Manual de Usuario

MiniAC Plus

Ver: 1.1

Marca Registrada

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

Exención de Responsabilidad

Este manual contiene información sobre la operación y mantenimiento del equipo ZKTeco. Los derechos de autor en todos los documentos, dibujos, etc. en relación con el equipo suministrado por ZKTeco se confieren 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 comenzar la operación y el mantenimiento del equipo suministrado. Si alguno de los contenidos del manual parece poco claro o está incompleto, comuníquese con ZKTeco antes de comenzar la operación y el mantenimiento de dicho equipo.

Es un pre-requisito esencial para la operación y mantenimiento satisfactorios que el personal de operación y mantenimiento esté completamente familiarizado con el diseño y que dicho personal haya recibido capacitación exhaustiva sobre el funcionamiento y mantenimiento de la máquina / unidad / equipo. Es 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 garantía o representación con respecto a la integridad de cualquier información contenida en este manual o cualquiera de las modificaciones hechas al mismo. ZKTeco no extiende la garantía de ningún tipo, incluida, entre otras, cualquier garantía de diseño, comerciabilidad o idoneidad para un particular
propósito.

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

ZKTeco en ningún caso será responsable ante el usuario o un tercero por daños incidentales, consecuentes, indirectos, especiales o ejemplares, incluidos, entre otros, pérdida de negocios, pérdida de ganancias, interrupción de negocios, pérdida de información comercial o cualquier pérdida material derivada de, en relación con, o relacionada con el uso de la información contenida o referenciada en este manual, incluso si ZKTeco tiene, 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 aquí contenida que se incorporará a nuevas adiciones / modificaciones 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 mejorar las operaciones de la máquina / unidad / equipo y dichas enmiendas no otorgarán ningún derecho a reclamar compensación o daños bajo ninguna circunstancia.

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

El producto se actualizará periódicamente sin previo aviso. Los últimos procedimientos de operación y documentos relevantes están disponibles en http://www.zkteco.com.
Si hay algún problema relacionado con el producto, contáctenos.

Sede Central de ZKTeco

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

Teléfono: +86 769 - 82109991

Fax: +86 755 - 89602394

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

Acerca de la Compañia

ZKTeco es uno de los mayores fabricantes de lectores de RFID y biométricos (huellas dactilares, faciales, venas digitales) más grandes del mundo. Las ofertas de productos incluyen Lectores y Paneles de Control de Acceso, Cámaras de Reconocimiento Facial de rango cercano y alejado, controladores de Ascensores, Torniquetes, Cámaras de Reconocimiento de Placas Vehiculares (LPR) y productos de Consumo, que incluyen cerraduras de puerta con lector de huellas digitales y cerraduras de puertas. Nuestras soluciones de seguridad son multilingües y están localizadas en más de 18 idiomas diferentes. En las modernas instalaciones de fabricación con certificación ISO9001 de 700,000 pies cuadrados de ZKTeco, controlamos la fabricación, el diseño de productos, el ensamblaje de componentes y la logística, todo bajo un mismo techo.

Los fundadores de ZKTeco se han determinado la investigación y el desarrollo independientes de los procedimientos y la producción del 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 las verificaciones biométricas, ZKTeco se estableció oficialmente en 2007 y ahora ha sido una de las empresas líderes a nivel mundial en la industria de verificación biométrica que posee varias patentes y es seleccionada como la Empresa Nacional de Alta Tecnología por 6 años consecutivos. Sus productos están protegidos por derechos de propiedad intelectual.

Acerca del Manual

Este manual presenta la Instalación de MiniAC Plus.

Todas las imágenes mostradas son sólo para fines ilustrativos. Las cifras en este manual pueden no ser exactamente consistentes con los productos reales.

Convenciones del Documento

La convención utilizada en este manual se enumeran a continuación:

Convención Gráfica

Del Software	
Convención	Descripción
Negrita	Se utiliza para identificar nombres de interfaz de software, ejemplo OK, Confirmar, Cancelar
>	Niveles múltiples de los Menús están separados por estos corchetes. Ejemplo, Archivo > Crear > Carpeta

Del Dispositivo	
Convención	Descripción
< >	Nombre de botones o teclas en el dispositivo. Ejemplo, presione <OK>
[ ]	Nombres de ventana, elementos de menú, tabla de datos y nombres de campo están entre corchetes. Ejemplo, abra la ventana [Nuevo Usuario]
/	Menús de varios niveles están separados por barras diagonales. Ejemplo, [Archivo / Crear / Carpeta]

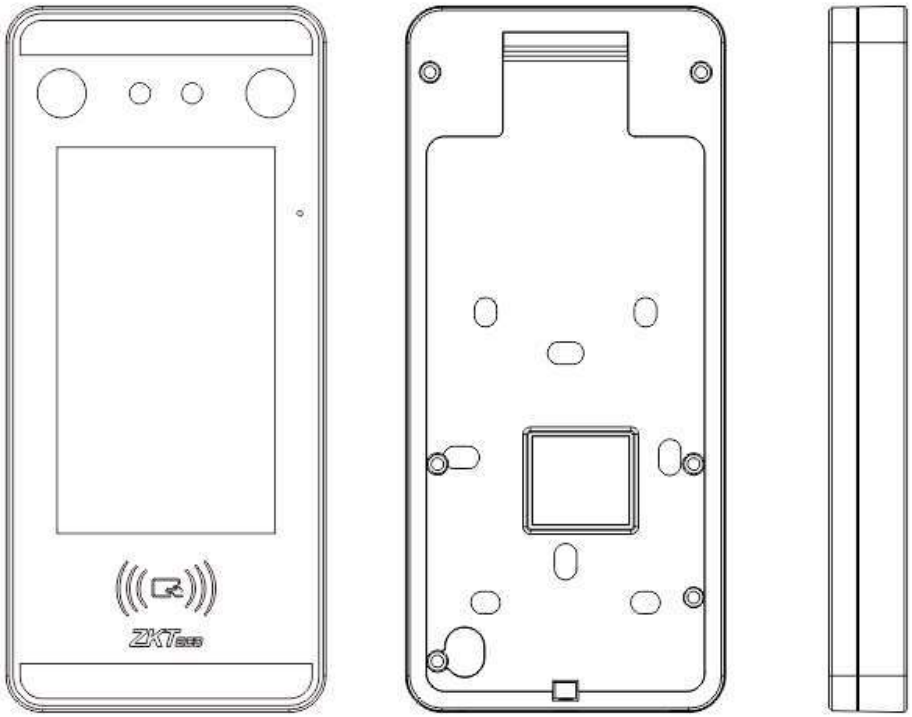
Símbolos	
Convención	Descripción
	Esto implica sobre el aviso o prestar atención, en el manual
	Información general que ayuda a realizar las operaciones más rápido
	Información que es importante
	Para evitar errores
	Declaración o evento de advertencia

CONTENIDO

1. Vista General

1.1 Apariencia

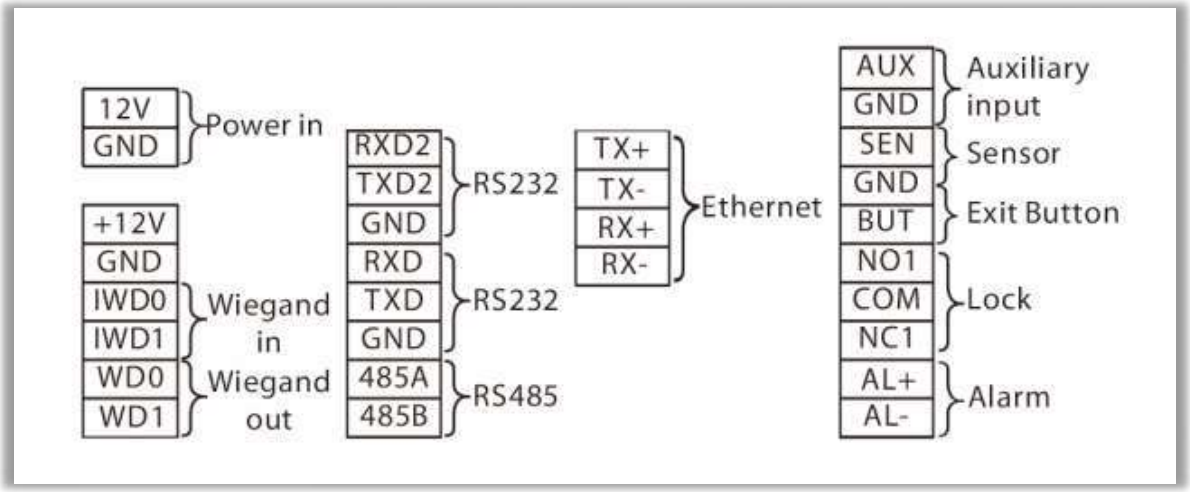
Vista Delantera y Trasera



1.2 Especificaciones del sistema

Categoría	Característica	Descripción
Cartas credenciales	Biometria	Cara / Palma
	Tarjeta	ID / Mifare (opcional)
	Contraseña	Números (máximo 8 dígitos)
General	Tipo de LCD	LCD TFT de 5 pulgadas
	Resolución LCD	72 0 * 1 2 8 0
	Temperatura de funcionamiento	0 ° C a 45 ° C (32 ° F a 113 ° F)
	Humedad de funcionamiento	20% a 80% de humedad relativa
	Dimensiones (AnxAlxPr)	92 (ancho) x203 (alto) x22.5 (profundidad) mm
	Usuarios máximos (1: N)	3000
	Cartas máximas	3000
Capacidad	Registros de transacciones máximas	1500
	Wifi	Soportado
Eléctrico	Poder	12 V, 3 A

1.3 Diagrama de PIN del producto



1.4 Configuración de la instalación

1.4.1 Precauciones de seguridad

- Mantenga el dispositivo alejado del agua o la humedad. Evite que entre agua o humedad en el chasis del dispositivo de asistencia.
- No coloque el dispositivo sobre una caja o escritorio inestable. El dispositivo podría dañarse gravemente en caso de caída

Asegure la ventilación adecuada de la sala de equipos y mantenga las rejillas de ventilación del dispositivo libres de obstrucciones.

- Asegúrese de que el voltaje de operación sea el mismo que el etiquetado en el dispositivo de asistencia.
- No abra el chasis cuando el dispositivo de asistencia esté en funcionamiento o cuando existan peligros eléctricos para evitar descargas eléctricas.

1.4.2Lugar de instalación

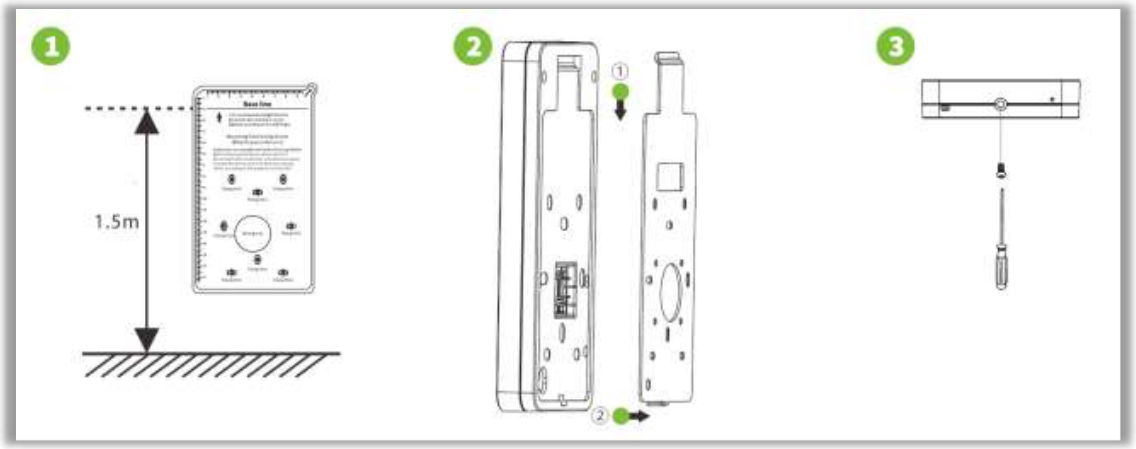
El dispositivo debe instalarse en interiores y debe reservarse un espacio suficiente en las rejillas de entrada / salida de aire para la disipación del calor.

1.4.3 Herramientas de instalación

- Destornillador de punta plana
- Destornillador Phillips: P2-150mm

1.4.4 Pasos de instalación

Asegúrese de que el dispositivo esté instalado según las instrucciones de instalación. Si desea abrir el chasis, debe comunicarse con el agente para obtener permiso. De lo contrario, sufrirá las consecuencias derivadas de sus acciones.



Paso 1: pegue el adhesivo de la plantilla de montaje en la pared y taladre los orificios de acuerdo con el papel de montaje. Fije la placa trasera en la pared con tornillos de montaje en pared.

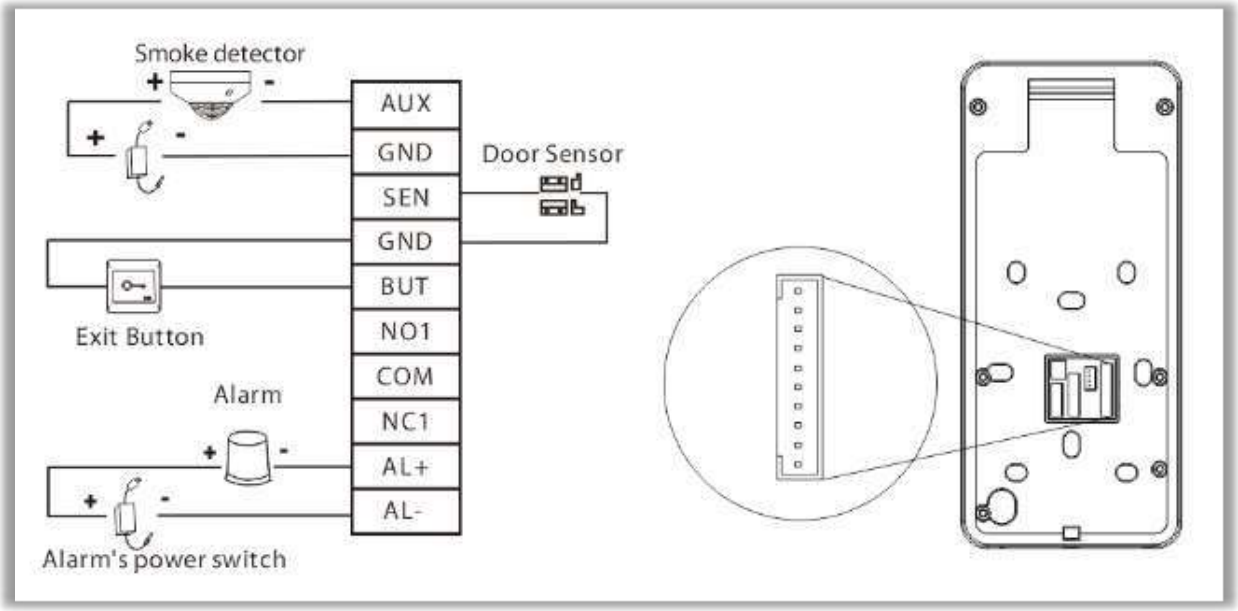
Paso 2: coloque el dispositivo en la placa posterior.

Paso 3 : Fije el dispositivo a la placa posterior con un tornillo de seguridad.

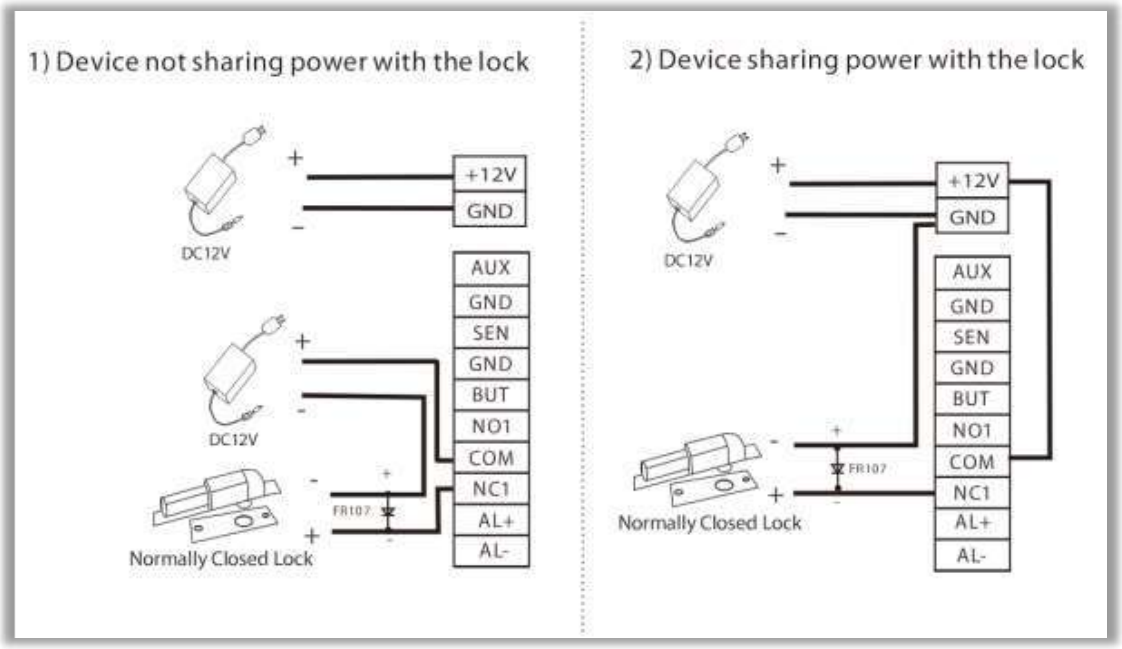
1.5 Procedimiento de conexión

1.5.1Conexión de botones y dispositivos auxiliares

- Conecte el botón Exit a los terminales GND y BUT
- Conecte el sensor de puerta a los terminales SEN y GND
- Conecte la alarma a los terminales AL + y AL-
- Conecte el dispositivo auxiliar a los terminales GND y AUX

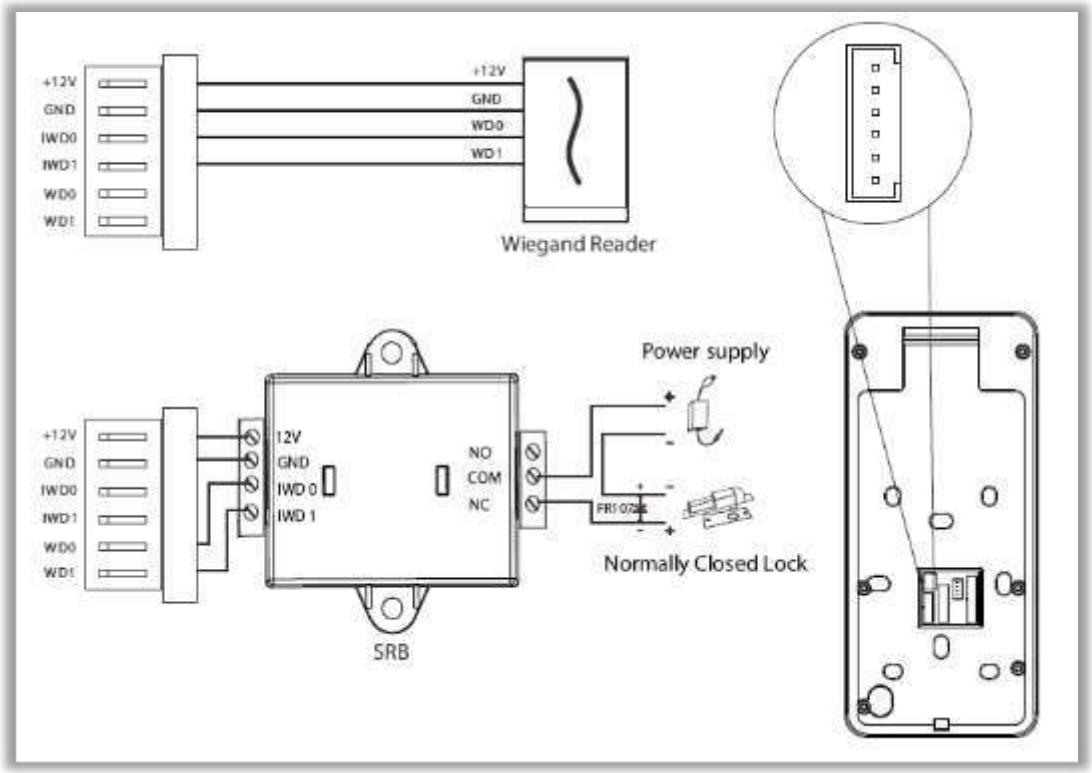


1.5.2 Conexión de relé a cerradura



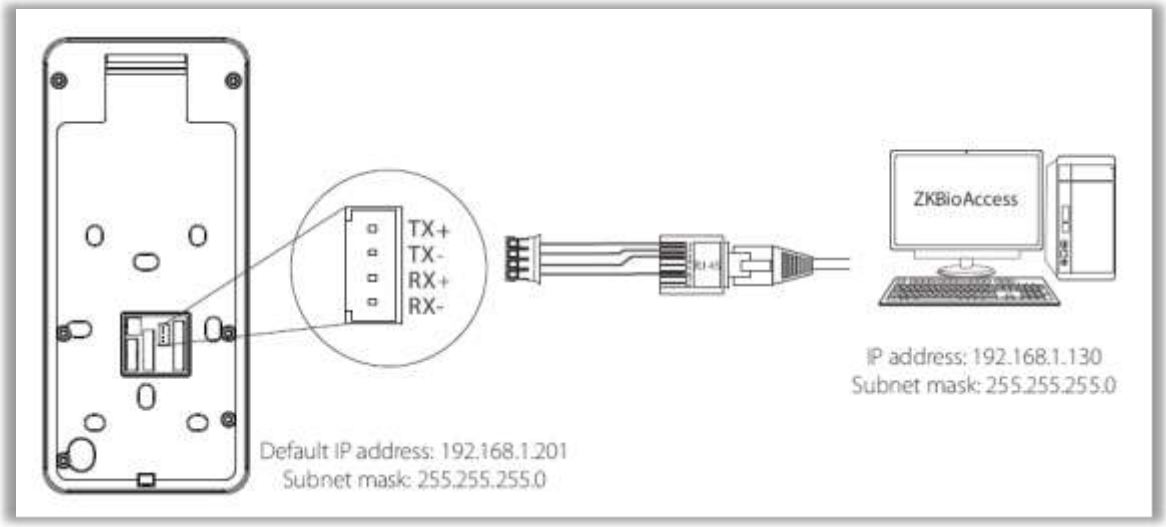
- El dispositivo admite condiciones normalmente abiertas y normalmente cerradas.
- La cerradura normalmente cerrada está conectada a los terminales NC 1 y COM.

1.5.3 Conexión del lector Weigand / SRB



- Conecte los terminales WD0 y WD1 al SRB .
- Conectar el IWD0, IWD1, GND, + 12V terminales hasta el lector de Weigand.

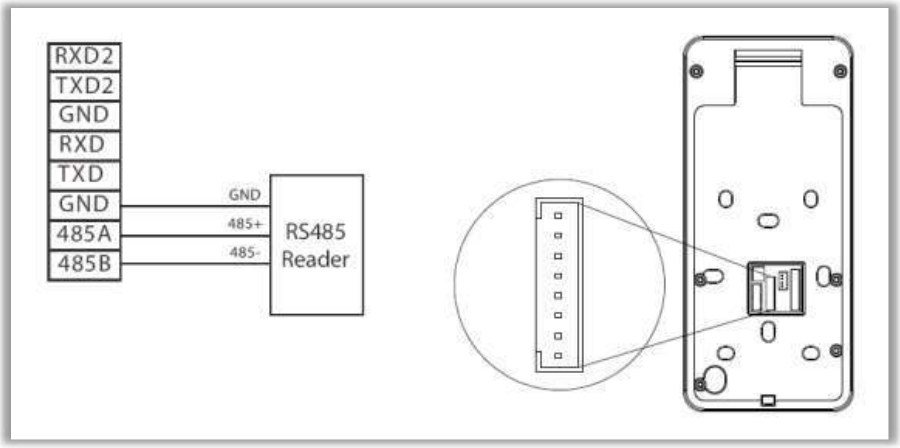
1.5.4 Conexión a Ethernet



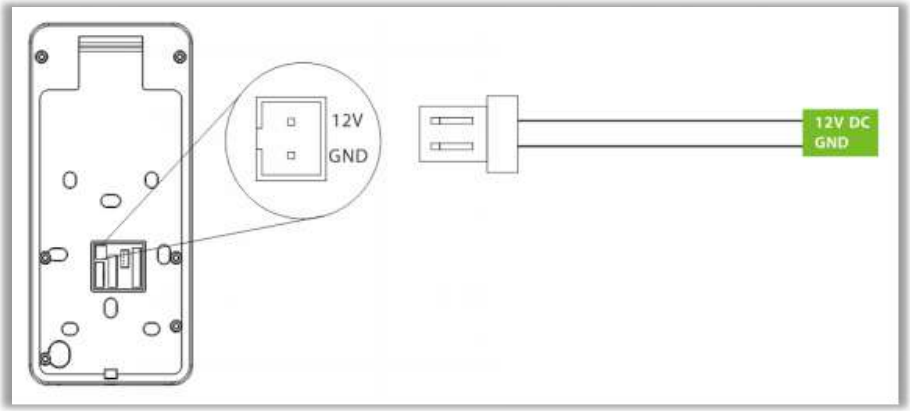
- Haga clic en [COM.] > [Ethernet] > [Dirección IP] , introduzca la dirección IP y haga clic en [Aceptar] .

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

1.5.5 Conexión a RS485



1.5.6 Energía



2. Procedimiento Operacional

2.1 Registro Facial

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

Precauciones para registrar un rostro :

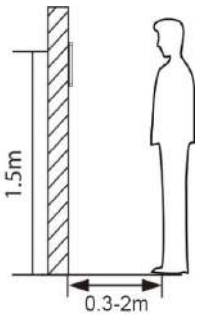
- Al registrar un rostro, mantenga una distancia de 40 cm a 80 cm entre el dispositivo y el rostro.
- Tenga cuidado de no a cambiar el rostro de expresión. (cara sonriente , cara dibujada , guiño, etc.)
- Si usted qué no sigue las instrucciones en la pantalla, el rostro de registro puede tomar más tiempo o puede fallar.
- Tenga cuidado de no a cubrir los ojos o cejas.
- No usar sombreros, máscaras, gafas de sol o gafas.
- Tenga cuidado de no a mostrar dos caras en la pantalla. Registre una persona en un tiempo.

Precauciones para autenticar un rostro :

- Asegúrese de que los cara aparece dentro de la directriz en la pantalla de la dispositivo.
- Si se han cambiado las gafas, la autenticación puede fallar. Si se ha registrado la cara sin gafas, autentique la cara sin gafas. Si solo se ha registrado la cara con gafas, autentique nuevamente la cara con las gafas usadas anteriormente.
- Si una parte de la cara está cubierta con un sombrero, una máscara, un parche en el ojo o anteojos de sol, la autenticación puede fallar. No , no cubrir la cara; permitir que el dispositivo para reconocer tanto las cejas y la cara.

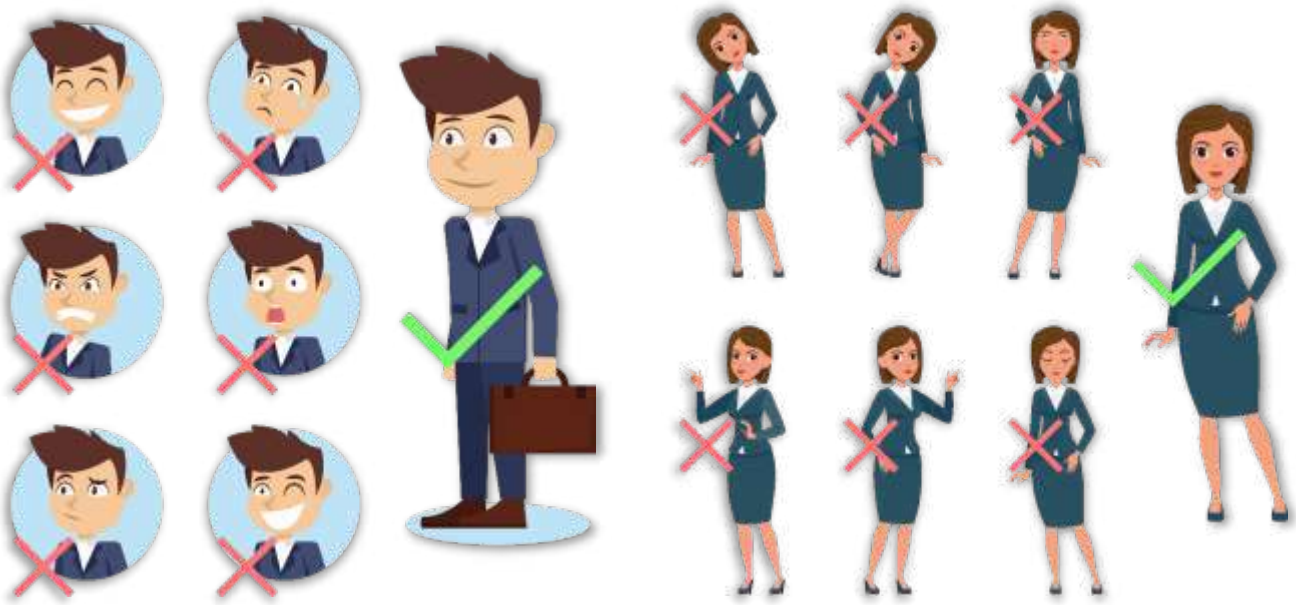
2.2 Posiciones correctas e incorrectas

- Posición de pie, expresión facial y postura :La distancia recomendada



Se recomienda que la distancia entre el dispositivo y un usuario cuya altura esté entre 1,4 y 1,8 m sea de 0,3 a 2 m. Los usuarios pueden moverse ligeramente hacia adelante y hacia atrás para mejorar la calidad de las imágenes faciales capturadas..

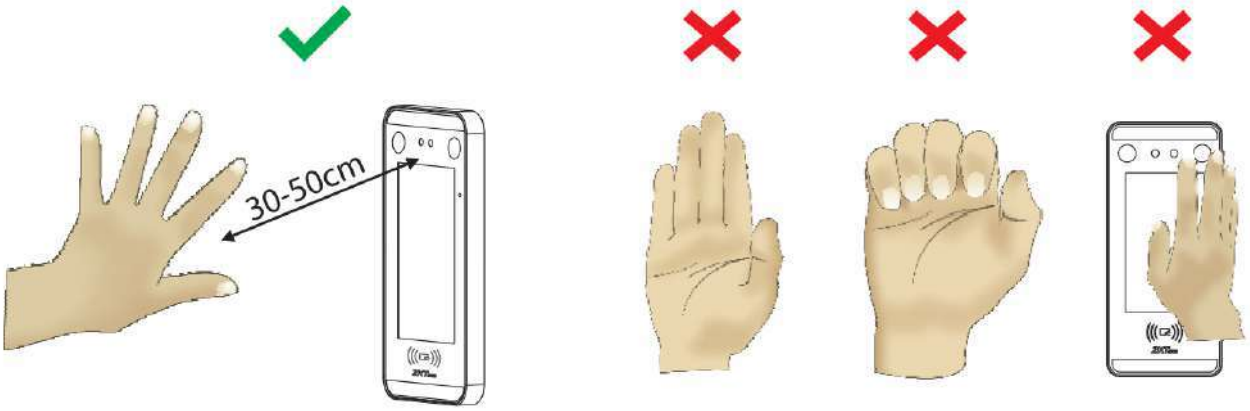
- Expresión facial y postura de pie



Nota: Durante la inscripción y la verificación, mantenga la expresión facial natural y la postura de pie.

2.3 Registro de palma

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



2.4 Modos de verificación

2.4.1 Palma

Modo de verificación de Palma 1:N

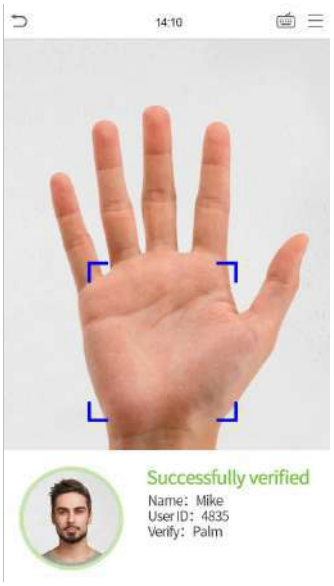
Compare la imagen de la palma recopilada por el colector de palma con todos los datos de la palma del dispositivo. El dispositivo distinguirá automáticamente entre la palma y el modo de verificación facial, y colocará la palma en el área que puede ser recolectada por el recolector de palma, y el dispositivo detectará automáticamente el modo de verificación de la palma.

Modo de verificación de Palma 1:1

Haga clic en el botón en la pantalla principal para ingresar al modo de verificación de palma 1: 1 .

1.Ingrese el ID de usuario y presione [OK].

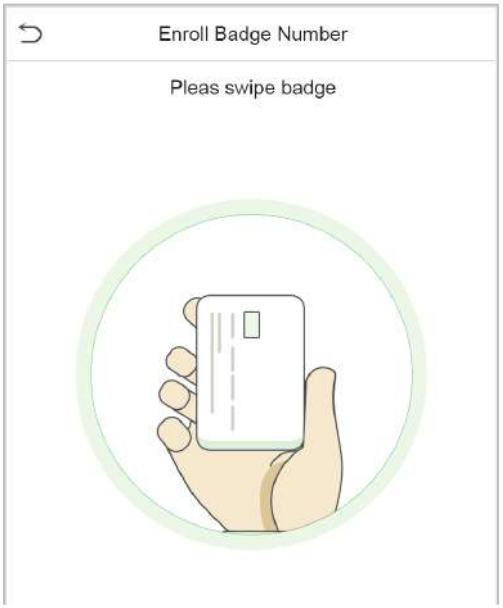
Si el usuario ha registrado el rostro , la contraseña y la insignia además de la palma de su mano, y el método de verificación está configurado como verificación de palma / rostro / contraseña / insignia , aparecerá la siguiente pantalla. Seleccione el icono de la palma para ingresar al modo de verificación de la palma.

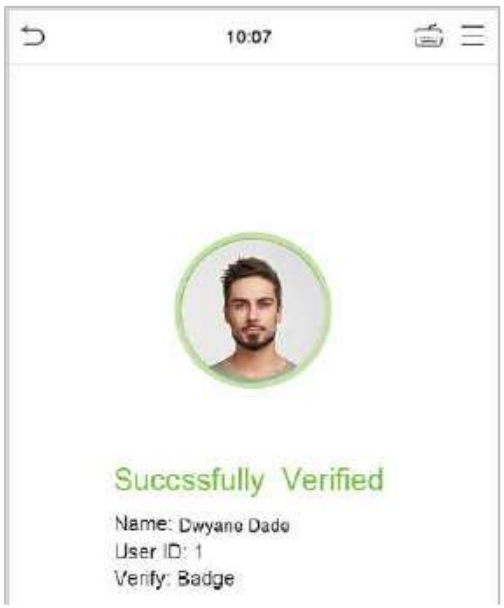


2.4.2 Tarjeta

Verificación de tarjeta 1: N

Coloque la tarjeta registrada en el área de lectura de tarjetas.





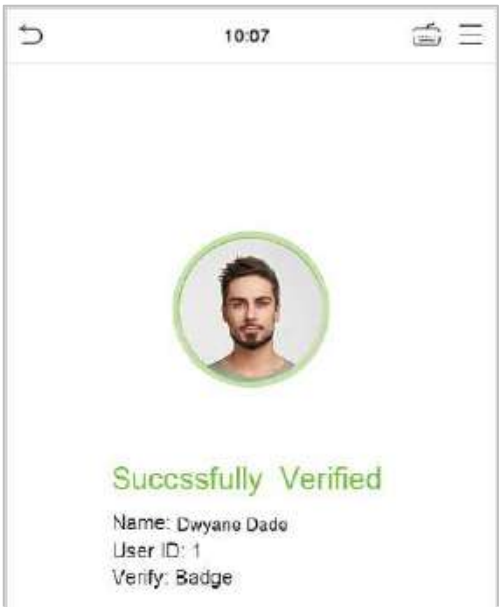
Verificación de tarjeta1 : 1

Presione en la pantalla principal para ingresar la verificación de tarjeta 1:1

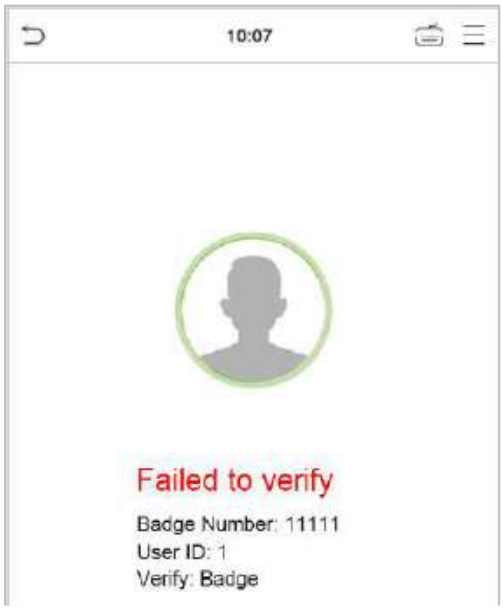
1.Ingrese su ID de usuario y haga clic en Aceptar.

2.Si el empleado registra cara, contraseña y palma además de tarjeta, aparecerá la siguiente pantalla. Seleccione el icono para ingresar al modo de verificación de credencial.

Verificación Exitosa



Verificación Fallida



2.4.3 Rostro

Verificación facial 1: N

Compare las imágenes faciales adquiridas con todos los datos faciales registrados en el dispositivo. A continuación se muestra el cuadro emergente del resultado de la comparación.

Verificación facial 1: 1

Compare el rostro capturado por la cámara con la plantilla facial relacionada con el ID de usuario ingresado.

Presione en la interfaz principal e ingrese al modo de verificación facial 1: 1.

1. Introduzca la ID de usuario y haga clic en Aceptar.

2. Si un empleado registra contraseña , credencial y palma, además de rostro, aparecerá la siguiente pantalla. Seleccione el icono para ingresar al modo de verificación facial.

3. Después de una verificación exitosa, aparecerá el cuadro de aviso "verificado correctamente".
Si la verificación falla, aparecerá el mensaje "¡Por favor, ajuste su posición!".

1.

2.

3.

2.4.4 Contraseña

Compare la contraseña ingresada con el ID de usuario y la contraseña registrados.

Haga clic en el botón en la pantalla principal para ingresar al modo de verificación de contraseña 1: 1.

1. Ingrese el ID de usuario y haga clic en Aceptar.

2. Si un empleado registra cara , credencial y palma además de la contraseña, aparecerá la siguiente pantalla. Seleccione el icono  para ingresar al modo de verificación de contraseña.

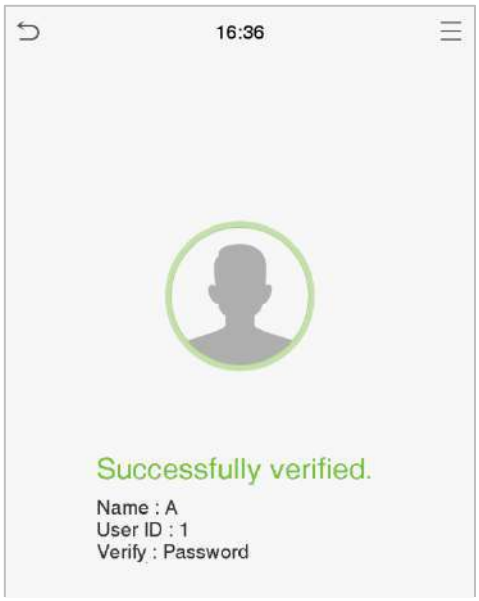
3. Introduzca la contraseña y haga clic en Aceptar.

1.

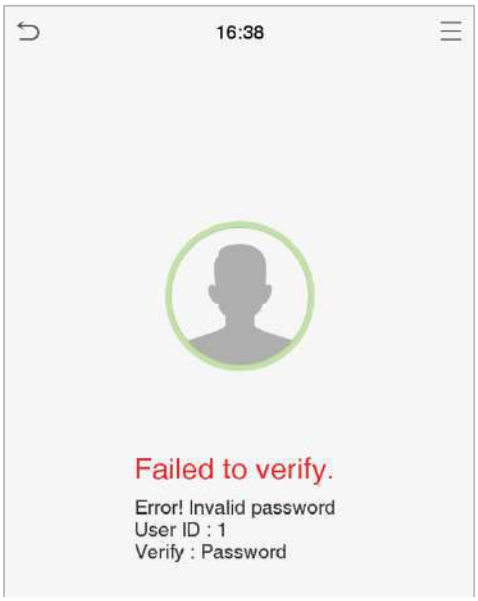
2.

3.

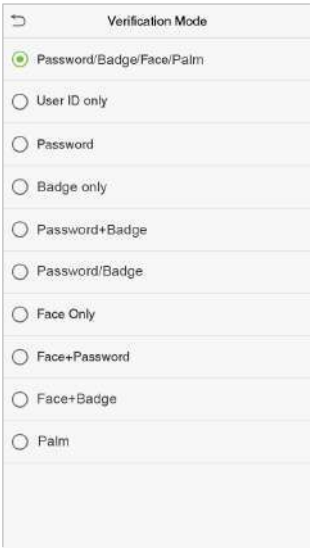
Verificación Exitosa



Error de Verificación



2.4.5 Combinación



Para aumentar la seguridad, este dispositivo ofrece la opción de utilizar múltiples formas de métodos de verificación.

Notas:
1. "/" significa "o" y "+" significa "y".

2. Debe registrar la información de verificación requerida antes de usar el modo de verificación de combinación; de lo contrario, la verificación puede fallar. Por ejemplo, si un usuario usa Registro facial pero el modo de verificación es Cara + Contraseña, este usuario nunca pasará la verificación.

3. Menú Principal

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

ARTÍCULOS	DESCRIPCIONES
Administrador de usuarios	Para una dd, editar, ver y borrar la información básica acerca de un usuario.
Rol del usuario	Para establecer el alcance del permiso del rol personalizado y el registrador, es decir, los derechos para operar el sistema .
COMM.	Para configurar los parámetros relevantes de red, conexión a PC, servidor en la nube y Wiegand.
Sistema	Para configurar los parámetros relacionados con el sistema, incluida la fecha y la hora, la configuración de los registros de acceso , los parámetros de la palma, los parámetros de la cara, restablecer los valores de fábrica.
Personalizar	Para personalizar la configuración de la pantalla de la interfaz, voz, timbre.
Gestión de datos	Para eliminar todos los datos relevantes en el dispositivo.
Control de acceso	Para configurar los parámetros de la cerradura y el dispositivo de control de acceso correspondiente.
Búsqueda de asistencia	Consulte el registro de asistencia / acceso especificado, verifique las fotos de asistencia y las fotos de la lista negra.
Auto test	Para probar automáticamente si cada módulo funciona correctamente, incluida la pantalla LCD, la voz, la cámara y el reloj en tiempo real.
Información del sistema	Para ver la capacidad de datos, el dispositivo y la información de firmware del dispositivo actual.

