MANUAL DE USUARIO

Elite Series

Elite Pass / Elite Access

Fecha: Octubre 2020

Versión: 2.1

Español

Green Label

Gracias por elegir nuestro producto. Lea atentamente las instrucciones 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**

Copyright © 2020 ZKTECO CO., LTD. Todos los Derechos Reservados

Marca Registrada

ZKTeco es una marca registrada de ZKTeco. Las 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 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 las operaciones de Elite Series.

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

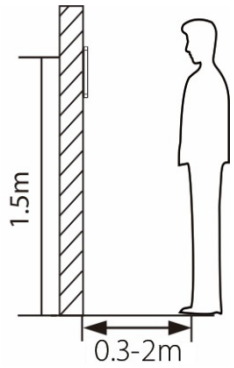
Contenido

1. Instrucción de Uso

Antes de llegar a las características de rostro y sus funciones del dispositivo, se recomienda familiarizarse con los fundamentos primarios.

Posición de pie , expresión facial y postura

- Distancia recomendada



Se recomienda tener un espacio de 0,5 m entre el dispositivo y el usuario cuya altura esté en un rango de 1,55m a 1,85 m. Los usuarios pueden moverse ligeramente hacia adelante o hacia atrás para mejorar el reconocimiento facial.

- Expresión facial de postura de pie

NOTA : Durante la inscripción y la verificación, por favor, mantener naturales facial expresión y de pie postura.

1. Instrucción de Uso

REGISTRO FACIAL

Trate de mantener la Rostro en el centro de la pantalla durante el registro. