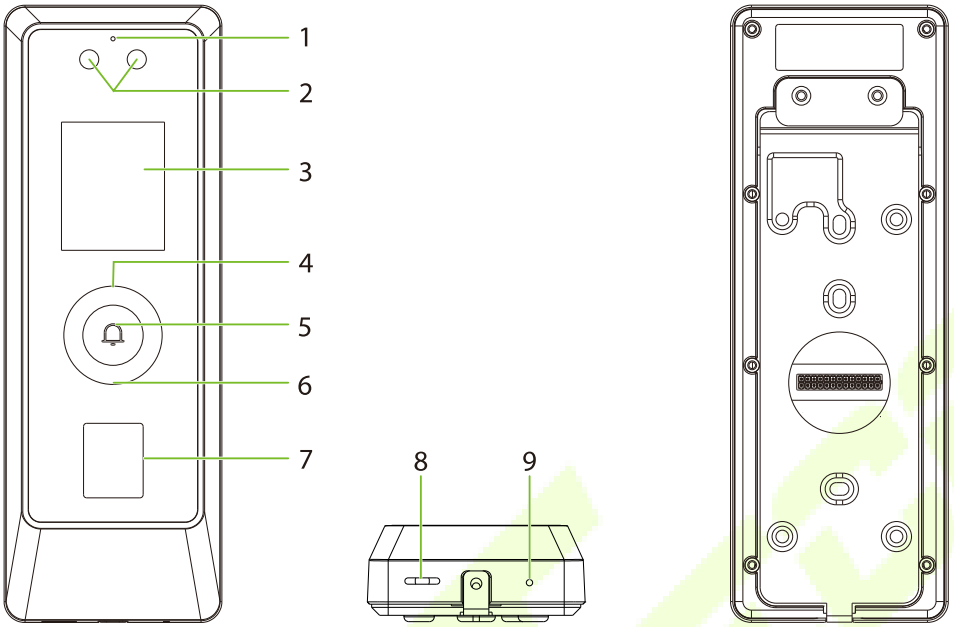
2Apariencia

2.1ProMA-QR



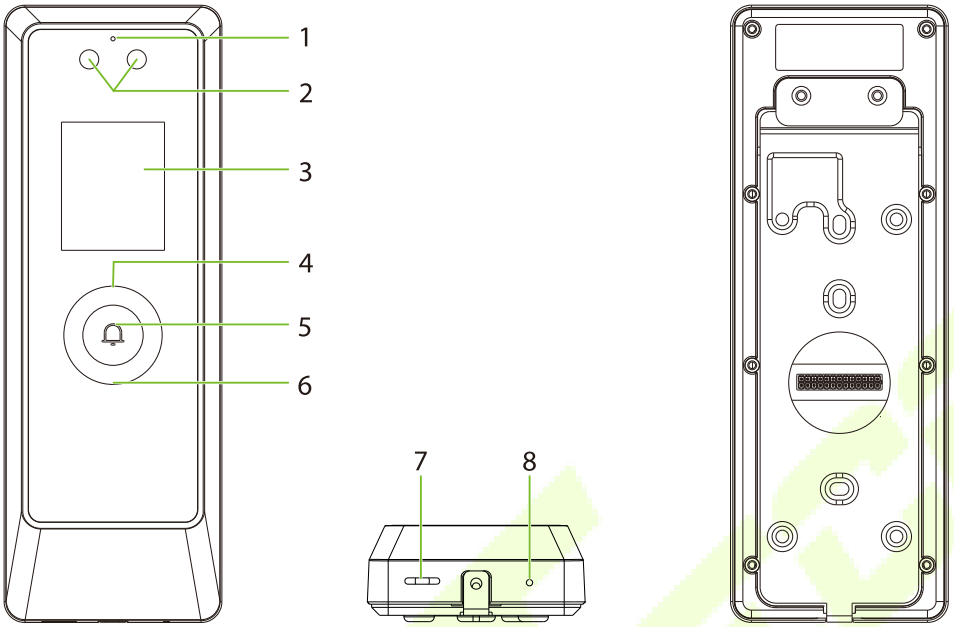
No.	Descripción
1	Micrófono
2	Cámara y Palma
3	Pantalla de visualización de 2"
4	Área de lectura de tarjetas
5	Botón de timbre
6	Destello
7	Escáner de código QR
8	Vocero
9	Reiniciar

2.2ProMA



No.	Descripción
1	Micrófono
2	Cámara y Palma
3	Pantalla de visualización de 2"
4	Área de lectura de tarjetas
5	Botón de timbre
6	Destello
7	Sensor de huellas dactilares
8	Vocero
9	Reiniciar

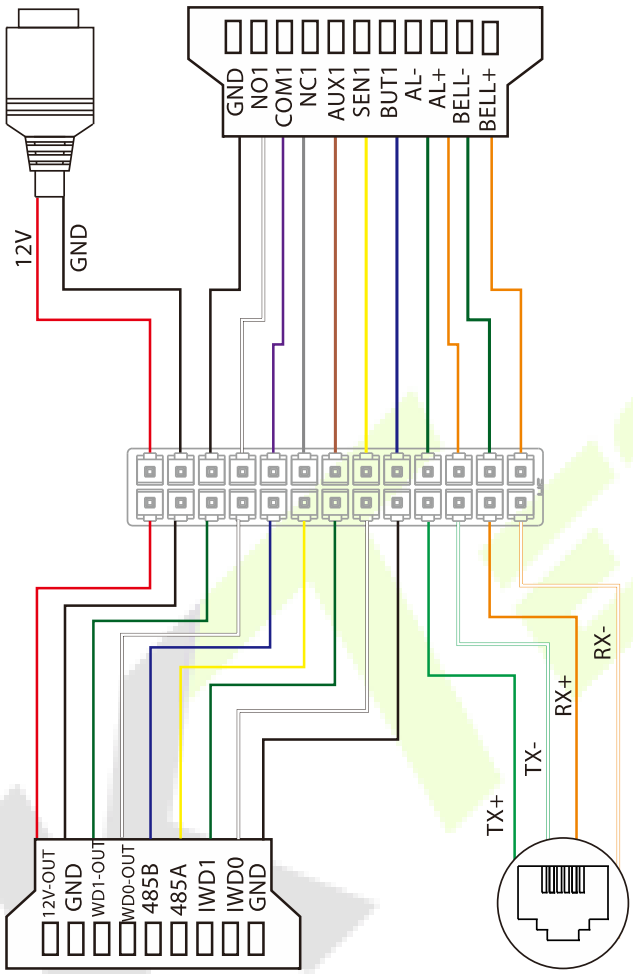
2.3ProMA-RF



No.	Descripción
1	Micrófono
2	Cámara y Palma
3	Pantalla de visualización de 2"
4	Área de lectura de tarjetas
5	Botón de timbre
6	Destello
7	Vocero
8	Reiniciar

2.4Descripción de terminales y cableado

2.4.1Descripción de terminales

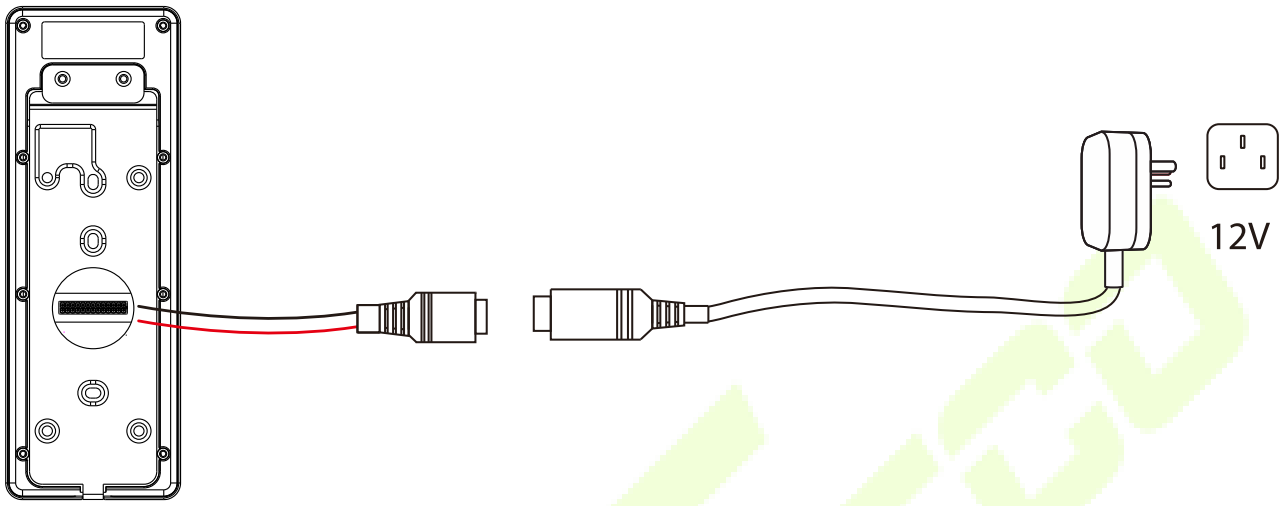


Interfaz	Descripción
12V	Entrada de alimentación de 12 V
TIERRA	
TIERRA	
NO1	Cerrar
COM1	
NC1	

AUX1	Entrada auxiliar
SEN1	Sensor
PERO1	Botón de salida
ALABAMA-	Alarma
AL+	
CAMPANA-	Campana
CAMPANA+	
SALIDA 12V	Sin electricidad
TIERRA	
WD1-SALIDA	Salida Wiegand
WD0-SALIDA	
485B	RS485
485A	
IWD1	Entrada Wiegand
IWD0	
TIERRA	
TX+	Interfaz de red
TX-	
RX+	
RX-	

2.5Descripción del cableado

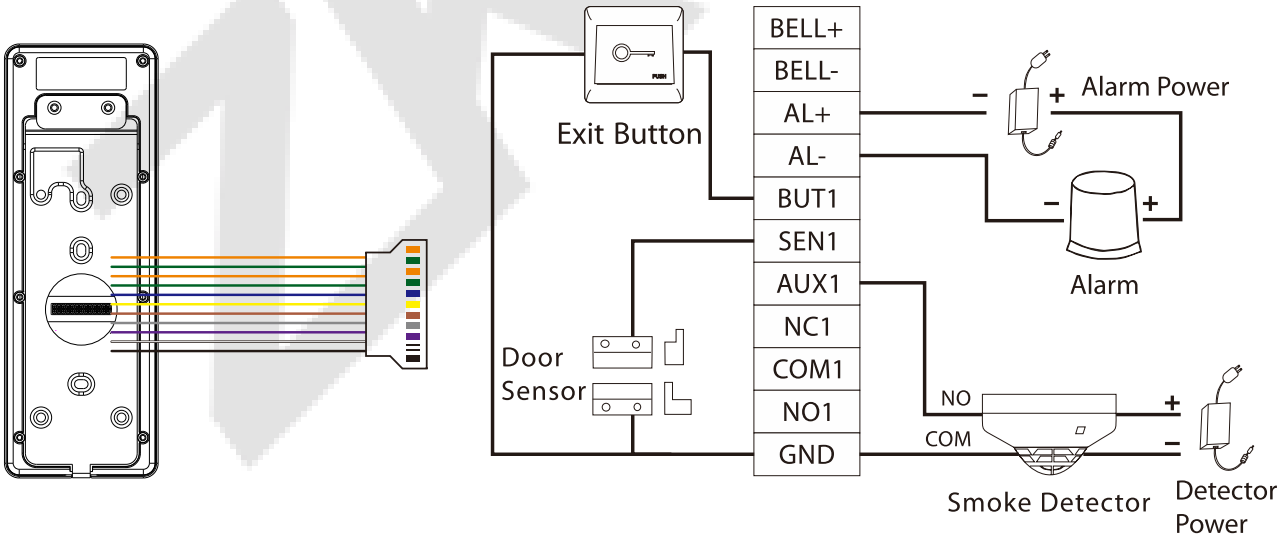
2.5.1Conexión eléctrica



Fuente de alimentación recomendada

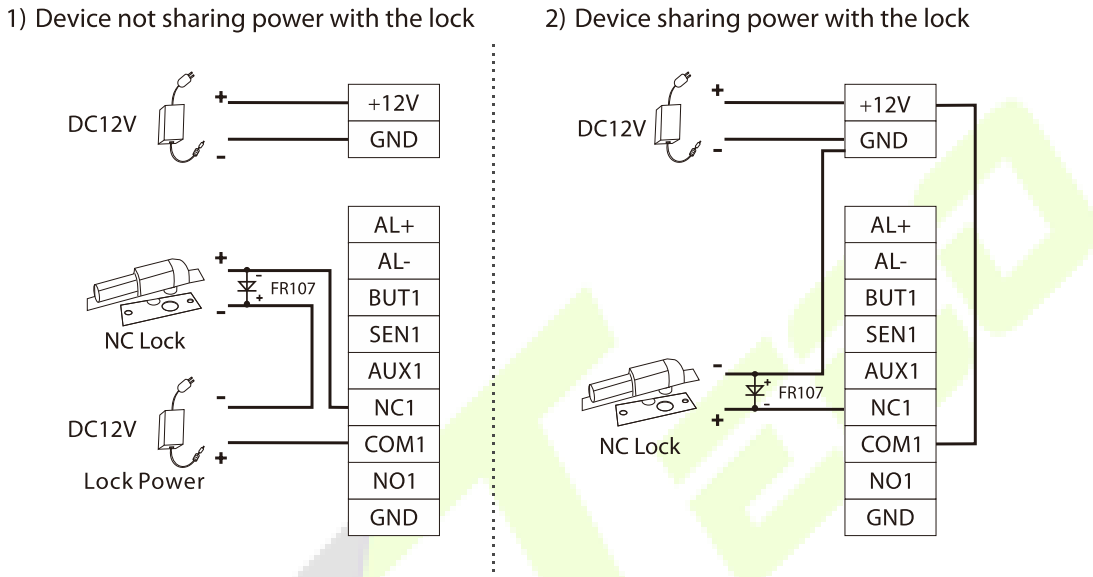
- Clasificación de 12V y 3A
- Para compartir la energía del dispositivo con otros dispositivos, use una fuente de alimentación con clasificaciones de corriente más altas.

2.5.2Sensor de Puerta, Botón de Salida, Alarma y Conexión Auxiliar



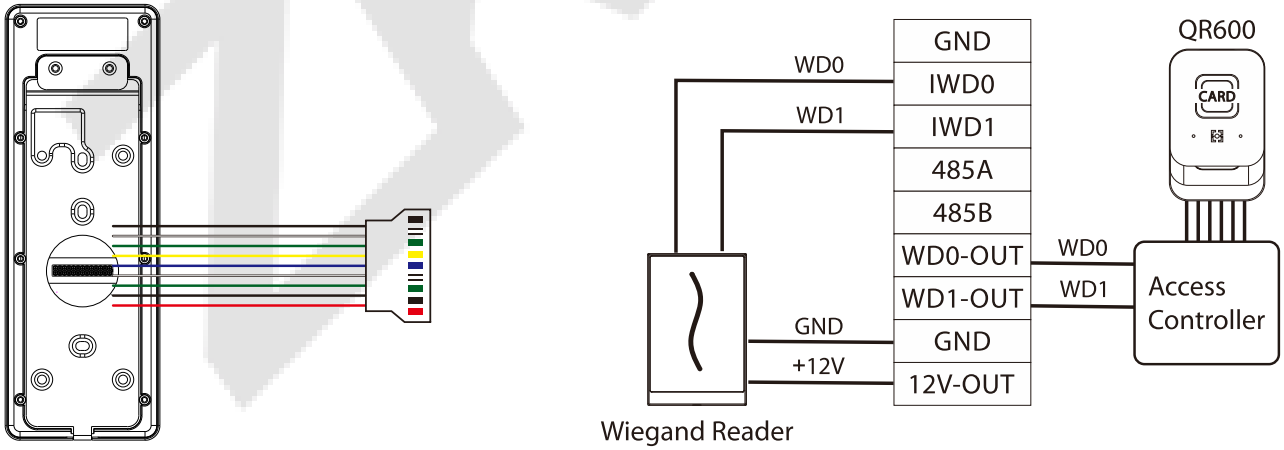
2.5.3Conexión del relé de bloqueo

El sistema admite tanto la cerradura normalmente abierta como la cerradura normalmente cerrada. La cerradura NO (normalmente abierta cuando está encendida) está conectada con los terminales 'NO1' y 'COM1', y la cerradura NC (normalmente cerrada cuando está encendida) está conectada con los terminales 'NC1' y 'COM1'. La energía se puede compartir con la cerradura o se puede usar por separado para la cerradura, como se muestra en el ejemplo con la cerradura NC a continuación:



2.5.4Conexión Wiegand

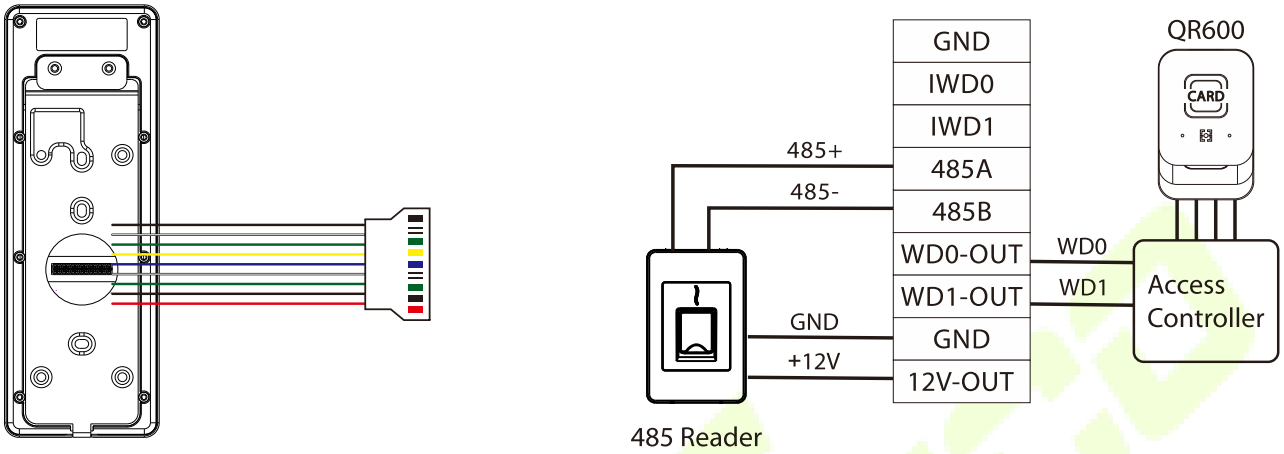
El lector de tarjetas Wiegand se conecta a los 4 pines superiores del terminal Wiegand y los dos últimos pines son utilizados por el controlador de acceso, como se muestra en la siguiente figura. Envía las credenciales al dispositivo a través de comunicación Wiegand.



Nota: El lector QR600 es una función exclusiva de ProMA-QR. Para obtener más información, consulte *Guía de inicio rápido del lector de códigos QR600*.

2.5.5Conexión RS485

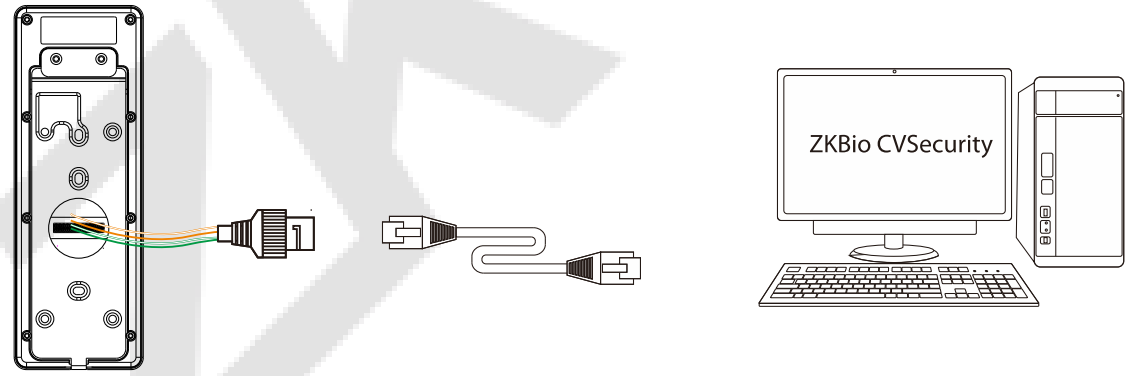
El RS485 permite a los usuarios conectarse a múltiples lectores al dispositivo. RS485 se puede conectar al terminal, como se muestra en la figura a continuación.



Nota: El lector QR600 es una función exclusiva de ProMA-QR. Para obtener más información, consulte *Guía de inicio rápido del lector de códigos QR600*.

2.5.6Conexión Ethernet

Conecte el dispositivo y el software de la computadora a través de un cable Ethernet. A continuación se muestra un ejemplo:



Default IP address: 192.168.1.201
Subnet mask: 255.255.255.0

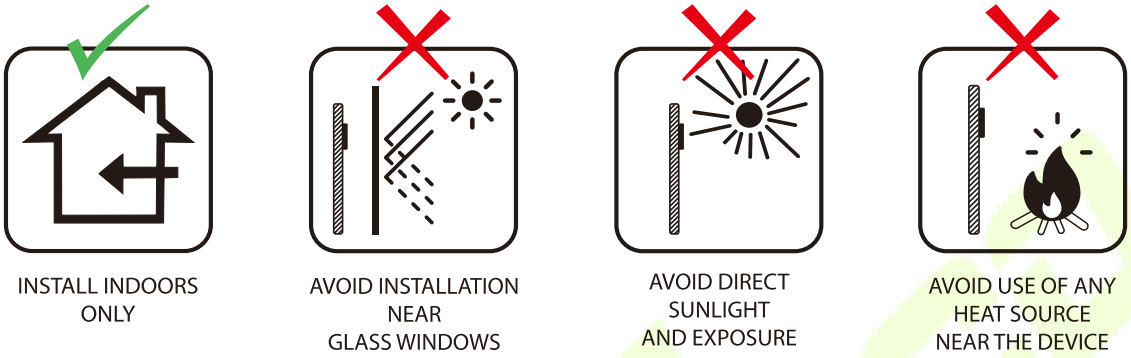
IP address: 192.168.1.130
Subnet mask: 255.255.255.0

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

3Instalación

3.1Entorno de instalación

Consulte las siguientes recomendaciones para la instalación.



3.2Instalación del dispositivo

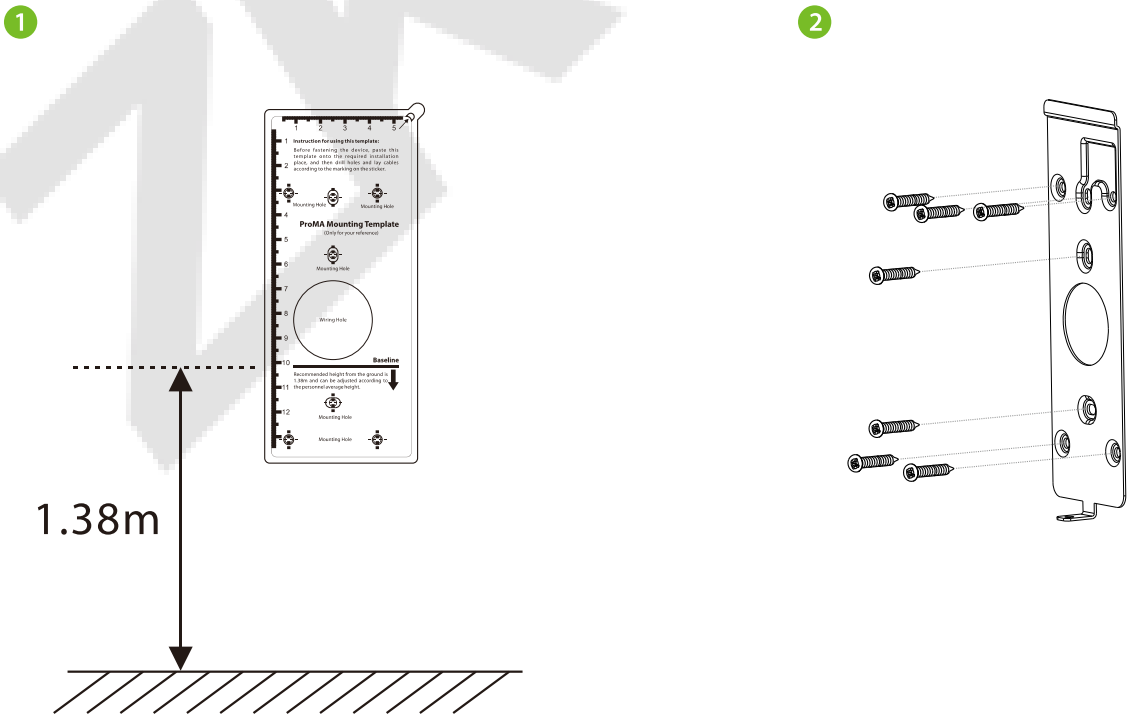
Las instalaciones de la serie ProMA son las mismas, el siguiente es un ejemplo de ProMA.

1.Fije la etiqueta adhesiva de la plantilla de montaje a la pared y taladre los orificios de acuerdo con el papel de montaje.

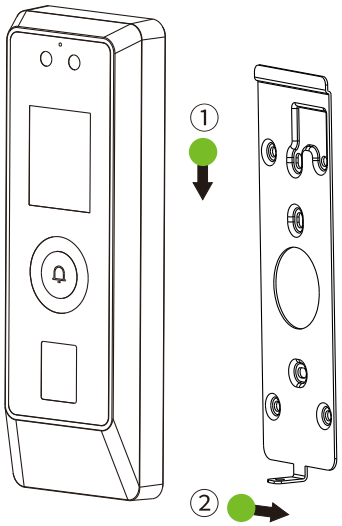
2.Fije la placa posterior a la pared con tornillos de montaje en pared.

3.Fije el dispositivo a la placa posterior.

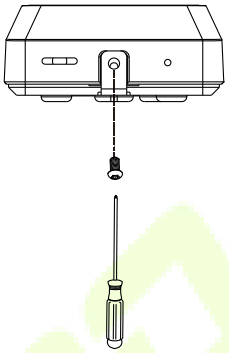
4.Fije el dispositivo a la placa trasera con un tornillo de seguridad.



3

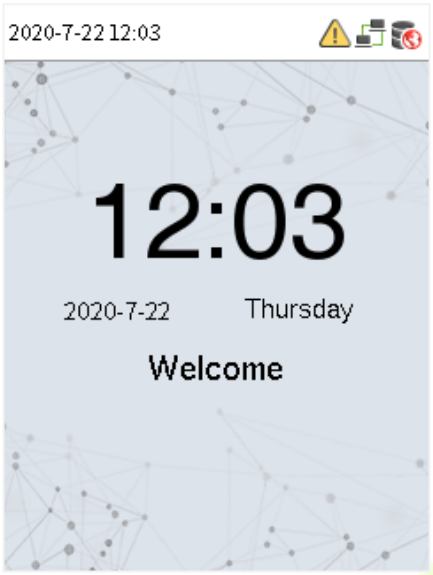


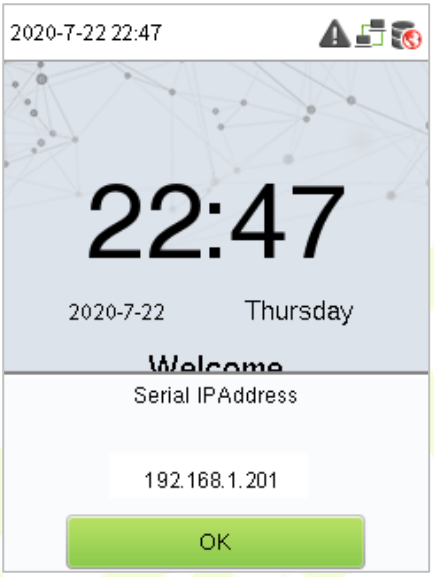
4



4Interfaz de espera

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





El dispositivo tiene una dirección IP integrada, que se puede utilizar para la comunicación del dispositivo, la conexión a WebServer y al software ZKBio CVSecurity, etc.

Nota: El dispositivo utiliza una pantalla de visualización de 2'', que no es compatible con la operación táctil y solo se utiliza para mostrar el estado y la información de verificación. Todas las operaciones, como la información del dispositivo, la configuración de comunicación, la gestión de usuarios y la configuración del sistema, se realizan y configuran en WebServer.

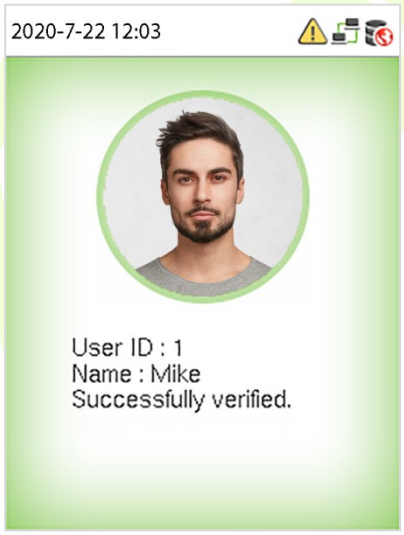
5Modo de verificación

5.1Verificación de código QR★

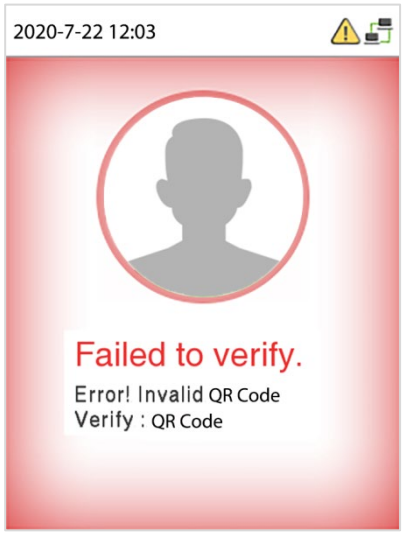
En este modo de verificación, el dispositivo compara la imagen del código QR recopilada por el colector de códigos QR con todos los datos del código QR en el dispositivo.

Grifo [**Credencial móvil**] en la aplicación ZKBioSecurity, y aparecerá un código QR, que incluye información de identificación del empleado y número de tarjeta (el código QR estático solo incluye el número de tarjeta). El código QR puede reemplazar una tarjeta física en un dispositivo específico para lograr la autenticación sin contacto. Por favor refiérase aCredencial móvil ★.

Verificado con éxito:



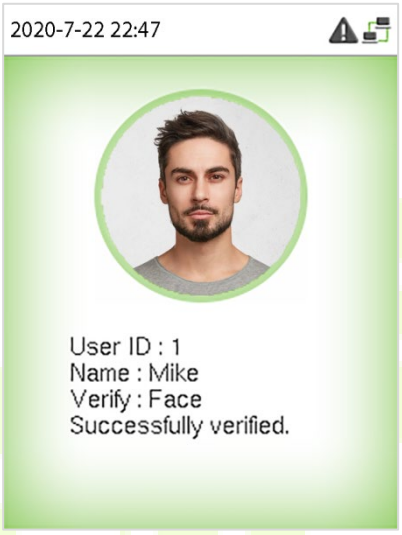
Error al verificar:



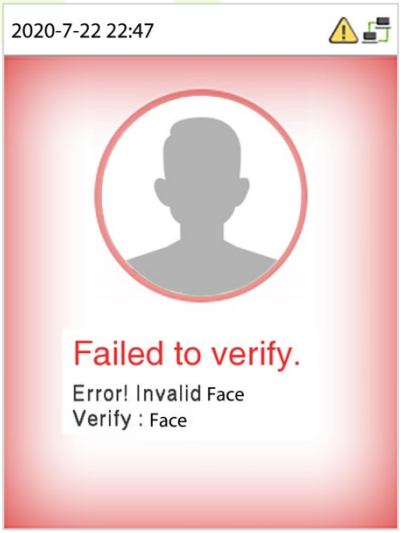
5.2Verificación facial

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

Verificado con éxito:



Error al verificar:

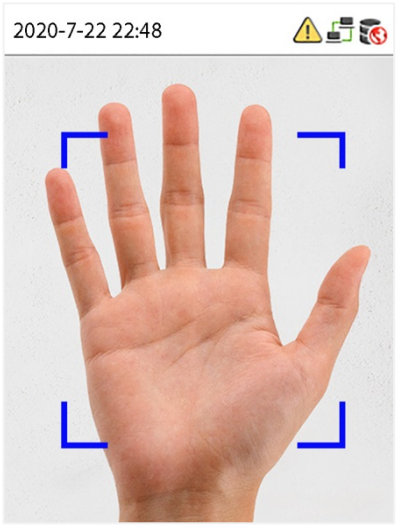


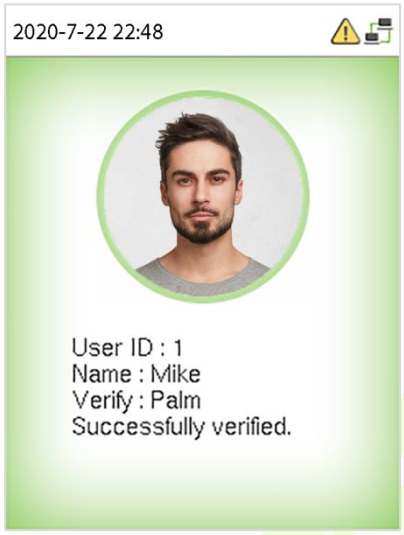
5.3Verificación de palma★

Este modo de verificación compara la imagen de la palma recopilada por el módulo de la palma con toda la plantilla de datos de la palma en el dispositivo.

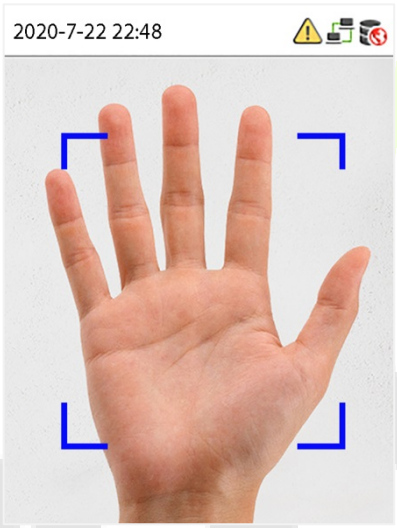
El dispositivo distinguirá automáticamente entre el modo de verificación de la palma y la cara. Coloque la palma de la mano en el área que puede recoger el módulo de la palma, de modo que el dispositivo cambie automáticamente al modo de verificación de la palma.

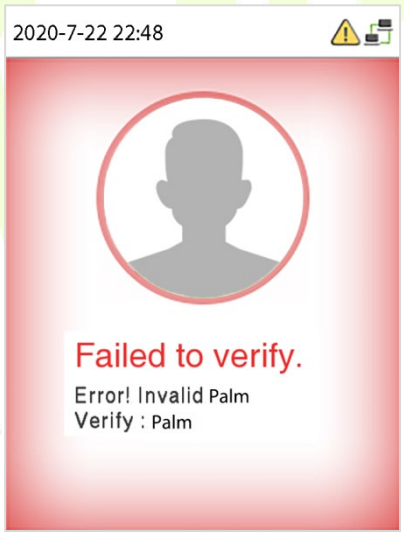
Verificado con éxito:





Error al verificar:



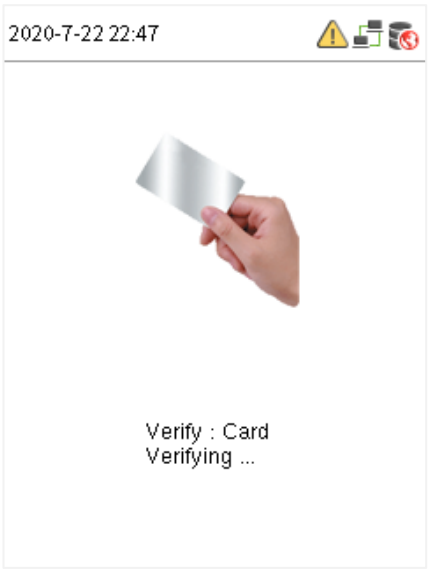


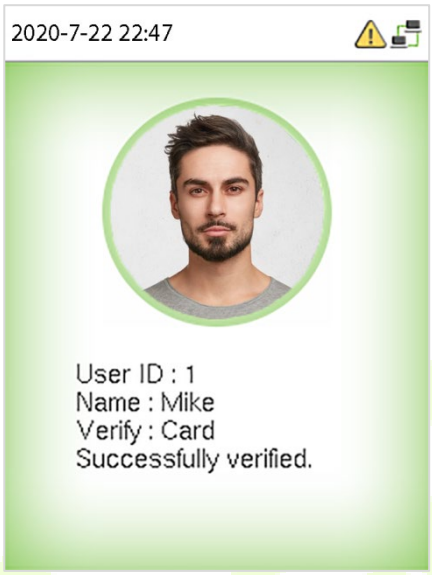
Nota: El reconocimiento de palma requiere la configuración de una cámara especial.

5.4 Verificación de tarjeta

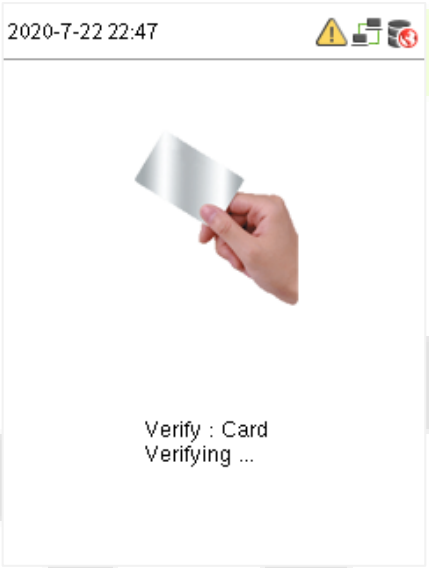
El modo de verificación de tarjeta compara el número de tarjeta en el área de inducción de tarjeta con todos los datos de número de tarjeta registrados en el dispositivo; La siguiente es la pantalla de verificación de la tarjeta.

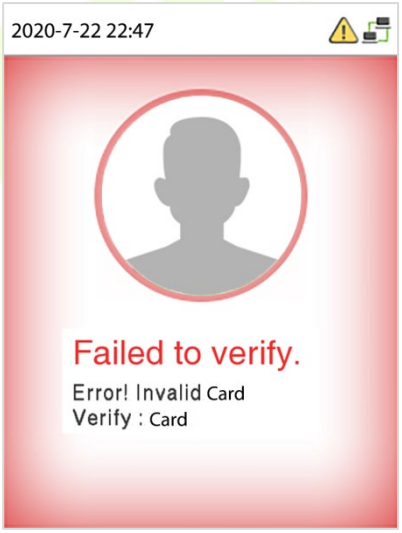
Verificado con éxito:





Error al verificar:





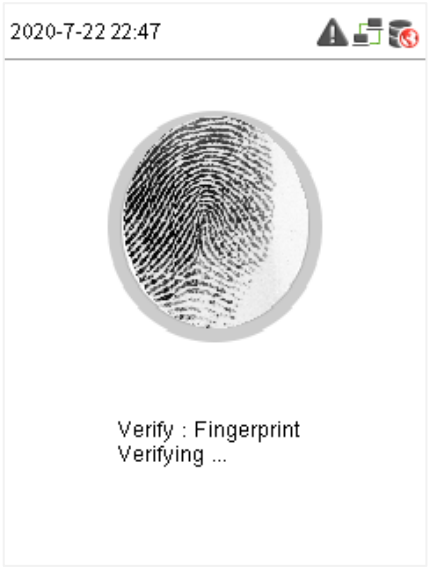
Nota: El ProMA-QR admite códigos ID PDF417 de Chile y Argentina.

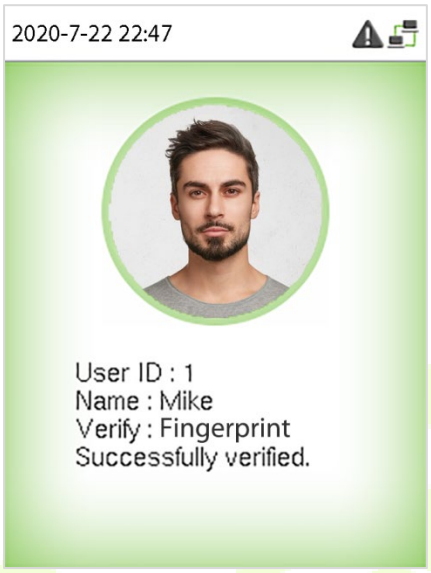
5.5 Verificación de huellas dactilares★

Este método compara la huella dactilar del usuario que se presiona en el lector de huellas dactilares con todos los datos de huellas dactilares prealmacenados en el dispositivo.

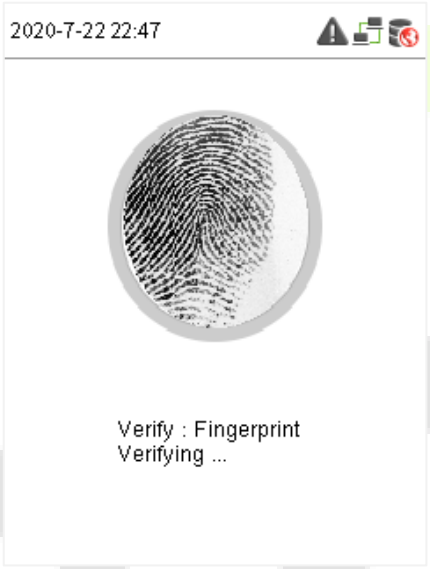
Para ingresar al modo de identificación de huellas dactilares, simplemente toque con el dedo el lector de huellas dactilares.

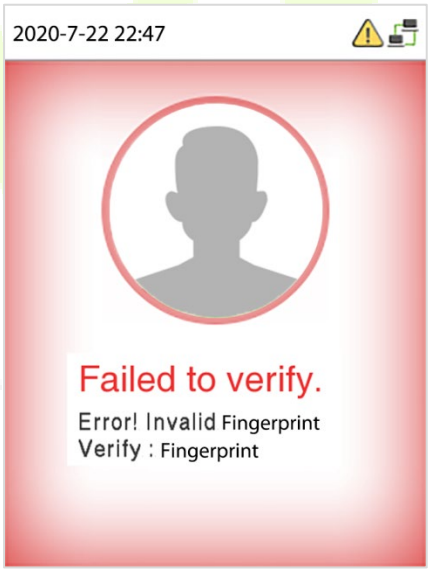
Verificado con éxito:





Error al verificar:

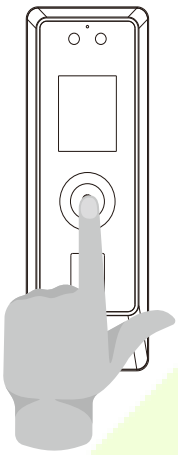




6Iniciar sesión en el servidor web

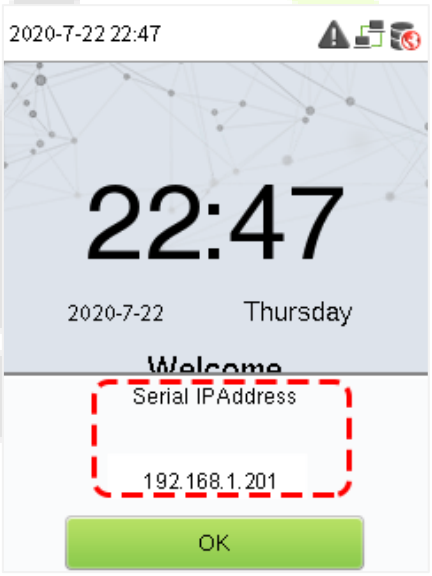
Un usuario puede abrir la aplicación web para configurar los parámetros relevantes del dispositivo.

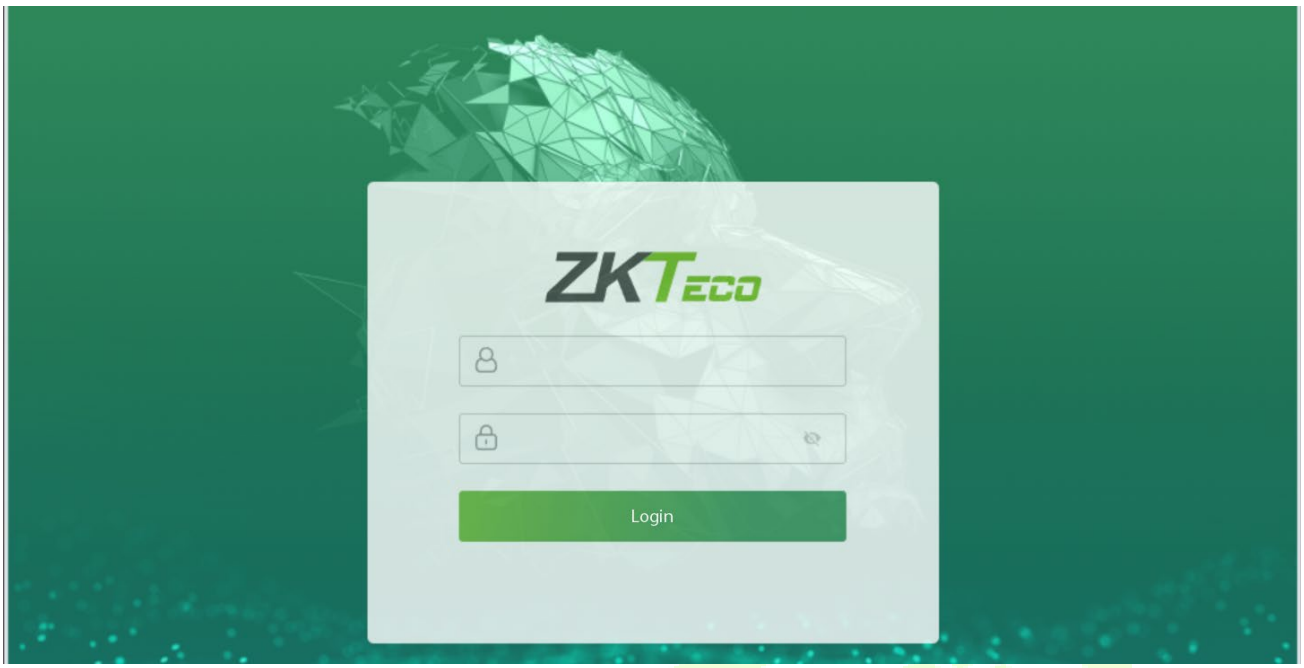
1.Mantenga presionado el botón del timbre del dispositivo hasta que aparezca la IP.



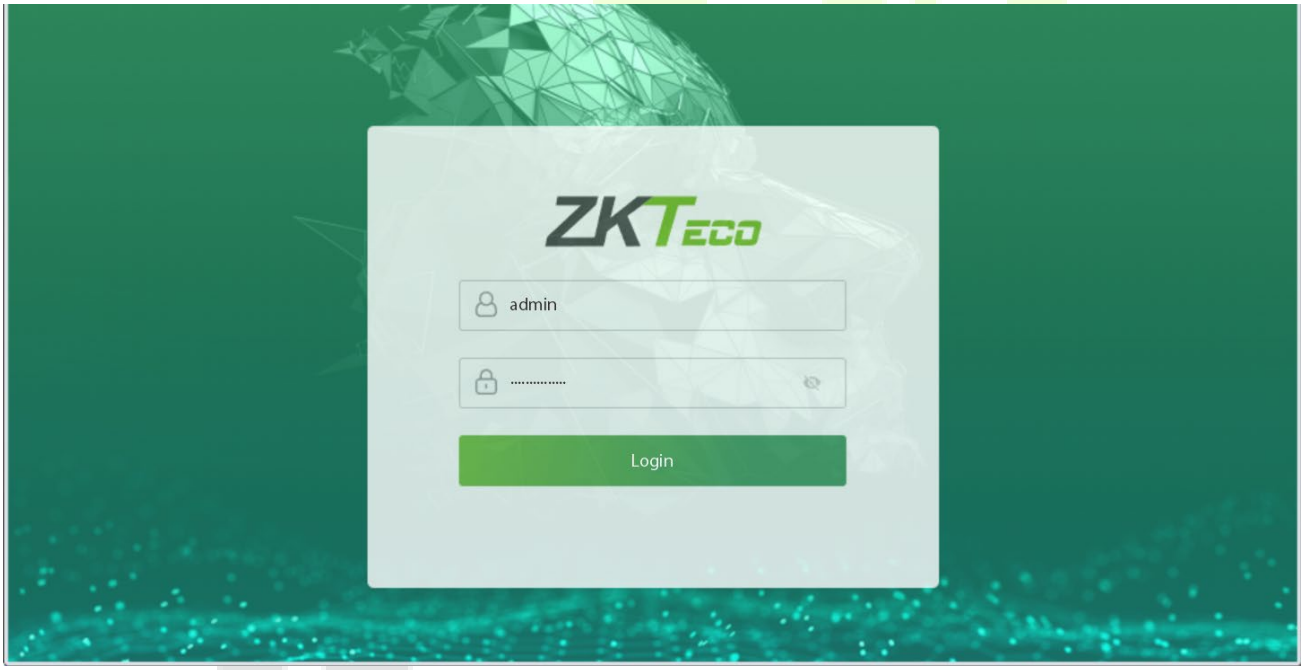
2.Abra un navegador para ingresar la dirección para iniciar sesión en el WebServer, la dirección es**https:// Dirección IP serie: 1443** . Por ejemplo:**https://192.168.1.201:1443.**

Nota:La dirección IP serie del dispositivo para la comunicación se puede modificar; para obtener más información, consulteConfiguración de comunicación .





3.Ingrese la cuenta y la contraseña del WebServer, la cuenta predeterminada es:**administración**, contraseña:**administrador@123**.



Nota:

1.Después de iniciar sesión por primera vez, los usuarios deben cambiar su contraseña original e iniciar sesión nuevamente antes de poder usarla, consulteCambiar la contraseña .

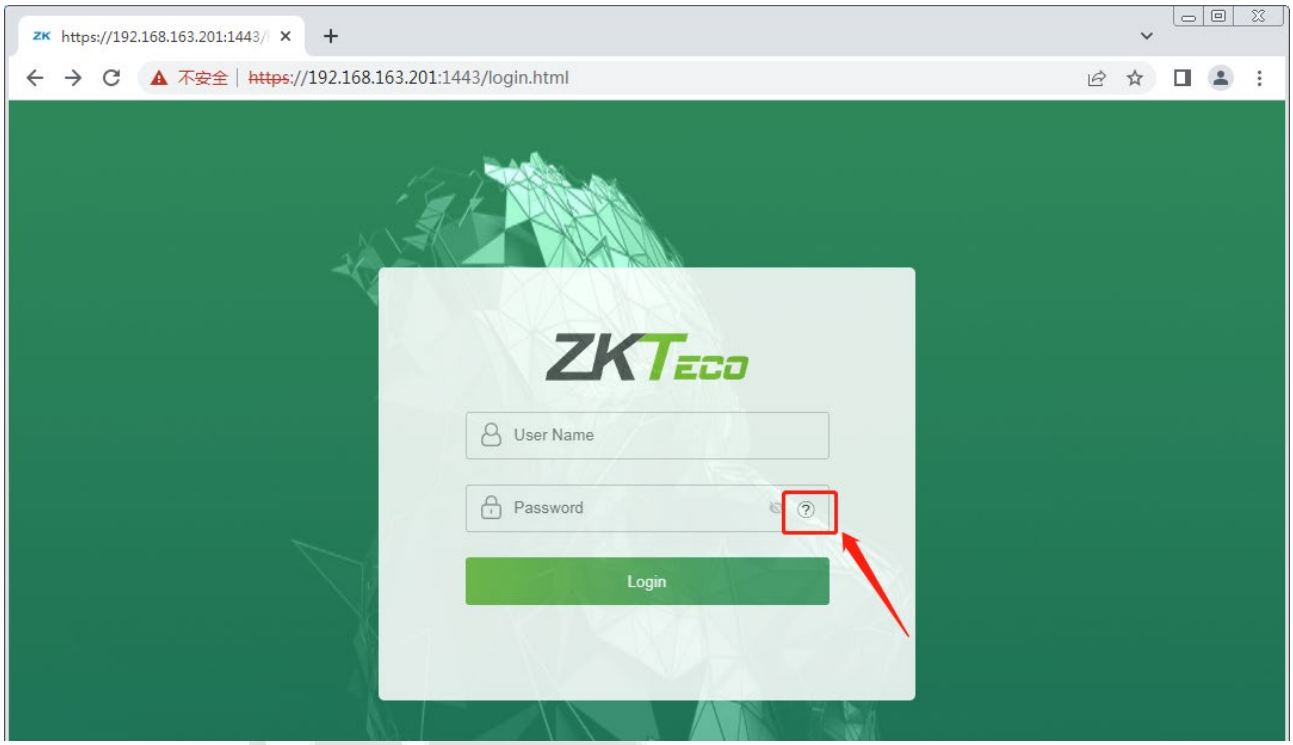
2.Para recuperar la contraseña fácilmente, primero registre un superadministrador, consulte8.1 Registro de Usuario .

7Has olvidado tu contraseña

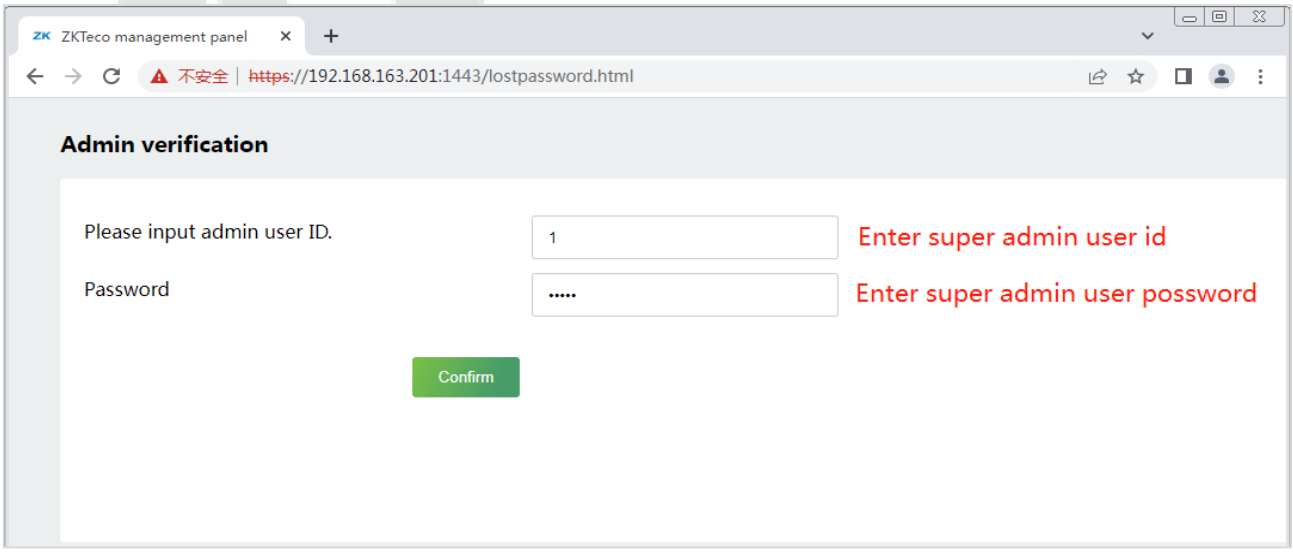
-Método 1 (cuando hay un superadministrador):

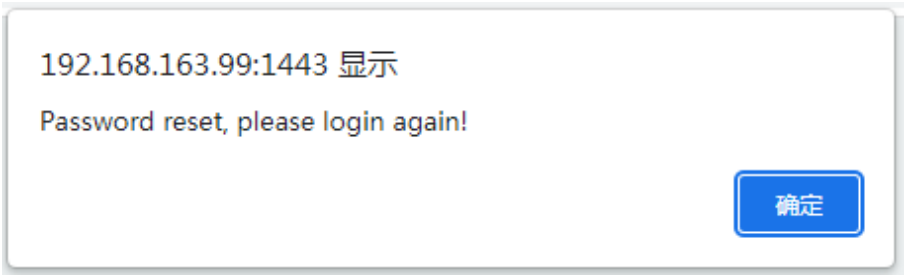
Si olvidó la contraseña de WebServer, puede restablecerla por el registradosúper administrador . Los pasos detallados son los siguientes:

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

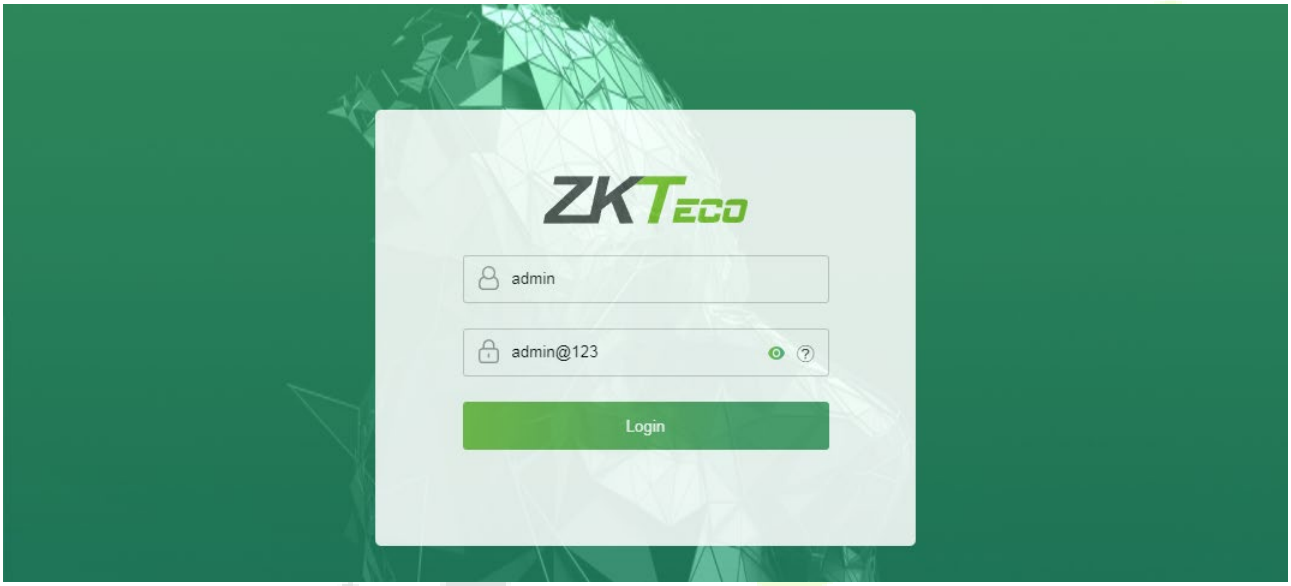


2.En la página emergente, ingrese la información relevante del usuario superadministrador cuando se le solicite.

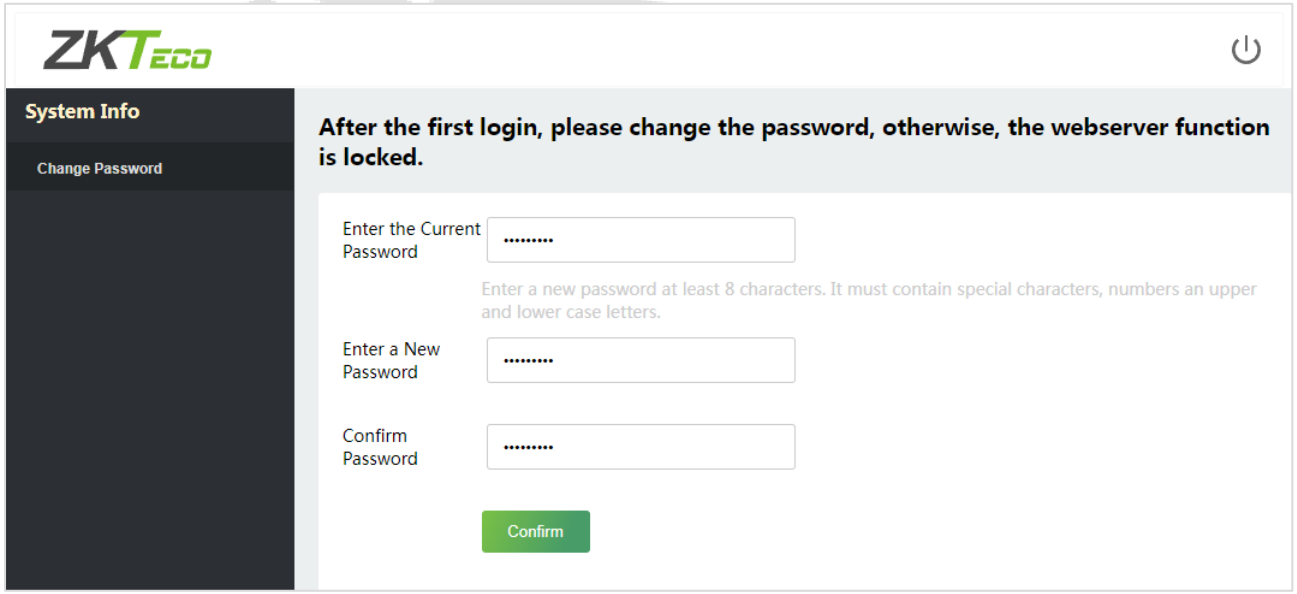




3.Después de un restablecimiento exitoso, ingrese la cuenta y la contraseña predeterminadas (cuenta:**administración**, contraseña: **administrador@123**) en la interfaz de inicio de sesión para iniciar sesión.



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

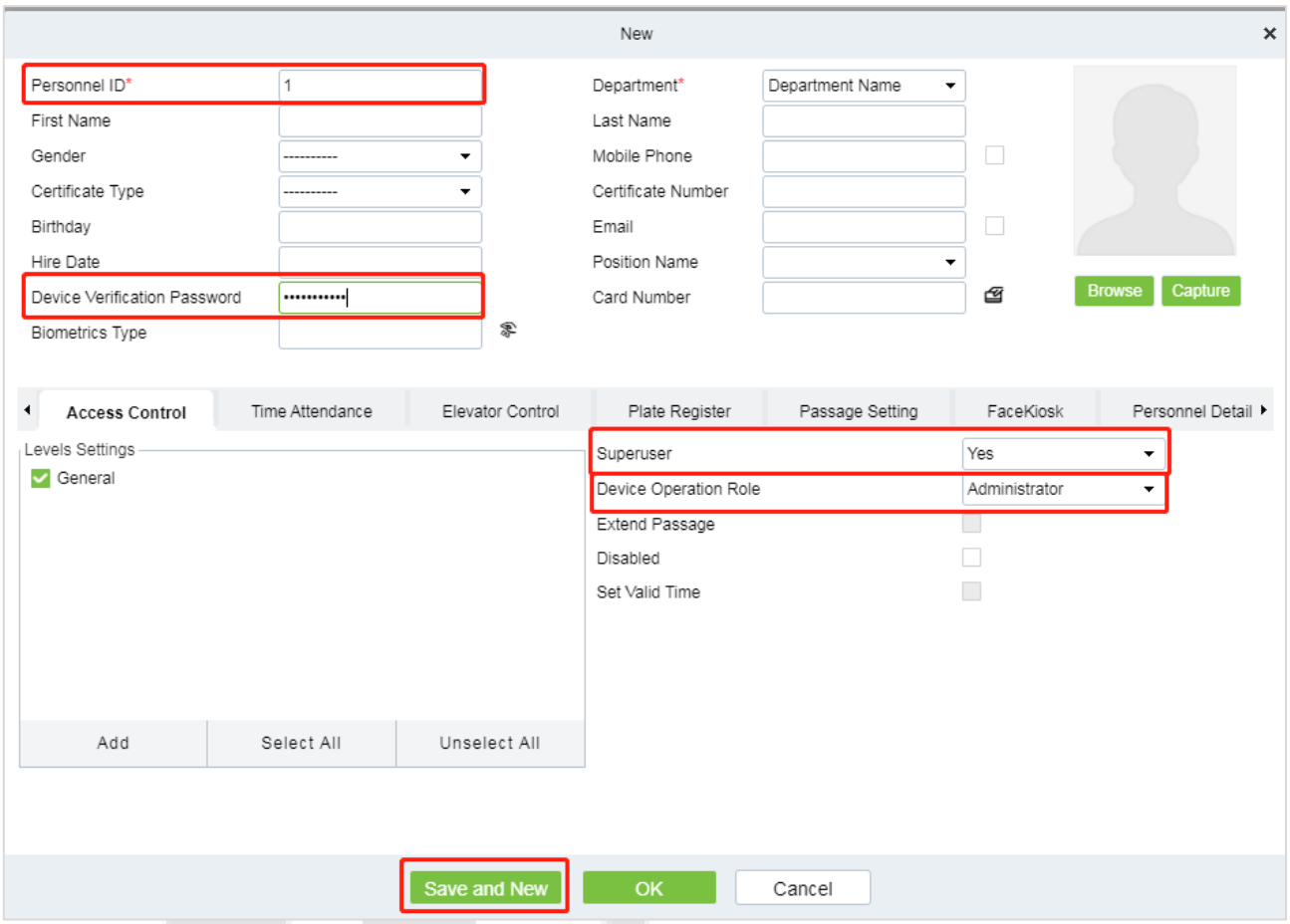


Nota:El superadministrador debe existir.

-Método 2 (cuando no hay un superadministrador):

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

1.Hacer clic**Personal**>**Persona**>**Nuevo**en el servidor ZKBio CVSecurity.



2.Después de registrar la información del superadministrador, haga clic en**Guardar y Nuevo**.

3.Hacer clic**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*Manual de usuario de ZKBio CVSecurity V6600*.

4.Después de que la sincronización de datos sea exitosa, puede restablecer la contraseña con el superadministrador recién registrado. Los pasos de la operación 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.

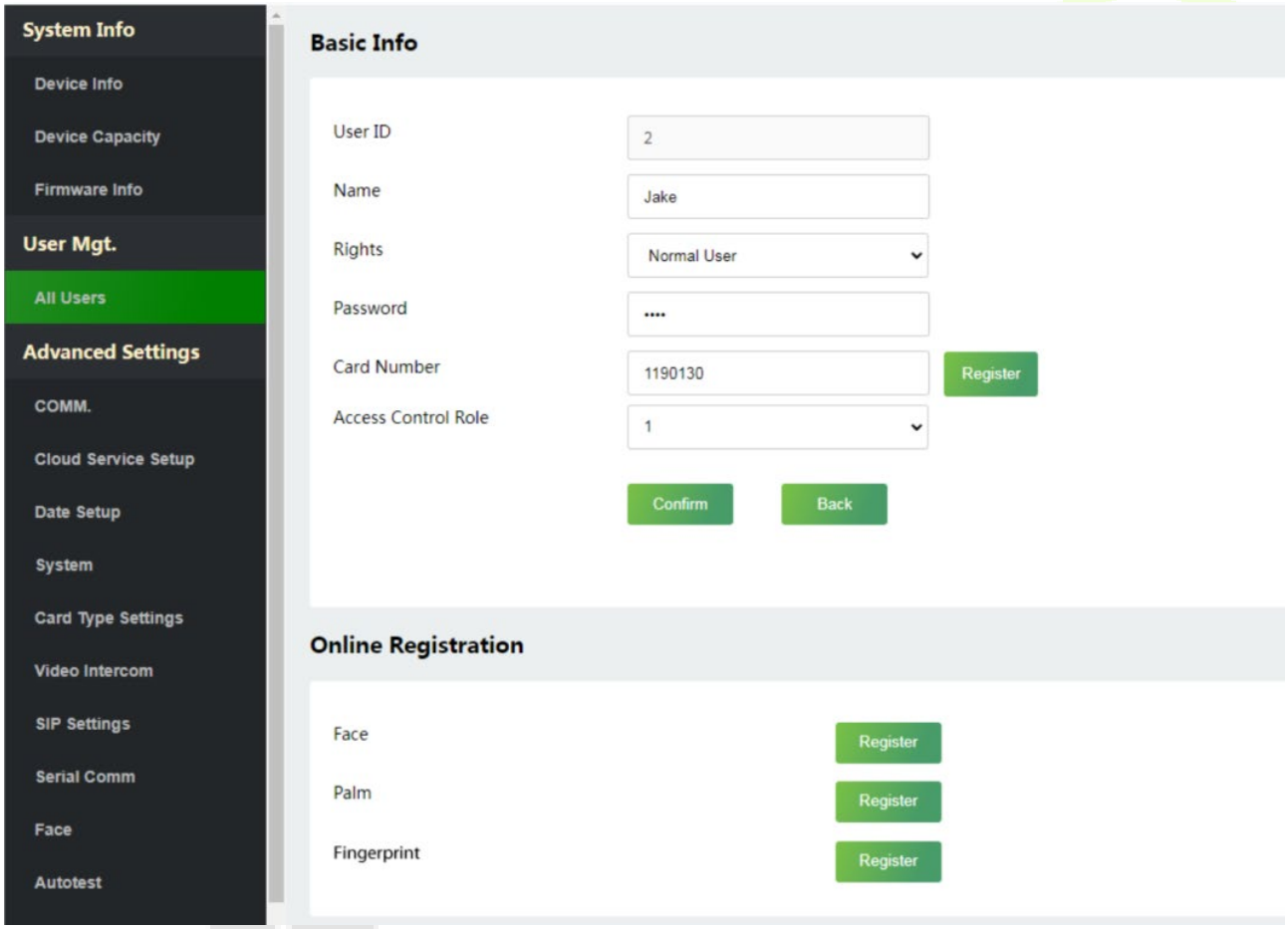
8Gestión de usuarios

8.1registro de usuario

8.1.1Información básica

Hacer clic**Todos los usuarios**en el servidor web.

En esta interfaz, puede registrar la identificación de usuario, el nombre, los derechos, la contraseña, el número de tarjeta y el rol de control de acceso del nuevo usuario, haga clic en**Confirmar**ahorrar.



Nombre de la función	Descripción
ID de usuario	El ID de usuario puede contener de 1 a 14 caracteres de forma predeterminada. Pueden ser números, letras, símbolos, etc.
Nombre	Un nombre puede tener hasta 63 caracteres.

Derechos	Establezca la función del usuario como Usuario normal o Superadministrador. - **Superadministrador:**El superadministrador posee 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 los privilegios para administrar el sistema y solo podrán acceder a las verificaciones de autenticación.
Contraseña	Establecer la contraseña de registro del usuario.
Número de tarjeta	Ingrese el número de tarjeta manualmente, después de registrar el número de tarjeta del usuario, el usuario puede deslizar la tarjeta para verificar. O detrás del número de tarjeta, haga clic en **Registro**, y el dispositivo mostrará la interfaz de registro de la tarjeta en tiempo real, deslice la tarjeta debajo del área de lectura de la tarjeta. El registro de la tarjeta será exitoso. ***Nota:***El ProMA-QR admite códigos de identificación PDF417 de Chile y Argentina, así como un lector esclavo QR600.
Función 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 agregarán al Grupo 1 de forma predeterminada, que se pueden reasignar a otros grupos requeridos. El sistema admite hasta 10 grupos de control de acceso.

Nota:

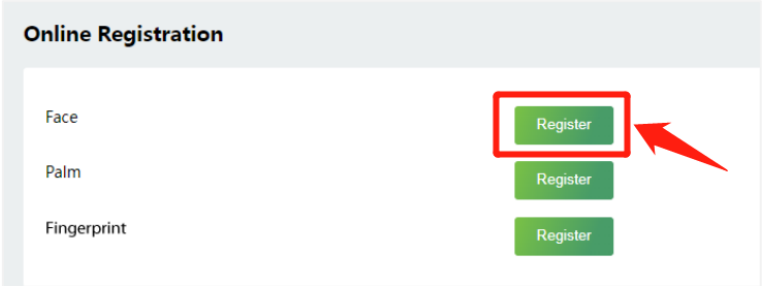
1. Durante el registro inicial, puede modificar su ID; no puede modificar la identificación registrada una vez después del registro exitoso.
2. si el mensaje**"¡La configuración falló!"**aparece, debe elegir una ID de usuario diferente porque la que ingresó ya existe.

8.1.2Registro en línea

En esta interfaz, puede registrar la cara del usuario, Palm★y huella dactilar★.El modo de verificación solo se puede registrar después de confirmar la información básica.

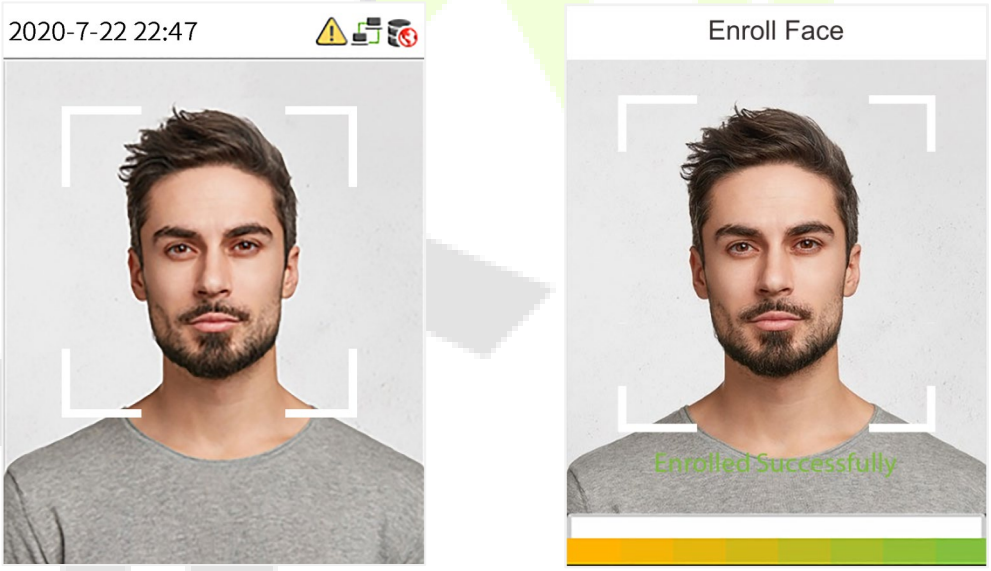
- **Registrar Cara**

En la interfaz actual, detrás de la barra frontal, haga clic en**Registro**y el dispositivo mostrará la interfaz de registro de rostros en tiempo real.



- Mire hacia la cámara y coloque su rostro dentro del cuadro guía blanco y quédese quieto durante el registro del rostro.
- Aparece una barra de progreso mientras se registra la cara y "**Inscrito con éxito**" se muestra hasta que se completa el registro.
- Si la cara ya está registrada entonces, el "**Cara duplicada**Aparece el mensaje ".

La interfaz de registro es la siguiente:



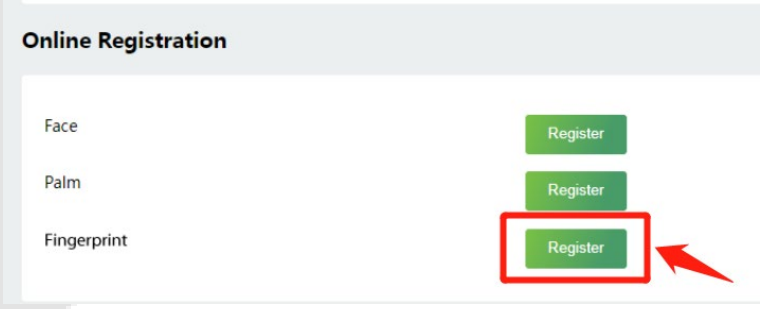
Nota:Al registrar una cara, el sistema captura automáticamente una imagen como foto de perfil. Si usted no registre una foto de perfil, el sistema establece automáticamente la imagen capturada durante el registro como la foto predeterminada.

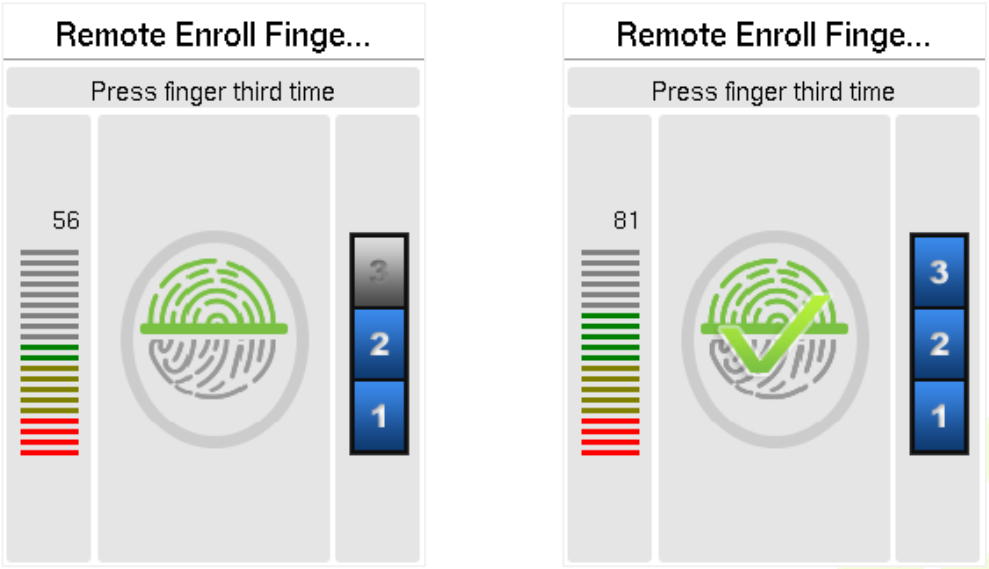
- **Registro Palma** ★

En la interfaz actual, detrás de la barra de palma, haga clic en**Registro**, y el dispositivo mostrará la interfaz de registro de palma en tiempo real.

- **Registrar Huella Dactilar ★**

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

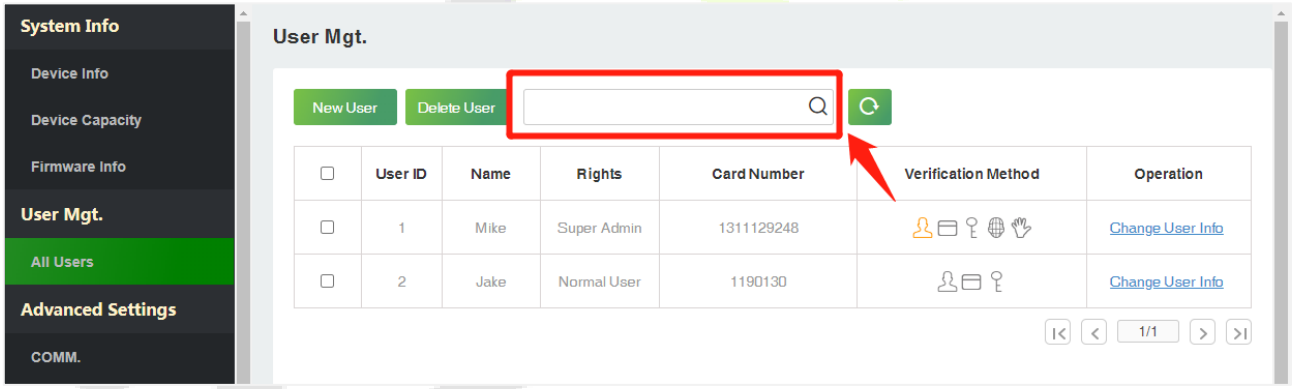




Para la operación de prensado de huellas dactilares, consulteColocación de los dedos .