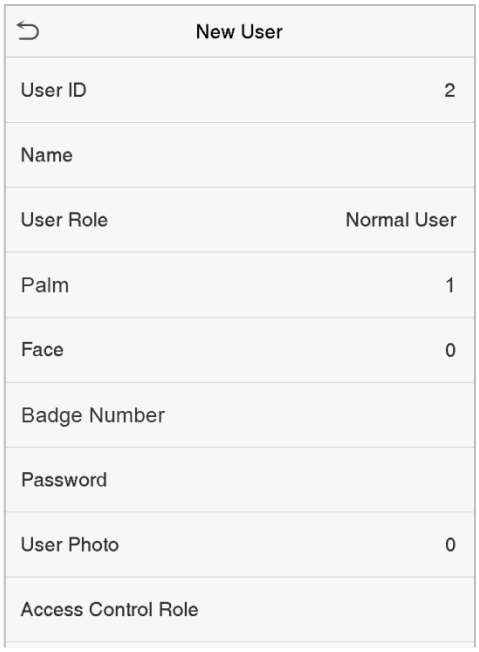
4. Gestión de Usuarios

4.1 Agregar usuarios

1. Haga clic en User Mgt. en el menú principal.

2. Haga clic en Nuevo usuario .
- Registre una ID de usuario y un nombre

3. Ingrese el ID de usuario y el nombre.



Notas:

1. Un nombre de usuario puede contener 17 caracteres.
2. La ID de usuario puede contener de 1 a 9 dígitos por defecto.
3. Durante el registro inicial, puede modificar su ID, que no se puede modificar después del registro.
4. Si aparece un mensaje "ID duplicado", debe elegir otro ID.

Configuración del rol de usuario

Hay dos tipos de cuentas de usuario: el usuario normal y el superadministrador . Si ya hay un administrador registrado, los usuarios normales no tienen derechos para administrar el sistema y solo pueden acceder a las verificaciones de autenticación. El administrador posee todos los privilegios de gestión. Si se establece un rol personalizado, también puede seleccionar permisos de rol definidos por el usuario para el usuario.

Haga clic en Función de usuario para seleccionar Usuario normal o Superadministrador.

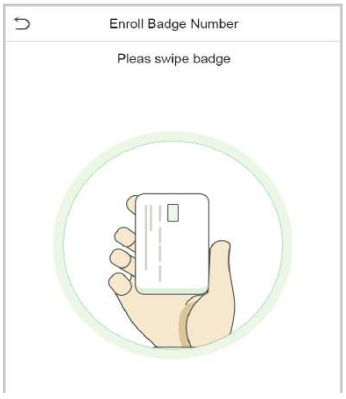
Nota: Si el rol de usuario seleccionado es el superadministrador, el usuario debe pasar la autenticación de identidad para acceder al menú principal. La autenticación se basa en los métodos de autenticación que ha registrado el superadministrador. Consulte 2.4 Método de verificación.

Registrar palma

Haga clic en palma para entrar en la página de registro de palma. Seleccione la palma que desea enrolar.

Registrar tarjeta

Haga clic en Badge number para ingresar a la página de registro de la tarjeta y coloque la tarjeta en el área de lectura de tarjetas . La interfaz de registro es la siguiente:



Registrar rostro

Haga clic en Rostro para ingresar a la página de registro de rostros. Mire hacia la cámara y quédese quieto durante el registro facial. La interfaz de registro es la siguiente:

Registrar contraseña

Haga clic en Contraseña para ingresar a la página de registro de contraseña. Ingrese una contraseña y vuelva a ingresarla. Haga clic en Aceptar . Si las dos contraseñas ingresadas son diferentes, aparecerá el mensaje "La contraseña no coincide"

Nota: La contraseña puede contener de uno a ocho dígitos por defecto..

Registrar foto de usuario

Cuando un usuario registrado con una foto pasa la autenticación, se mostrará la foto registrada. Haga clic en Foto de usuario , haga clic en el icono de la cámara para tomar una foto. El sistema volverá a la interfaz de nuevo usuario después de tomar una foto.

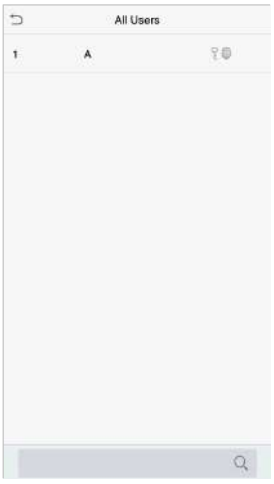
Nota: Al registrar un rostro, el sistema capturará automáticamente una imagen como foto de usuario. Si no desea registrar una foto de usuario, el sistema establecerá automáticamente la imagen capturada como la foto predeterminada.

Rol de control de acceso

El control de acceso del usuario establece los derechos de desbloqueo de la puerta de cada persona, incluido el grupo al que pertenece el usuario, el modo de verificación y si se aplica el período de tiempo del grupo.
Haga clic en Función de control de acceso > Grupo de acceso , asigne los usuarios registrados a diferentes grupos para una mejor gestión. Los nuevos usuarios pertenecen al Grupo 1 de forma predeterminada y se pueden reasignar a otros grupos. El dispositivo admite hasta 99 grupos de control de acceso.

4.2 Búsqueda de usuarios

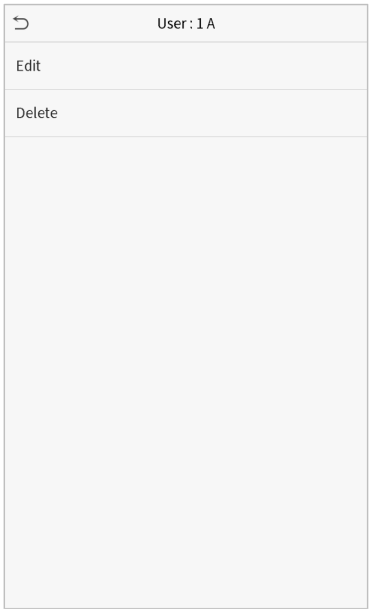
Haga clic en la barra de búsqueda en la lista de usuarios e ingrese la palabra clave de recuperación (la palabra clave puede ser una identificación, apellido o nombre completo). El sistema buscará los usuarios relacionados con la información.

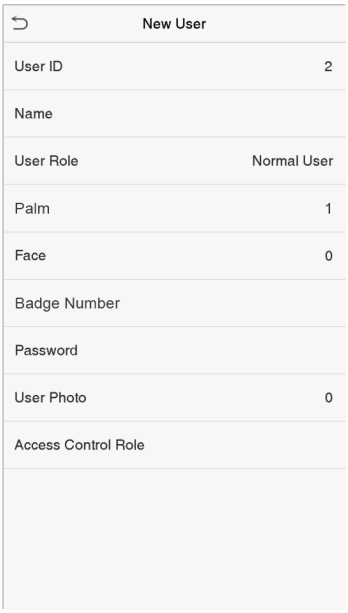


4.3 Editar usuarios

Elija un usuario de la lista y haga clic en Editar para ingresar a la interfaz de edición de usuario:

Nota: La operación de editar un usuario es la misma que la de agregar un usuario, excepto que el ID de usuario no se puede modificar al editar un usuario. El método de operación se refiere a " 4.1 Agregar usuarios ".





4.4 Eliminar usuarios

Elija un usuario de la lista y haga clic en Eliminar para ingresar a la interfaz de eliminación de usuario. Seleccione la información del usuario que desee eliminar y haga clic en Aceptar.

Nota: Si selecciona Eliminar usuario , se eliminará toda la información del usuario.

5. Rol de Usuario

Si necesita asignar algunos permisos específicos a ciertos usuarios, puede editar el "Rol definido por el usuario " en el menú Rol del usuario .
Puede establecer el alcance del permiso del rol personalizado (hasta 3 roles) y el registrador, es decir, el alcance del permiso del menú de operación.

Haga clic en Rol de usuario en la interfaz del menú principal.

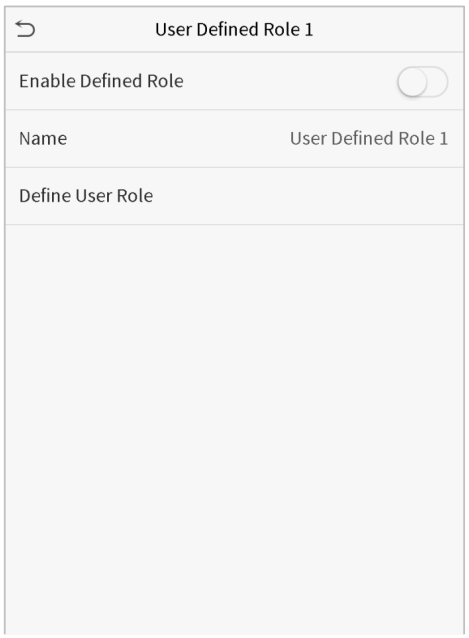
1. Haga clic en cualquier elemento para establecer una función definida. Haga clic en la fila de Habilitar rol definido para habilitar este rol definido. Haga clic en Nombre e ingrese el nombre del rol.

2. Haga clic en Definir función de usuario para asignar los privilegios a la función. Se completa la asignación de privilegios. Haga clic en Volver.

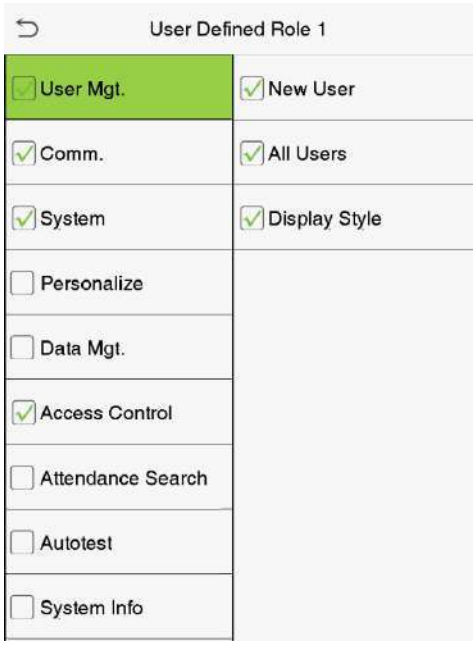
Nota: Durante la asignación de privilegios, el menú principal está a la izquierda y sus submenús están a la derecha. Solo necesita seleccionar las funciones en los submenús. Si el dispositivo tiene una función habilitada, puede asignar las funciones que estableció a los usuarios haciendo clic en Administración de usuarios. > Nuevo usuario> Rol de usuario.

Si no hay ningún superadministrador registrado, el dispositivo le preguntará "¡Primero enrole al superadministrador!" después de hacer clic en la barra de habilitar.

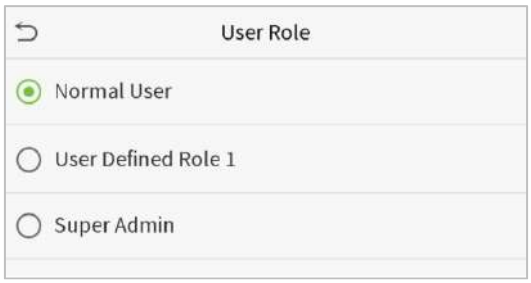
1.



2.



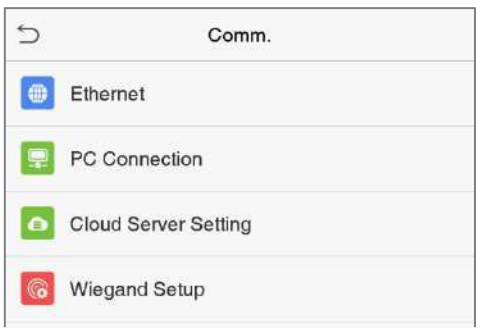
Nota



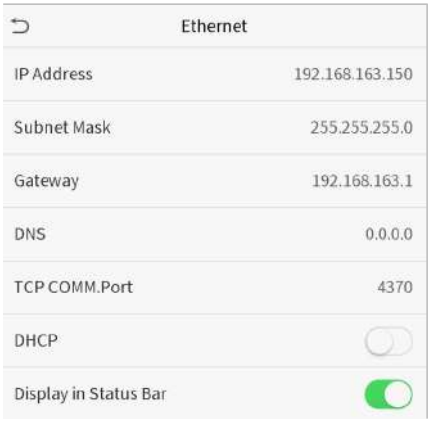
6. Configuración de Comunicación

Configure los parámetros de la red, la conexión a la PC, el servidor en la nube y Wiegand.

Toque COMM. en el menú principal.



6.1 Configuración de la red

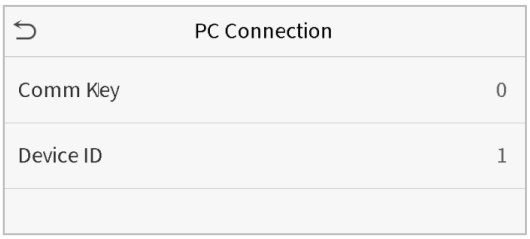


Cuando el dispositivo necesita comunicarse con una PC a través de Ethernet, debe configurar los ajustes de red y asegurarse de que el dispositivo y la PC se conecten al mismo segmento de red.

Haga clic en Ethernet en Comm. Interfaz de configuración.

ARTÍCULOS	DESCRIPCIONES
Dirección IP	El valor predeterminado de fábrica es 192.168.1.201. Ajústelos de acuerdo con la situación real de la red.
Máscara de subred	El valor predeterminado de fábrica es 255.255.255.0. Ajústelos de acuerdo con la situación real de la red.
Puerta	La dirección predeterminada de fábrica es 0.0.0.0. Ajústelos de acuerdo con la situación real de la red.
DNS	La dirección predeterminada de fábrica es 0.0.0.0. Ajústelos de acuerdo con la situación real de la red.
TCP COMM. Puerto	El valor predeterminado de fábrica es 4370. Ajústelos de acuerdo con la situación real de la red.
DHCP	Protocolo de configuración dinámica de host, que consiste en asignar dinámicamente direcciones IP para clientes a través del servidor.
Mostrar en la barra de estado	Para configurar si se muestra el icono de red en la barra de estado.

6.2 Conexión a PC



Para mejorar la seguridad de los datos, configure una clave de comunicación para la comunicación entre el dispositivo y la PC.

Si se configura una clave de comunicación, esta contraseña de conexión debe ingresarse antes de que el dispositivo pueda conectarse al software de la PC.

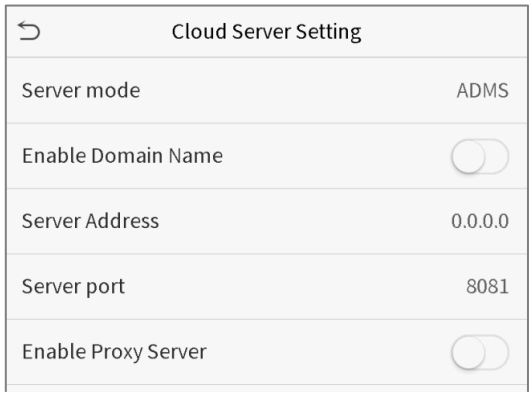
Haga clic en Conexión de PC en Comm. Interfaz de configuración.