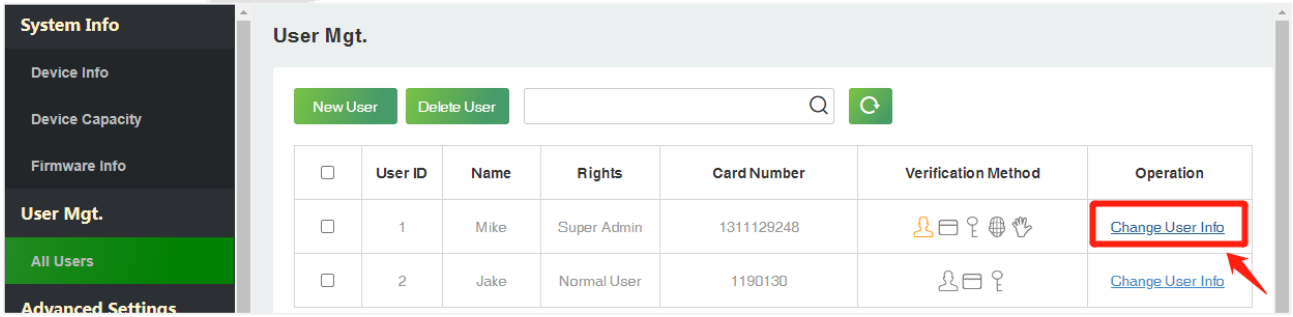
8.2Buscar usuarios

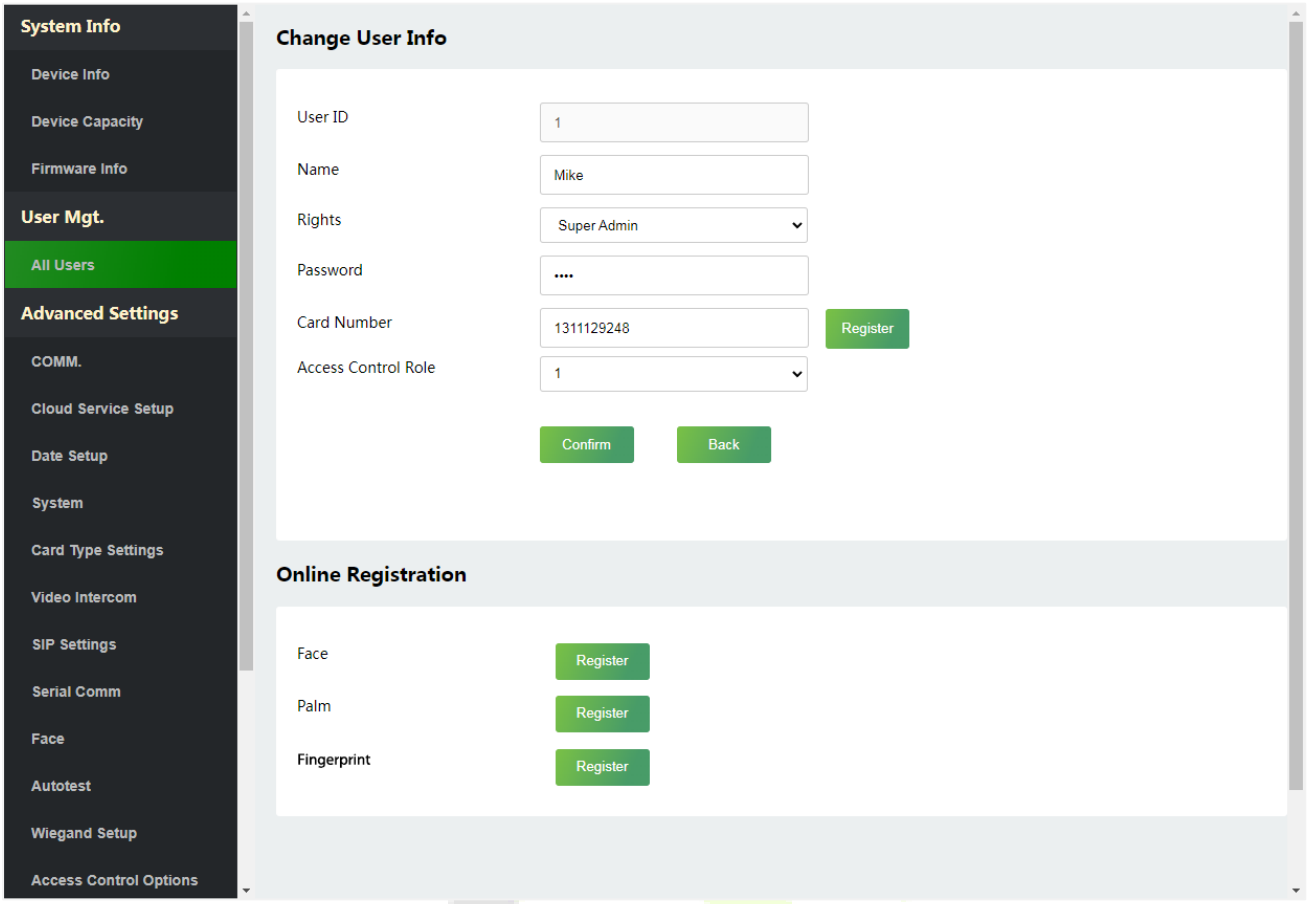
Hacer clic**Todos los usuarios**en el WebServer, haga clic en la barra de búsqueda para ingresar la palabra clave de recuperación requerida (donde la palabra clave puede ser la identificación del usuario, el apellido o el nombre completo) y el sistema buscará la información del usuario relacionada.



8.3editar usuario

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

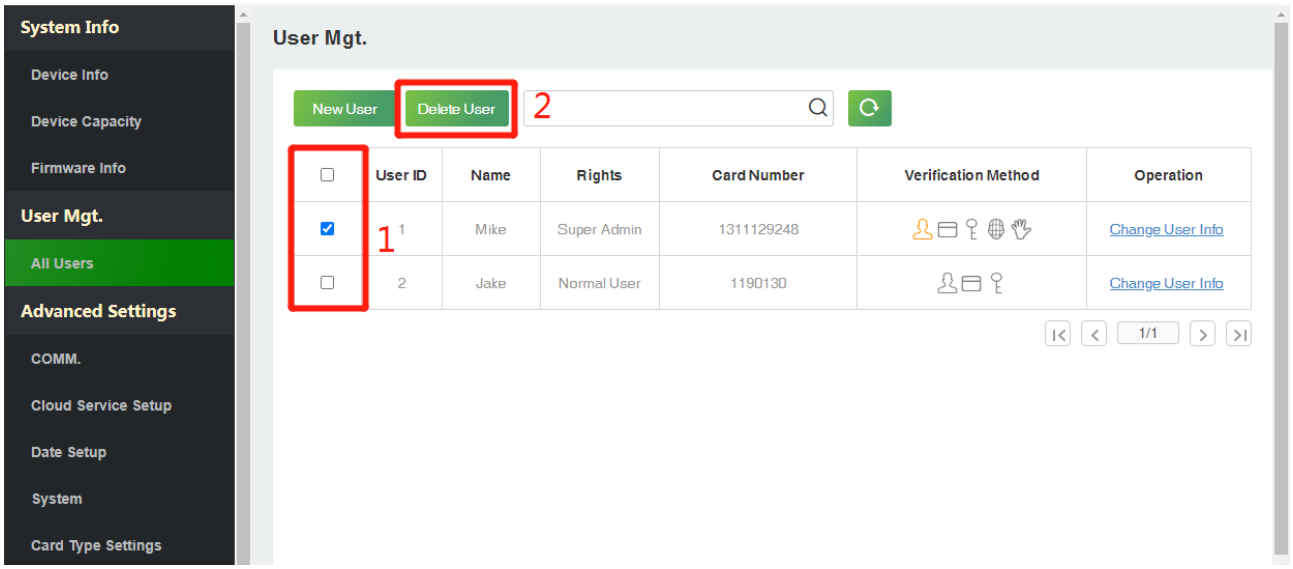




Nota:El proceso de editar la información del usuario es el mismo que el de agregar un nuevo usuario, excepto que la identificación del usuario no se puede modificar. El proceso en detalle se refiere a8.1 Registro de Usuario .

8.4Borrar usuario

Sobre el**Todos los usuarios**interfaz, seleccione el usuario requerido de la lista y haga clic en**Borrar usuario**para eliminar el usuario. Aquí está disponible la eliminación individual y la eliminación por lotes.

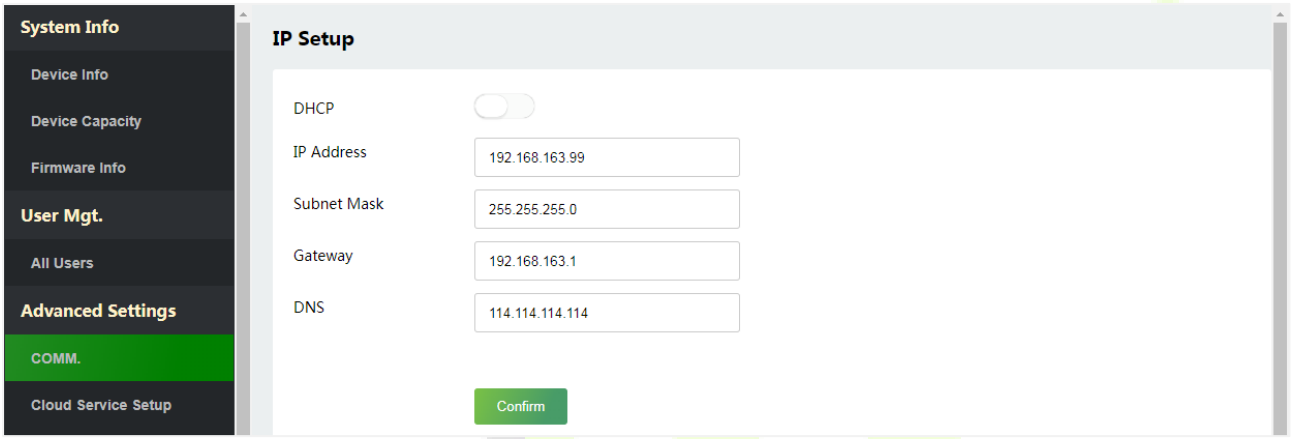


9Ajustes avanzados

9.1Configuración de comunicación

Hacer clic**COM.**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 de IP.



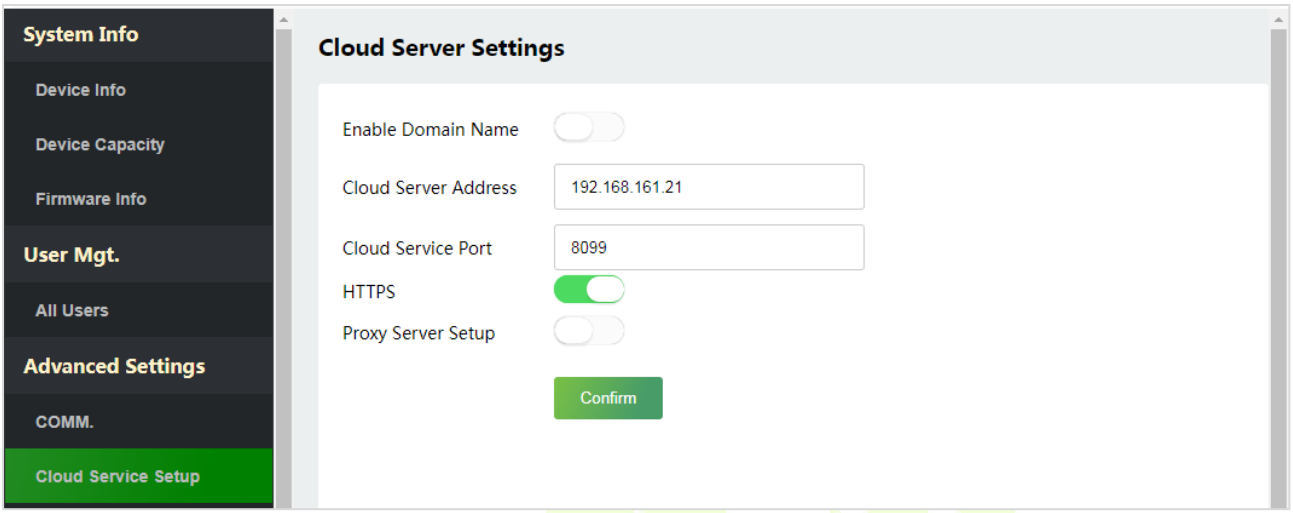
Nombre de la función	Descripción
DHCP	Seleccione si desea obtener la dirección IP automáticamente.
Dirección IP	La dirección IP predeterminada es 192.168.1.201. Se puede modificar según la disponibilidad de la red.
Máscara de subred	La máscara de subred predeterminada es 255.255.255.0. Se puede modificar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

Nota:Después de que la dirección IP del dispositivo se cambie con éxito, debe cerrar sesión en el actual WebServer e inicie sesión nuevamente con la dirección IP que acaba de cambiar para conectarse al dispositivo. Para conocer los detalles de inicio de sesión del servidor web, consulteIniciar sesión en el servidor web .

9.2Configuración del servidor en la nube

Hacer clic**Configuración del servicio en la nube**en el servidor web.

Se usó la configuración del servidor en la nube para conectarse al software ZKBio CVSecurity, consulte12.1 Establecer la dirección de comunicación .



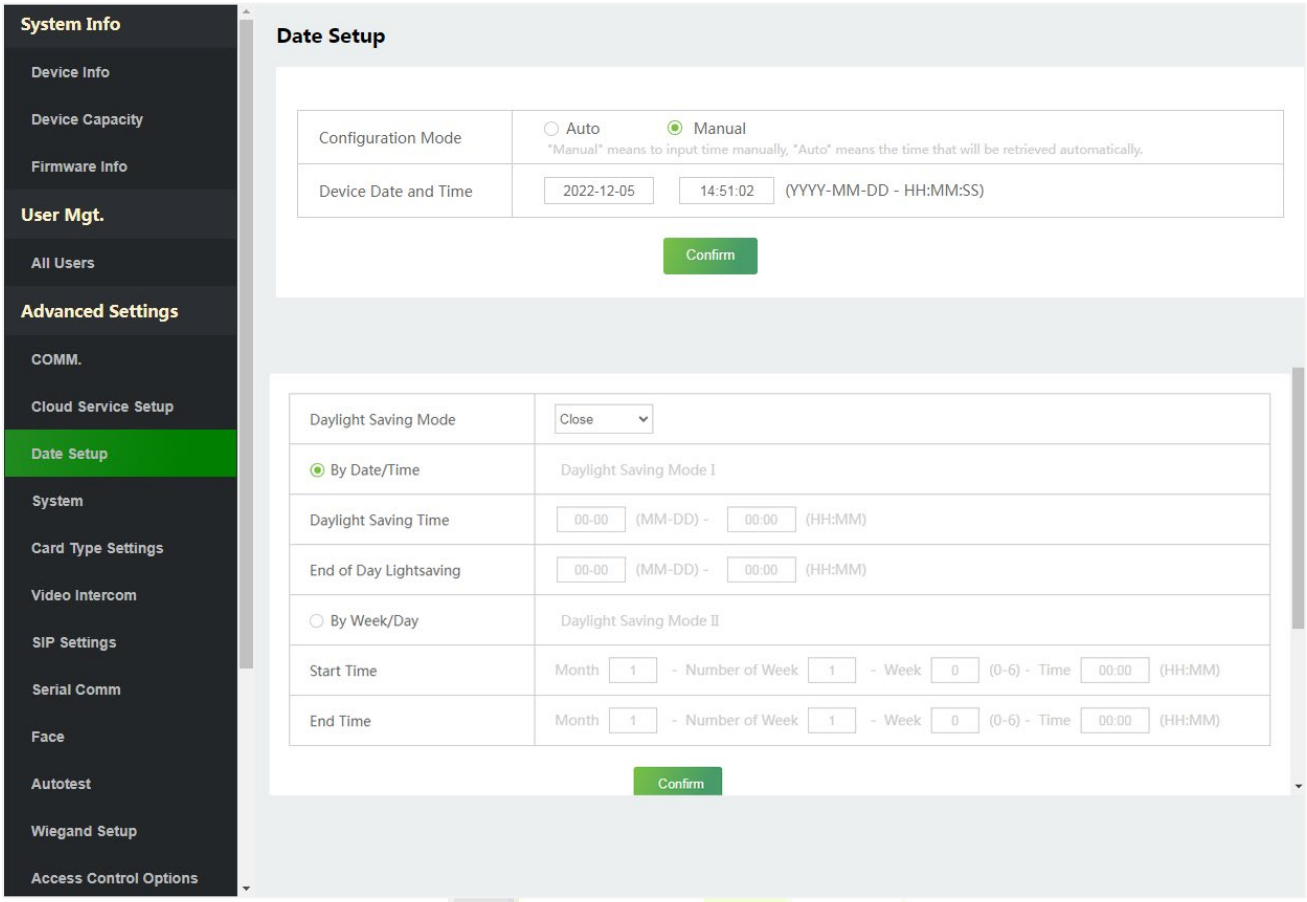
Nombre de la función		Descripción
Permitir Dominio Nombre	**Dirección del servidor**	Una vez que esta función está habilitada, se utilizará el modo de nombre de dominio “http://...”, como http://www.XYZ.com, mientras que “XYZ” denota el nombre de dominio (cuando este modo está activado).**EN**).
Desactivar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

9.3Configuración de fecha

Hacer clic**Configuración de fecha**en el servidor web.

-Hacer clic**Manual**para establecer manualmente la fecha y la hora y haga clic en**Confirmar**ahorrar.

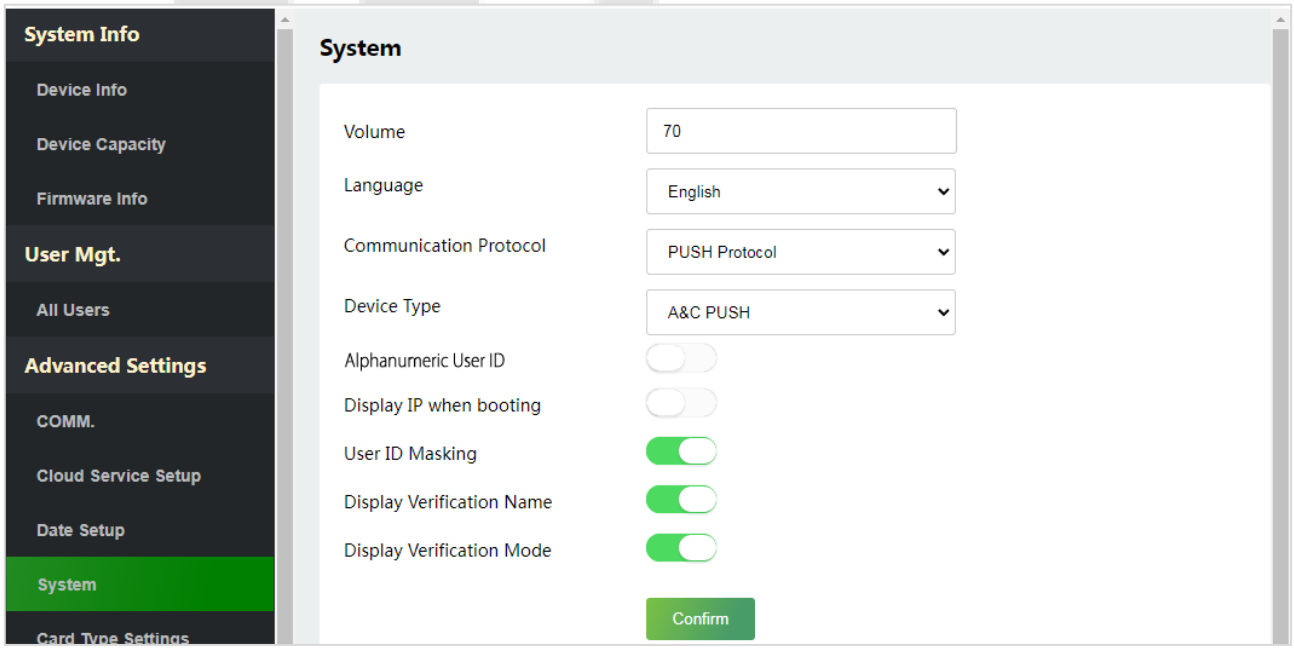
- Seleccione Abrir o Cerrar el**Modo de ahorro de luz diurna**función. Si está abierto, configure el**Horario de verano** y **Fin del horario de verano**.



9.4Ajustes del sistema

Hacer clic**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 se puede establecer entre 0 y 100.
Idioma	Seleccione el idioma del WebServer y del dispositivo.
Comunicación Protocolo	Establecer el protocolo de comunicación del dispositivo
Tipo de dispositivo	Configure el dispositivo como terminal de control de acceso o terminal de asistencia. ***Nota:*** Después de cambiar el tipo de dispositivo, el dispositivo eliminará todos los datos y se reiniciará, y algunas funciones se ajustarán en consecuencia.
Usuario alfanumérico IDENTIFICACIÓN	Habilitar/Deshabilitar el alfanumérico como ID de Usuario.
Mostrar IP cuando arrancando	Habilita/deshabilita la función de mostrar IP al arrancar.
Enmascaramiento de ID de usuario	Cuando está habilitado, y luego el usuario se compara y verifica con éxito, la ID de usuario en el resultado de verificación que se muestra se reemplazará con un * para lograr una protección segura de los datos privados confidenciales.
Verificación de pantalla Nombre	Establezca si mostrar el nombre de usuario en la interfaz de resultados de verificación.
Verificación de pantalla Modo	Establezca si desea mostrar el modo de verificación en la interfaz de resultados de verificación.

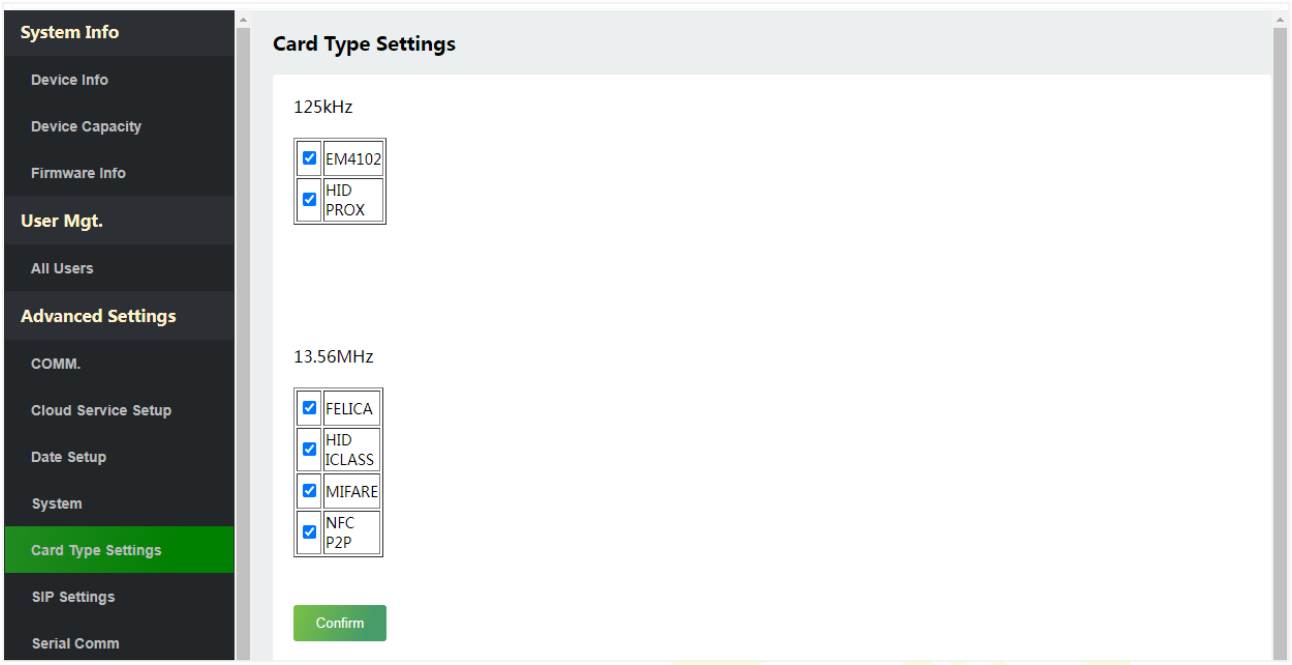
Nota:

1. Después de seleccionar el idioma y hacer clic en **Confirmar**, el dispositivo se reiniciará automáticamente y mostrará el idioma modificado.
2. Entonces WebServer no mostrará el idioma cambiado hasta que el dispositivo se reinicie y vuelva a iniciar sesión.

9.5 Configuración del tipo de tarjeta

Hacer clic **Configuración del tipo de tarjeta** en el servidor web.

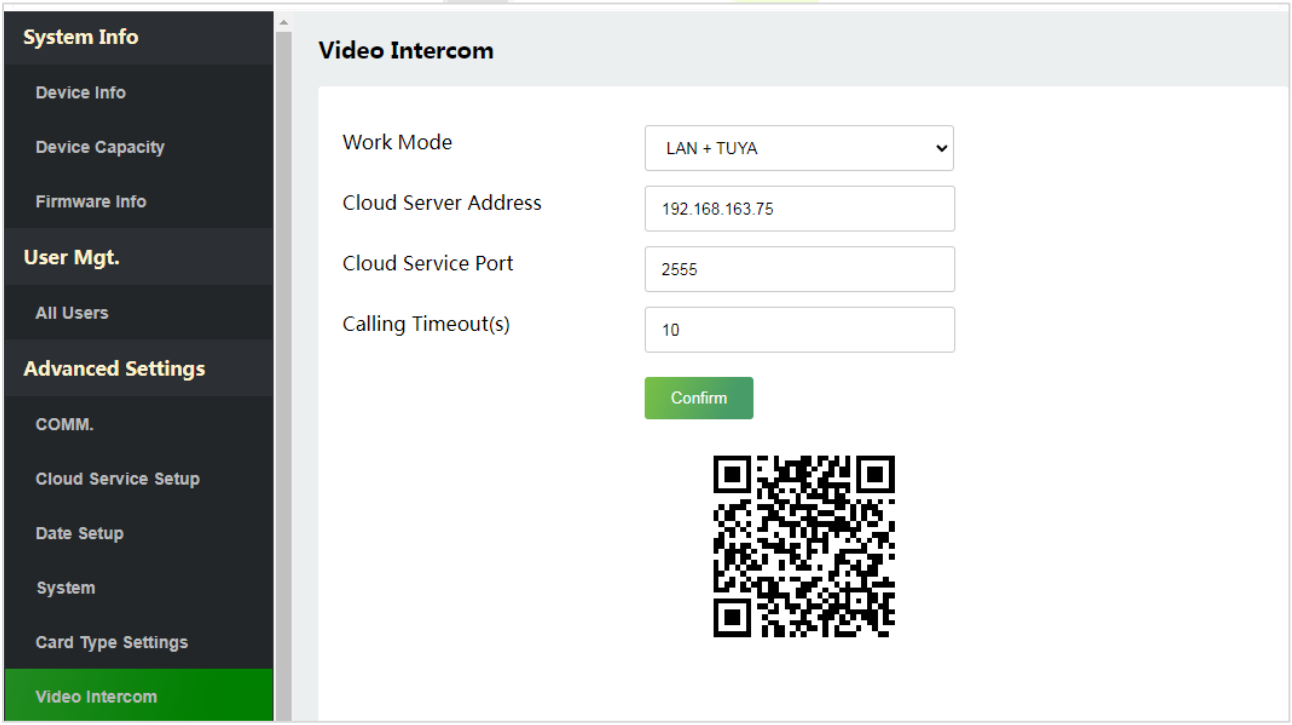
El dispositivo admite tarjetas de banda de 125 kHz y 13,56 MHz; seleccione el tipo de tarjeta correspondiente según sus necesidades.



9.6Video portero★

Hacer clic**Video portero**en el servidor web.

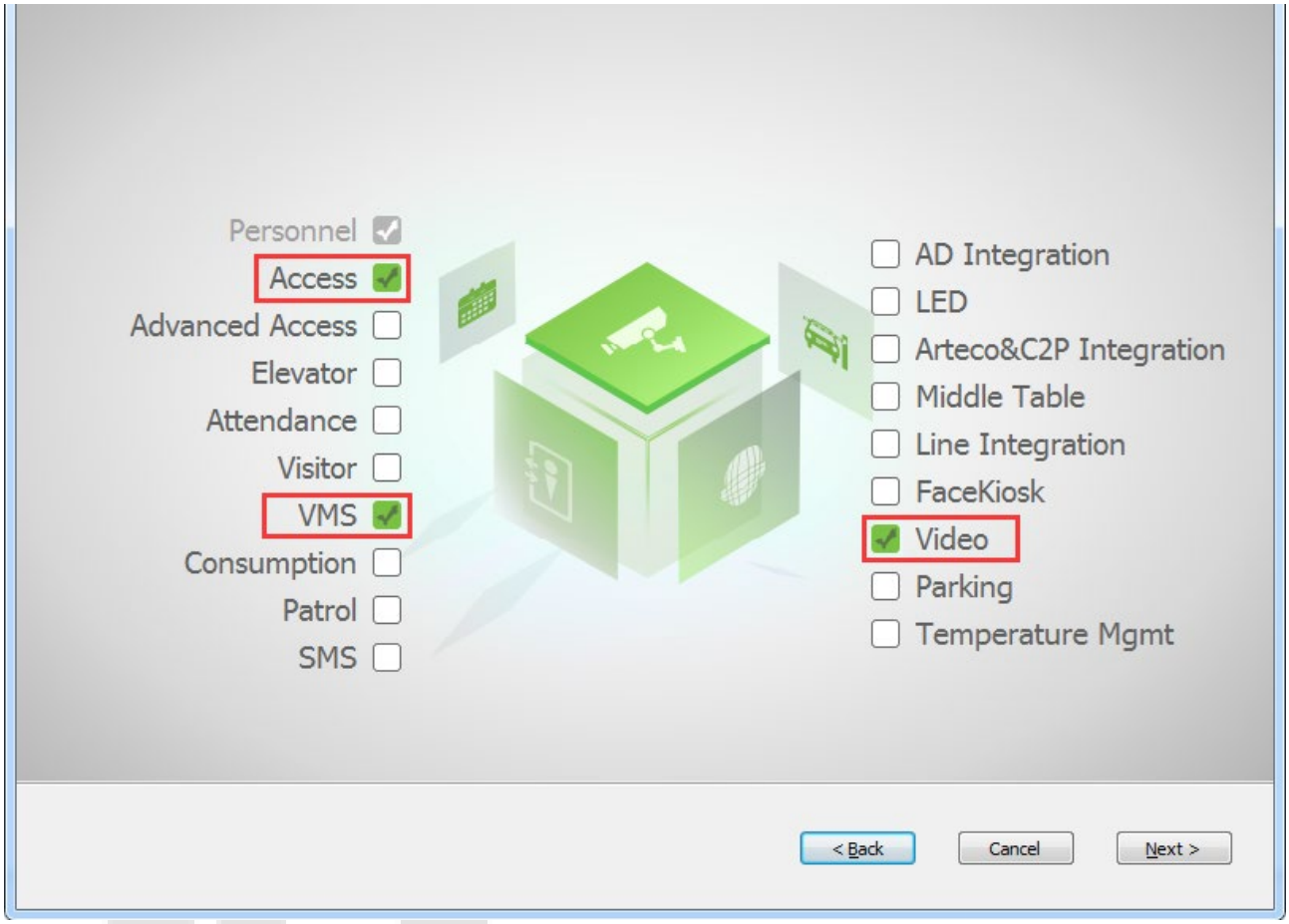
La función de videoportero es compatible con LAN y WAN, LAN es adecuada para PC y WAN es adecuada para teléfonos móviles.



9.6.1 Ajustes de la función de intercomunicador de vídeo LAN

1. Instalación del complemento ZKBio VMS en el software ZKBio CVSecurity

Durante la instalación, seleccione el módulo "VMS" del software ZKBio CVSecurity para instalar, como se muestra en la siguiente interfaz de instalación.



Nota: El módulo de Video y el módulo VMS no se pueden seleccionar al mismo tiempo.

Haga doble clic en el proporcionado **ZKBioVMSPlugin_sqlite.exe** para instalar el complemento ZKBio VMS.

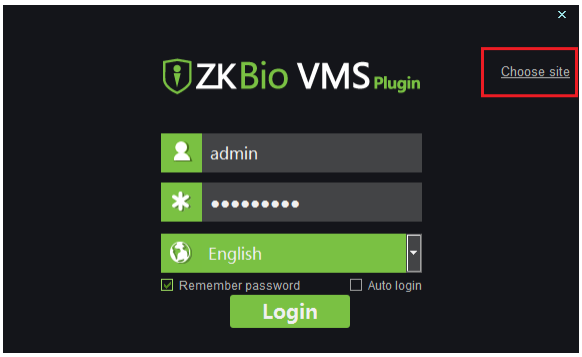
Nota: El software ZKBio CVSecurity y ZKBio VMS Plugin deben abrirse simultáneamente para reconocer la función de intercomunicador.

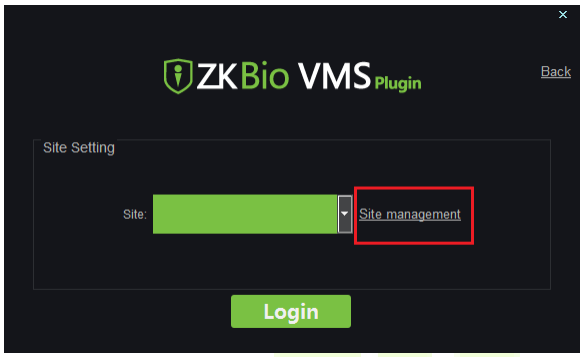
2. Parámetros de configuración

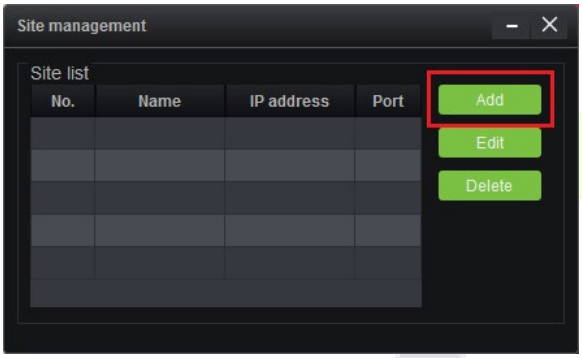
Establezca correctamente los parámetros necesarios para garantizar una conexión entre el dispositivo y el software.

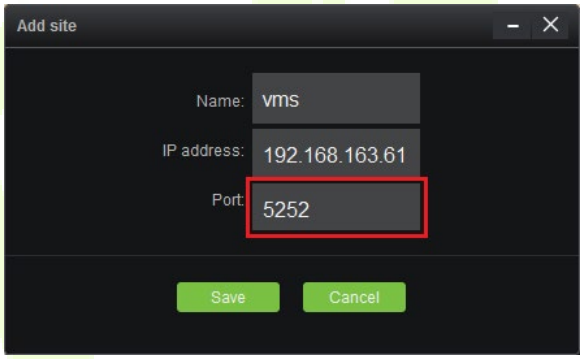
- **Agregar sitio en el complemento Video-VMS**

1)Haga doble clic en el icono para abrir el complemento Video-VMS. Hacer clic***elegir sitio**>**Manejo de sitio**> Añadir en la interfaz de inicio de sesión. Luego, ingrese el Nombre, la dirección IP y el Puerto para agregar un sitio, como se muestra en la siguiente figura.



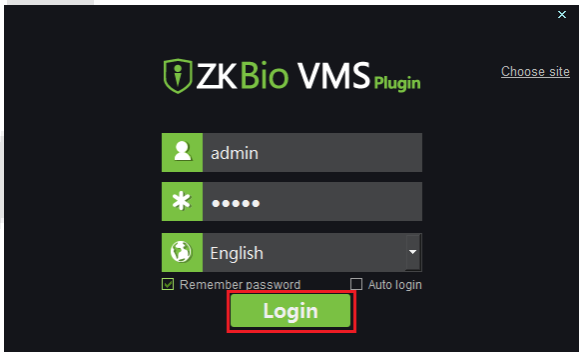






- **Dirección IP:**Introduzca la dirección IP local.
- **Puerto:**El puerto predeterminado es 5252.

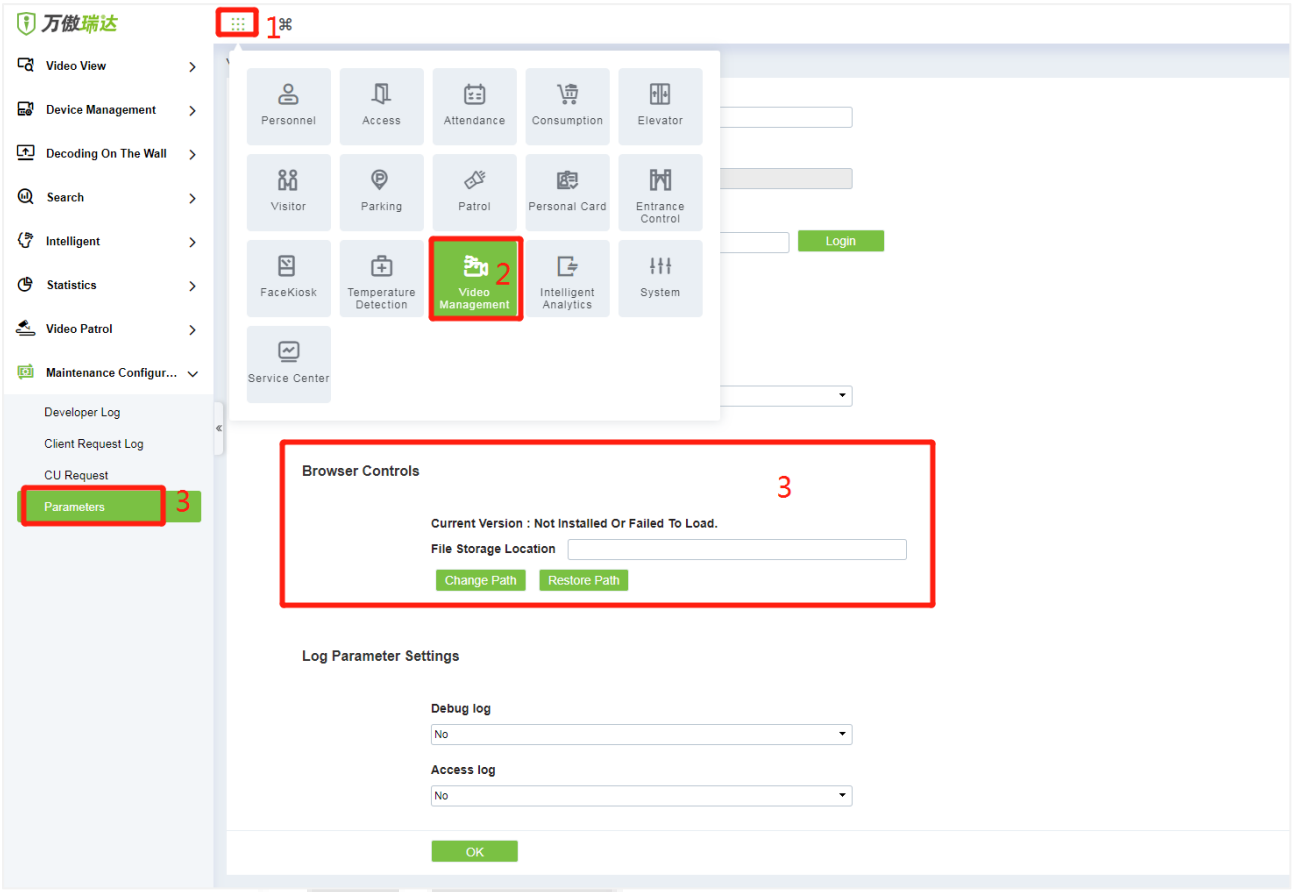
2)Ingrese el nombre de usuario y la contraseña después de agregar el sitio y haga clic en**Acceso**para iniciar sesión en el complemento Video-VMS. El nombre de usuario y la contraseña inicial son ambos**administración**.



Nota:Cuando el complemento Video-VMS se conecta correctamente a ZKBio CVSecurity, la contraseña cambia de forma sincrónica a la contraseña de usuario administrador de ZKBio CVSecurity.

- **Configure la ruta de conexión del complemento ZKBio CVSecurity y VMS**

Hacer clic**Video**>**Configuración de mantenimiento**>**Controles del navegador**en el software ZKBio CVSecurity para cambiar la ruta, como se muestra en la siguiente imagen:



Ruta de conexión VMS

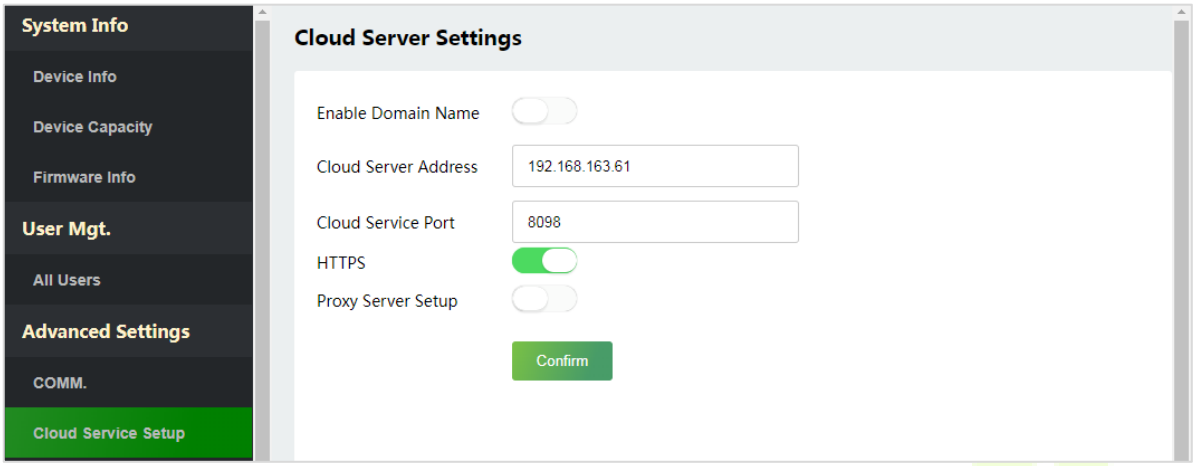
- **URL:**"http://dirección IP local: puerto"
- **Puerto:**Es**8489**por defecto (por ejemplo, http://192.168.163.61:8489).

Ruta del servidor

- **URL:**"http://dirección IP del servidor: puerto"
- **Puerto:**El puerto es el puerto de servicio configurado durante la instalación (p. ej.,http://192.168.163.61:8098) (no el puerto ADMS).

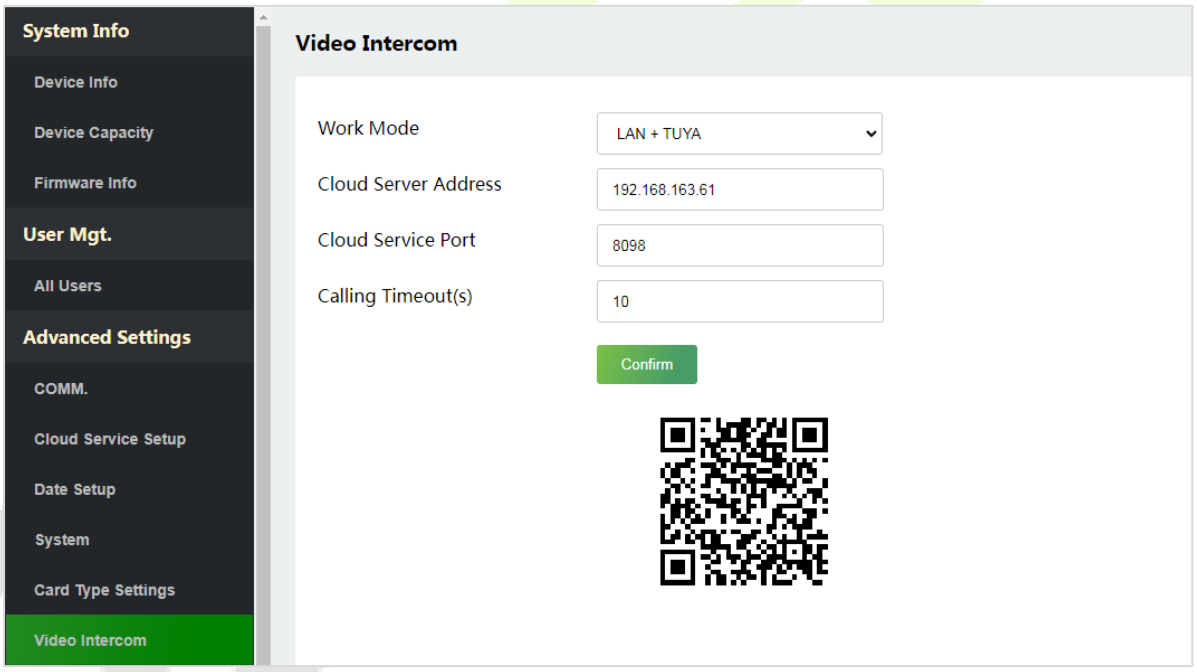
- **Configure los parámetros en el ProMA**

1)Hacer clic**Configuración del servidor en la nube**en WebServer para configurar la dirección del servidor y el puerto del servidor, es decir, la dirección IP y el número de puerto del servidor después de instalar el software. Si el dispositivo se comunica con el servidor con éxito, el icono se muestra en la esquina superior derecha de la interfaz de espera.



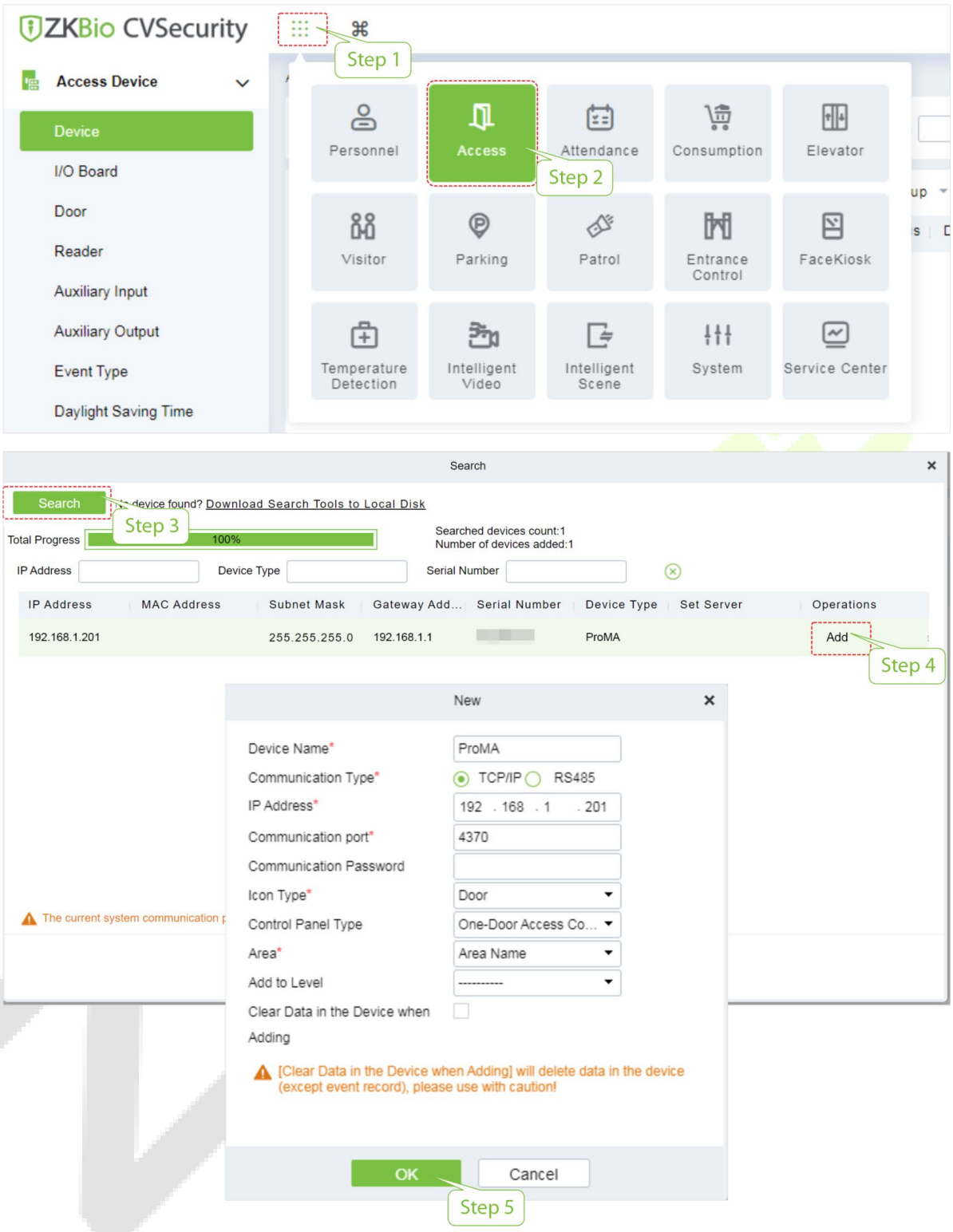
2)Hacer clic**Video portero**para establecer la dirección del servidor y el puerto del servidor.

- **Dirección del servidor en la nube:**Introduzca la dirección IP de instalación de ZKBio CVSecurity.
- **Puerto del servidor en la nube:**El puerto es el puerto de servicio establecido durante la instalación (no el puerto ADMS).

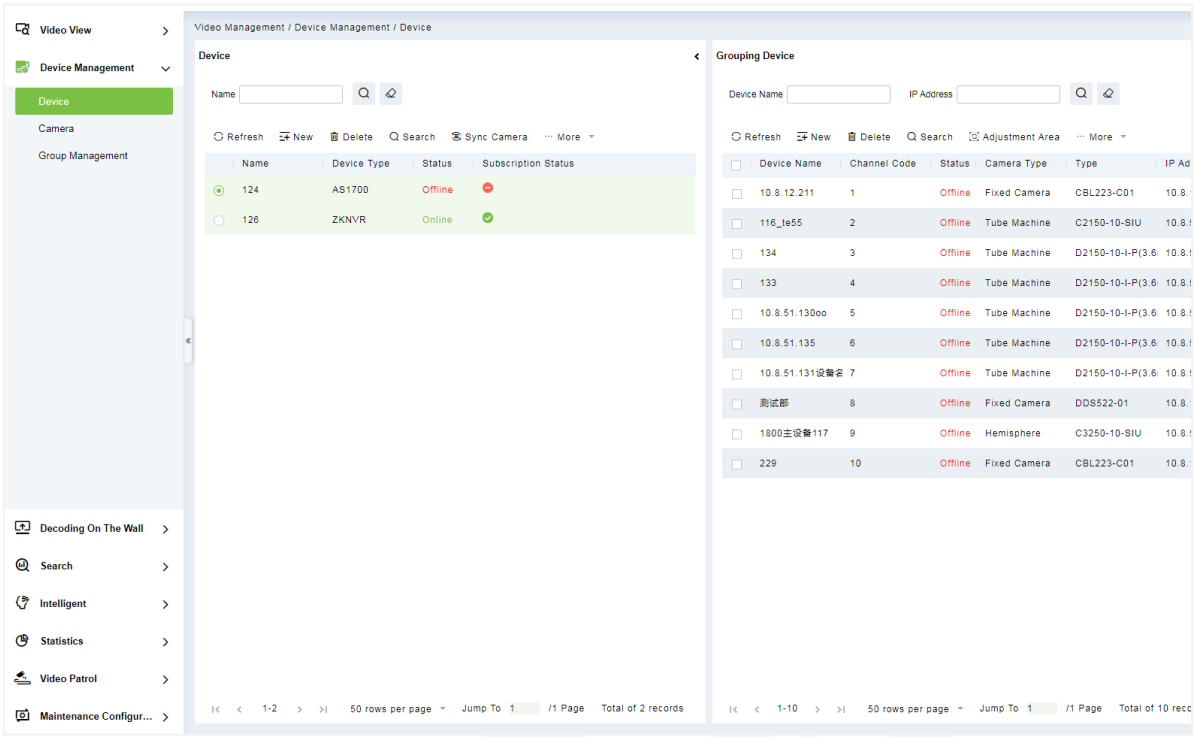


- **Agregar dispositivo en el software ZKBio CVSecurity**

1)Hacer clic**Acceso**>**Dispositivo**>**Dispositivo**>**Buscar**para agregar el dispositivo en el software ZKBio CVSecurity.



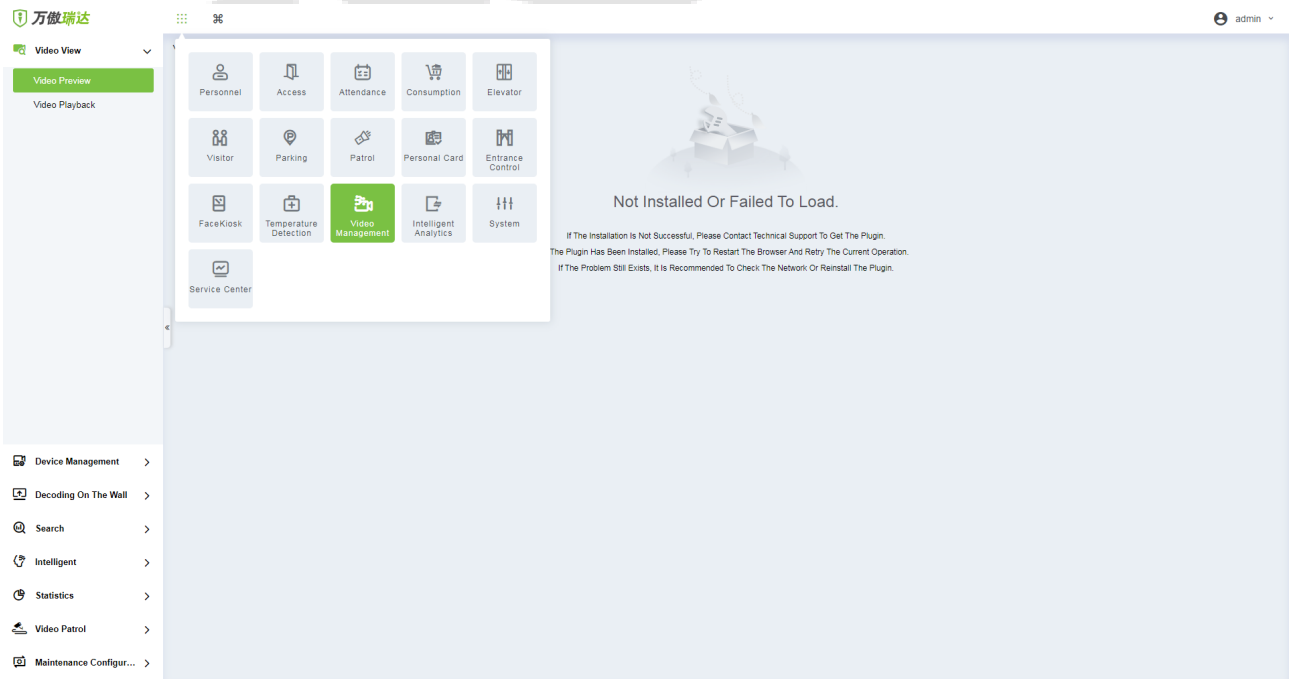
2)Una vez que el dispositivo se agrega con éxito al módulo de acceso, se agrega automáticamente al módulo de video. El usuario puede hacer clic**Video**>**Dispositivo de vídeo**>**Buscar**para ver.



Nota: Si el dispositivo no se agrega al módulo de video, verifique si la configuración de los parámetros es correcta.

3. Vista previa de video sobre el software ZKBio CVSecurity

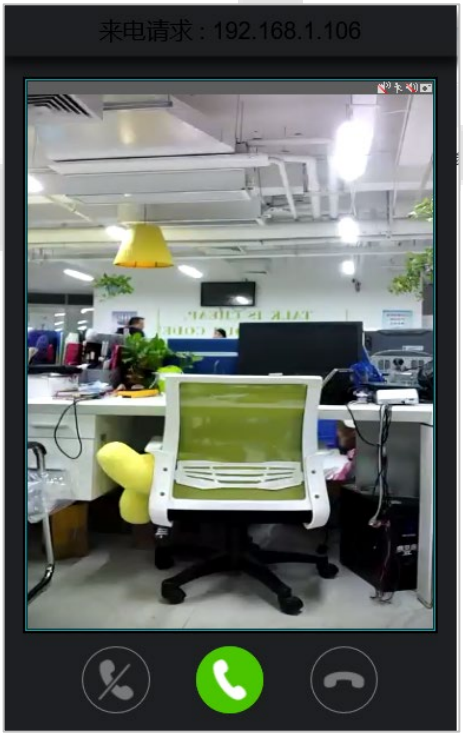
Hacer clic **Video** > **Vista previa de vídeo** para entrar en la interfaz de vista previa del dispositivo.

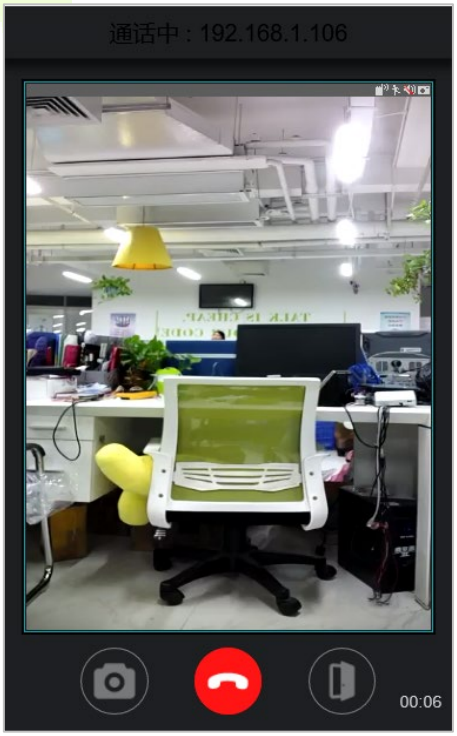


4.Hacer una llamada en el dispositivo

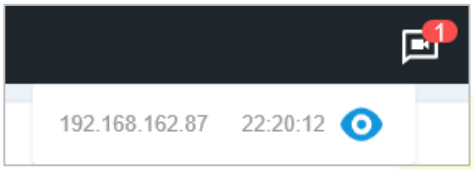
1)Toque el icono en el ProMA para hacer una llamada.

2)La página del servidor muestra la ventana de llamada de forma predeterminada, como se muestra en la siguiente figura.





Función descriptiva

Función Nombre	Descripción
	Es la tecla Contestar, el usuario puede hacer clic para contestar la llamada actual. Después de responder, ingrese a la ventana durante la llamada y active el audio y el video de manera predeterminada.
	Es la tecla Colgar. Después de colgar, finalice inmediatamente la llamada actual.
	Es la tecla Ignorar, utilizada para ignorar la llamada actual. Haga clic en él para cerrar la ventana de llamadas y el ícono en la esquina superior derecha mostrará la cantidad de llamadas pendientes, como este . El usuario puede hacer clic en el ícono en el menú desplegable para abrir nuevamente la ventana de llamada del dispositivo actual y elegir responder, como se muestra en la siguiente figura. 
	Es la tecla Colgar, utilizada para colgar la llamada actual.
	Es la tecla Instantánea, que se utiliza para tomar una instantánea.
	Es la tecla de apertura remota, que se utiliza para abrir la puerta de forma remota. El tiempo de manejo de bloqueo predeterminado es de 5 segundos.

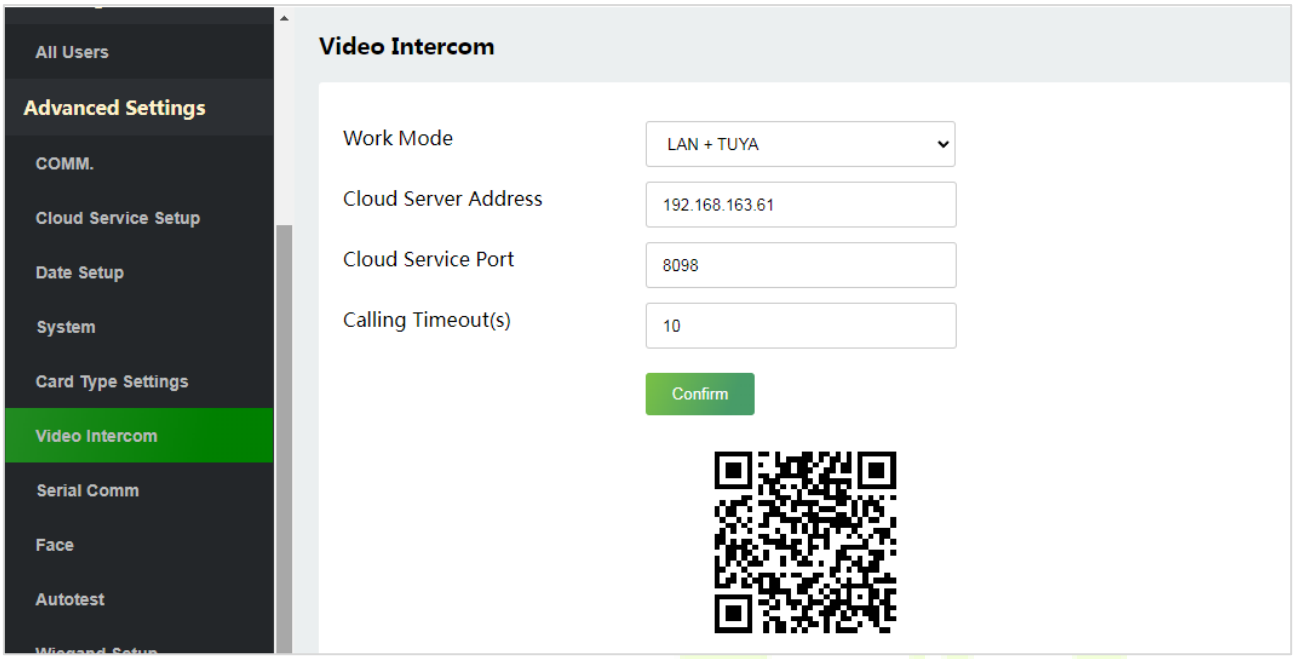
Nota: Si la interfaz de vista previa del dispositivo se abre en el software ZKBio CVSecurity, la interfaz de llamada ya no se mostrará en esta ventana de llamada.

9.6.2 Conexión al software ZKBio Talk

Descargue e instale el software ZKBio Talk. Luego, mantenga la configuración de parámetros del software ZKBio CVSecurity sin cambios para la configuración relevante. (Por favor refiérase a Ajustes de la función de intercomunicador de vídeo LAN).

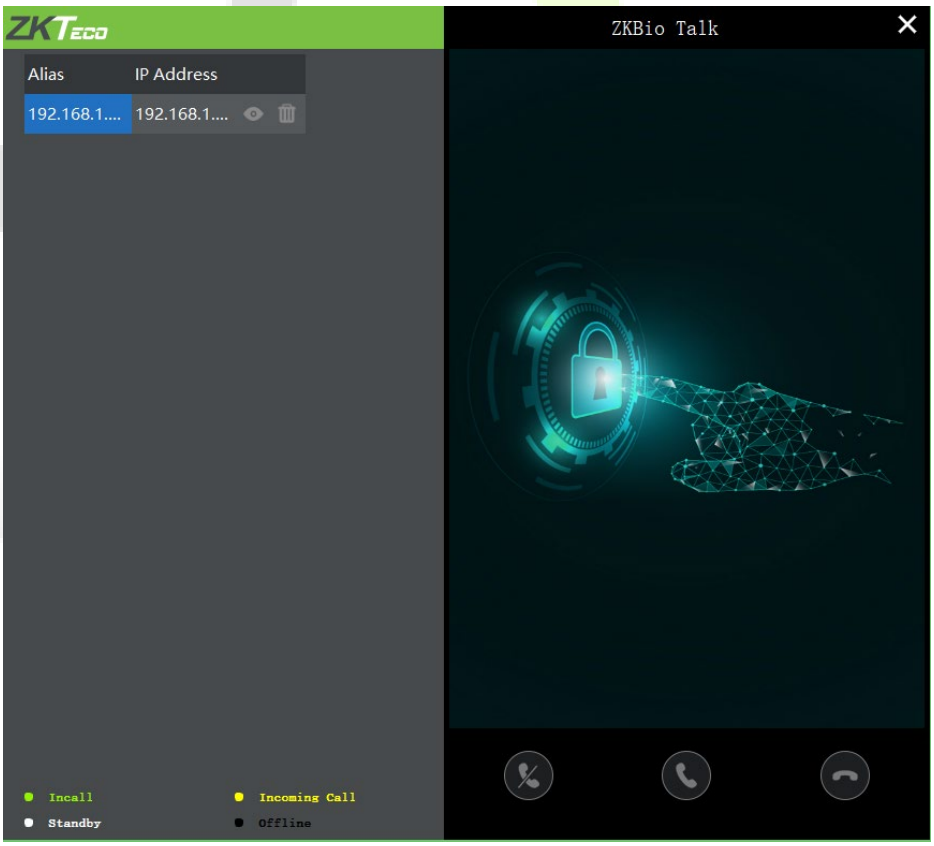
Los siguientes son los pasos para conectar ZKBio Talk al software ZKBio CVSecurity:

1. En primer lugar, cambie el parámetro en el ProMA. Haga clic en Video Intercom en el WebServer para cambiar la dirección del servidor y el puerto del servidor, como se muestra en la siguiente figura.

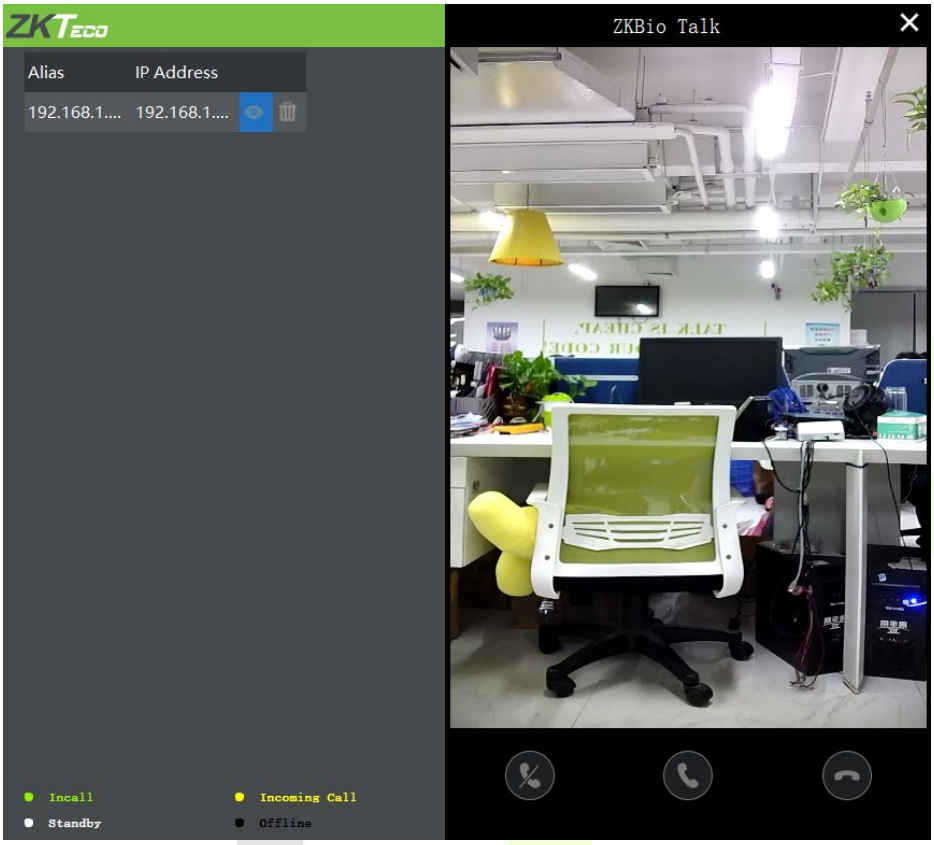


- **Dirección del servidor:**Introduzca la dirección IP de instalación del servidor actual.
- **Puerto de servicio:**El puerto del servidor predeterminado es**25550**.

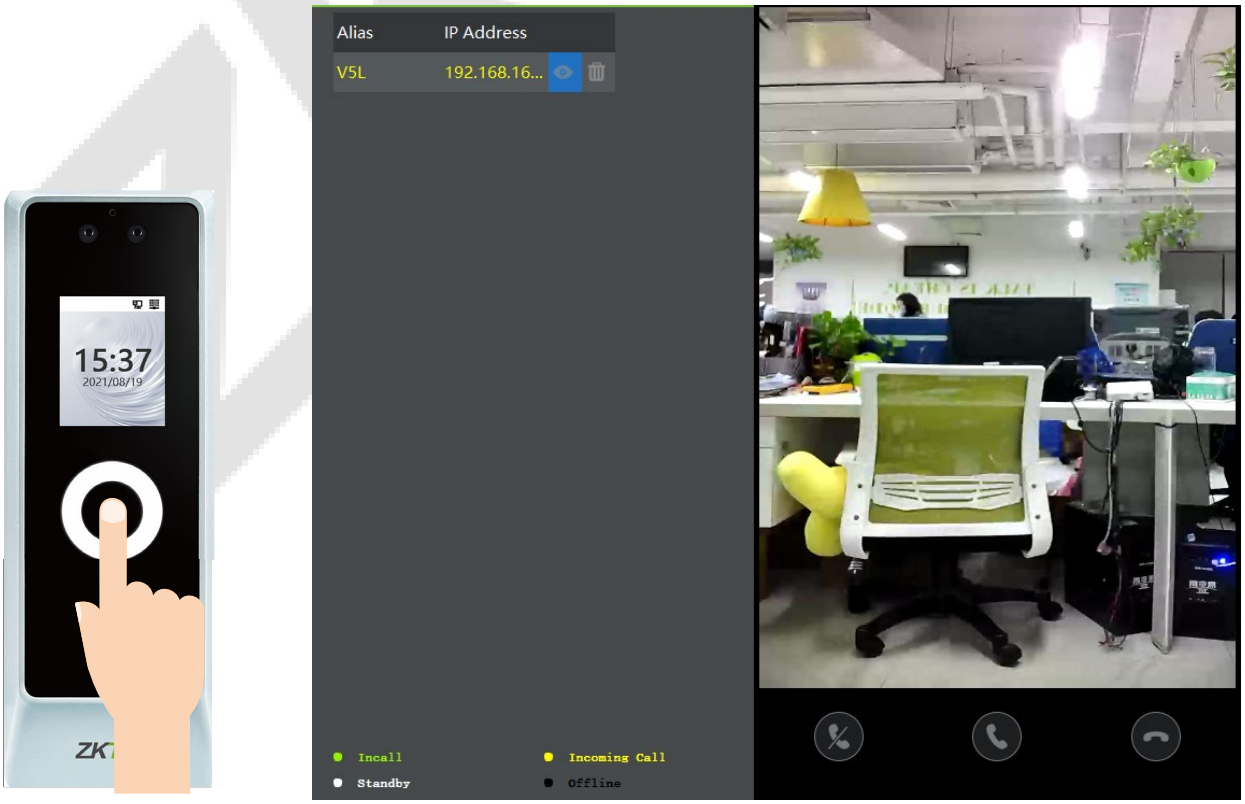
2. Haga doble clic en el icono para abrir el software ZKBio Talk. Cuando los parámetros del intercomunicador de video del lado del dispositivo están configurados correctamente, el dispositivo empuja automáticamente la lista de dispositivos a la izquierda, como se muestra en la siguiente figura.



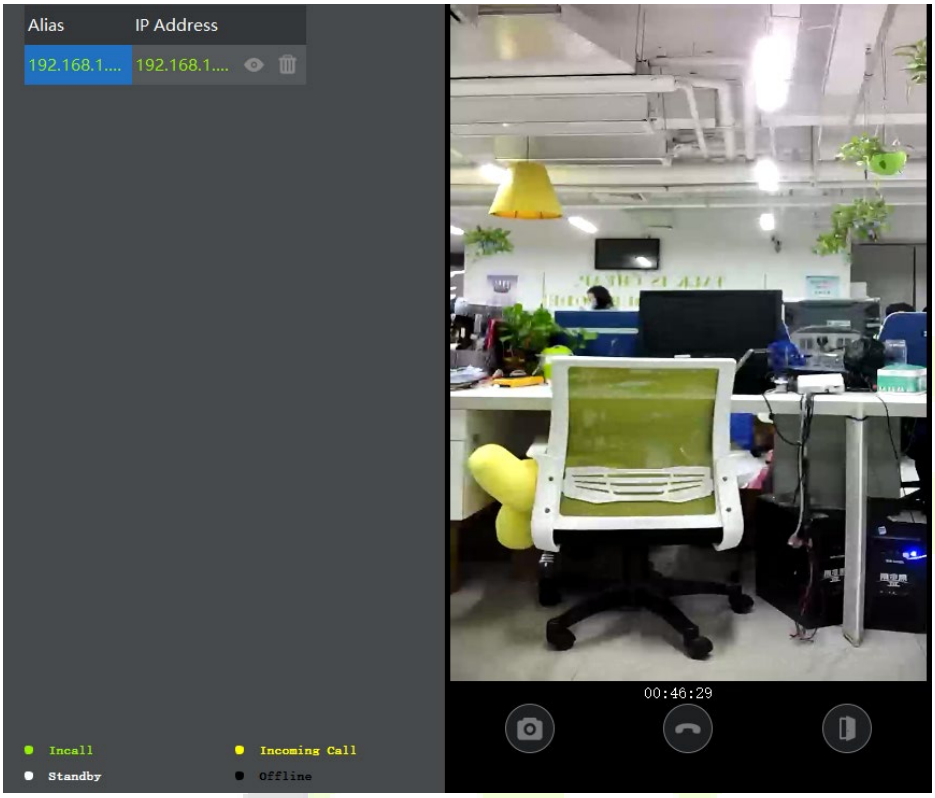
3.Un usuario puede hacer clic en para obtener una vista previa del video de la derecha. Al hacer clic o icono, un usuario puede cerrar la pantalla de vista previa. No se toman medidas cuando se hace clic.



4.Cuando un usuario toca el icono en el ProMA para hacer una llamada, la interfaz del software muestra la dirección IP del dispositivo que llama en amarillo.



5.Cuando el usuario hace clic en el  icono para contestar la llamada, la dirección IP se muestra en verde mientras está en el llamar. La duración de la llamada también se muestra justo encima del icono.



Función descriptiva

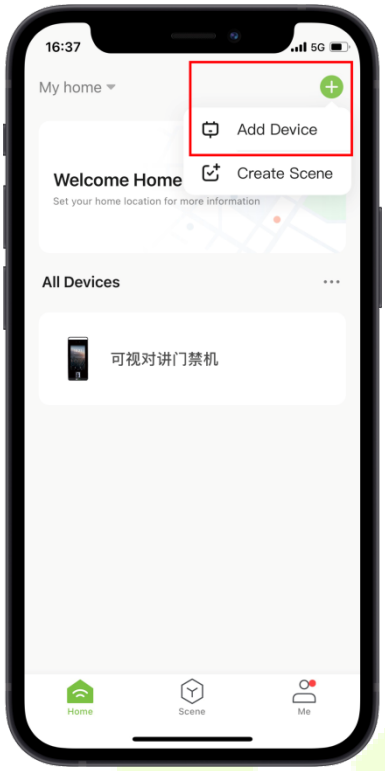
Nombre de la función	Descripción
	Es la tecla Instantánea, que se utiliza para tomar una instantánea.
	Es la tecla de apertura remota, que se utiliza para abrir la puerta de forma remota. El tiempo de manejo de bloqueo predeterminado es de 5 segundos.