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

6.3 Configuración del servidor en la nube

Esto representa la configuración utilizada para conectarse con el servidor ADMS.

Haga clic en Configuración del servidor en la nube en Comm. Interfaz de configuración.

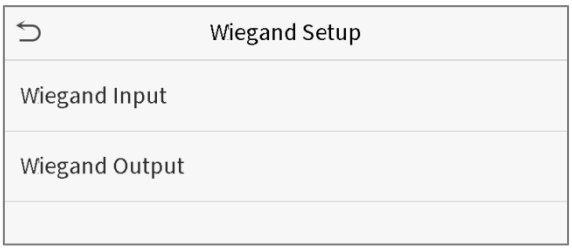


	ARTÍCULOS	DESCRIPCIONES
Habilitar nombre de dominio	Dirección del servidor	Cuando esta función está habilitada, se usará el modo de nombre de dominio "http: // ...", como http://www.XYZ.com, mientras que "XYZ" indica el nombre de dominio cuando este modo está encendido.
Deshabilitar el nombre de dominio	Dirección del servidor	Dirección IP del servidor ADMS.
	Puerto de servicio	Puerto utilizado por el servidor ADMS.
Habilitar servidor proxy		Cuando elige habilitar el proxy, debe configurar la dirección IP y el número de puerto del servidor proxy.

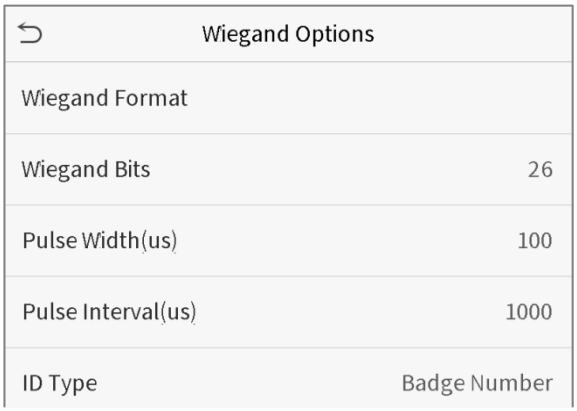
6.4 Configuración de Wiegand

Para configurar los parámetros de entrada y salida de Wiegand.

Haga clic en Configuración de Wiegand en Comm. Interfaz de configuración.



Entrada Wiegand

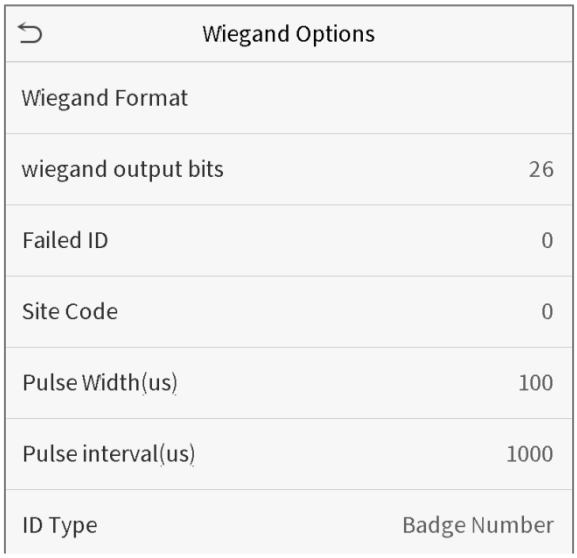


ARTÍCULOS	DESCRIPCIONES
Formato Wiegand	Los valores oscilan entre 26 bits, 34 bits, 36 bits, 37 bits y 50 bits.
Bits de salida Wiegand	Después de elegir el formato Wiegand, puede seleccionar uno de los dígitos de salida correspondientes en el formato Wiegand
Identificación fallida	Si la verificación falla, el sistema enviará la identificación fallida al dispositivo y reemplazará el número de tarjeta o la identificación del personal por los nuevos.
Código del sitio	Es similar al ID del dispositivo. La diferencia es que un código de sitio se puede configurar manualmente y es repetible en un dispositivo diferente. El valor válido varía de 0 a 256 de forma predeterminada.
Ancho de pulso (EE.UU.)	El ancho de tiempo representa los cambios de la cantidad de carga eléctrica con capacitancia de alta frecuencia regularmente dentro de un tiempo especificado.
Intervalo de pulso (nosotros)	El intervalo de tiempo entre pulsos.
Tipo de identificación	Seleccione entre ID de usuario y número de placa.

Definiciones de varios formatos Wiegand comunes::

Formato Wiegand	Definiciones
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El 1 st bit es el bit de paridad par de los 2 nd a 13 th bits de, mientras que el 26 º bit es el bit de paridad impar del 14 º a 25 º bits. Los 2 nd a 25 th bits son los números de tarjetas.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El 1 st bit es el bit de paridad par de los 2 nd a 13 th bits de, mientras que el 26 º bit es el bit de paridad impar del 14 º a 25 º bits. Los 2 nd a 9 th bits son los códigos de sitio, mientras que el 10 º a 25 º bits son los números de tarjetas.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El 1 st bit es el bit de paridad par de los 2 nd a 17 th bits de, mientras que el 34 º bit es el bit de paridad impar de los 18 º a 33 rd bits. Los 2 nd a 25 th bits son los números de tarjetas.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El 1 st bit es el bit de paridad par de los 2 nd a 17 th bits de, mientras que el 34 º bit es el bit de paridad impar de los 18 º a 33 rd bits. Los 2 nd a 9 th bits son los códigos de sitio, mientras que el 10 º a 25 º bits son los números de tarjetas.
Wiegand36	APAGADOFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El 1 st bit es el bit de paridad impar de los 2 nd a 18 th bits de, mientras que el 36 º bit es el bit de paridad incluso del 19 º a 35 º bits. Los 2 nd a 17 th bits son los códigos de dispositivo. Los 18 º a 33 rd bits son los números de tarjeta, y el 34 º a 35 º bits son los códigos de fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consta de 36 bits de código binario. El 1 st bit es el bit de paridad par de los 2 nd a 18 th bits de, mientras que el 36 º bit es el bit de paridad impar del 19 º a 35 º bits. Los 2 nd a 19 th bits son los códigos de dispositivo, y los 20 º a 35 º bits son los números de tarjetas.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCE Consta de 37 bits de código binario. El 1 st bit es el bit de paridad impar de los 2 nd a 18 th bits de, mientras que el 37 º bit es el bit de paridad incluso del 19 º a 36 º bits. Los bits 2º al 4º son los códigos del fabricante. Los 5 º a 16 º bits son los códigos de sitio, y la 21 st a 36 th bits son los números de tarjetas.
Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consta de 37 bits de código binario. El 1 st bit es el bit de paridad par de los 2 nd a 18 th bits de, mientras que el 37 º bit es el bit de paridad impar del 19 º a 36 º bits. Los bits 2º al 4º son los códigos del fabricante. Los 5 º a 14 º bits son los códigos de dispositivo, y 15 º a 20 º bits son los códigos de sitio, y la 21 st a 36 th bits son los números de tarjetas.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 50 bits de código binario. El 1 st bit es el bit de paridad par de los 2 nd a 25 th bits de, mientras que el 50 º bit es el bit de paridad impar del 26 º a 49 º bits. Los 2 º y 17 º bits son los códigos de sitio, y los 18 º a 49 º bits son los números de las tarjetas.
"C " denota el número de tarjeta; “ **E”** denota el bit de paridad par; “ **O”** denota el bit de paridad impar; **"F** " indica el código de la instalación; “ **M”** indica el código del fabricante; " **P"** denota el bit de paridad; y " **S"** indica el código del sitio.	

Salida Wiegand

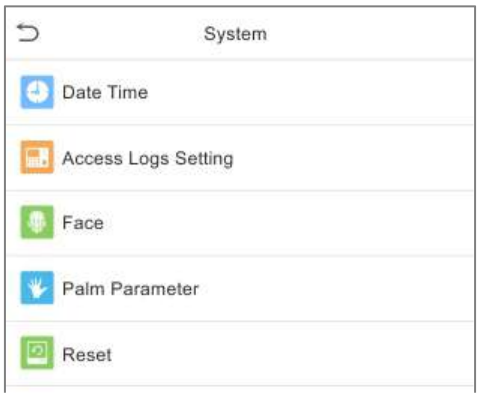


ARTÍCULOS	DESCRIPCIONES
Formato Wiegand	Los valores oscilan entre 26 bits, 34 bits, 36 bits, 37 bits y 50 bits.
Bits de salida Wiegand	Después de elegir el formato Wiegand, puede seleccionar uno de los dígitos de salida correspondientes en el formato Wiegand
Identificación fallida	Si la verificación falla, el sistema enviará la identificación fallida al dispositivo y reemplazará el número de tarjeta o la identificación del personal por los nuevos.
Código del sitio	Es similar al ID del dispositivo. La diferencia es que un código de sitio se puede configurar manualmente y es repetible en un dispositivo diferente. El valor válido varía de 0 a 256 de forma predeterminada.
Ancho de pulso (EE. UU.)	El ancho de tiempo representa los cambios de la cantidad de carga eléctrica con capacitancia de alta frecuencia regularmente dentro de un tiempo especificado.
Intervalo de pulso (nosotros)	El intervalo de tiempo entre pulsos.
tipo de identificación	Seleccione entre ID de usuario y número de placa.

7. Configuración del Sistema

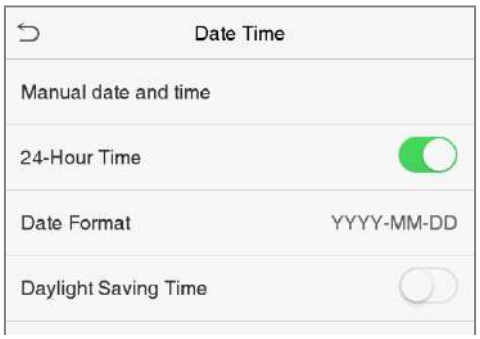
Configure los parámetros del sistema relacionados para optimizar el rendimiento del dispositivo.

Haga clic en Sistema en la interfaz del menú principal.



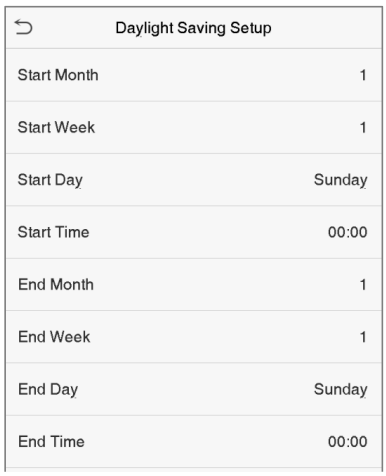
7.1 Fecha y hora

Haga clic en Fecha y hora en la interfaz del sistema.

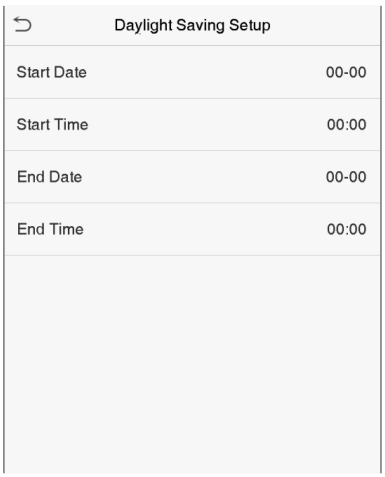


1. Puede configurar manualmente la fecha y la hora y hacer clic en Confirmar para guardar.
2. Haga clic en Hora de 24 horas para habilitar o deshabilitar este formato y seleccione el formato de fecha.
3. Haga clic en Horario de verano para habilitar o deshabilitar la función. Si está habilitado, seleccione un modo de horario de verano y configure la hora de cambio.

Modo Semana



Modo Fecha

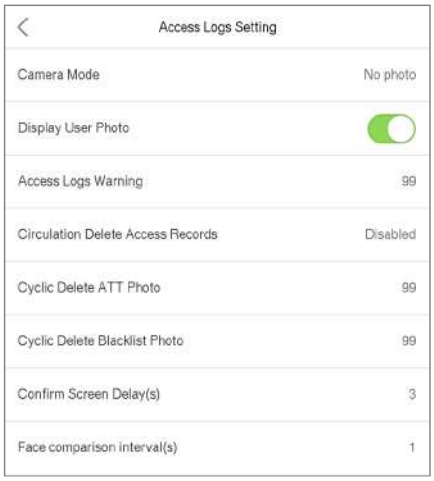


Al restaurar la configuración de fábrica, la hora (24 horas) y el formato de fecha (AAAA-MM-DD) se pueden restaurar, pero la fecha y la hora del dispositivo no se pueden restaurar.

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

7.2 Ajuste de eventos de acceso

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



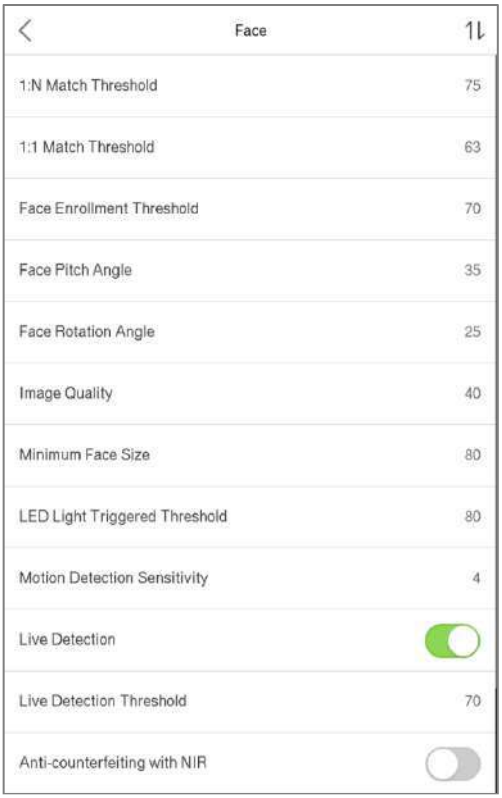
ARTÍCULOS	DESCRIPCIONES
Modo cámara	Ya sea para capturar y guardar la imagen instantánea actual durante la verificación. Hay 5 modos: **Sin foto:** no se toma ninguna foto durante la verificación del usuario. **Tomar foto, no guardar:** la foto se toma pero no se guarda durante la verificación. **Tomar una foto y guardar:** la foto se toma y se guarda durante la verificación. **Guardar en la verificación exitosa:** se toma una foto y se guarda para cada verificación exitosa. **Guardar en verificación fallida:** la foto se toma y se guarda durante cada verificación fallida.
Mostrar foto de usuario	Si mostrar la foto del usuario cuando el usuario pasa la verificación.
Advertencia de registros de acceso	Cuando el espacio de registro restante alcanza un valor establecido, el dispositivo mostrará automáticamente una advertencia de memoria de registro restante. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999.