9.6.3Conexión a la aplicación ZSmart

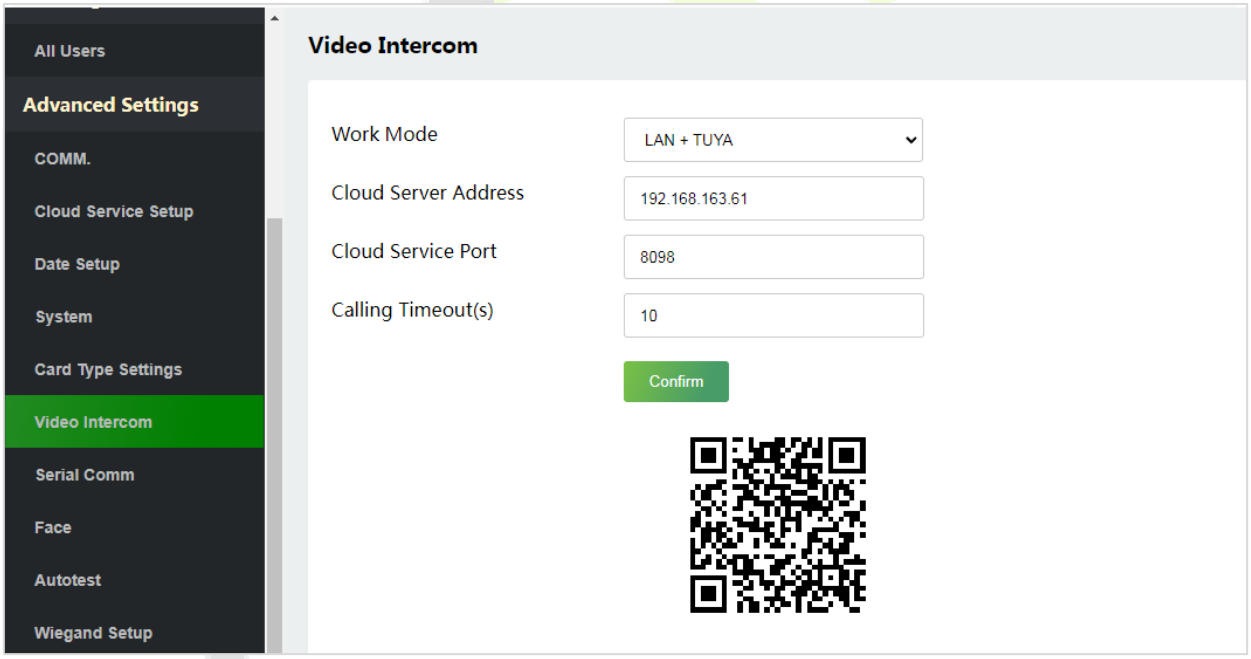
- **Agregar dispositivo en la aplicación ZSmart**

Después de descargar e instalar la aplicación ZSmart en su teléfono, cree una cuenta de usuario inicialmente con su Identificación de correo. Después de crear la cuenta de usuario, inicie sesión en la aplicación y toque  o  icono en la parte superior la esquina derecha de la pantalla para agregar un dispositivo. El proceso es el siguiente:

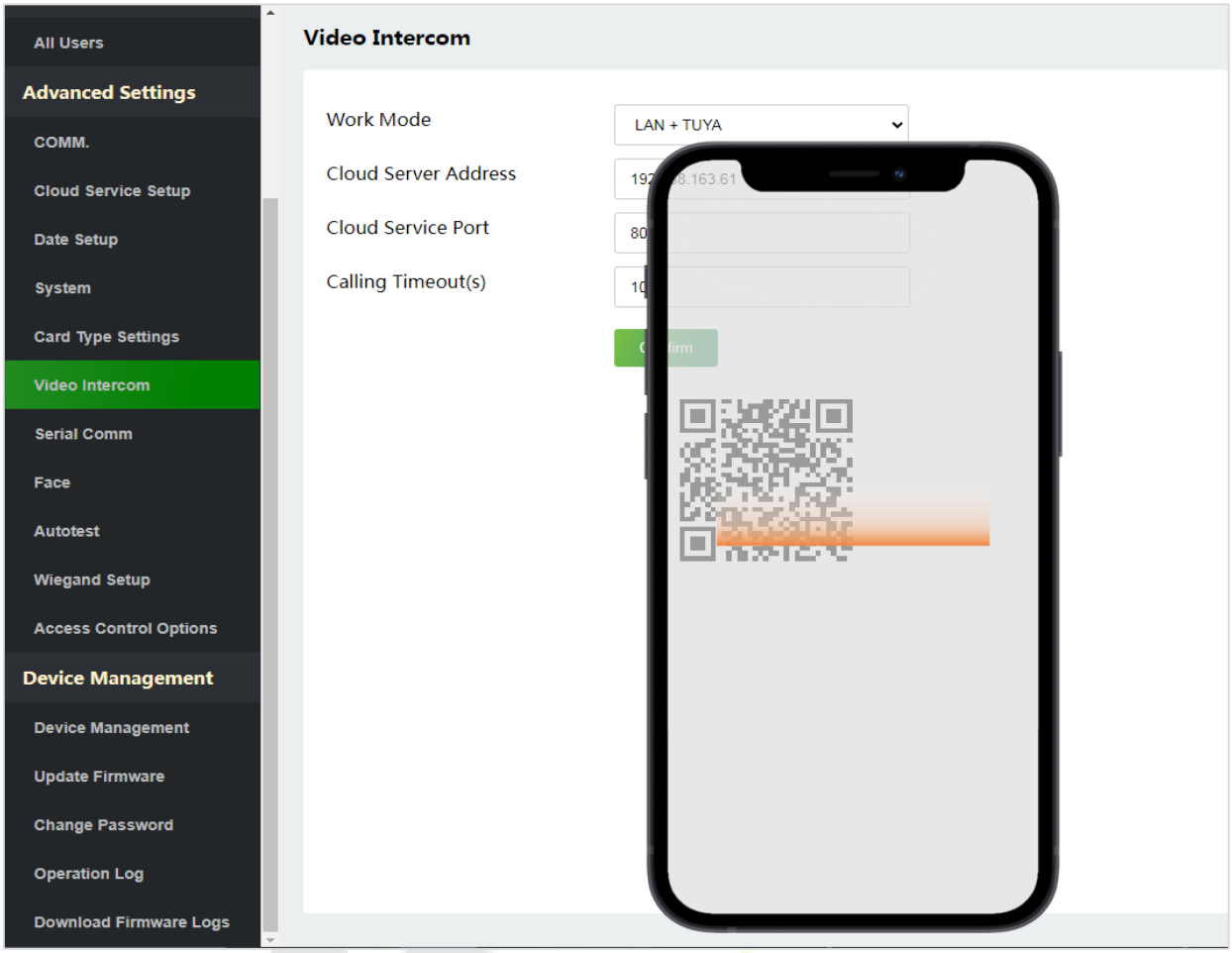
1.Hacer clic**Añadir dispositivo**en la página de inicio.

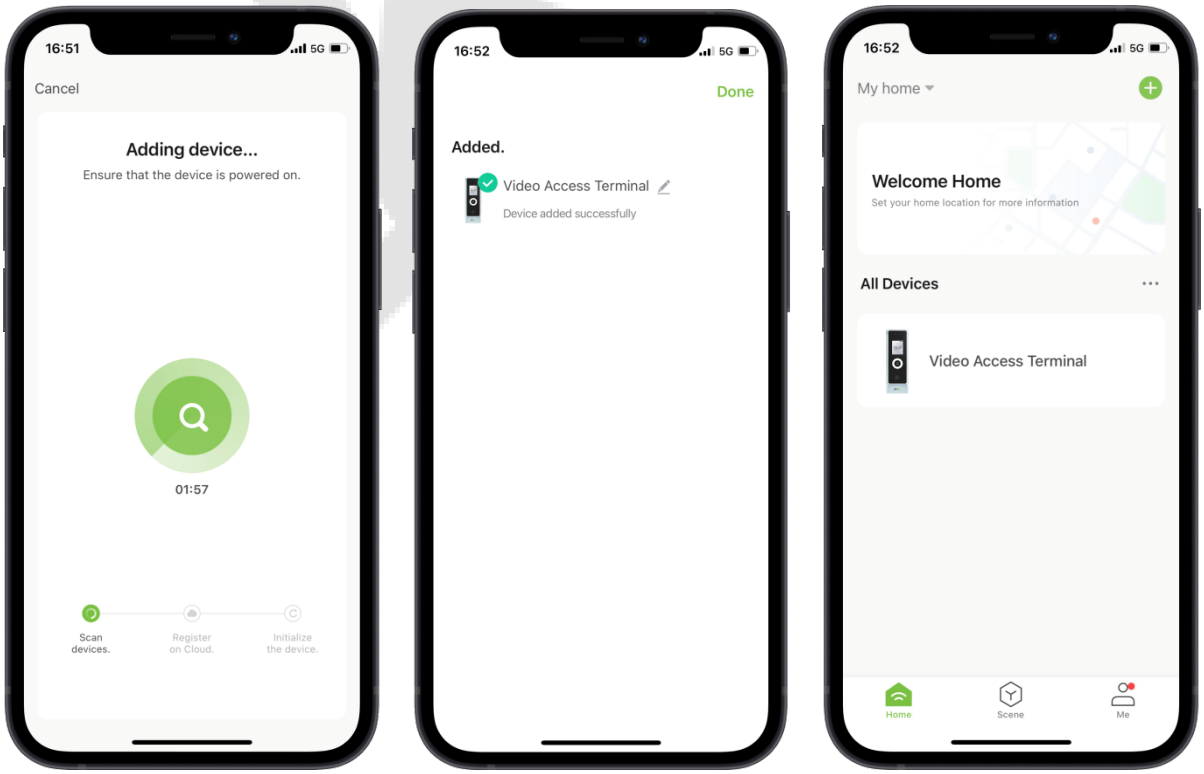


2.Hacer clic**Video portero**en el servidor web.



3.Toque en el icono en la esquina superior derecha.



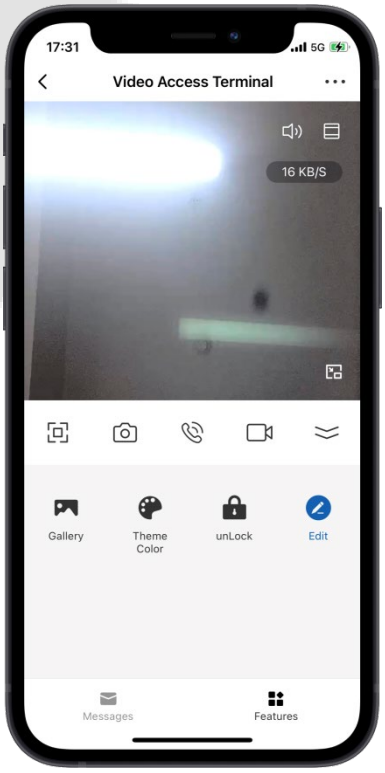


- **Hacer una llamada en el dispositivo**

Grifo en el ProMA para hacer una llamada. Después de recibir la llamada, deslice hacia arriba para abrir la puerta de forma remota.

- **Pantalla de vigilancia**

Encuentre el ProMA incluido en la aplicación ZSmart para ver la pantalla en tiempo real.



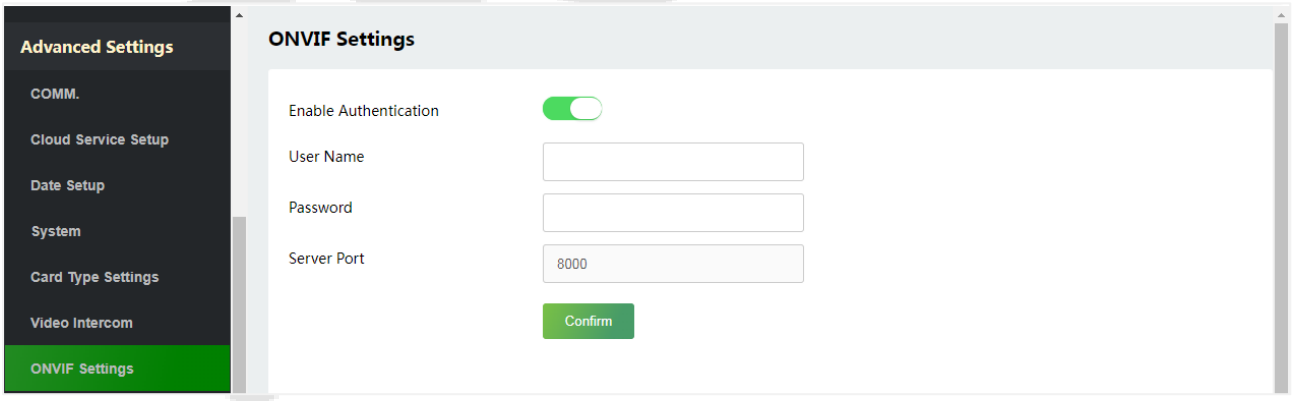
Función descriptiva

Función Nombre	Descripción
	Tóquelo para cambiar a la pantalla completa.
	Capture una imagen en el álbum de fotos en la aplicación.
	Tóquelo para hablar con las personas frente al dispositivo.
	Grabe manualmente un video en el álbum de fotos en la aplicación.
	Para silenciar o reactivar el sonido del dispositivo.
Galería	Revisa las fotos grabadas al detectar el movimiento.
Color del tema	Cambie el tema de la interfaz de usuario al modo claro o al modo oscuro.
Desbloquear	Apertura remota de puertas y visualización de registros de apertura de puertas.

9.7Configuración de Onvif

Nota:Esta función debe usarse con la grabadora de video en red (NVR)★.

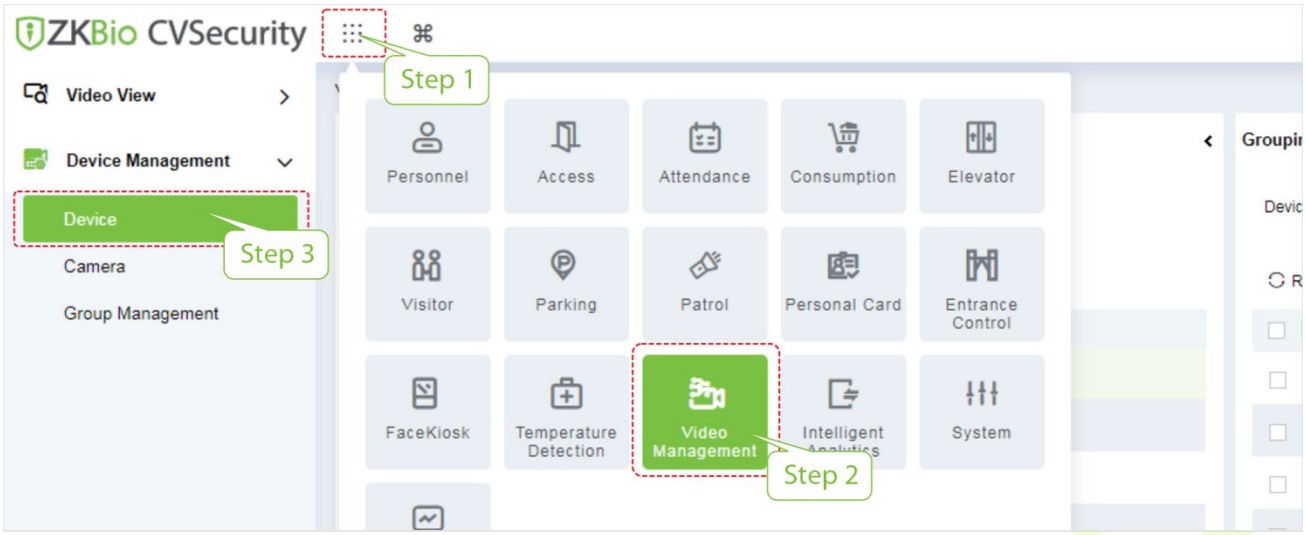
Hacer clic**Configuración ONVIF**en el servidor web.

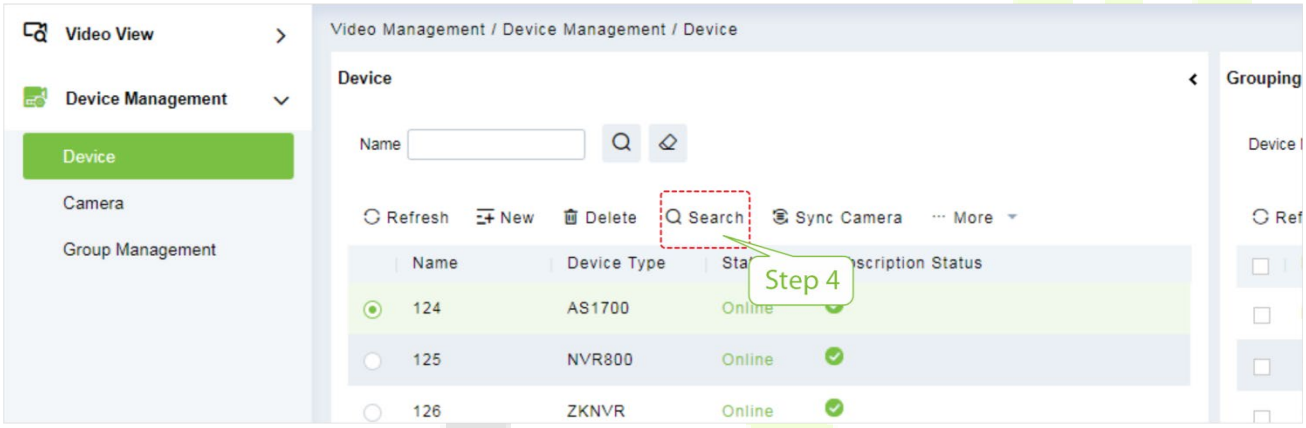


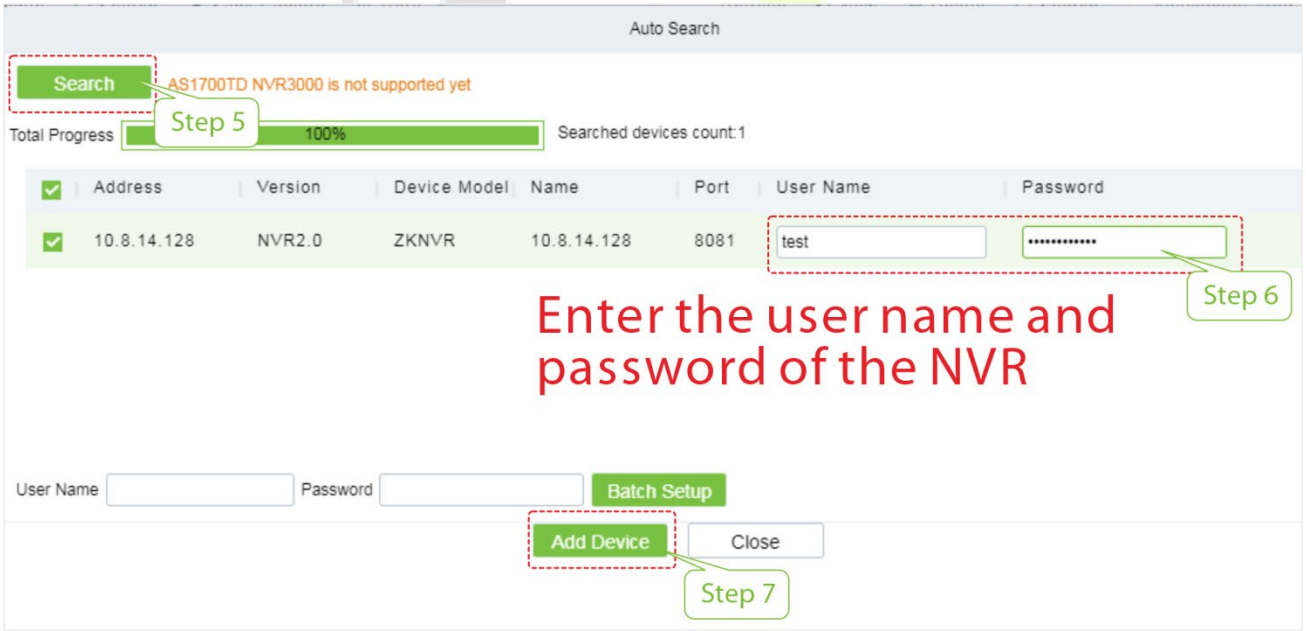
9.7.1Grabadora de video en red (NVR)

1.Después de encender el dispositivo NVR, conecte el puerto de cableado del NVR a través del cable Ethernet.

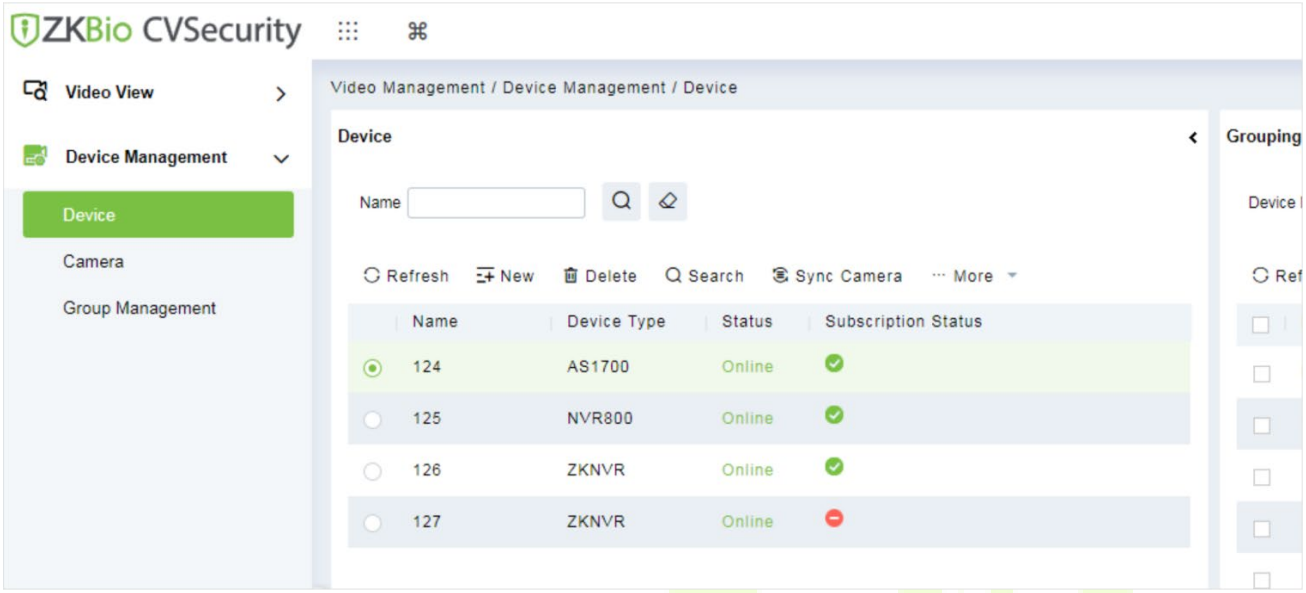
2.Hacer clic**[Gestión de vídeos]**>**[Dispositivo]**>**[Buscar]**en el servidor ZKBio CVSecurity para agregar NVR.





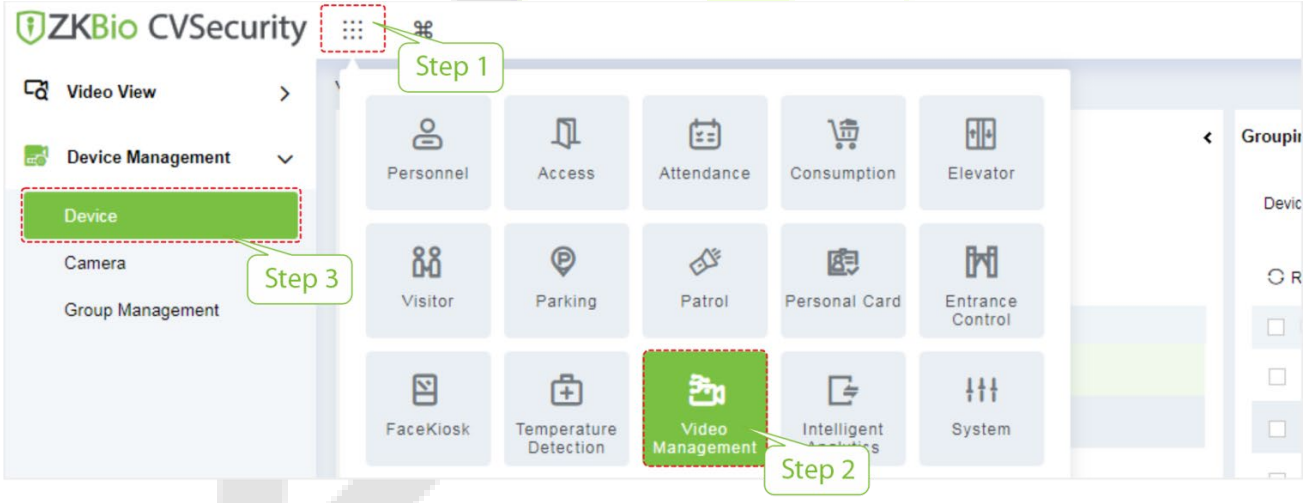


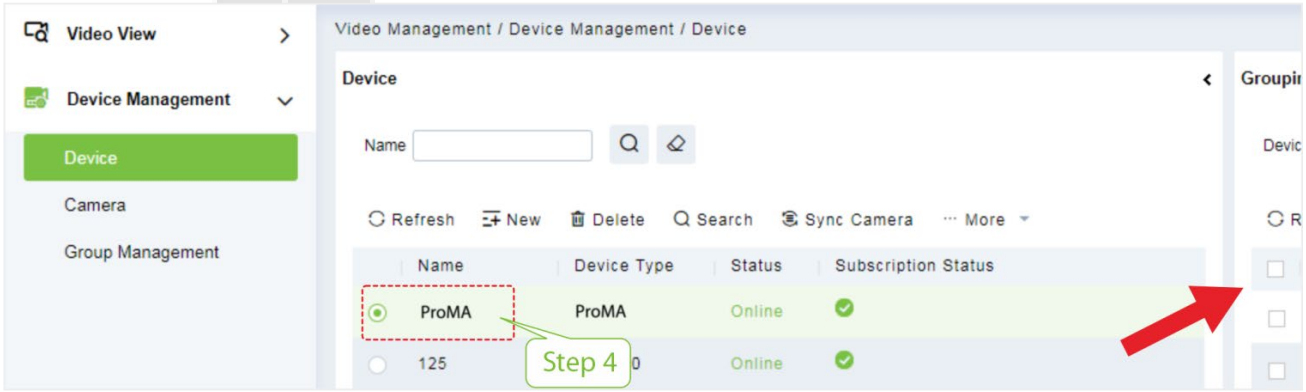
Los NVR agregados con éxito se muestran en la lista de dispositivos, como se muestra en la siguiente figura.



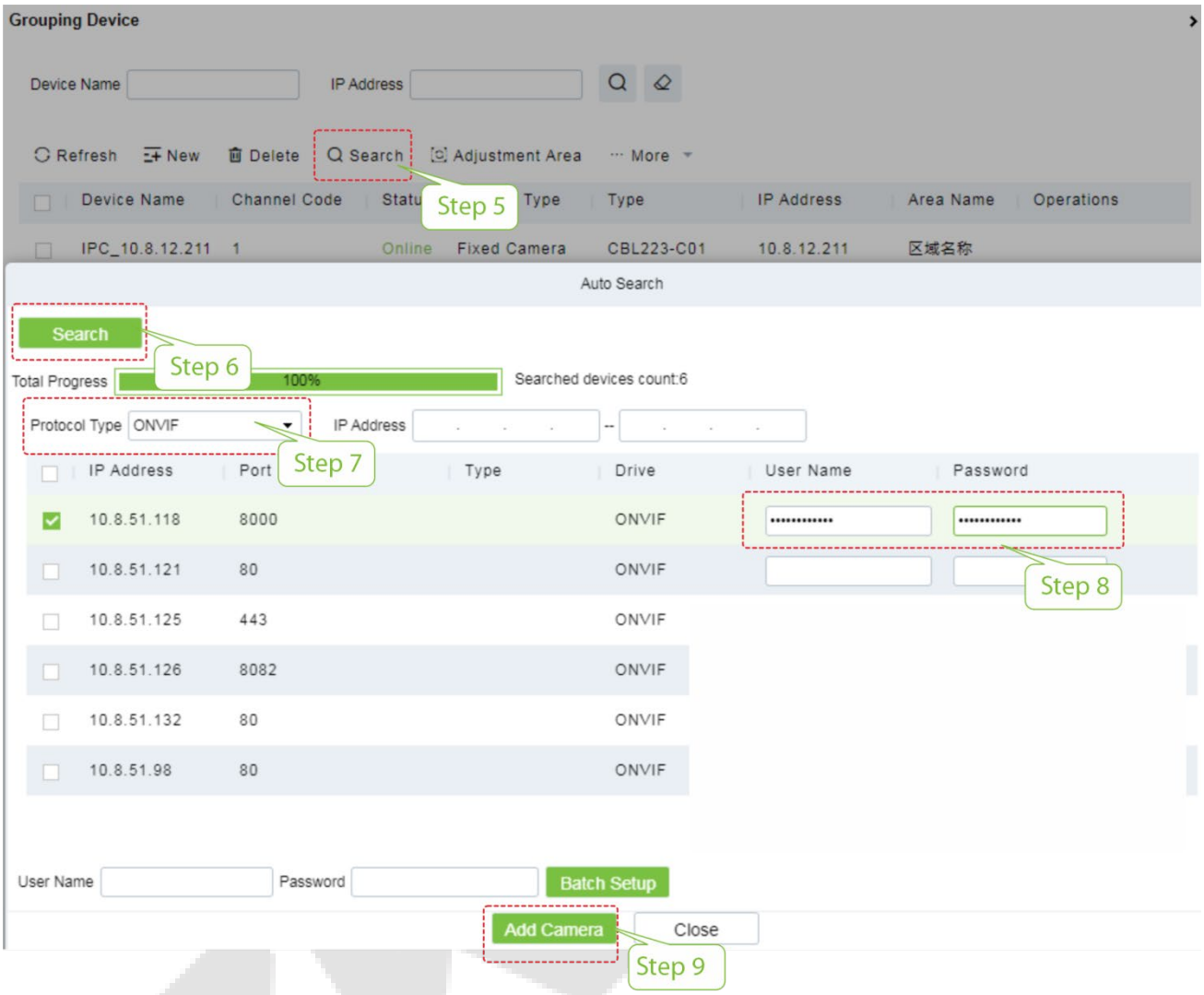
9.7.2Agregue ProMA a NVR

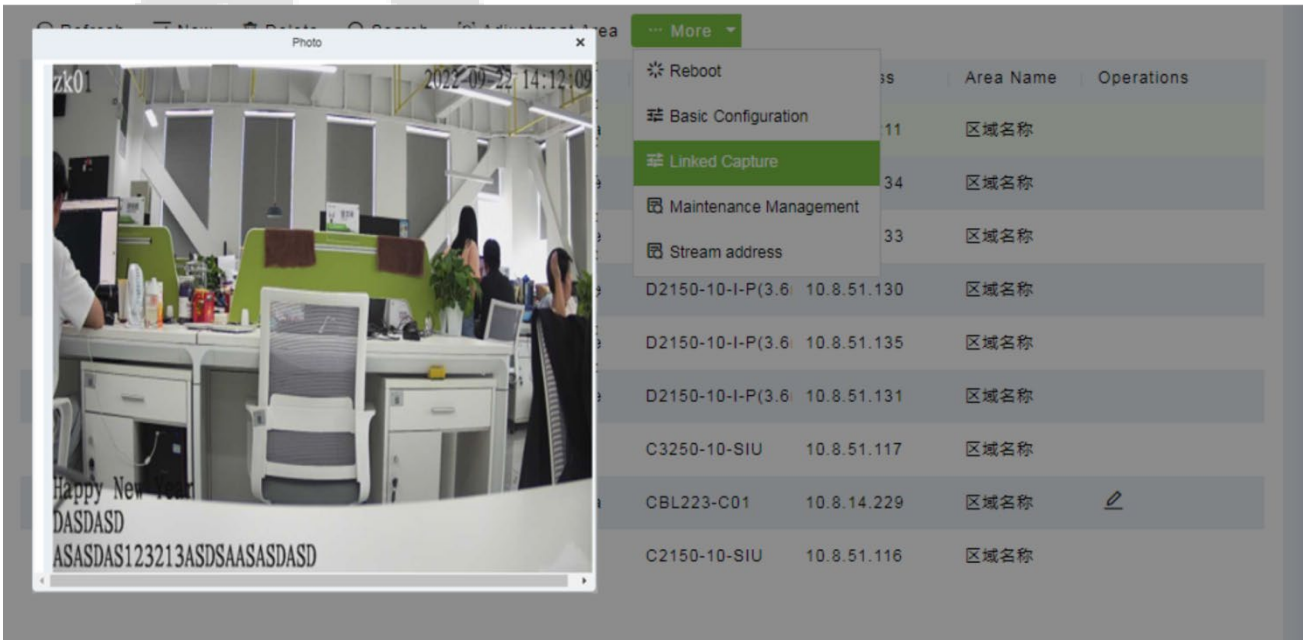
1.Hacer clic**[Gestión de vídeos]**>**[Dispositivo]**>**[Buscar]**en el servidor ZKBio CVSecurity para seleccionar el NVR al que necesita agregar el ProMA en la lista de dispositivos.





2.En la lista de dispositivos, haga clic en**[Buscar]**>**[Iniciar busqueda]**, el NVR busca automáticamente en la misma cámara LAN IPC a través del cable de red, agréguelo.

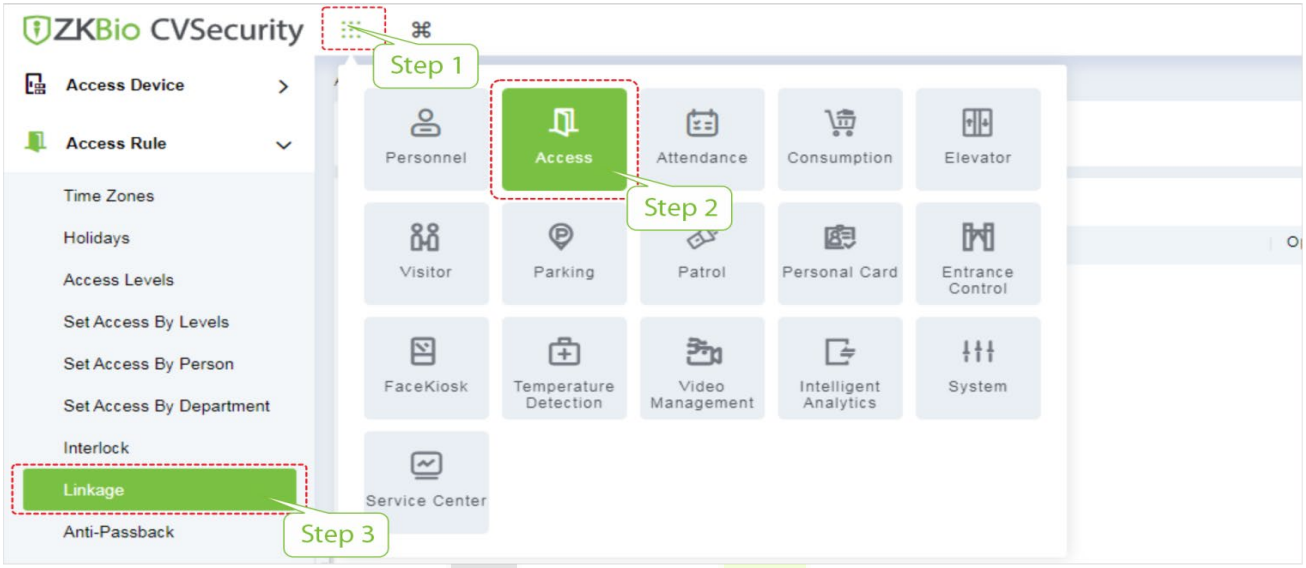


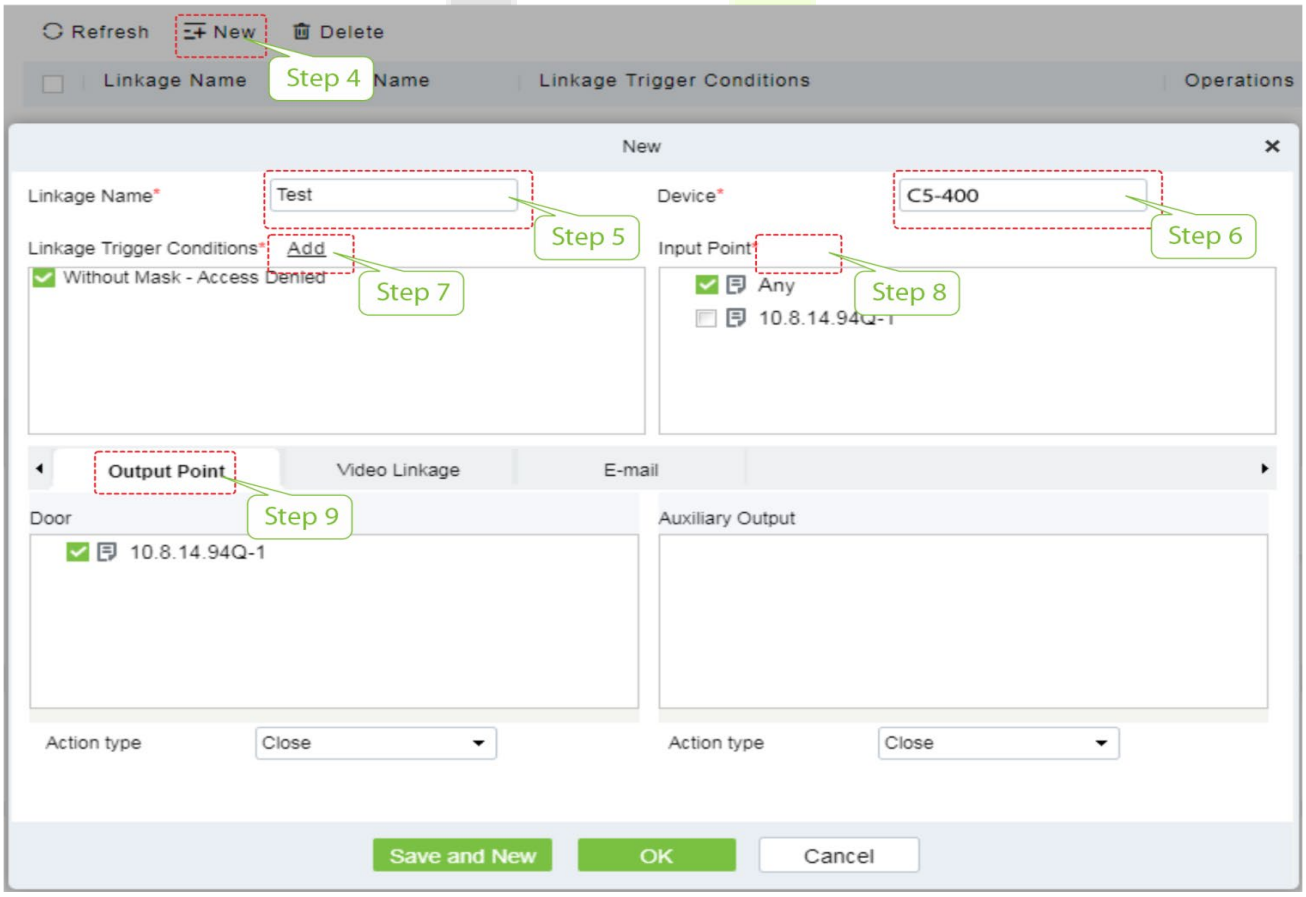


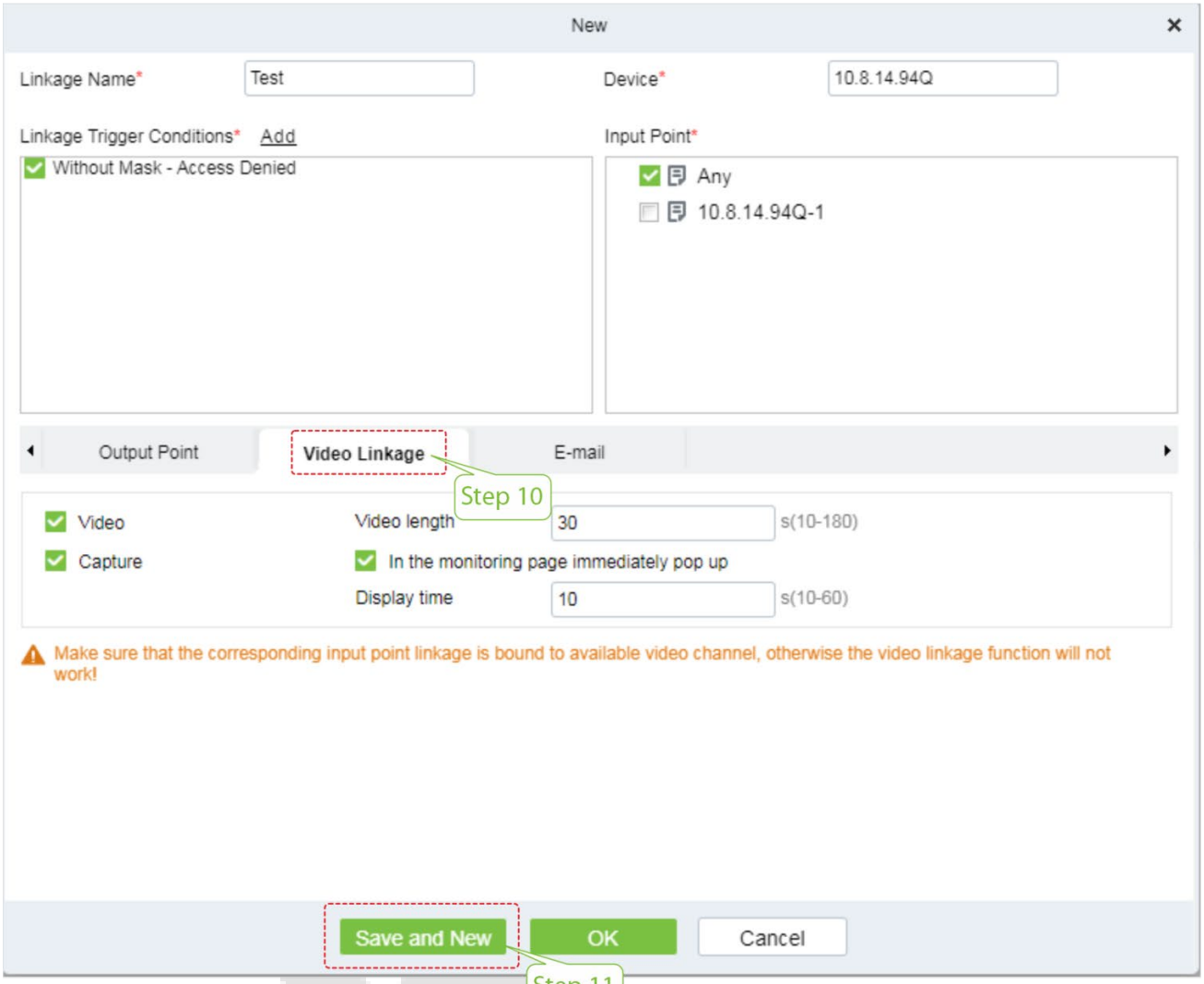
9.7.3Enlace

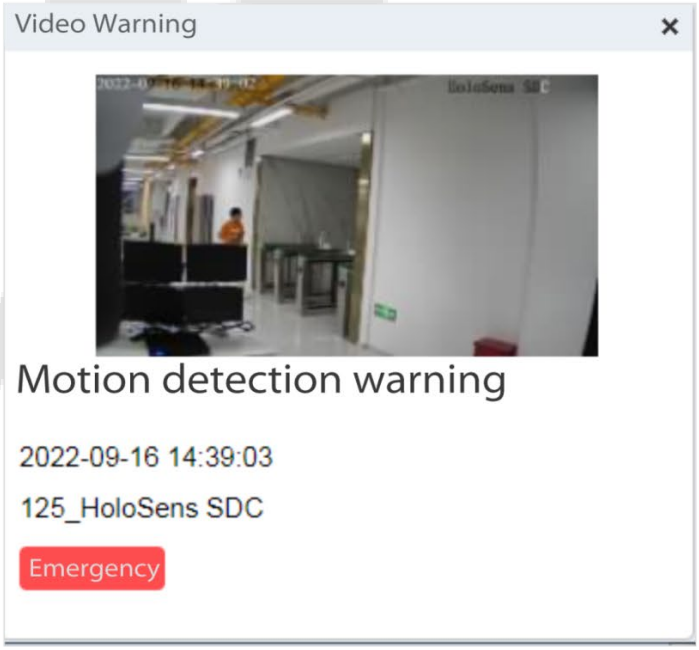
Después de configurar el controlador de acceso, NVR y ProMA, puede configurar el enlace de activación de eventos para acceso ilegal, verificación de apertura de puertas, alarma, anormalidad, etc., que se mostrarán en la lista de eventos de monitoreo correspondiente.

Hacer clic**[Acceso]**>**[Enlace]**>**[Agregar]**en el servidor para establecer los parámetros relacionados con el enlace. Para obtener más detalles, consulte*Manual de usuario de ZKBio CVSecurity*.





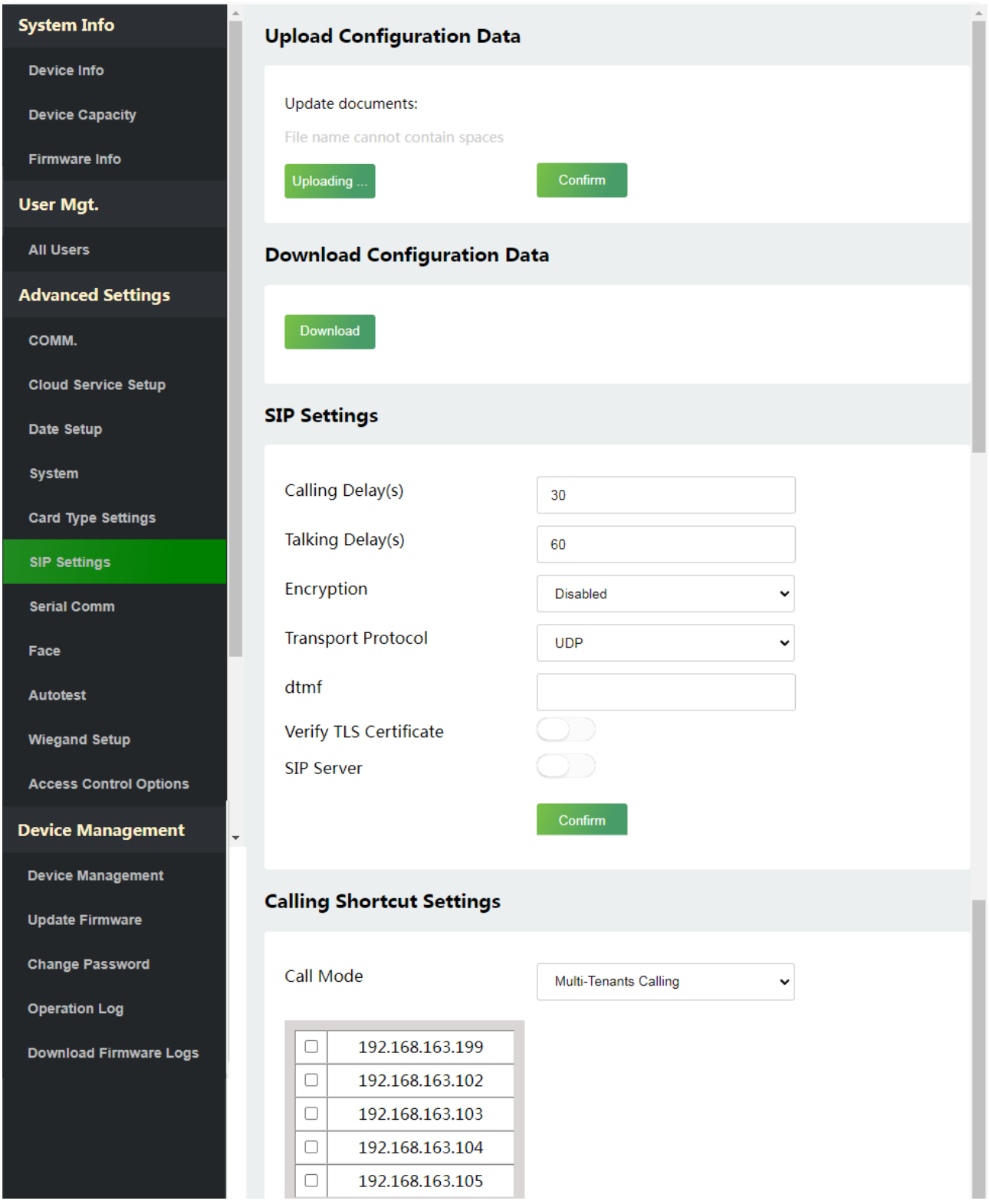




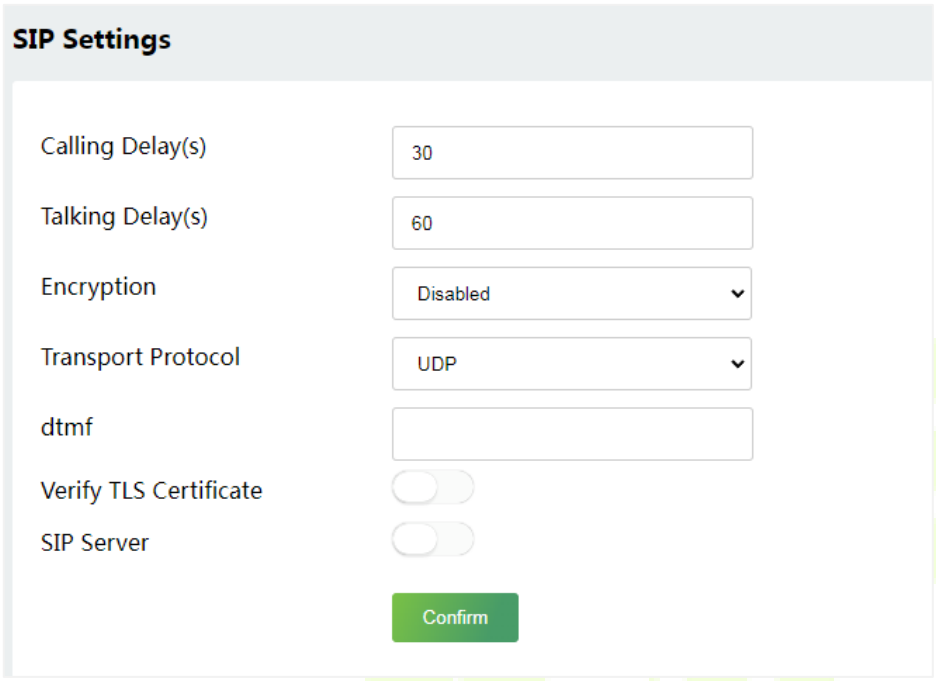
9.8Configuración SIP★

Nota:Esta función debe utilizarse con la estación interior Vpad A2★.

Hacer clic**Configuración SIP**en el servidor web.



9.8.1 Configuración SIP

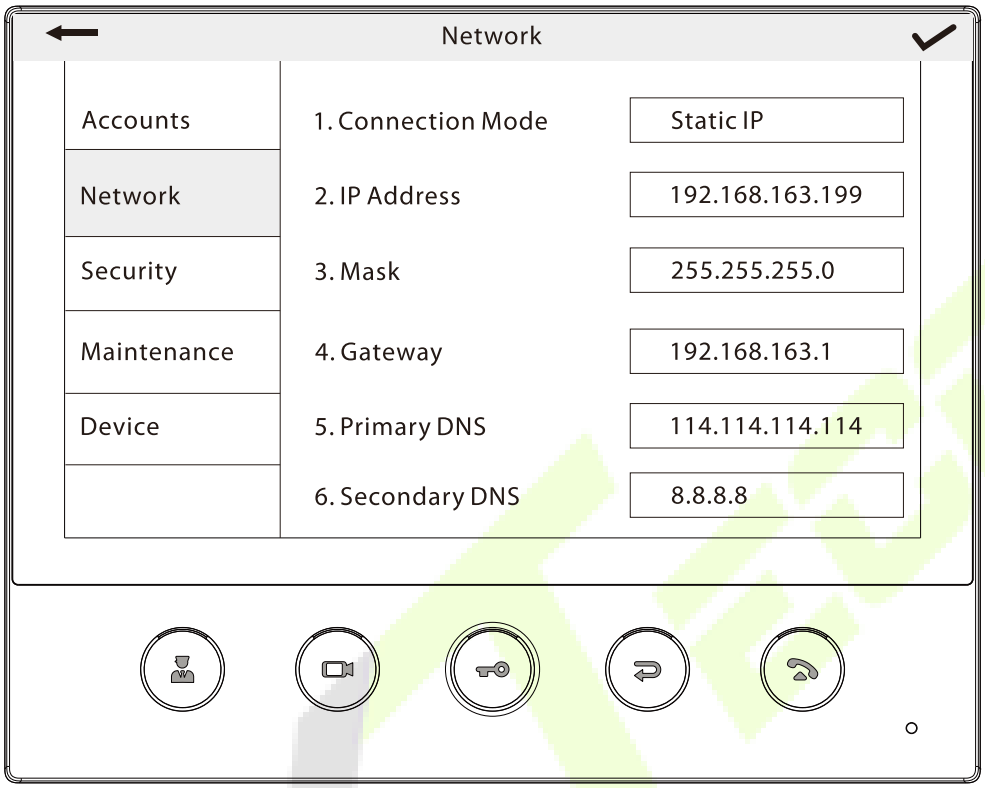


Nombre de la función	Descripción
Demora(s) de llamada	Configure el tiempo de llamada, valor válido de 30 a 60 segundos.
Hablando Demora(s)	Configure el tiempo de intercomunicación, valor válido de 60 a 120 segundos.
Cifrado	Cuando se habilite, esta comunicación de video portero será encriptada.
Protocolo de transporte	Configure el protocolo de transporte entre ProMA y la estación interior Vpad A2.
dtmf	El valor de WebServer es el mismo que el valor de DMTF en el dispositivo para desbloquearlo.
Verificar certificado TLS	Habilite/desactive la verificación del certificado TLS.
Servidor SIP	Seleccione si habilitar la dirección del servidor. Una vez que se haya conectado al servidor, puede llamarlo ingresando el nombre de usuario de la estación interior. Para obtener más información, consulte 9.8.3 Servidor SIP.

El ProMA y la estación interior para lograr video portero hay dos modos, respectivamente, el servidor LAN y SIP. Se puede seleccionar cualquiera de los dos métodos para lograr el intercomunicador de video SIP, cuando la LAN y el servidor SIP se configuran al mismo tiempo, al hacer clic en el botón del timbre de ProMA se iniciará primero el servidor SIP.

9.8.2Uso de la red de área local

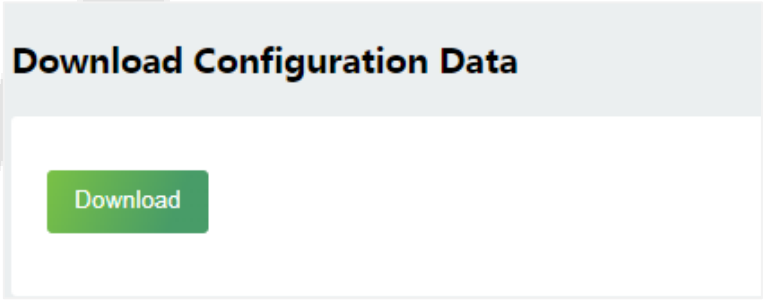
Establezca la dirección IP en la estación interior, toque**Menú**>**Avanzado**>**Red**>**1. Red**>**1. IPv4**.

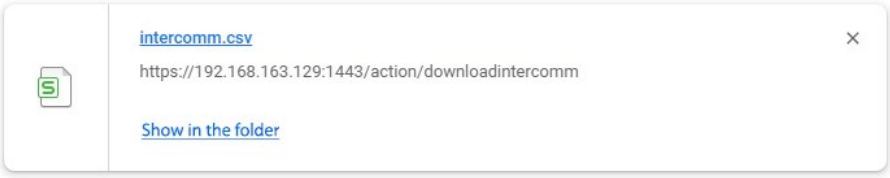


Nota:En LAN, las direcciones IP de la estación interior y ProMA deben estar en el mismo segmento de red.

1.Descargar datos de configuración

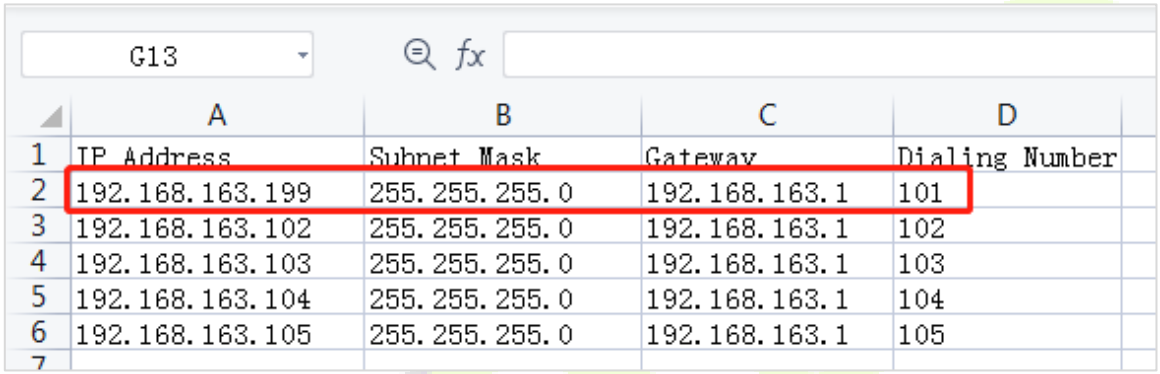
1)Hacer clic**Descargar**para descargar el archivo y configurar los parámetros del videoportero.





2)Abra el archivo descargado y modifique manualmente los parámetros del videoportero según sea necesario. Guarde los parámetros establecidos para sincronizar los parámetros con ProMA.

Nota: La dirección IP/máscara de subred/puerta de enlace debe ser la misma que la estación interior que se va a conectar.

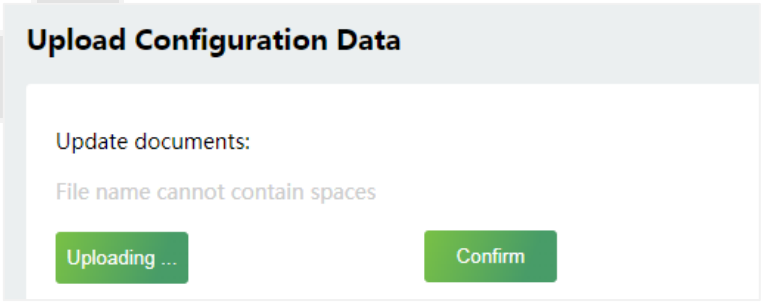


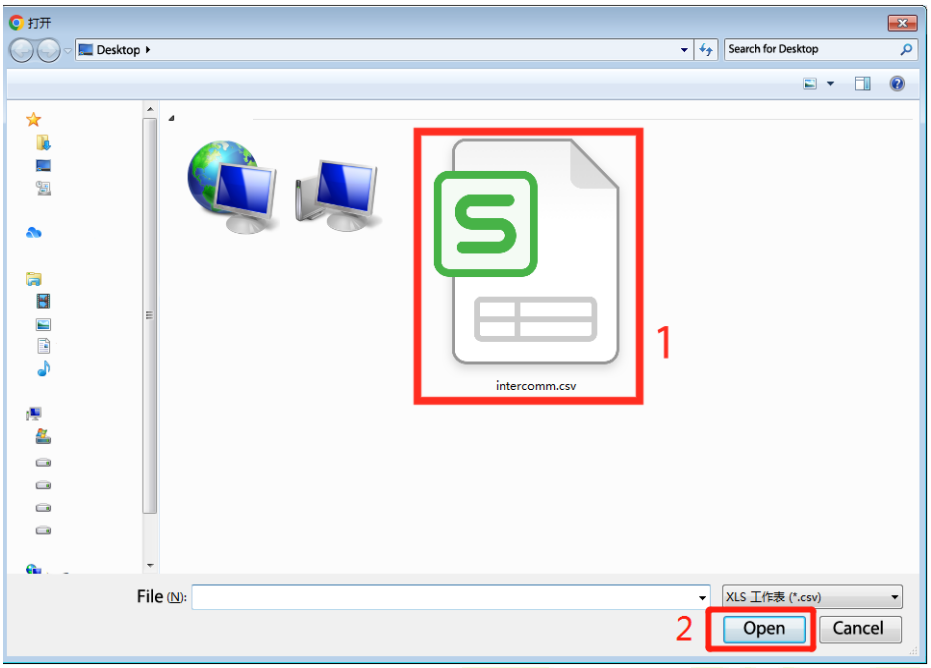
G13

	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

2.Cargar datos de configuración

1)Hacer clic**Subiendo...**para encontrar los parámetros configurados para el videoportero.

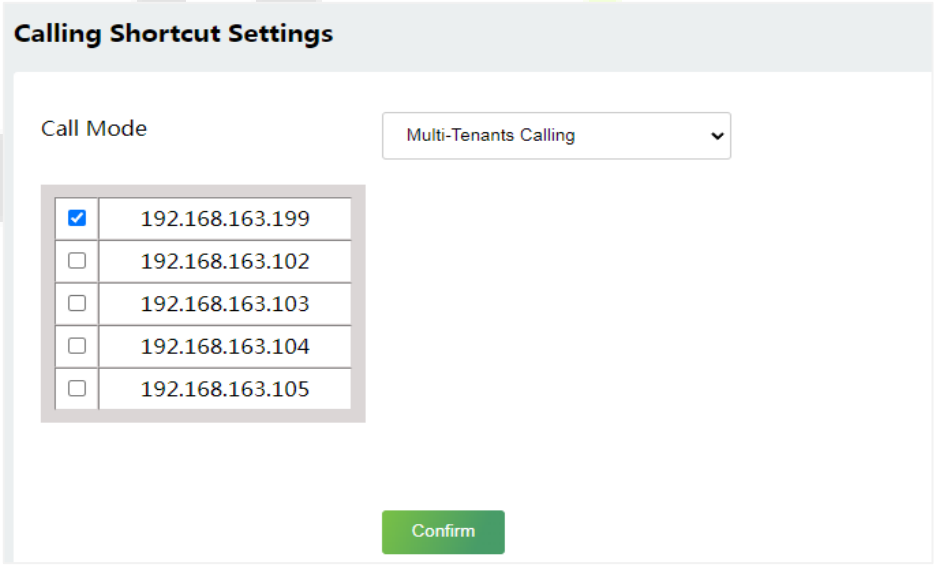




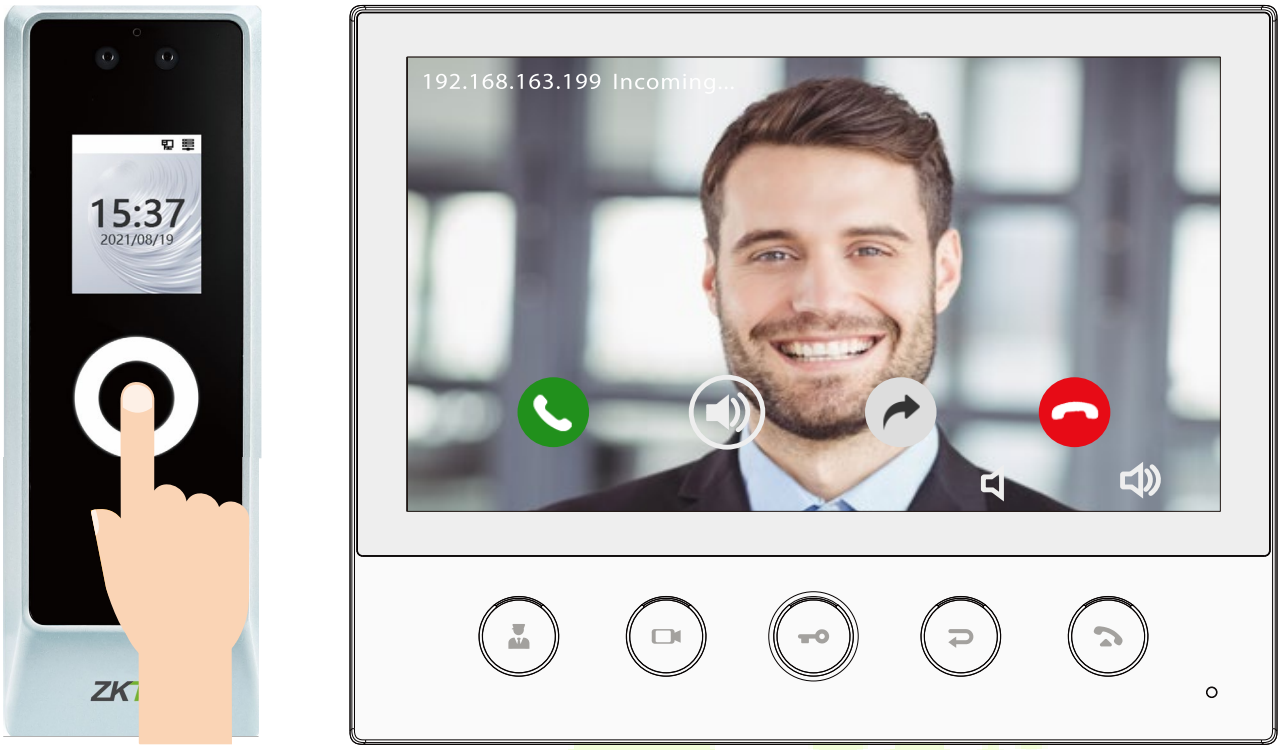
2)Hacer clic**Confirmar**para sincronizar los parámetros con ProMA.

3.Configuración de accesos directos de llamadas

Los parámetros configurados se sincronizarán con el WebServer (ProMA), admitiendo llamadas uno a uno y de múltiples inquilinos.



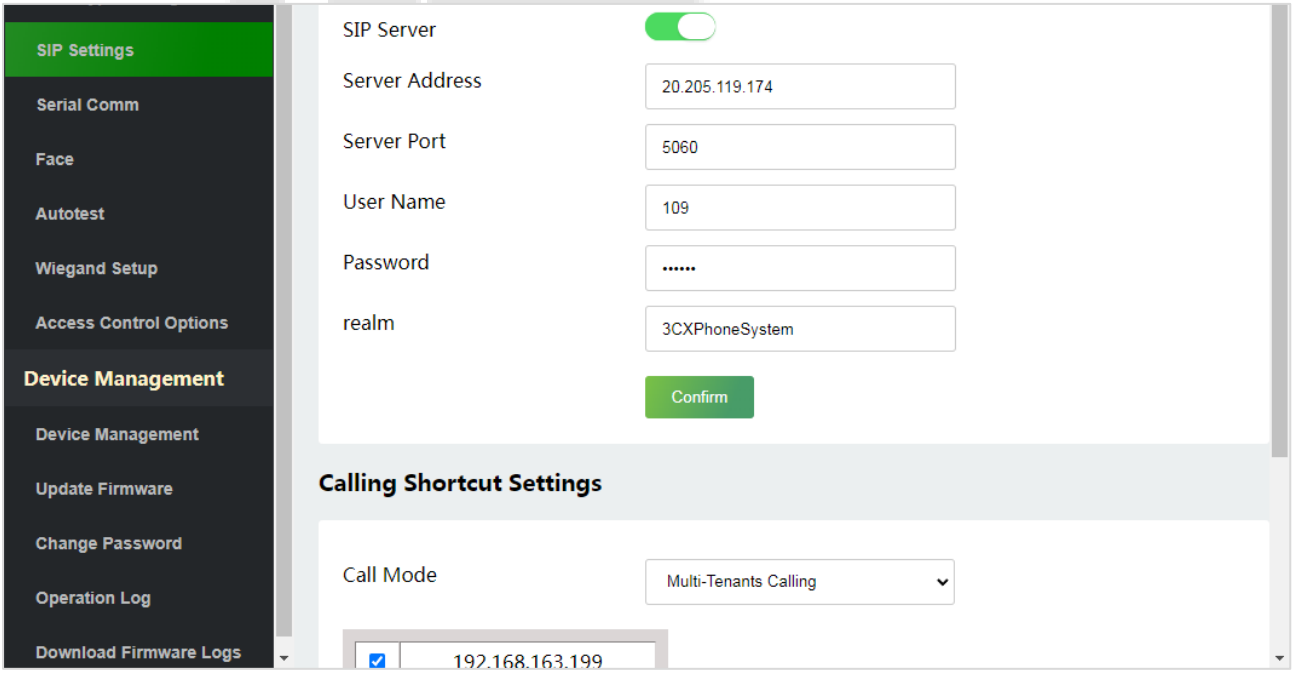
Una vez que la estación interior está configurada con la red, la función de videoportero se puede realizar tocando el icono en el ProMA.



9.8.3Servidor SIP

En WebServer, habilite el servidor SIP e ingrese los parámetros del servidor para la estación interior Vpad A2.

El servidor SIP configurado no se ve afectado por la red y responde más rápidamente. Puede llamar al número de habitación con precisión de acuerdo con los parámetros configurados.

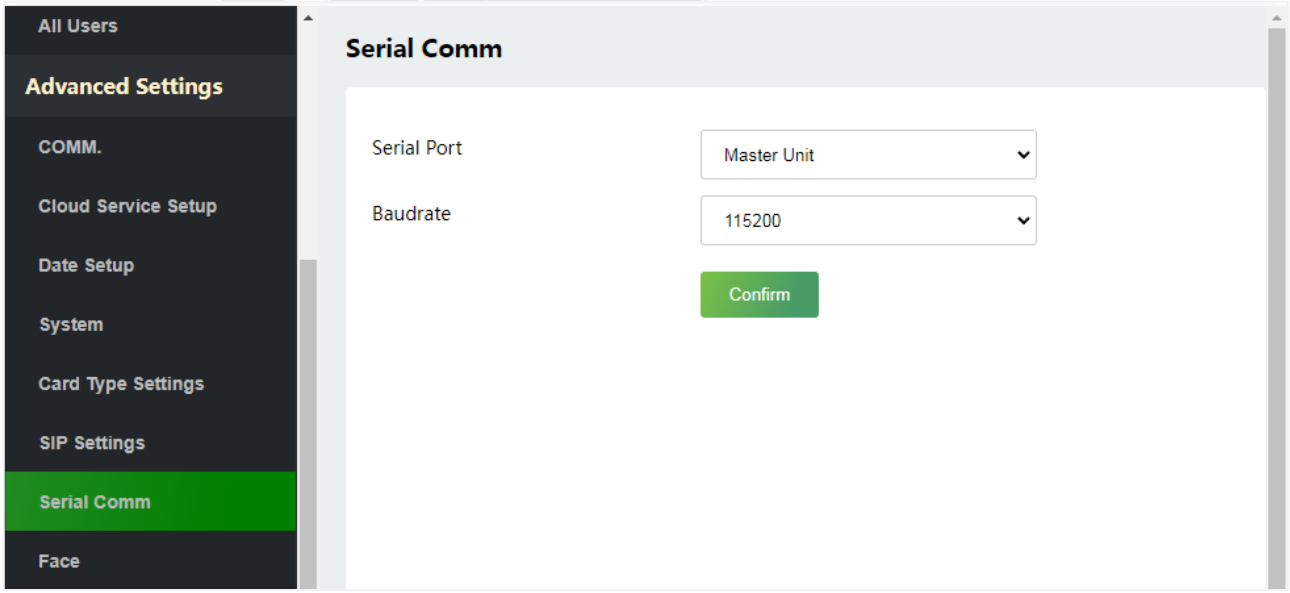


Una vez que el servidor SIP esté configurado correctamente, puede llamar al nombre de cuenta de la estación interior.

Para obtener más información sobre el funcionamiento y el uso de la estación interior, consulte el*manual de usuario de la estación interior*.

9.9Comunicación serie

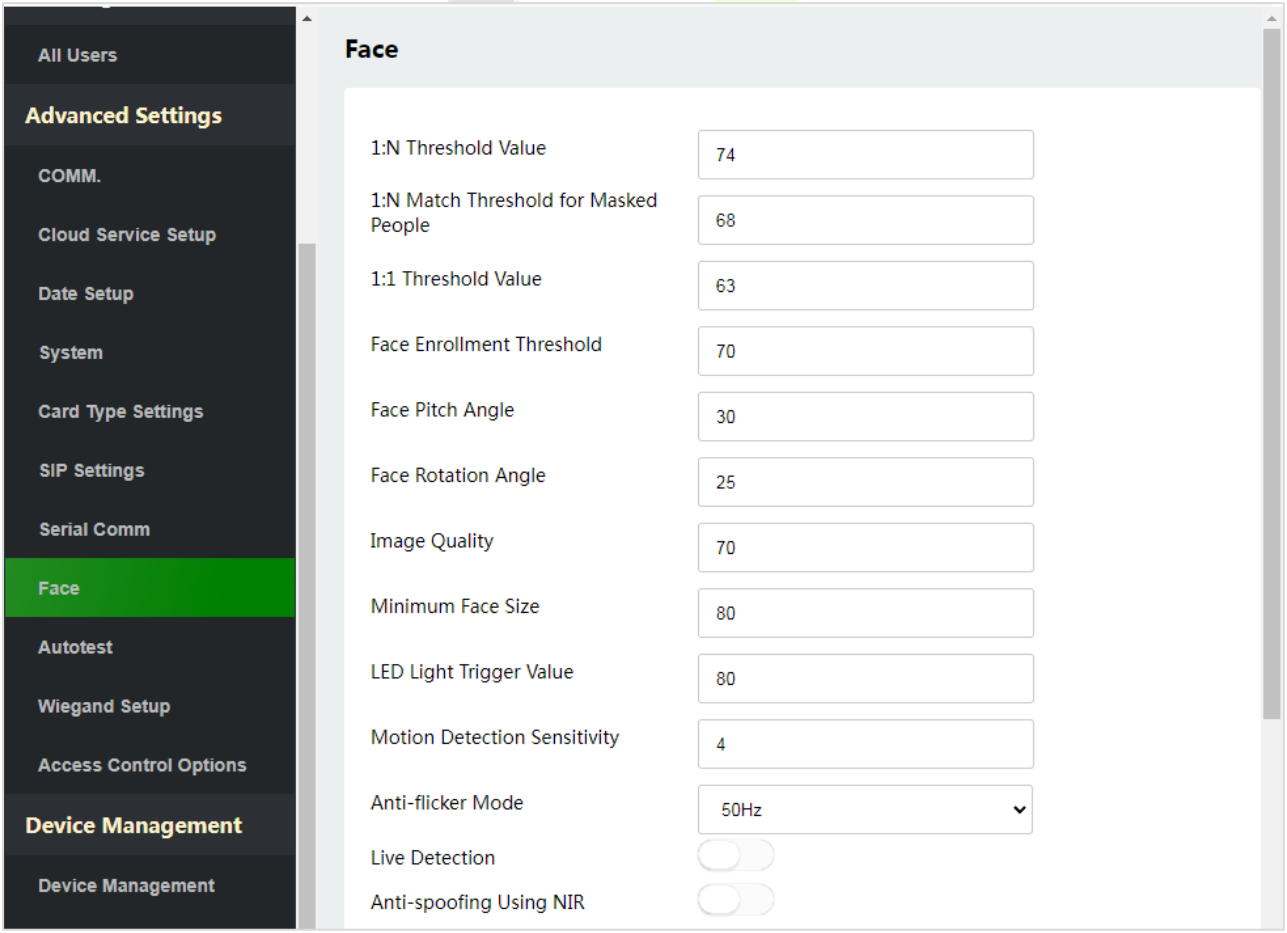
Hacer clic**Comunicación serie**en el servidor web.

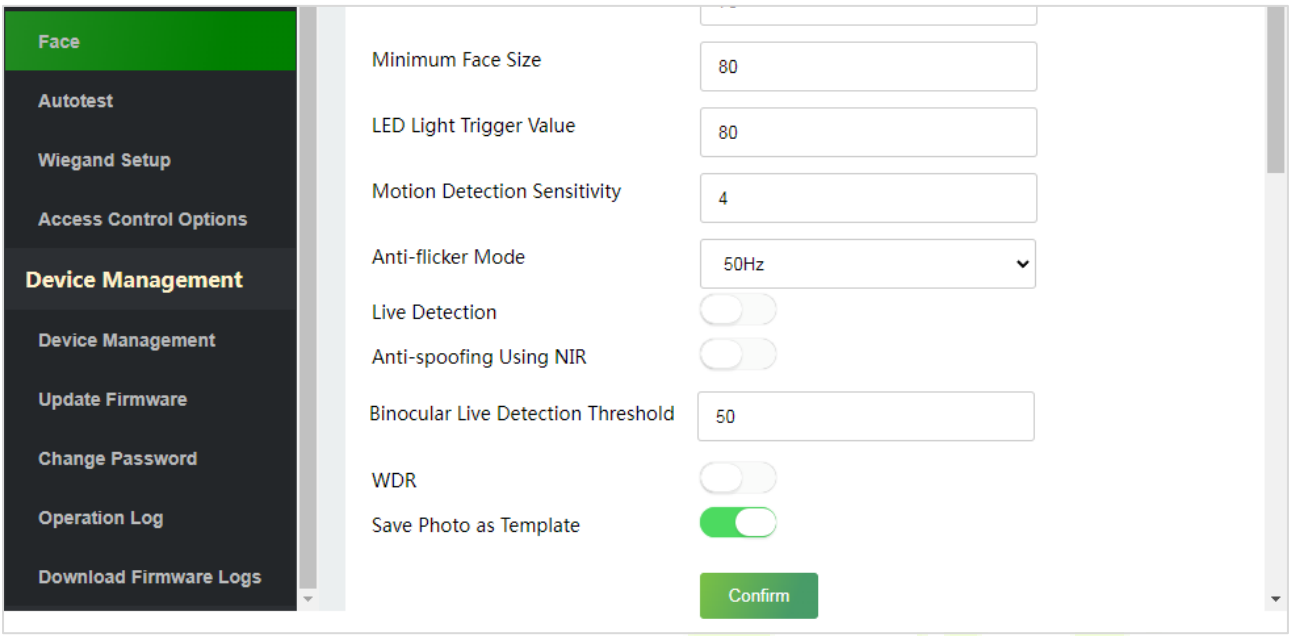


Nombre de la función	Descripción
Puerto serial	**Sin usar:**No hay comunicación con el dispositivo a través del puerto serie. **RS485 (ordenador):**Comunicarse con el dispositivo a través del puerto serie RS485. **Unidad maestra:**Cuando se utiliza RS485 como función de la "unidad maestra", se puede conectar a un lector de tarjetas. **DM10:**Comuníquese con el dispositivo a través del puerto serie DM10.
Velocidad de transmisión	Hay 5 opciones de velocidad de transmisión en las que los datos se comunican con la PC. Ellos son: 115200 (predeterminado), 57600, 38400, 19200 y 9600. Cuanto mayor sea la tasa de baudios, más rápida es la velocidad de comunicación, pero también menos confiable. Por lo tanto, se puede usar una tasa de baudios más alta cuando la distancia de comunicación es corta; cuando la distancia de comunicación es larga, elegir una tasa de baudios más baja es más confiable.

9.10Parámetros de la cara

Hacer clic**Rostro**en el servidor web.





Nombre de la función	Descripción
Valor de umbral 1:N	En el modo de verificación facial, la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas sea mayor que el valor establecido. El valor válido varía de 0 a 100. Cuanto más altos sean los umbrales, menor será la tasa de error de juicio, mayor será la tasa de rechazo y viceversa. Se recomienda establecer el valor predeterminado de 74.
Umbral de coincidencia 1:N para personas enmascaradas	Cuanto más altos sean los umbrales, menor será la tasa de error de juicio, mayor será la tasa de rechazo y viceversa. Se recomienda establecer el valor predeterminado de 68.
Valor de umbral 1:1	En el modo de verificación 1:1, la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y las plantillas faciales del usuario registradas en el dispositivo sea mayor que el valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será la tasa de errores de apreciación y mayor la tasa de rechazo, y viceversa. Se recomienda establecer el valor predeterminado de 63.
Inscripción de rostros Límite	Durante el registro presencial, se utiliza la comparación 1:N para determinar si el usuario ya se ha registrado anteriormente. Cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas es mayor que este umbral, indica que la cara ya ha sido registrada.