Circulación Eliminar registros de acceso	Cuando los registros de acceso hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un valor establecido de registros de acceso antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 999.
Eliminación cíclica de foto ATT	Cuando las fotos de asistencia hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un valor establecido de fotos de asistencia antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Eliminación cíclica de foto en lista negra	Cuando las fotos de la lista negra hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un valor establecido de las fotos antiguas de la lista negra. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Confirmar el retraso de la pantalla	El período de tiempo que se muestra el mensaje de verificación exitosa. Valor válido: 1 ~9 segundos.
Intervalo (s) de comparación de caras	Para configurar el intervalo de tiempo de coincidencia de la plantilla facial según sea necesario. Valor válido: 0 ~9 segundos.

7.3 Parámetros faciales

Haga clic en Rostro en la interfaz del sistema.

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

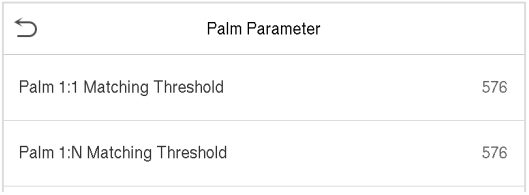


Articulo	Descripción
Umbral de coincidencia 1: N	En el modo de verificación 1: N, la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas sea mayor que el valor establecido. El valor válido varía de 65 a 120. Cuanto más altos sean los umbrales, menor será la tasa de errores de juicio, mayor será la tasa de rechazo y viceversa. Se recomienda el valor predeterminado de 75.
Umbral de coincidencia 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 registradas en el dispositivo sea mayor que el valor establecido. El valor válido varía de 55 a 120. Cuanto más altos sean los umbrales, menor será la tasa de errores de juicio, mayor será la tasa de rechazo y viceversa. Se recomienda el valor predeterminado de 63.
Umbral de inscripción de rostros	Durante el registro facial, se utiliza la comparación 1: N para determinar si el usuario ya se ha registrado antes. Cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas es mayor que 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 facial y la comparación. Si una cara ' s ángulo de paso supera este valor de ajuste, se filtra por el algoritmo, es decir, ignorada por el terminal por lo tanto no interfaz de registro y la comparación se activará.
Ángulo de rotación de la cara	La tolerancia del ángulo de rotación de una cara para el registro y la comparación de plantillas faciales. Si una cara ' s ángulo de rotación supera este valor de ajuste, se filtra por el algoritmo, es decir, ignorada por el terminal por lo tanto no interfaz de registro y la comparación se activará.
Calidad de la imagen	Calidad de imagen para registro facial y comparación. Cuanto mayor sea el valor, más clara será la imagen requerida.

Tamaño mínimo de cara	Requerido para el registro facial y la comparación. Si un objeto ' tamaño s es menor que este valor de ajuste, el objeto se filtró y no se reconoce 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 el algoritmo obtendrá el píxel de la cara más pequeño. Por lo tanto, ajustar este parámetro puede ajustar la distancia de comparación más lejana de caras. Cuando el valor es 0, la distancia de comparación de caras no está limitada.
Umbral activado por luz LED	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, con más frecuencia se encenderá la luz LED.
Sensibilidad de detección de movimiento	Una medida de la cantidad de cambio en una cámara ' campo s de vista que califica como la detección de movimiento potencial que despierta el terminal desde el modo en 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 se activa con frecuencia.
Detección en vivo	Detectar un intento de falsificación determinando si la fuente de una muestra biométrica es un ser humano vivo o una representación falsa utilizando imágenes de luz visible.
Umbral de detección en vivo	Ayudar a juzgar si la imagen visible proviene de un cuerpo vivo. Cuanto mayor sea el valor, mejor será el rendimiento anti-spoofing de la luz visible.
Lucha contra la falsificación con NIR	Uso de imágenes de espectros de infrarrojo cercano para identificar y prevenir ataques de fotos y videos falsos.
WDR	Amplio rango dinámico (WDR), que equilibra la luz y extiende la visibilidad de la imagen para videos de vigilancia en escenas de iluminación de alto contraste y mejora la identificación de objetos en ambientes brillantes y oscuros.
Modo anti-parpadeo	Se usa cuando WDR está apagado. Esto ayuda a reducir el parpadeo cuando el dispositivo ' s pantalla parpadea en la misma frecuencia que la luz.
Notas	Un ajuste inadecuado de los parámetros de exposición y calidad puede afectar gravemente el rendimiento del dispositivo. Ajuste el parámetro de exposición solo bajo la guía del personal de servicio postventa de nuestra empresa.

7.4 Parámetros de la palma

Haga clic en Palm en la interfaz del sistema



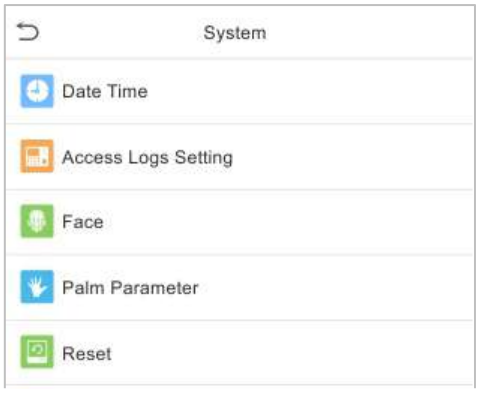
Articulo	Descripción
Umbral de coincidencia de Palm 1: 1	En el método de verificación 1: 1, solo cuando la similitud entre la palma de verificación y la palma registrada del usuario es mayor que este valor, la verificación puede tener éxito.
Palma 1: N Partido ing Umbral	En el método de verificación 1: N, solo cuando la similitud entre la palma verificadora y toda la palma registrada es mayor que este valor, la verificación puede tener éxito.

7.5 Restablecimiento de fábrica

Restaure el dispositivo, como la configuración de comunicación y la configuración del sistema, a la configuración de fábrica (no borre los datos de usuario registrados).

Haga clic en Restablecer en la interfaz del sistema.

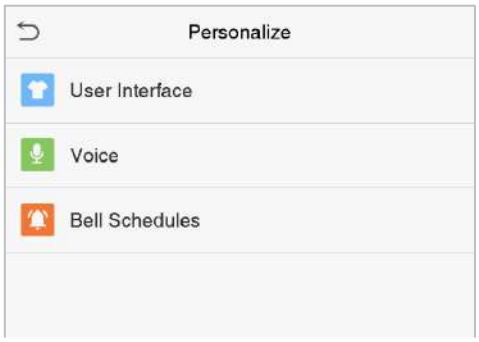
Haga clic en OK para restablecer.



8. Configuración de Personalización

Puede personalizar la configuración de la interfaz, voz, timbre.

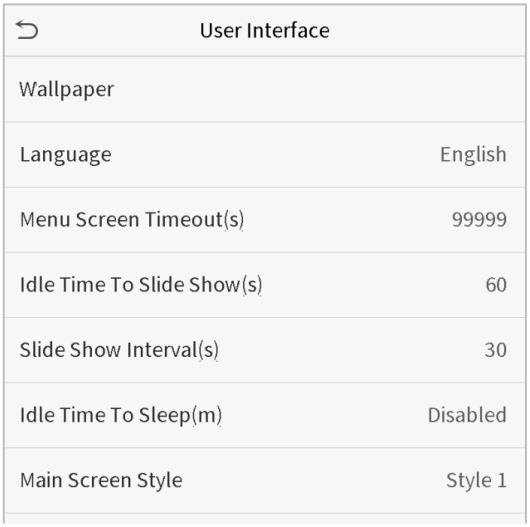
Haga clic en Personalizar en la interfaz del menú principal.



8.1 Configuración de la interfaz

Puede personalizar el estilo de visualización de la interfaz principal.

Haga clic en Interfaz de usuario en la interfaz Personalizar.

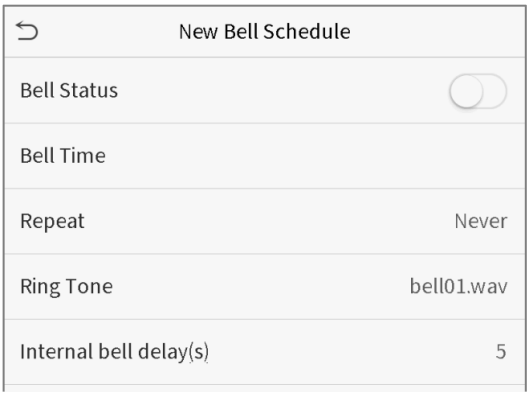


Articulo	Descripción
Fondo de pantalla	Para seleccionar el fondo de pantalla de la pantalla principal de acuerdo con sus preferencias personales.
Idioma	Para seleccionar el idioma del dispositivo.
Tiempo de espera de la pantalla de menú (s)	Cuando no hay operación y el tiempo excede el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. Puede desactivar la función o establecer el valor entre 60 y 99999 segundos.
Tiempo de inactividad para la presentación de diapositivas	Cuando no hay ninguna operación y el tiempo excede el valor establecido, se reproducirá una presentación de diapositivas. Puede desactivarse o puede establecer el valor entre 3 y 999 segundos.
Intervalo (s) de presentación de diapositivas	Esto se refiere al intervalo de tiempo que cambia diferentes imágenes de presentación de diapositivas. La función puede desactivarse o puede establecer el intervalo entre 3 y 999 segundos.
Tiempo inactivo para dormir (m)	Si ha activado el modo de suspensión, cuando no haya ninguna operación, el dispositivo entrará en modo de espera. Presione cualquier tecla o dedo para reanudar el modo de trabajo normal. Puede desactivar esta función o establecer un valor entre 1 y 999 minutos.
Estilo de pantalla principal	Para seleccionar el estilo de la pantalla principal según sus preferencias personales.

8.2 Configuración de voz

Haga clic en Voz en la interfaz Personalizar.

Articulo	Descripción
Mensaje de voz	Seleccione si desea habilitar las indicaciones de voz durante el funcionamiento.
Toque Indicación	Seleccione si desea habilitar los sonidos del teclado.
Volumen	Ajuste el volumen del dispositivo; valor válido: 0-100.



Articulo	Descripción
Estado de la campana	Establezca si habilitar el estado de la campana.
Tiempo de campana	A esta hora del día, el dispositivo hace sonar el timbre automáticamente.
Repetir	Configure el ciclo de repetición de la campana.
Tono de llamada	Seleccione un tono de llamada.
Retardo de campana interna	Establezca la duración de la campana interna. Los valores válidos oscilan entre 1 y 999 segundos.

2.Regrese a la interfaz de Horarios de Campana, haga clic en Todos los Horarios de Campana para ver la campana recién agregada.

Editar una campana

En la interfaz Todos los horarios de timbre, toque el timbre para editarlo.

Haga clic en Editar , el método de edición es el mismo que las operaciones de agregar una campana.

Eliminar una campana

En la interfaz de Todos los horarios de timbre, toque el timbre para eliminarlo.

Toque Eliminar y seleccione [Sí] para eliminar la campana.

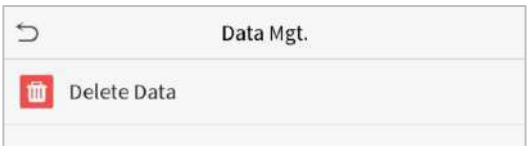
9. Gestión de Datos

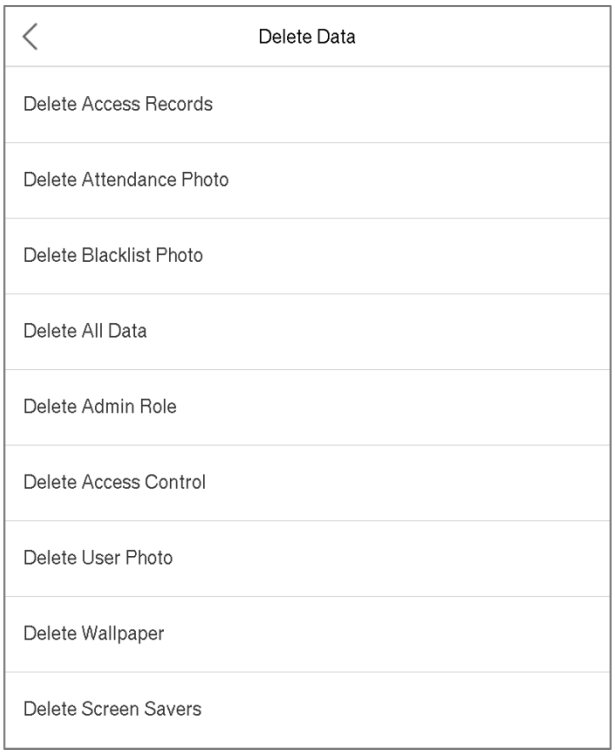
Para eliminar los datos relevantes en el dispositivo.

Haga clic en Data Mgt. en la interfaz del menú principal.

9.1 Eliminar datos

Haga clic en Eliminar datos en el Administrador de datos. interfaz.

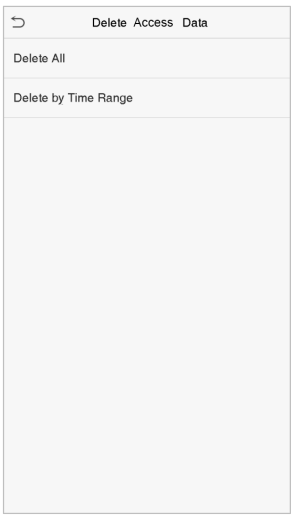




Articulo	Descripción
Eliminar registros de acceso	Eliminar registros de acceso condicionalmente.
Eliminar foto de asistencia	Eliminar fotos de asistencia del personal designado.
Eliminar foto de la lista negra	Para eliminar las fotos tomadas durante verificaciones fallidas.
Eliminar todos los datos	Eliminar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

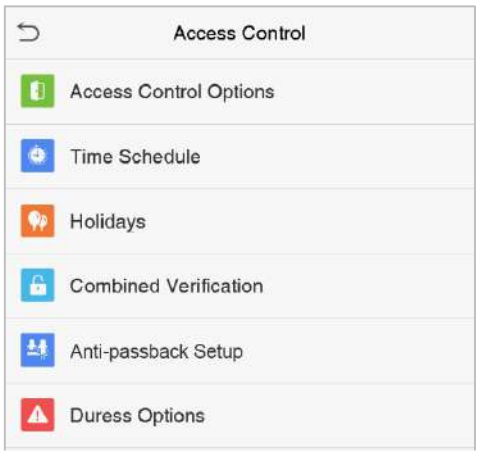
Nota: Al eliminar los datos de asistencia / registros de acceso, las fotos de asistencia o las fotos de la lista negra, puede seleccionar Eliminar todo o Eliminar por intervalo de tiempo. Al seleccionar Eliminar por rango de tiempo, debe establecer un rango de tiempo específico para eliminar todos los datos con el período, y haga clic en Aceptar

Seleccione Eliminar por rango de tiempo.