Ángulo de inclinación de la cara	La tolerancia del ángulo de inclinación de una cara para el registro y la comparación facial. Si el ángulo de inclinación de una cara supera este valor establecido, el algoritmo lo filtrará, es decir, el terminal lo ignorará, por lo que no se activará ninguna interfaz de registro y comparación.
Ángulo de rotación de la cara	La tolerancia del ángulo de rotación de una cara para el registro y comparación de plantillas faciales. Si el ángulo de rotación de una cara excede este valor establecido, será filtrado por el algoritmo, es decir, ignorado por el terminal, por lo que no se activará ninguna interfaz de registro y comparación.
Calidad de la imagen	Calidad de imagen para registro facial y comparación. Cuanto mayor sea el valor, más clara requiere la imagen.
Tamaño mínimo de la cara	Necesario para el registro facial y la comparación. Si el tamaño mínimo de la figura capturada es más pequeño que este valor establecido, se filtrará y no se reconocerá como una cara. Este valor puede entenderse como la distancia de comparación de caras. Cuanto más lejos esté la persona, más pequeña será la cara y más pequeño será el píxel de la cara obtenido por el algoritmo. Por lo tanto, ajustar este parámetro puede ajustar la distancia de comparación más lejana de las caras. Cuando el valor es 0, la distancia de comparación de caras no está limitada.
Luz LED activada Valor	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, con más frecuencia se encenderá la luz LED.
Detección de movimiento Sensibilidad	Es para establecer el valor de la cantidad de cambio en el campo de visión de una cámara, lo que se conoce como detección de movimiento potencial que activa el terminal desde el modo de espera a la interfaz de comparación. Cuanto mayor sea el valor, más sensible será el sistema, es decir, si se establece un valor mayor, la interfaz de comparación es mucho más fácil y la detección de movimiento se activa con frecuencia.
Modo antiparpadeo	Se utiliza cuando WDR está desactivado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea a la misma frecuencia que la luz.
Detección en vivo	Detectar el intento de falsificación utilizando imágenes de luz visible para determinar si la muestra fuente biométrica proporcionada es realmente una persona (un ser humano vivo) o una representación falsa.
Detección en vivo Límite	Facilita juzgar si la imagen visible capturada es realmente una persona (un ser humano vivo). Cuanto mayor sea el valor, mejor será el rendimiento contra la suplantación de identidad con luz visible.
Uso de la suplantación de identidad RIN	Uso de imágenes de espectros de infrarrojo cercano para identificar y prevenir ataques de fotos y videos falsos.

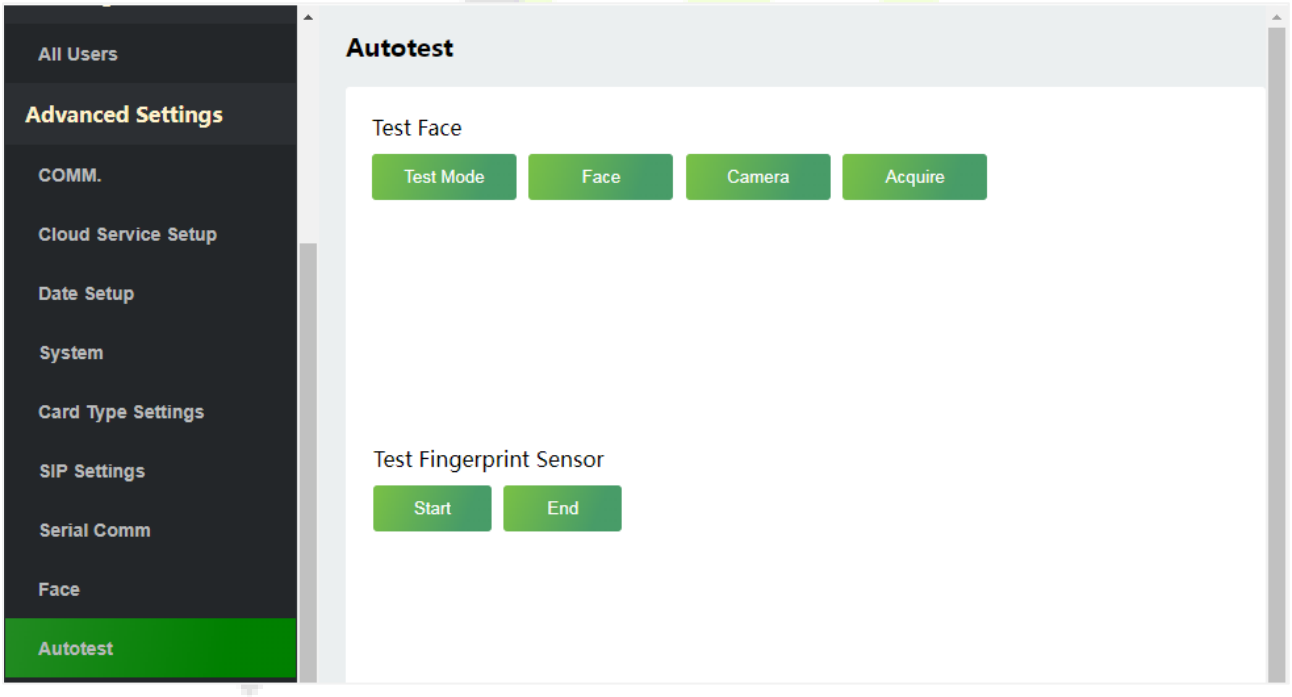
Binocular en vivo Umbral de detección	Facilita juzgar si la imagen visible capturada es realmente una persona (un ser humano vivo). Cuanto mayor sea el valor, mejor será el rendimiento contra la suplantación de identidad con luz visible.
WDR	Amplio rango dinámico (WDR), que equilibra la luz y amplía la visibilidad de la imagen para videos de vigilancia en escenas de iluminación de alto contraste y mejora la identificación de objetos en entornos brillantes y oscuros.
Guardar foto como Plantilla	Seleccione si desea guardar la foto registrada.

Nota: El ajuste inadecuado de los parámetros de exposición y calidad puede afectar gravemente a la rendimiento del dispositivo. Ajuste el parámetro de exposición solo bajo la guía del personal de servicio posventa de nuestra empresa.

9.11 Auto prueba

Hacer clic**Auto prueba**en el servidor web.

Permite que el sistema pruebe automáticamente si las funciones de varios módulos funcionan normalmente.



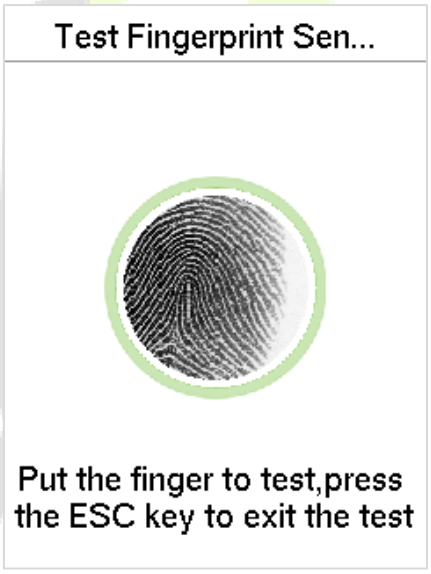
9.11.1 Cara de prueba

Hacer clic**Modo de prueba**, el dispositivo ProMA mostrará la interfaz Test Face en tiempo real, haga clic en**Fin de la prueba**para salir de la prueba.

Después de abrir el modo de prueba, la esquina superior izquierda de la pantalla del dispositivo mostrará el valor de la cara en tiempo real, cuanto mayor sea el valor, mejor será la calidad de la cara.

9.11.2Prueba del sensor de huellas dactilares

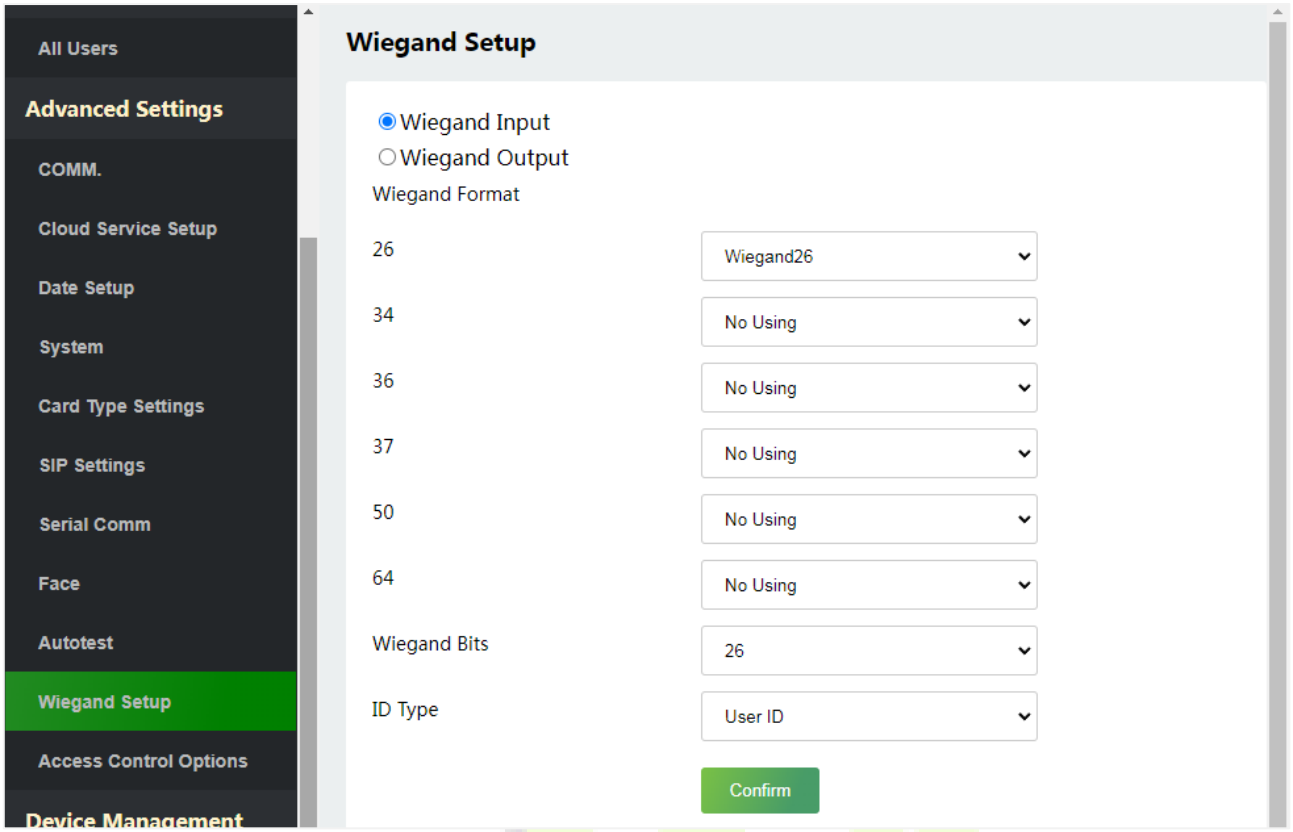
Hacer clic**Comenzar**, el dispositivo ProMA mostrará la interfaz Test Fingerprint en tiempo real, haga clic en**Fin**para salir de la prueba.

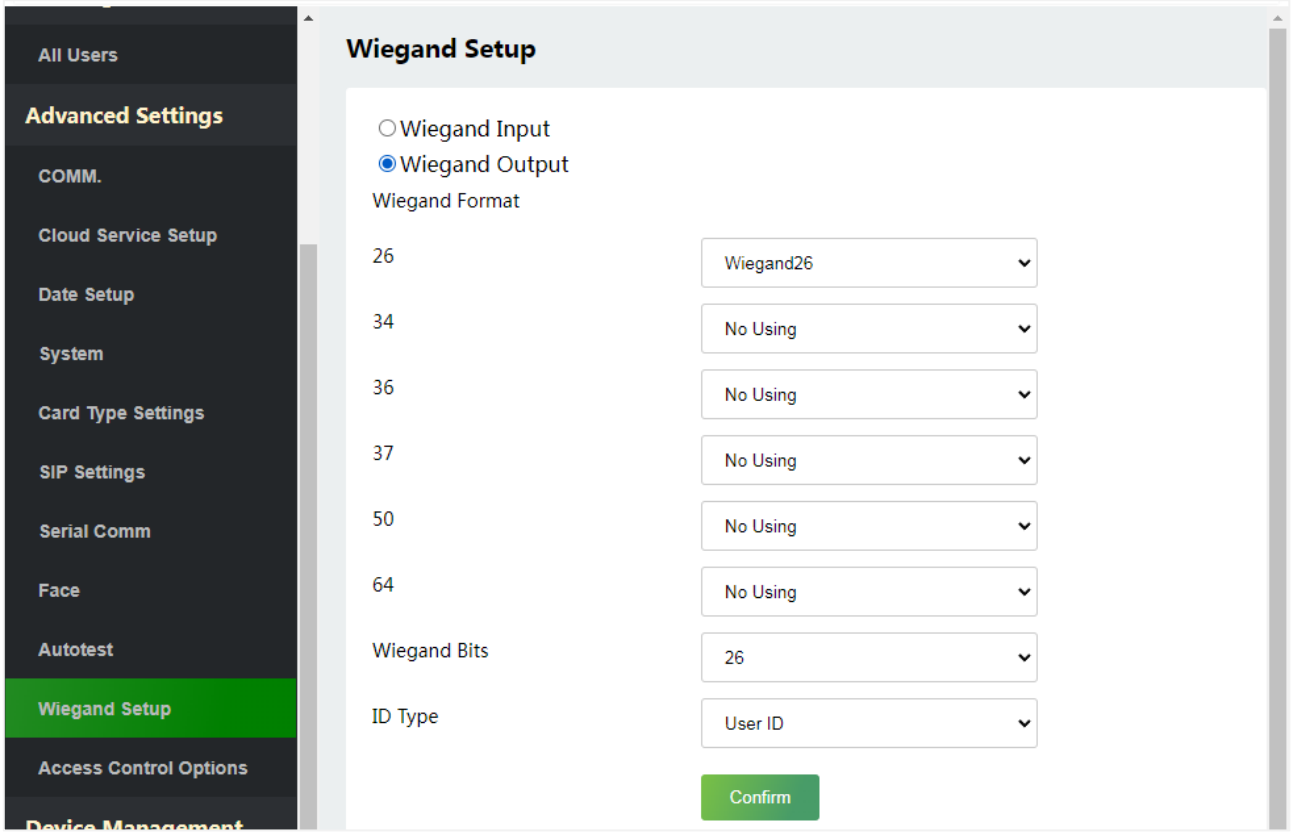


9.12Configuración Wiegand

Hacer clic**Configuración Wiegand**en el servidor web.

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





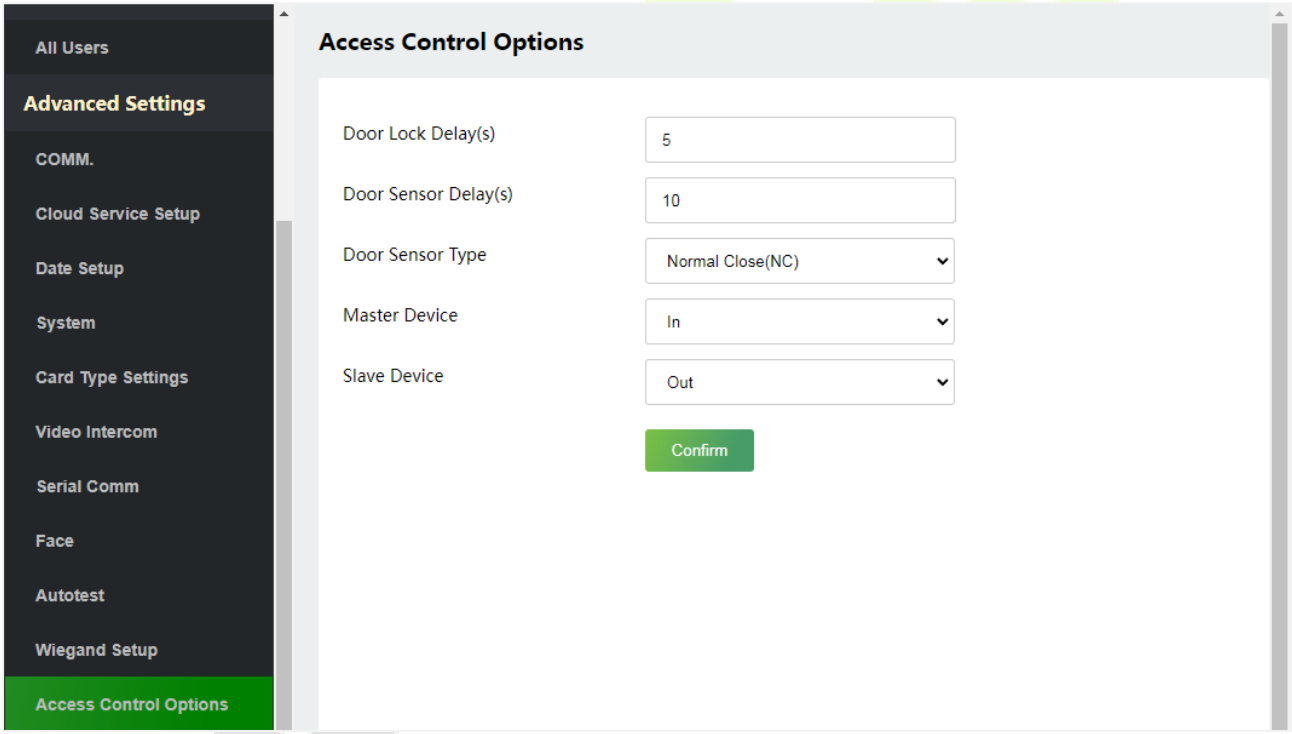
Nombre de la función	Descripción
Formato Wiegand	Su valor puede ser de 26 bits, 34 bits, 36 bits, 37 bits, 50 bits y 60 bits.
Bits Wiegand	El número de bits de los datos Wiegand.
tipo de identificación	Seleccione entre el ID de usuario y el número de tarjeta.

9.13Opciones de control de acceso

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

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

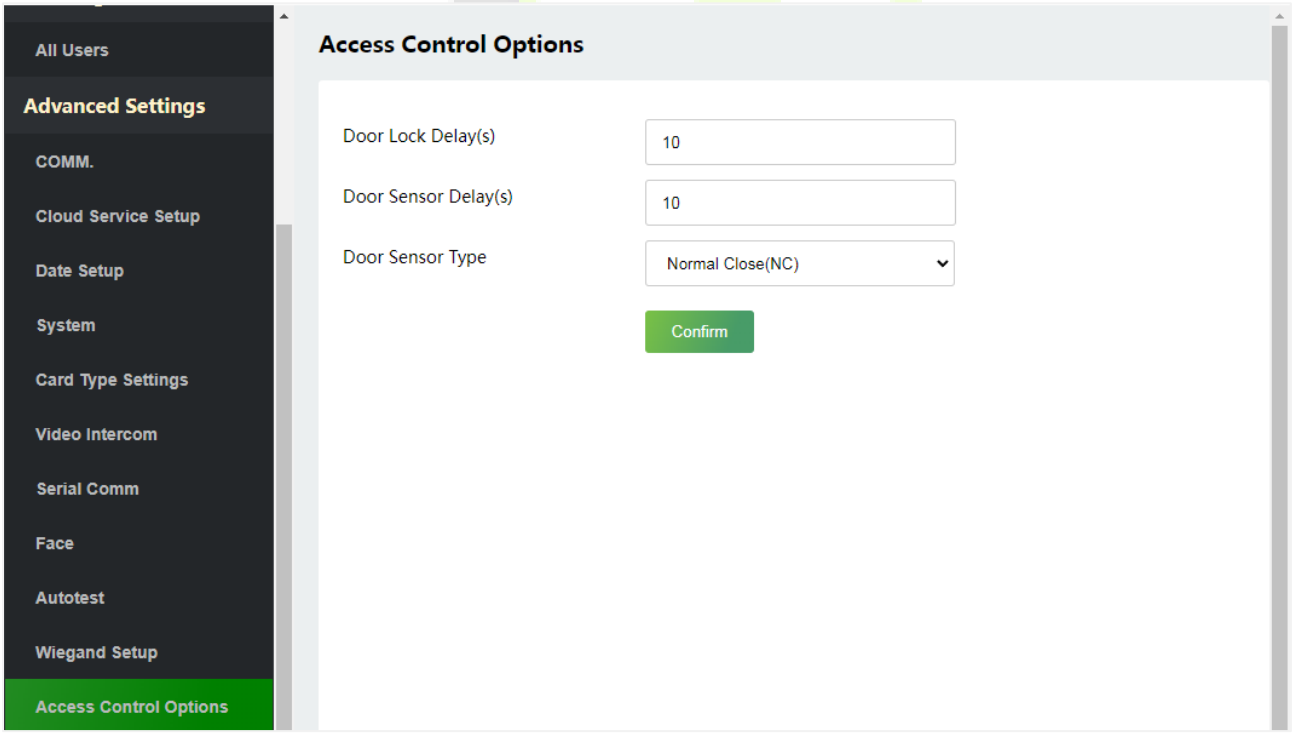
Terminal de control de acceso:



Nombre de la función	Descripción
Demora(s) de bloqueo de puerta	La cantidad de tiempo que el dispositivo controla que la cerradura eléctrica esté en estado de desbloqueo. Valor válido: 1~99 segundos; 0 segundos representa la desactivación de la función.
Retardo(s) del sensor de puerta	Si la puerta no está bloqueada y se deja abierta durante un tiempo determinado (retraso del sensor de puerta), se activará una alarma. El valor válido de Demora del sensor de puerta oscila entre 1 y 255 segundos.

Tipo de sensor de puerta	Hay tres tipos de sensores:**Ninguno**,**normalmente abierto**, y**Normal Cerrado**. **Ninguno:**Significa que el sensor de la puerta no está en uso. **Normalmente abierto:**Significa que la puerta siempre se deja abierta cuando hay energía eléctrica. **Normalmente cerrado:**Significa que la puerta siempre se deja cerrada cuando hay energía eléctrica.
Dispositivo maestro	Mientras configura los dispositivos maestro y esclavo, puede configurar el estado del maestro como**Afuera**o**En**. **Afuera:**Un registro de verificación en el dispositivo maestro es un registro de salida. **En:**Un registro de verificación en el dispositivo maestro es un registro de registro.
Dispositivo esclavo	Mientras configura los dispositivos maestro y esclavo, puede configurar el estado del esclavo como**Afuera**o**En**. **Afuera:**Un registro de verificación en el dispositivo esclavo es un registro de salida. **En:**Un registro de verificación en el dispositivo esclavo es un registro de registro.

Terminal de Asistencia:

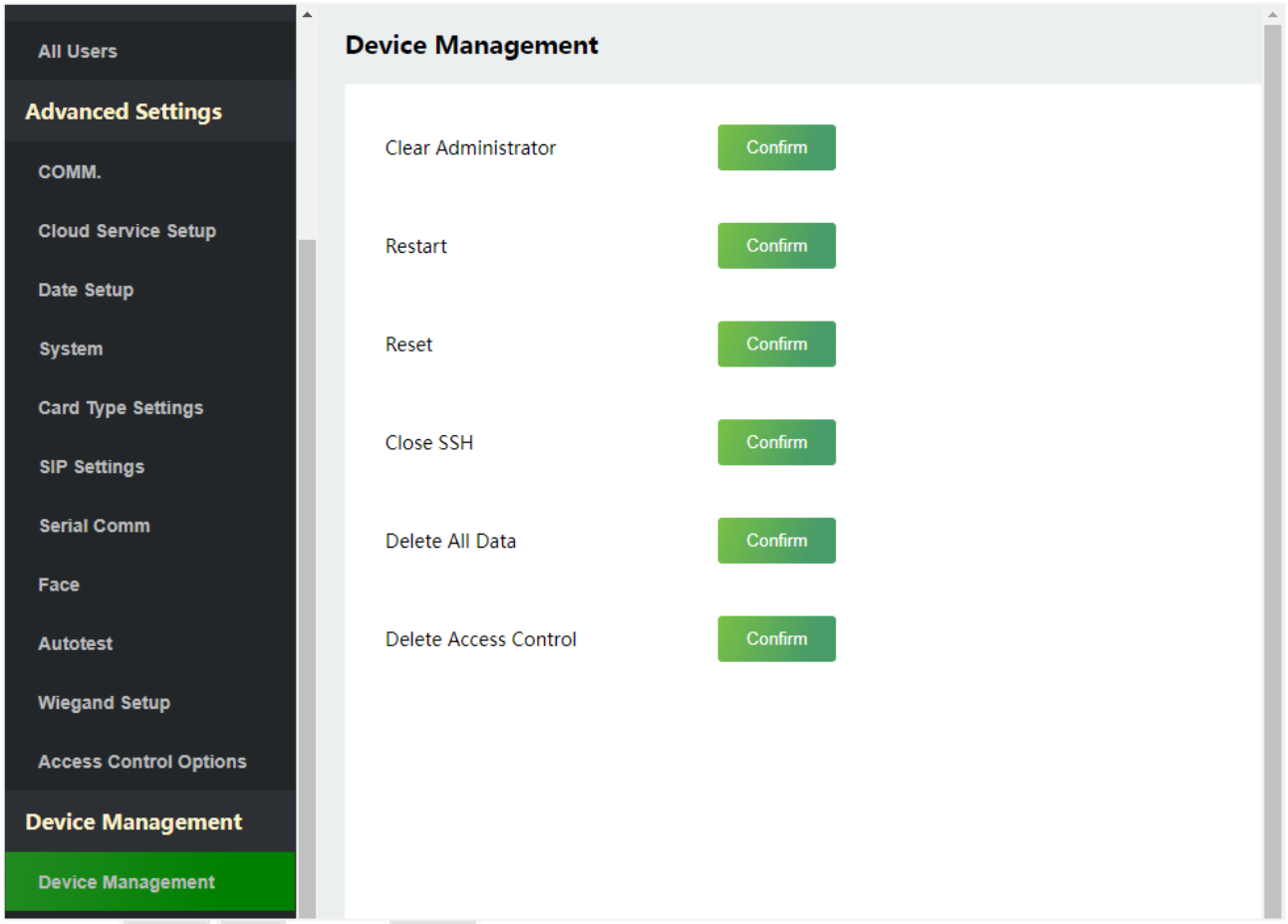


Nombre de la función	Descripción
Demora(s) de bloqueo de puerta	La cantidad de tiempo que el dispositivo controla que la cerradura eléctrica esté en estado de desbloqueo. Valor válido: 1~255 segundos; 0 segundos representa la desactivación de la función.
Retardo(s) del sensor de puerta	Si la puerta no está bloqueada y se deja abierta durante un tiempo determinado (retraso del sensor de puerta), se activará una alarma. El valor válido de Demora del sensor de puerta oscila entre 1 y 255 segundos.
Tipo de sensor de puerta	Hay tres tipos de sensores:**Ninguno**,**normalmente abierto**, y**Normal Cerrado**. **Ninguno:**Significa que el sensor de la puerta no está en uso. **Normalmente abierto:**Significa que la puerta siempre se deja abierta cuando hay energía eléctrica. **Normalmente cerrado:**Significa que la puerta siempre se deja cerrada cuando hay energía eléctrica.

10Gestión de dispositivos

10.1Gestión de dispositivos

Hacer clic**Gestión de dispositivos**en el servidor web.



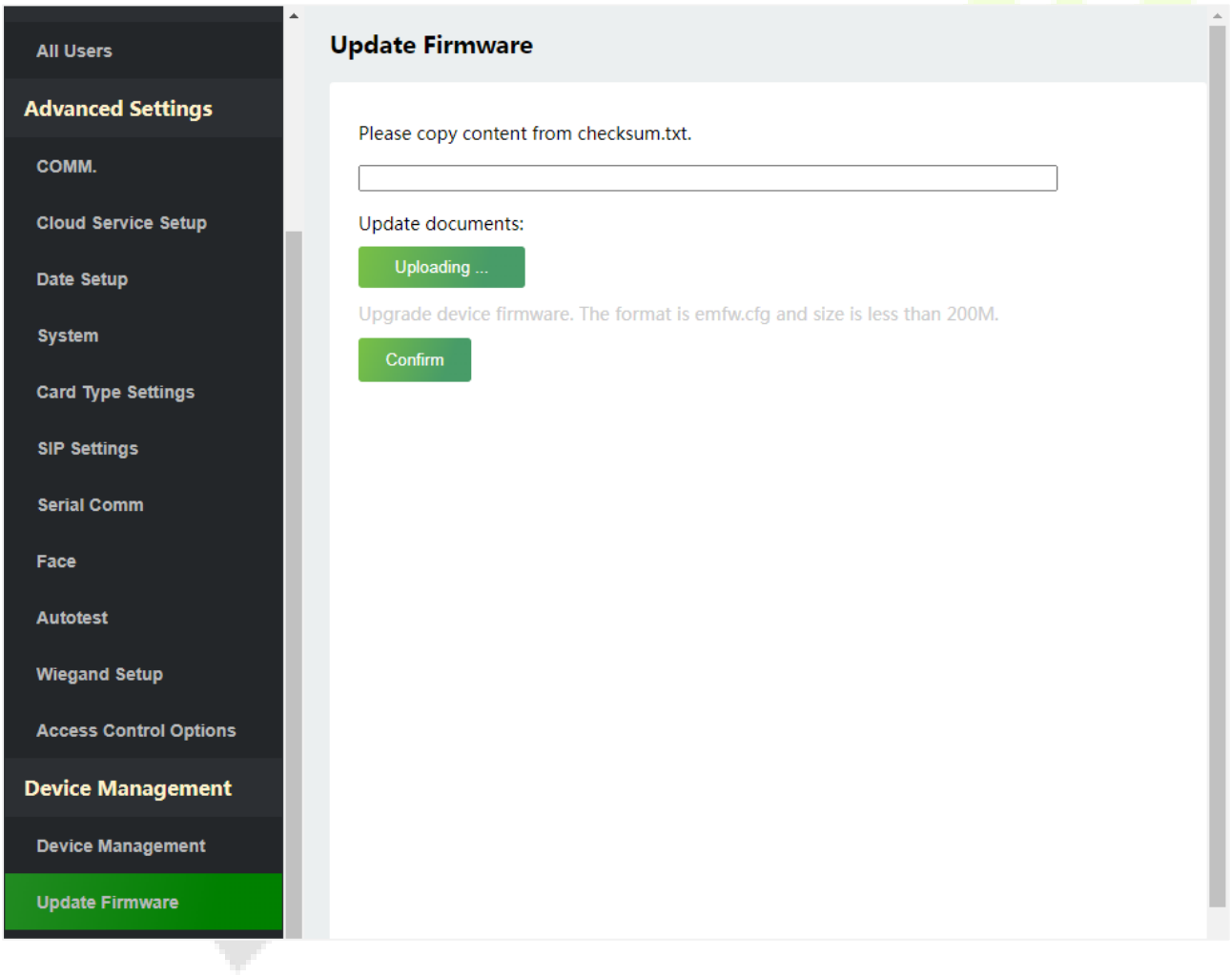
Nombre de la función	Descripción
Borrar administrador	Elija si desea cambiar el superadministrador a un usuario normal.
Reanudar	Elija si desea reiniciar el dispositivo.
Reiniciar	La función Restablecer restaura la configuración del dispositivo, como la comunicación y la configuración del sistema, a la configuración predeterminada de fábrica (esta función no borra los datos de usuario registrados). ***Nota:***Después del reinicio, la IP del dispositivo se restaura a la original 192.168.1.201, consulte9.1 Configuración de comunicación para modificar la IP.

Cerrar SSH	SSH se usa para ingresar al fondo del dispositivo para mantenimiento, elija si desea cerrar el SSH.
Eliminar todos los datos	Eliminar la información y los registros de asistencia/acceso de todos los usuarios registrados.
Eliminar control de acceso	Para eliminar los datos de control de acceso del ProMA.

10.2Actualizar firmware

Hacer clic**Actualizar firmware**en el servidor web.

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

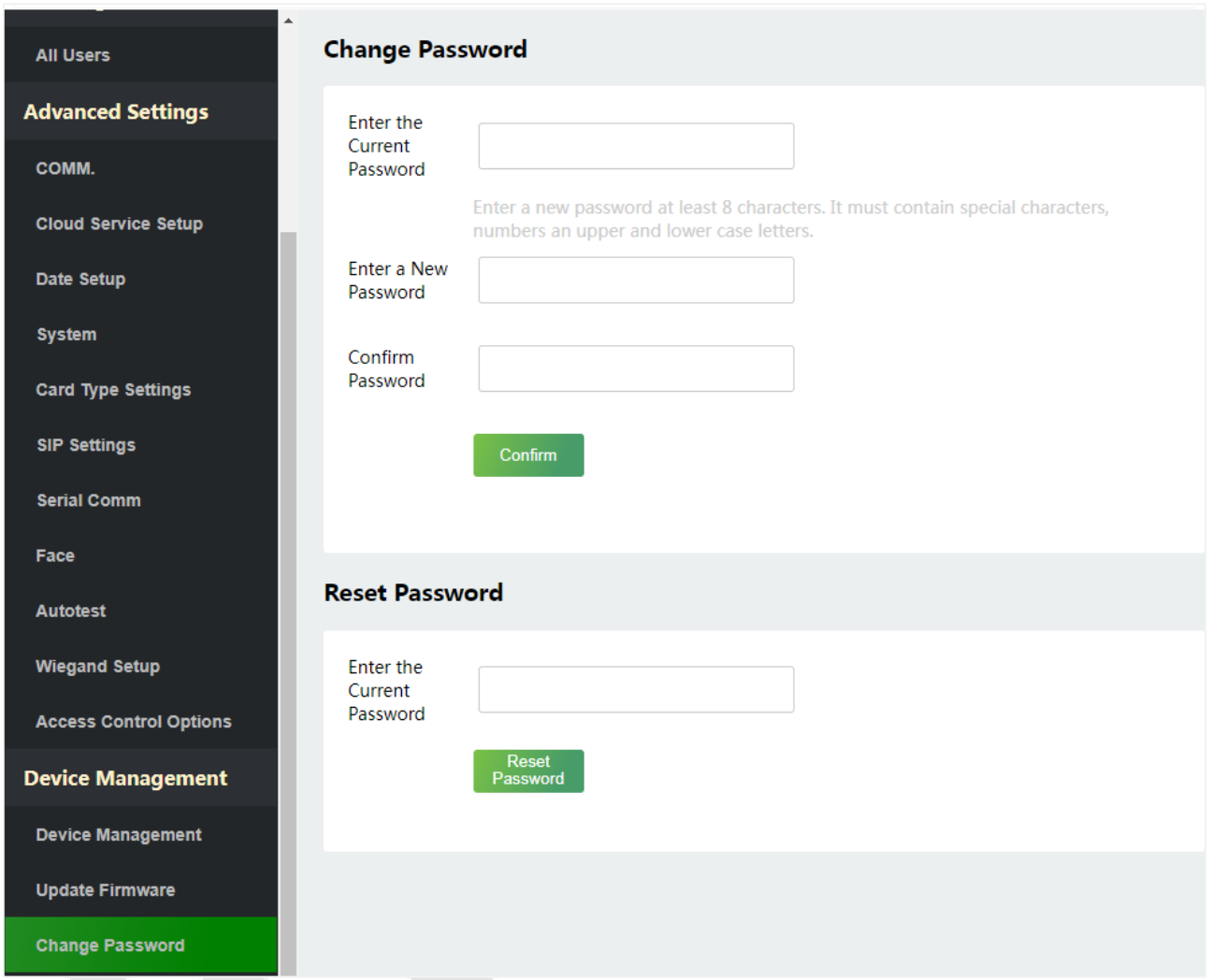


Nota:Si necesita el archivo de actualización, comuníquese con nuestro soporte técnico. La actualización del firmware no se recomienda en circunstancias normales.

10.3Cambiar la contraseña

Hacer clic**Cambiar la contraseña**en el servidor web.

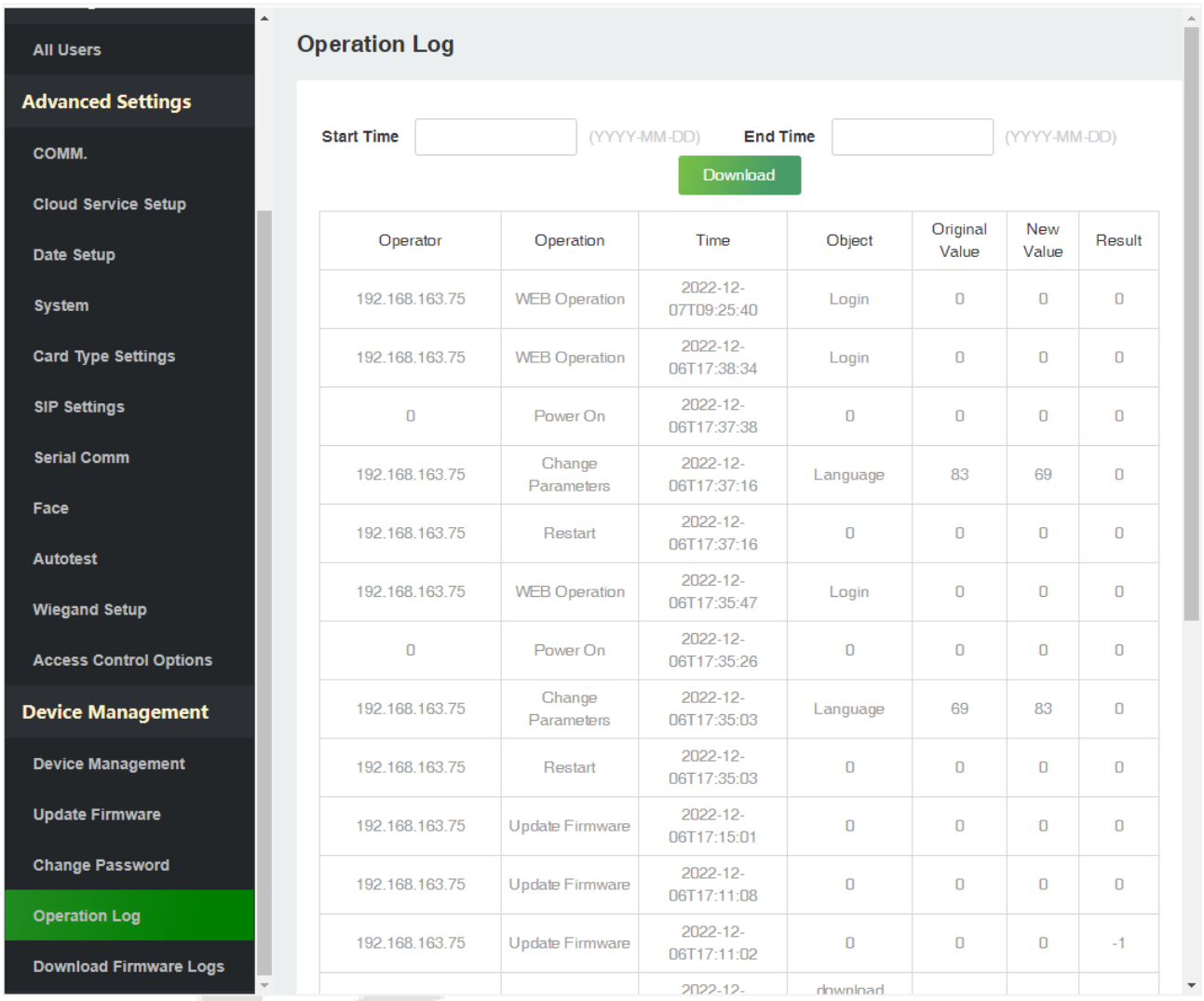
En esta interfaz, puede cambiar la contraseña y restablecer la contraseña de WebServer.



10.4Registro de operaciones

Hacer clic**Registro de operaciones**en el servidor web.

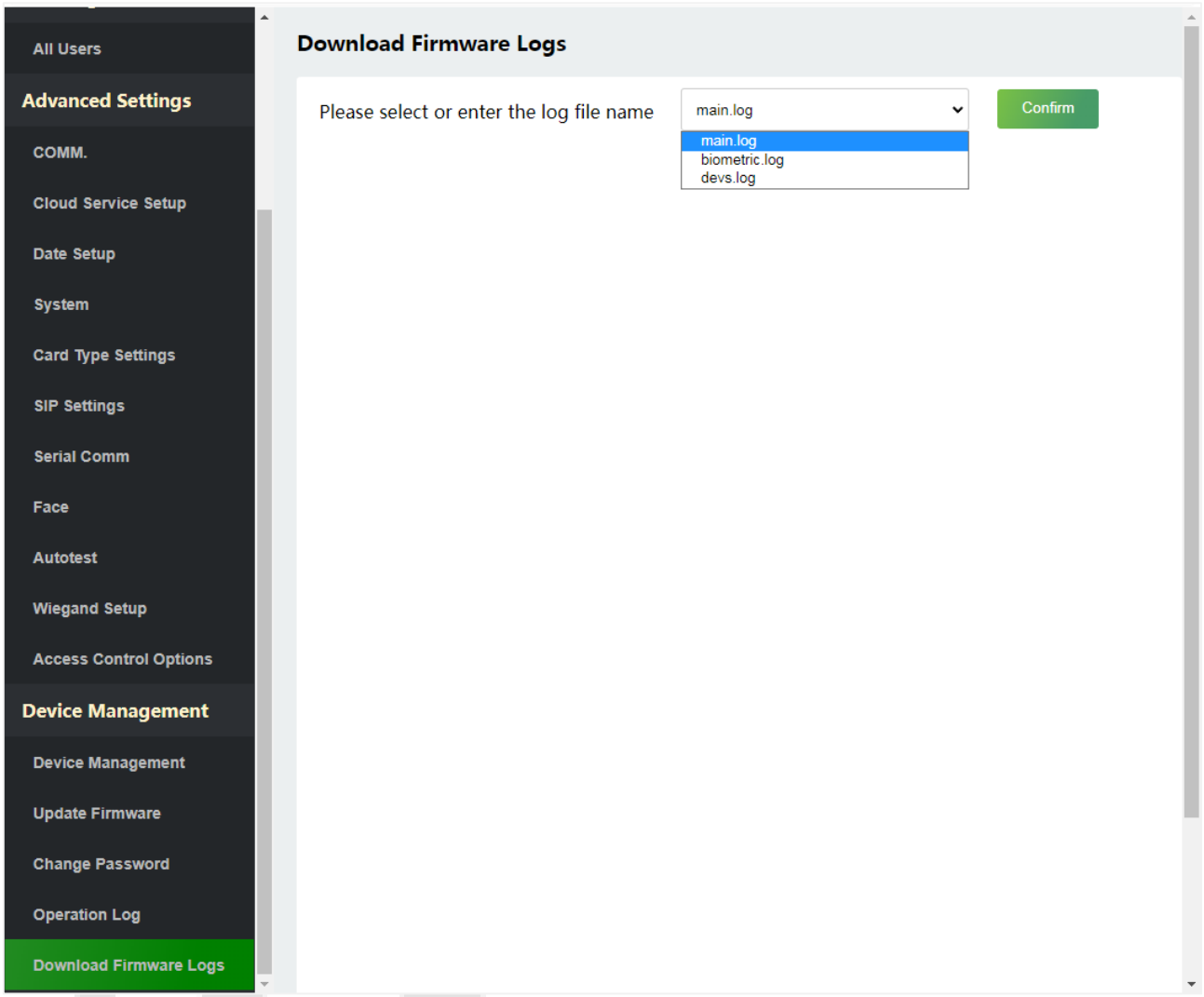
Se guardan todos los registros de operaciones del usuario en el dispositivo o WebServer. Los usuarios pueden buscar y descargar estos registros por tiempo.



10.5Descargar registros de firmware

Hacer clic**Registro de operaciones**en el servidor web.

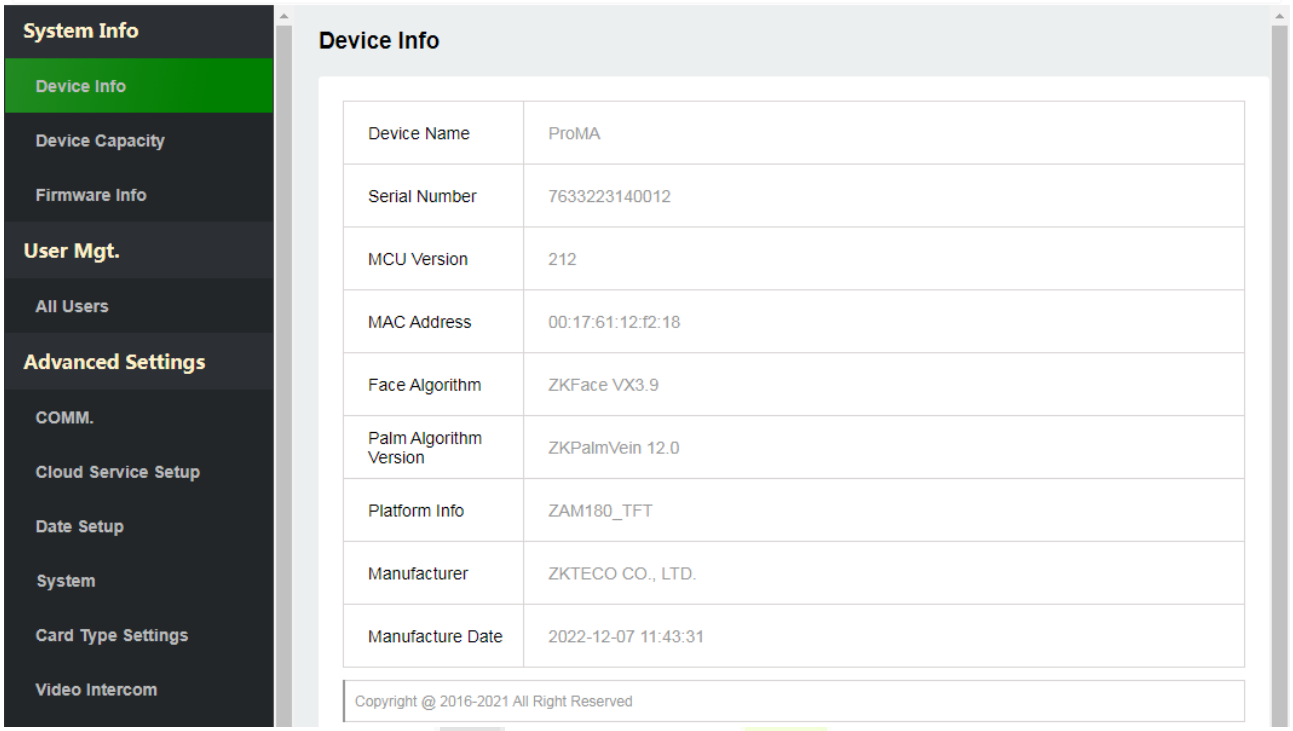
En esta interfaz, puede seleccionar descargar el registro principal, biométrico o de desarrollo.

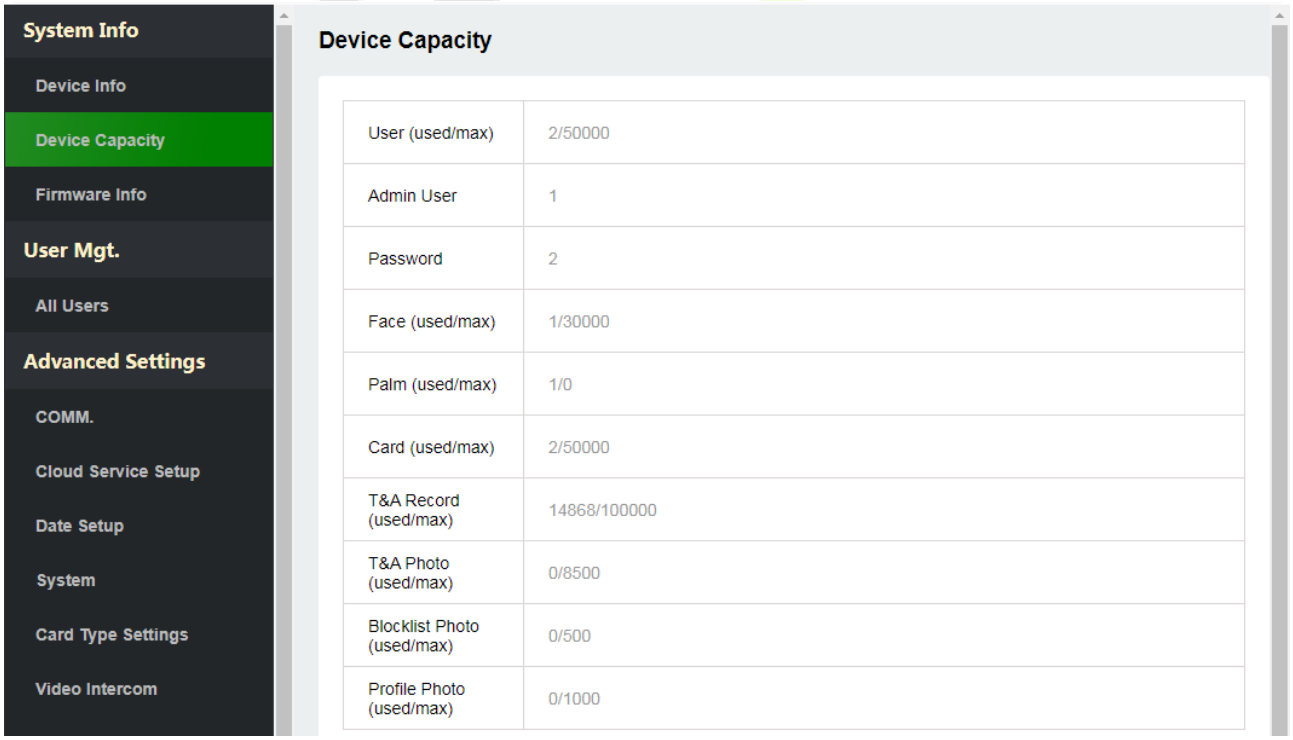


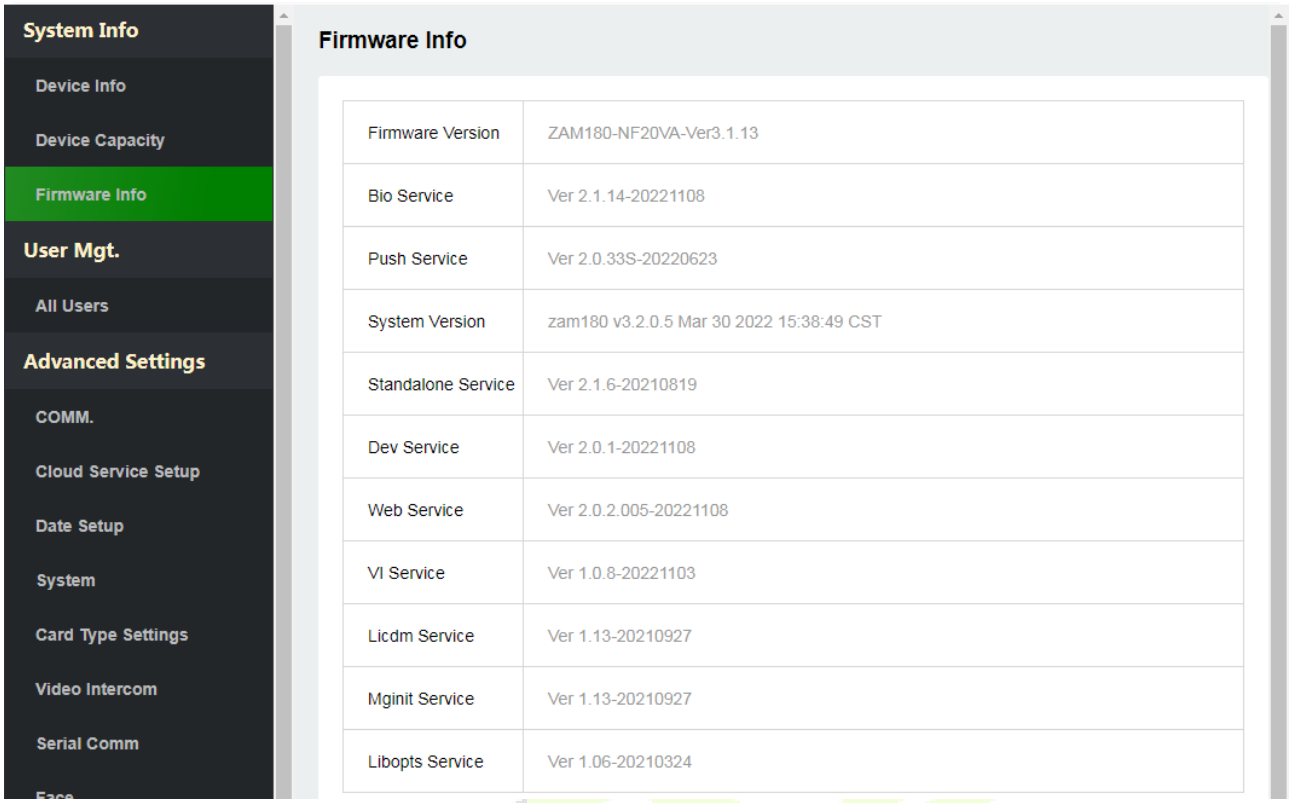
11 Información del sistema

Hacer clic**Información del sistema**en el servidor web.

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







Nombre de la función	Descripción
Información del dispositivo	Muestra el nombre del dispositivo, número de serie, versión de MCU, dirección MAC, huella digital★ y la información de la versión del algoritmo facial, la plataforma y la información del fabricante.
Capacidad del dispositivo	Muestra el almacenamiento de usuario, la contraseña y la palma de la mano del dispositivo actual.★,huella dactilar ★,almacenamiento de tarjetas y rostros, administradores, registros de asistencia, asistencia y fotos de listas prohibidas.
firmware Información	Muestra la versión del firmware y otra información de la versión del dispositivo.

12 Conéctese al software ZKBio CVSecurity

12.1 Establecer la dirección de comunicación

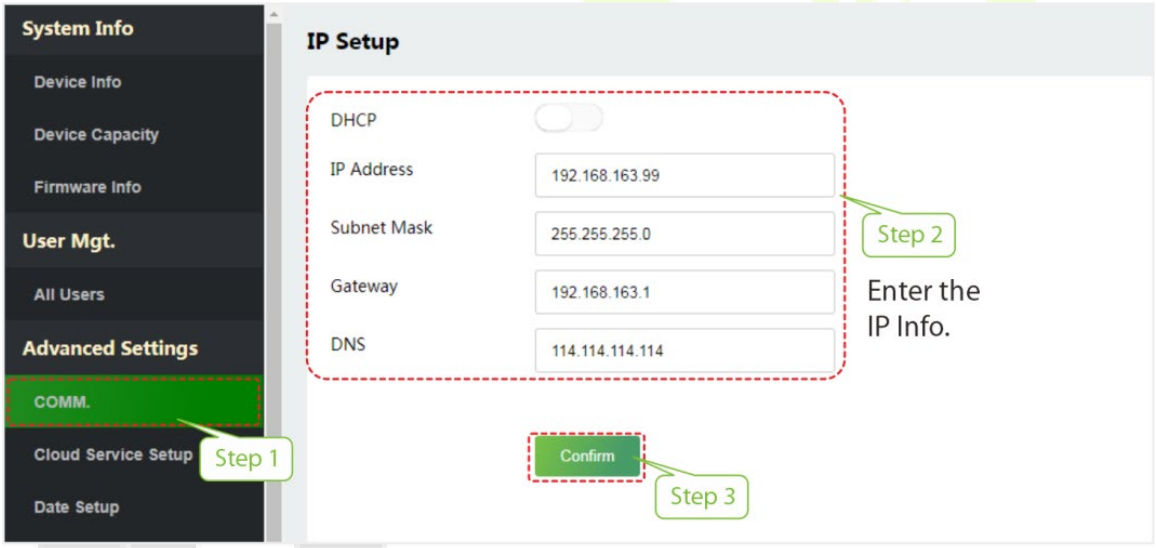
1. Hacer clic **COM.** > **Configuración de IP** en el WebServer para establecer la dirección IP y la puerta de enlace del dispositivo.

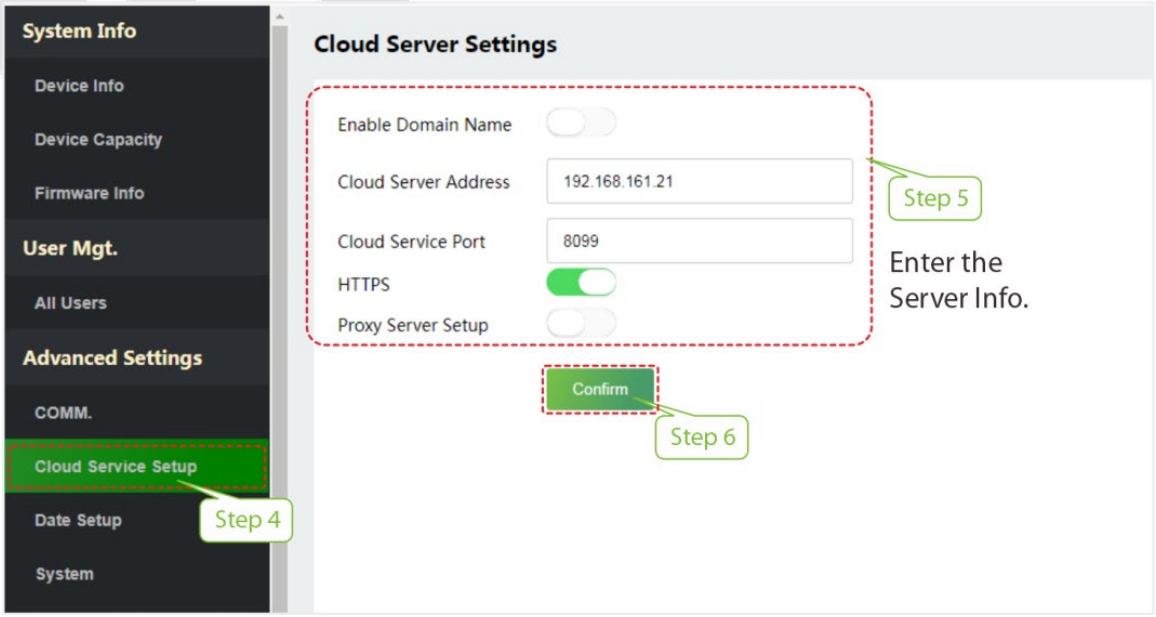
   (***Nota:*** La dirección IP debe poder comunicarse con el servidor ZKBio CVSecurity, preferiblemente en el mismo segmento de red con la dirección del servidor)

2. En el servidor web, haga clic en **Configuración del servidor en la nube** para establecer la dirección del servidor y el puerto del servidor.

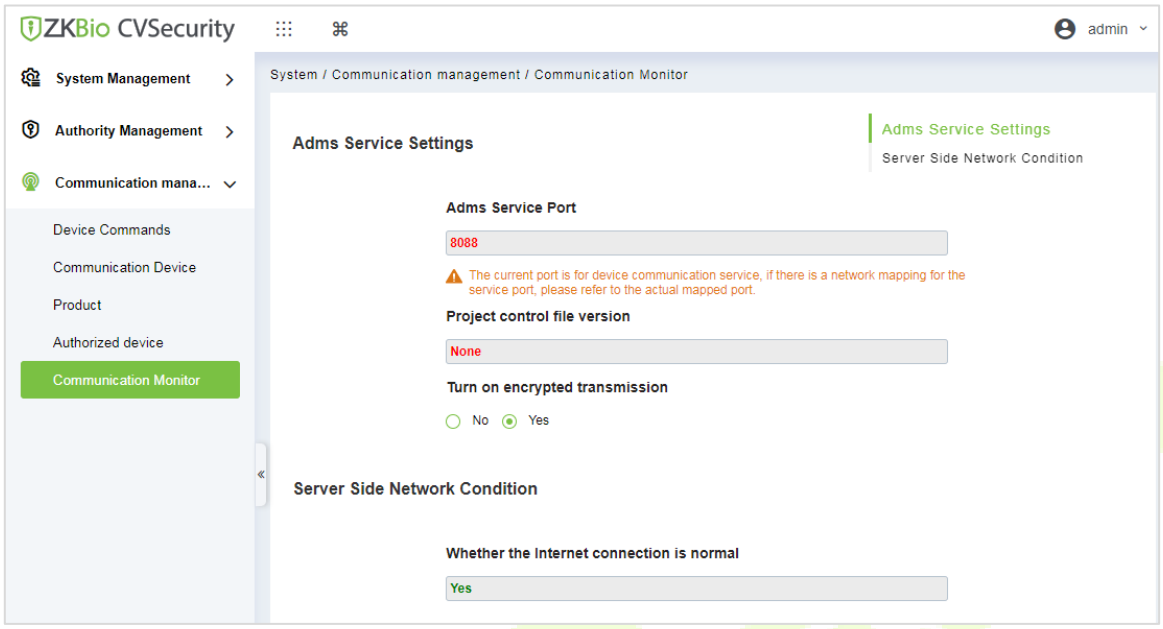
   Dirección del servidor: Establezca la dirección IP a partir del servidor ZKBio CVSecurity. **Puerto de servicio:**

   Configure el puerto del servidor a partir de ZKBio CVSecurity (el valor predeterminado es 8808).





3.Inicie sesión en el software ZKBio CVSecurity, haga clic en**Sistema**>**Gestión de la comunicación**> **monitor de comunicación**para configurar el puerto de servicio ADMS, como se muestra en la siguiente figura:



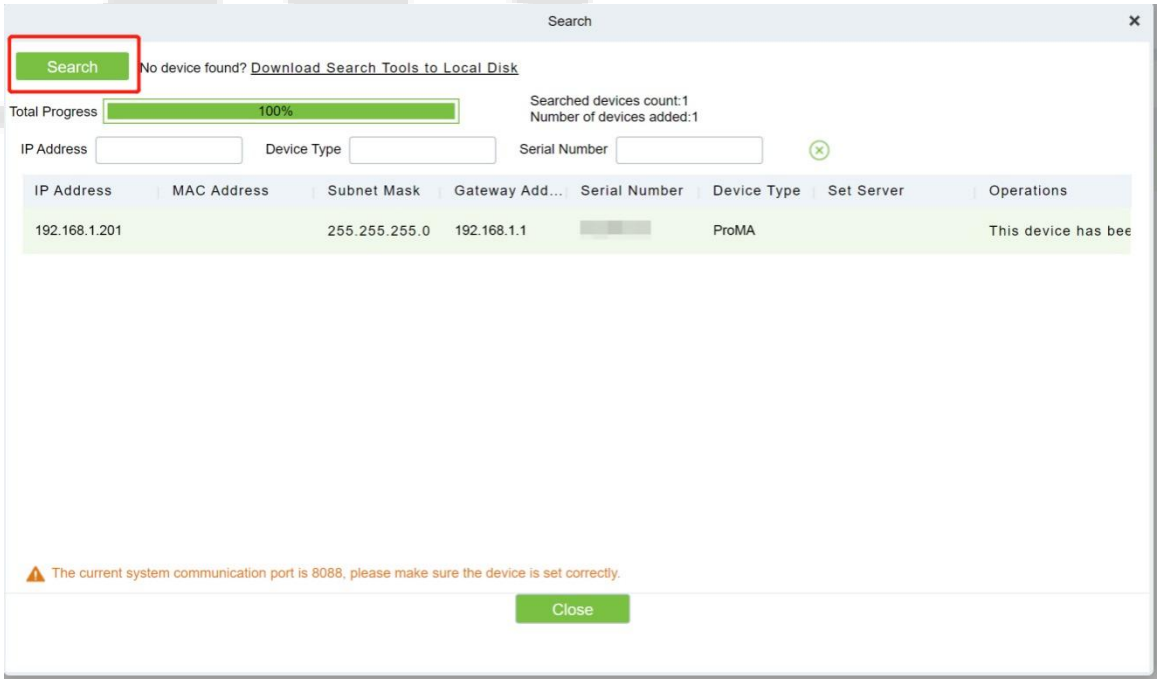
12.2Agregar dispositivo en el software

Agregue el dispositivo buscando. El proceso es el siguiente:

1) Hacer clic**Acceso**>**Dispositivo**>**Buscar**, para abrir la interfaz de búsqueda en el software.

2) Hacer clic**Buscar**, y le pedirá**buscando**.....

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

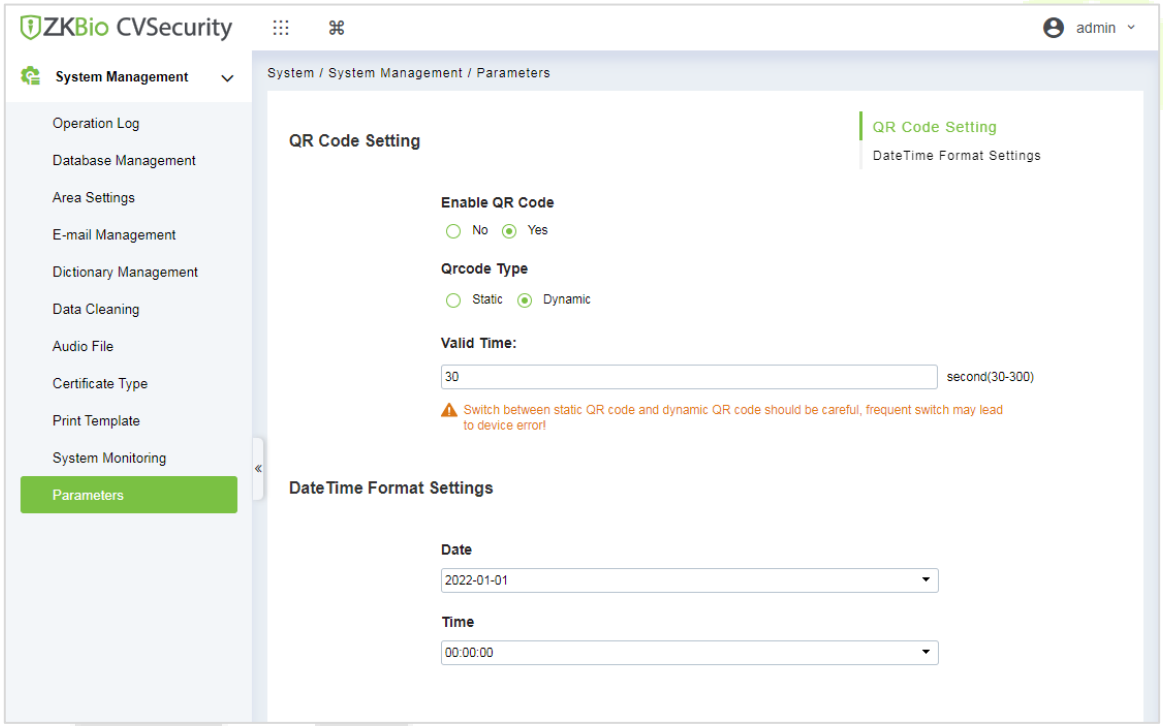


Hacer clic**Agregar**en la columna de operación, aparecerá una nueva ventana. Seleccione el tipo de icono, el área y Agregar al nivel de cada menú desplegable y haga clic en**DE ACUERDO**para agregar el dispositivo.

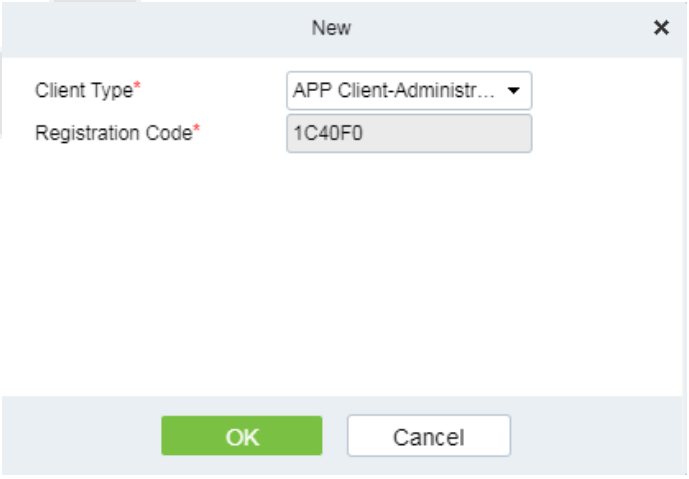
12.3Credencial móvil★

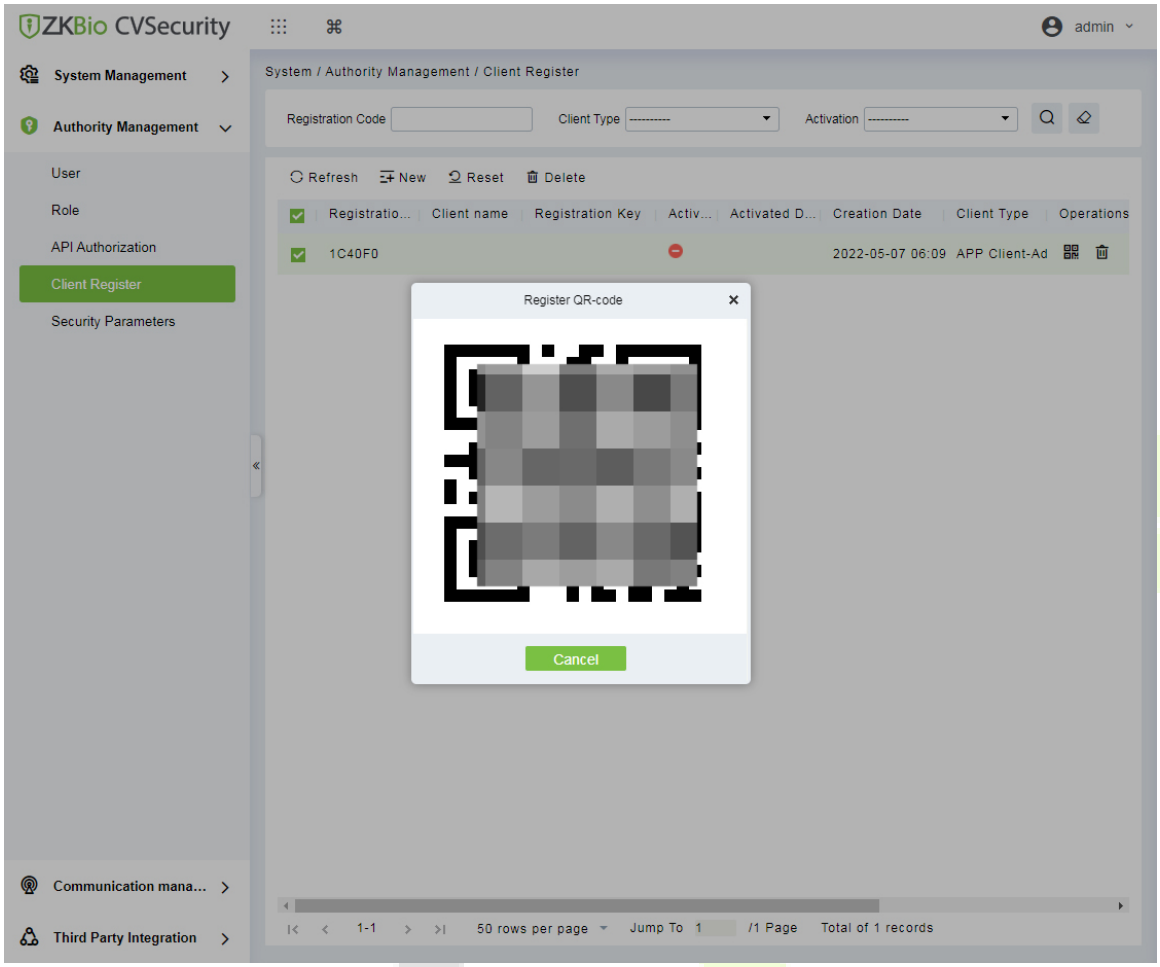
Después de descargar e instalar la aplicación, el usuario debe configurar el servidor antes de iniciar sesión. Los pasos se dan a continuación:

1. En**ZKBio CVSeguridad**>**Sistema**>**Gestión del sistema**>**Parámetros**, colocar**Habilitar código QR**a "Sí", y seleccione el estado del código QR de acuerdo con la situación real. El valor predeterminado es**Dinámica**, se puede configurar el tiempo válido del código QR.



2. En el servidor, elija**Sistema**>**Gestión de autoridad**>**Registro de clientes**para agregar un cliente de aplicación registrado.

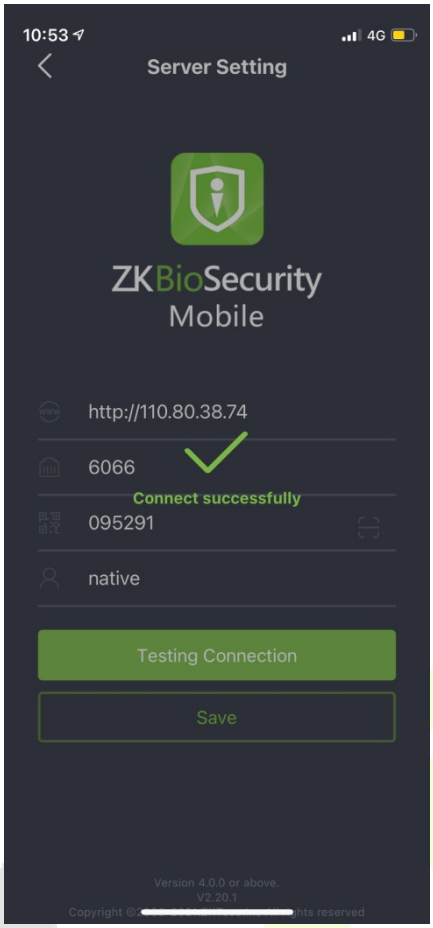




3. Abra la aplicación en el teléfono inteligente. En la pantalla de inicio de sesión, toque**Configuración del servidor**y escriba la dirección IP o el nombre de dominio del servidor y su número de puerto.

4. Toque en el**Código QR**icono para escanear el código QR del nuevo cliente de la aplicación. Después de que el cliente se identifique con éxito, configure el Nombre del cliente y toque**Prueba de conexión**.

5. Una vez que la red se haya conectado correctamente, toque**Ahorrar**.

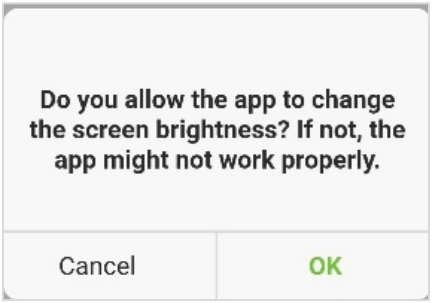


La función de credencial móvil solo es válida cuando inicia sesión como empleado, toque Empleado para cambiar a la pantalla de inicio de sesión de empleado. Ingrese el ID de empleado y la contraseña (predeterminado: 123456) para iniciar sesión.

6. Grifo**Credencial móvil**en la aplicación, y aparecerá un código QR, que incluye información de identificación del empleado y número de tarjeta (el código QR estático solo incluye el número de tarjeta).

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

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



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

Nota: Para otras operaciones específicas, consulte *Manual de usuario de la aplicación móvil ZKBioSecurity*.

Apéndice 1

Requisitos de Recogida en Vivo y Registro de Visible

Imágenes de Rostro Ligero

1) Se recomienda realizar el registro en un ambiente interior con una luz adecuada fuente sin subexposición o sobreexposición.
2) No dispare hacia fuentes de luz exteriores como puertas o ventanas u otras fuentes de luz potentes.
3) Se recomienda ropa de color oscuro que sea diferente del color de fondo para registro.
4) Muestre su rostro y frente, y no cubra su rostro y cejas con su cabello.
5) La foto digital debe ser de bordes rectos, coloreada y medio retratada con una sola persona, y la persona debe ser desconocida y casual. Las personas que usan anteojos deben quedarse para ponerse los anteojos para tomar fotografías.
6) No use accesorios como bufanda o máscara que puedan cubrir su boca o barbilla.
7) Mire a la derecha hacia el dispositivo de captura y ubique su rostro en el área de captura de imágenes como se muestra en la imagen 1.
8) No incluya más de una cara en el área de captura.
9) Se recomiendan 50 cm - 80 cm para capturar la distancia ajustable según la altura del cuerpo.

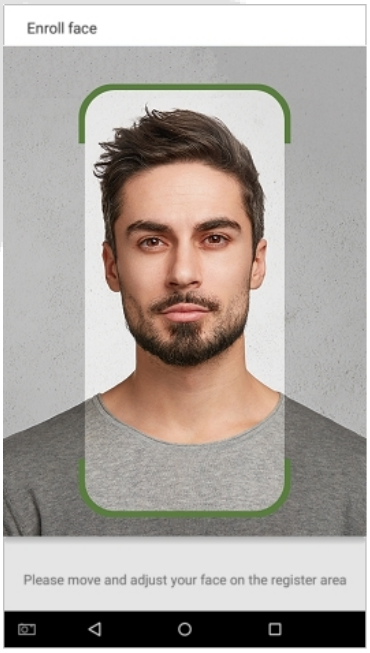


Image1 Área de captura de rostros

Requisitos para los datos de imágenes faciales digitales de luz visible

La foto digital debe ser de bordes rectos, coloreada, medio retratada con una sola persona, y la persona debe estar desconocida y en ropa informal. Las personas que usan anteojos deben quedarse para ponérselos para tomar una foto.

-Distancia del ojo

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

-Expresión facial

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

-Gesto y Angel

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

-Accesorios

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

-Rostro

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

-Formato de imagen

Debe estar en BMP, JPG o JPEG.

-Requisito de datos

Debe cumplir con los siguientes requisitos:

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

Apéndice 2

política de privacidad

Aviso:

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

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

I. Información recopilada

Para garantizar el funcionamiento normal del producto y ayudar a mejorar el servicio, recopilaremos la información que usted proporcione voluntariamente o que usted autorice durante el registro y el uso o que se genere como resultado de su uso de los servicios.

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

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

II. Seguridad y gestión de productos

1.Cuando utilice nuestros productos por primera vez, deberá establecer el privilegio de administrador antes de realizar operaciones específicas. De lo contrario, se le recordará con frecuencia que establezca el privilegio de administrador cuando ingrese a la interfaz del menú principal.**Si 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 de visualización de la información biométrica están deshabilitadas en nuestros productos por defecto. Puede elegir Menú > Configuración del sistema para configurar si desea mostrar la información biométrica. Si habilita estas funciones, asumimos que conoce los riesgos de seguridad de la privacidad personal especificados en la política de privacidad.

3.Solo su ID de usuario se muestra de forma predeterminada. Puede configurar si mostrar otra información de verificación del usuario (como Nombre, Departamento, Foto, etc.) bajo el privilegio de Administrador.**Si elige mostrar dicha información, asumimos que conoce los posibles riesgos de seguridad (por ejemplo, su foto se mostrará en la interfaz del dispositivo).**

4.La función de cámara está deshabilitada en nuestros productos por defecto. Si desea habilitar esta función para tomar fotografías de usted mismo para el registro de asistencia o tomar fotografías de extraños para el control de acceso, el producto habilitará el tono rápido 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 cargados por el Administrador a 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 necesita procesar los datos y conoce el riesgo potencial de seguridad. En tal caso, usted asumirá la responsabilidad de almacenar los datos. Debe saber que algunos datos no se pueden descargar por motivos de seguridad.

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

tercero Otros

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

Operación ecológica

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

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

Sustancias peligrosas o tóxicas y sus cantidades

Componente Nombre	Sustancia/elemento peligroso/tóxico					
	Dirigir (Pb)	Mercurio (Hg)	Cadmio (Cd)	hexavalente Cromo (Cr6+)	polibromado bifenilos (PB)	polibromado Éteres de difenilo (PBDE)
Resistencia de microprocesador	×	○	○	○	○	○
Condensador de chips	×	○	○	○	○	○
inductor de chips	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
EDS componente	×	○	○	○	○	○
Zumbador	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Tornillos	○	○	○	×	○	○

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

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

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

Parque Industrial ZKTeco, No. 32, Vía Industrial,

Ciudad de Tangxia, Dongguan, China.

Teléfono : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com