Establezca el intervalo de tiempo

10. Control de Acceso



El Control de acceso se utiliza para establecer el horario de apertura de puertas, control de cerraduras y otros ajustes de parámetros relacionados con el control de acceso.

Haga clic en Control de acceso en la interfaz del menú principal.

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

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

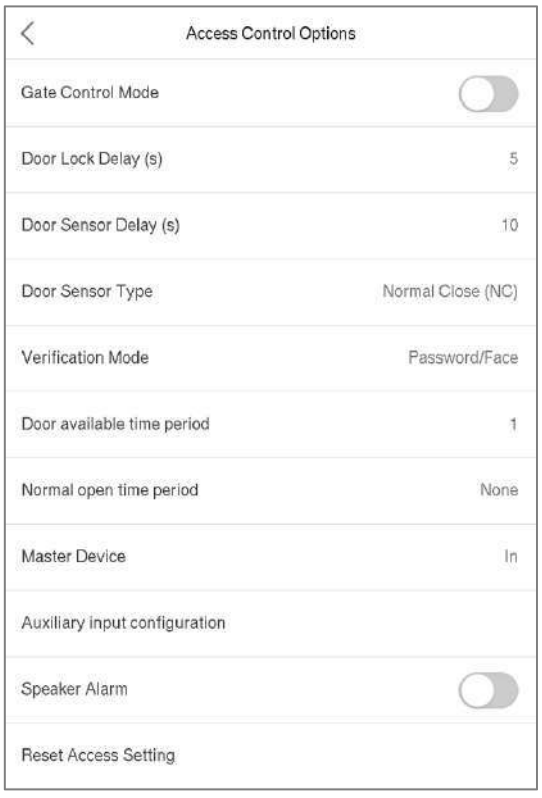
2. El grupo de usuarios debe estar en la combinación de desbloqueo de puertas (cuando hay otros grupos en el mismo combo de acceso, también se requiere la verificación de los miembros de esos grupos para desbloquear la puerta).

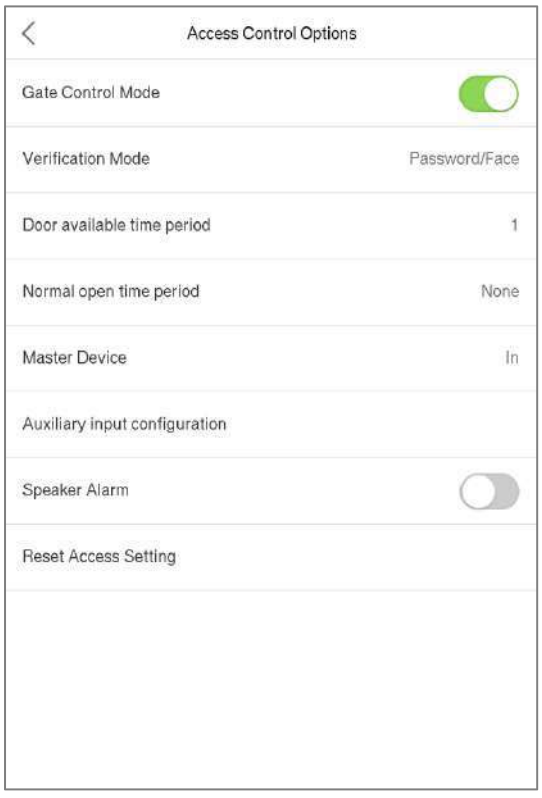
En la configuración predeterminada, los nuevos usuarios se asignan al primer grupo con la zona horaria del grupo predeterminado y el combo de acceso como "1" y se establecen en el estado de desbloqueo.

10.1 Opciones de control de acceso

Para configurar los parámetros de la cerradura de control del terminal y equipos relacionados.

Haga clic en Opciones de control de acceso en la interfaz de Control de acceso.





Articulo	Descripción
Modo de control de puerta	Seleccione si desea habilitar el modo de control de puerta. Cuando está habilitado, el relé de bloqueo de puerta, el relé de sensor de puerta y el tipo de sensor de puerta no se mostrarán.
Retraso de bloqueo de puerta (s)	El dispositivo controla la duración de la apertura de la cerradura eléctrica. Valor válido: 1 ~ 10 segundos; 0 segundos representa la desactivación de la función.
Retraso (s) del sensor de puerta	Si la puerta no está cerrada y bloqueada después de abrirse durante un tiempo determinado (retardo del sensor de puerta), se activará una alarma. El valor válido del retardo del sensor de puerta varía de 1 a 255 segundos.
Tipo de sensor de puerta	Hay tres tipos: Ninguno, Normal Abierto y Normal Cerrado. Ninguno significa que el sensor de la puerta no está en uso; Normalmente abierto significa que la puerta siempre está abierta cuando la electricidad está encendida; Normalmente cerrado significa que la puerta siempre está cerrada cuando hay electricidad.
Modo de verificación	El modo de verificación admitido incluye contraseña / rostro, solo ID de usuario, contraseña, solo rostro y rostro + contraseña.
Período de tiempo disponible de la puerta	El período de tiempo en el que el usuario puede abrir la puerta, se puede establecer en cualquiera de las 50 reglas de tiempo.
Período de tiempo abierto normal	mpo programado para el modo de "apertura normal", de modo que la puerta siempre esté desbloqueada período.
Dispositivo maestro	Al configurar los dispositivos maestro y esclavo, el estado del dispositivo maestro se puede establecer como fuera o dentro. **Salida:** el registro verificado en el host es el registro de salida. **En:** El registro verificado en el host es el registro de entrada.
Configuración de entrada auxiliar	Configure el período de tiempo de desbloqueo de la puerta y el tipo de salida auxiliar del dispositivo terminal auxiliar. Los tipos de salidas auxiliares incluyen Ninguno, Puerta del gatillo abierta, Alarma del gatillo, Puerta del gatillo abierta y Alarma.
Alarma de altavoz	Para transmitir una alarma sonora o una alarma de desmontaje desde el local. Cuando la puerta esté cerrada o la verificación sea exitosa, el sistema cancelará la alarma del local.
Restablecer configuración de acceso	Los parámetros de control de acceso restaurados incluyen el retardo de la cerradura de la puerta, el retardo del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el período de tiempo disponible de la puerta , el período de tiempo de apertura normal, el dispositivo maestro y la alarma. Sin embargo, no incluye los datos de control de acceso eliminados en Gestión de datos.

10.2 Horario

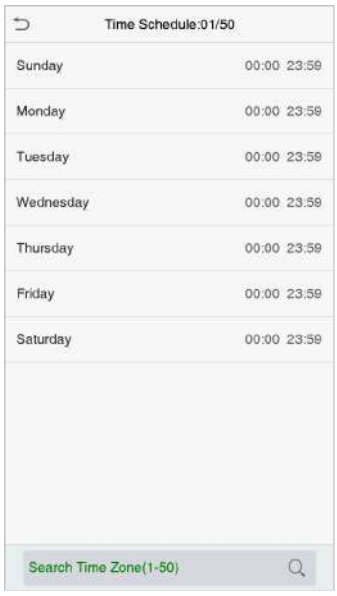
Todo el sistema puede definir hasta 50 períodos de tiempo. Cada período de tiempo representa siete zonas horarias, es decir, una semana, y cada zona horaria es un período de tiempo válido dentro de las 24 horas del día. El usuario solo puede verificar dentro del período de tiempo válido. Cada formato de zona horaria del período de tiempo: HH MM-HH MM, que tiene una precisión de minutos según el reloj de 24 horas.

Haga clic en Horario en la interfaz de Control de acceso.

1. Haga clic en el cuadro gris para ingresar una zona horaria para buscar. Ingrese el número de zona horaria (máximo: 50 zonas).

2. Haga clic en la fecha en la que se requiere la configuración de la zona horaria. Ingrese la hora de inicio y finalización, y luego presione OK.

1.



2.

Notas:

1. Cuando la hora de finalización es anterior a la hora de inicio, como 23: 57 ~ 23: 56, indica que el acceso está prohibido durante todo el día; cuando la hora de finalización es posterior a la hora de inicio, como 00: 00 ~ 23: 59, indica que el intervalo es válido.

2. El período de tiempo efectivo para desbloquear la puerta: abrir todo el día (00: 00 ~ 23: 59) o cuando la hora de finalización es posterior a la hora de inicio, como 08: 00 ~ 23: 59.

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

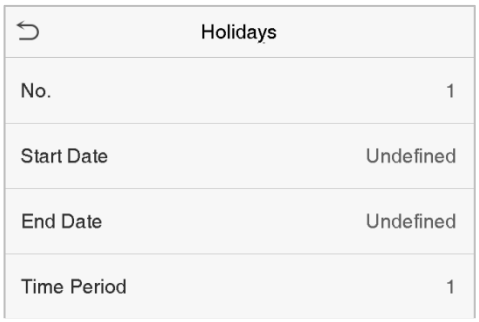
10.3 Configuración de vacaciones

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

Haga clic en Vacaciones en la interfaz de Control de acceso.

Agregar un nuevo día festivo

Haga clic en Agregar vacaciones en la interfaz de vacaciones y configure los parámetros de vacaciones.



Editar un día festivo

En la interfaz de vacaciones, seleccione un elemento de vacaciones para modificarlo. Haga clic en Editar para modificar los parámetros de vacaciones.

Eliminar un feriado

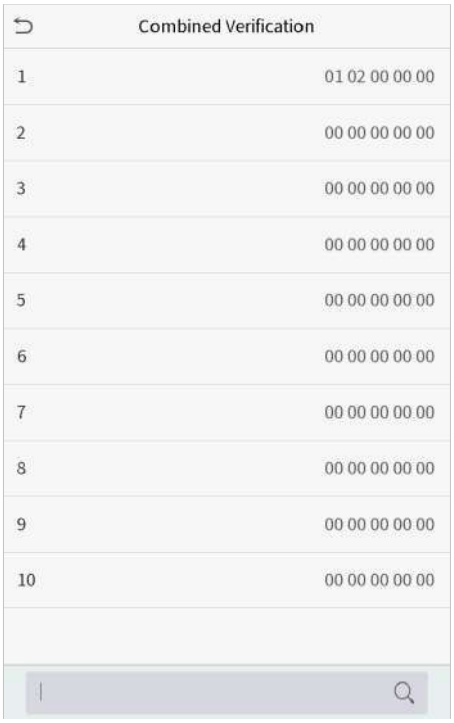
En la interfaz de vacaciones, seleccione un elemento de vacaciones para eliminar y haga clic en Eliminar. Haga clic en Aceptar para confirmar la eliminación. Después de la eliminación, este día festivo ya no se muestra en la interfaz de Todos los días festivos.

10.4 Configuración de verificación combinada

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

Haga clic en Verificación combinada en la interfaz de Control de acceso.

Haga clic en la combinación de desbloqueo de puertas que desee configurar. Haga clic en las flechas hacia arriba y hacia abajo para ingresar el número de combinación, luego presione OK.



Ejemplos:

La combinación de desbloqueo de puerta 1 se establece como (01 03 05 06 08), lo que indica que la combinación de desbloqueo 1 consta de 5 personas y las 5 personas pertenecen a 5 grupos, es decir, grupo de control de acceso 1 (grupo de CA 1), CA grupo 3, grupo de CA 5, grupo de CA 6 y grupo de CA 8, respectivamente.

La combinación de desbloqueo de puerta 2 se establece como (02 02 04 04 07), lo que indica que la combinación de desbloqueo 2 consta de 5 personas; los dos primeros son del grupo 2 de CA, los dos siguientes son del grupo 4 de CA y la última persona es del grupo 7 de CA.

La combinación de desbloqueo de puertas 3 se establece como (09 09 09 09 09), lo que indica que hay 5 personas en esta combinación; todos los cuales son del grupo AC 9.

La combinación de desbloqueo de puerta 4 se establece como (03 05 08 00 00), lo que indica que la combinación de desbloqueo 4 consta de tres personas. La primera persona es del grupo AC 3, la segunda persona es del grupo AC 5 y la tercera persona es del grupo AC 8.

Delete a door-unlocking combination

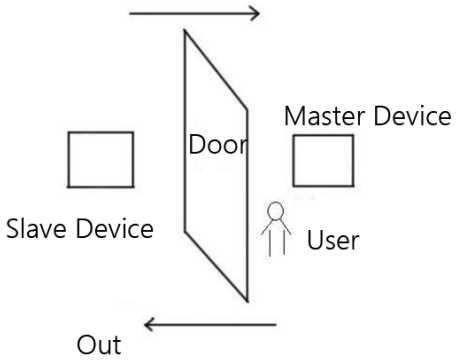
Set all group number as 0 if you want to delete door-unlocking combinations.

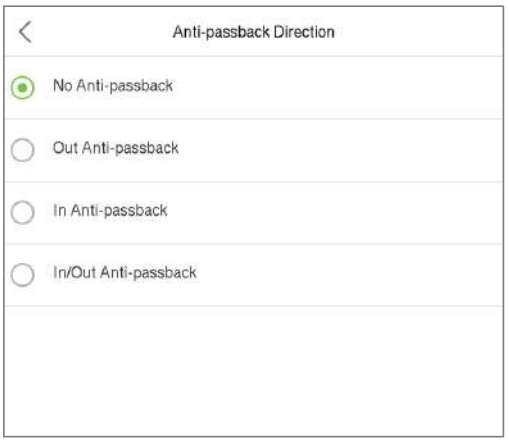
10.5 Configuración de anti-passback

Para evitar que algunas personas sigan a los usuarios y entren por la puerta sin verificación, lo que resultará en un problema de seguridad, los usuarios pueden habilitar la función anti-passback. El registro de entrada debe coincidir con el registro de salida para poder abrir la puerta.

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

Haga clic en Configuración de Anti-passback en la interfaz de Control de acceso.



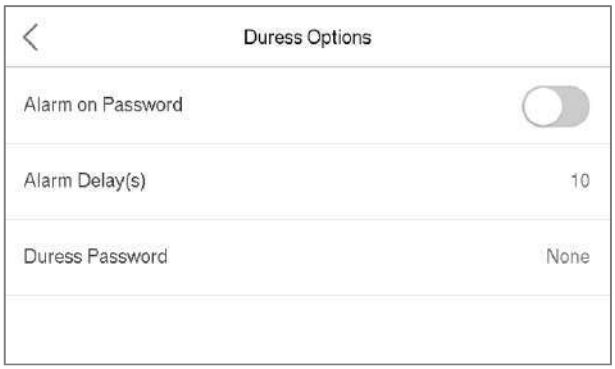


Articulo	Descripciones
Sin Anti-passback	La función Anti-Passback está deshabilitada, lo que significa que pasar la verificación en el dispositivo maestro o en el dispositivo esclavo puede desbloquear la puerta. El estado de asistencia no está reservado.
Fuera Anti-passback	Después de que un usuario se retira, solo si el último registro es un registro de entrada, el usuario puede volver a retirar; de lo contrario, se activará la alarma. Sin embargo, el usuario puede registrarse libremente.
En Anti-passback	Después de que un usuario se registra, solo si el último registro es un registro de salida, el usuario puede registrarse nuevamente; de lo contrario, se activará la alarma. Sin embargo, el usuario puede salir libremente.
Antirretorno de entrada / salida	Después de que un usuario se registra de entrada / salida, solo si el último registro es un registro de salida, el usuario puede volver a registrarse, o un registro de entrada puede volver a retirar; de lo contrario, se activará la alarma.

10.6 Configuración de opciones de amago

Si un usuario activó la función de verificación de amagocon métodos de autenticación específicos, cuando esté bajo coacción durante la autenticación con dicho método, el dispositivo desbloqueará la puerta como de costumbre, pero al mismo tiempo se enviará una señal para activar la alarma.

Haga clic en Opciones de coacción en la interfaz de Control de acceso.



Articulo	Descripción
Alarma en contraseña	Cuando un usuario utiliza el método de verificación de contraseña, se generará una señal de alarma; de lo contrario, no habrá señal de alarma.
Retardo de alarma (s)	La señal de alarma no se transmitirá hasta que haya transcurrido el tiempo de retardo de la alarma. El valor varía de 1 a 999 segundos.
Contraseña de amago	Configure la contraseña de amago de 6 dígitos. Cuando el usuario ingresa esta contraseña de coacción para verificación, se generará una señal de alarma.

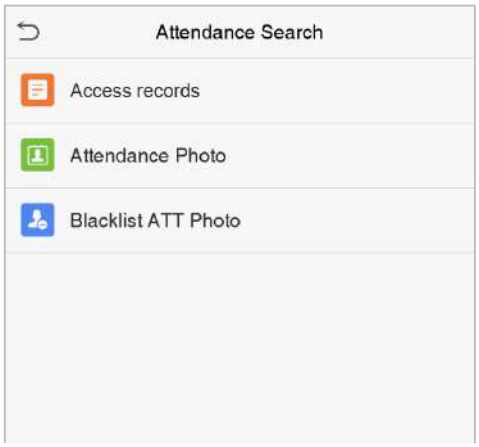
11. Búsqueda de Asistencia

Cuando se verifica la identidad de un usuario, el registro de acceso se guardará en el dispositivo. Esta función permite a los usuarios comprobar sus registros de acceso .

Haga clic en Búsqueda de asistencia en la interfaz del menú principal.

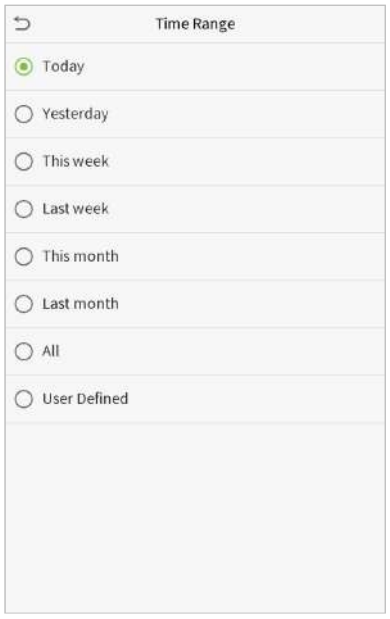
El proceso de búsqueda de fotos de asistencia y listas negras es similar al de buscar registros de asistencia / acceso. El siguiente es un ejemplo de búsqueda de registros de acceso .

En la interfaz de búsqueda de asistencia, haga clic en Registros de acceso .



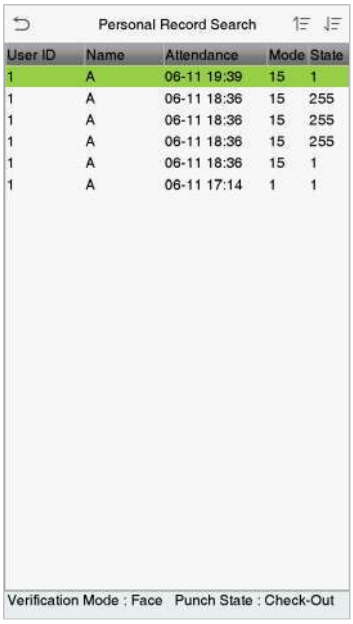
1. Introduzca la ID de usuario que se buscará y haga clic en Aceptar. Si desea buscar registros de todos los usuarios, haga clic en Aceptar sin ingresar ningún ID de usuario..

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



3. La búsqueda de registros se realiza correctamente. Haga clic en el registro en verde para ver sus detalles.

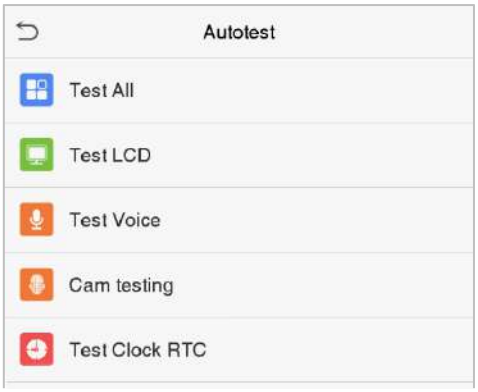
4. La siguiente figura muestra los detalles del registro seleccionado.



12. Autotest

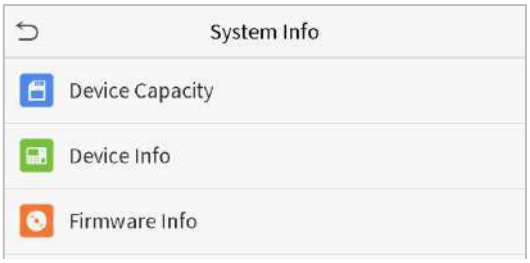
Para probar automáticamente si todos los módulos en el dispositivo funcionan correctamente, que incluyen la pantalla LCD, voz, cámara y reloj en tiempo real (RTC).

Haga clic en Autotest en la interfaz del menú principal.



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

13. Información del Sistema



Con la opción de información del sistema, puede ver el estado del almacenamiento, la información de la versión del dispositivo, etc.

Haga clic en Información del sistema en la interfaz del menú principal.

Articulo	Descripción
Capacidad del dispositivo	Muestra el almacenamiento del usuario, la contraseña, la insignia, el almacenamiento en la palma y la cara del dispositivo actual , administradores, registros de a cc e ss , fotos de asistencia y listas negras y fotos de usuario.
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la dirección MAC, la información de la versión del algoritmo facial, la información de la plataforma y el fabricante.
Información de firmware	Muestra la versión de firmware y otra información de versión del dispositivo.

14. Apéndice I

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

1) Se recomienda realizar el registro en un entorno interior con una fuente de luz adecuada sin subexposición o sobreexposición.

2) No enfoque hacia fuentes de luz exteriores como puertas o ventanas u otras fuentes de luz fuertes.

3) Se recomienda durante el registro las prendas de color oscuro sean diferentes al del color de fondo.

4) Por favor muestre su cara y frente, y no cubra su cara y cejas con su cabello.

5) Se recomienda mostrar una expresión facial sencilla. Sonreír es aceptable, pero no cierre los ojos ni incline la cabeza en ninguna orientación. Se requieren dos imágenes para personas con anteojos, una imagen con anteojos y otra sin anteojos.

6) No use accesorios como bufandas o mascarillas 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.

1)9) Se recomiendan 50 cm - 80 cm para capturar un sujeto a distancia ajustable a la altura del cuerpo.

Image1 Face Capture Area

14.2 Requisitos para datos de imagen facial digital con luz visible

La fotografía digital debe ser de bordes rectos, coloreada, retratada a medias con una sola persona, y la persona debe ser inexplorada y sin uniforme. Las personas que usan anteojos deben quedarse para ponerse los anteojos para tomar fotografías.

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

Expresión facial
Se recomienda una cara sencilla o una sonrisa con los ojos naturalmente abiertos.

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

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

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

Formato de imagen
Debe estar en BMP, JPG o JPEG.

Requisito de datos
Debe cumplir con los siguientes requisitos:

1) Fondo blanco con ropa de color oscuro.

2) Modo de color verdadero de 24 bits.

3) Imagen comprimida en formato JPG con un tamaño máximo de 20 kb.

4) Tasa de definición entre 358 x 441 y 1080 x 1920.

5) La escala vertical de la cabeza y el cuerpo debe ser 2: 1.

6) La foto debe incluir los hombros de la persona capturada al mismo nivel horizontal.

7) La persona capturada debe tener los ojos abiertos y el iris claramente visible.

8) De preferencia una sonrisa plana y no mostrar los dientes

1)9) La persona capturada debe verse claramente, de color natural y sin torsiones obvias en la imagen, sin sombras, puntos de luz o reflejos en la cara o el fondo, y con un nivel apropiado de contraste y luminosidad.

15. Apéndice II

15.1 Declaración sobre el derecho a la privacidad

Queridos clientes:

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

Declaramos que:

1.Todos nuestros dispositivos civiles de reconocimiento de huellas dactilares capturan solo características, no imágenes de huellas dactilares, y no involucran protección de privacidad.

2.Ninguna de las características de la huella dactilar que capturamos se puede utilizar para reconstruir una imagen de la huella dactilar original y no implica la protección de la privacidad.

3.Como proveedor de este dispositivo, no asumiremos ninguna responsabilidad directa o indirecta por las consecuencias que puedan resultar de su uso de este dispositivo.

4.Si desea disputar cuestiones de derechos humanos o privacidad relacionados con el uso de nuestro producto, comuníquese directamente con su distribuidor.

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

Nota:

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

1.No habrá arresto, detención, registro o infracción ilegal de personas.

2.La dignidad personal está relacionada con la libertad personal y no debe ser violada.

3.La casa de un ciudadano no puede ser violada.

4.El derecho a la comunicación de un ciudadano y la confidencialidad de esa comunicación están protegidos por la ley.

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

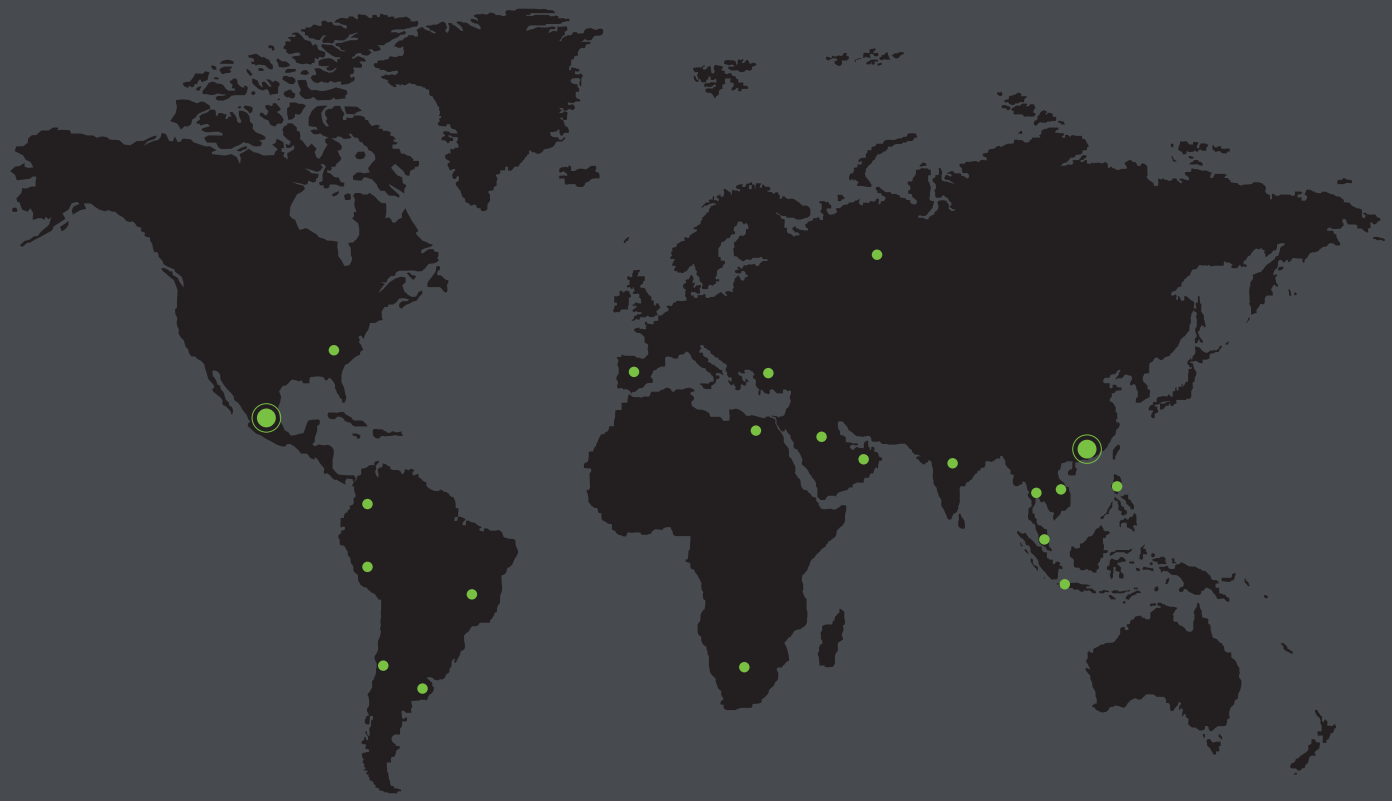
15.2 Operación ecológica

El "período operativo ecológico" del producto se refiere al período de tiempo durante el cual este producto no descargará ninguna sustancia tóxica o peligrosa cuando se use 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

Nombre del componente	Sustancia / elemento peligroso / tóxico					
	Plomo (Pb)	Mercurio (Hg)	Cadmio (Cd)	Cromo hexavalente (Cr6 +)	Bifenilos polibromados (PBB)	Éteres de difenilo polibromados (PBDE)
Resistencia de chip	×	○	○	○	○	○
Condensador de chip	×	○	○	○	○	○
Inductor de chip	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
Componente ESD	×	○	○	○	○	○
Zumbador	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Empulgueras	○	○	○	×	○	○

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



www.zkteco.com

www.zktecolatinoamerica.com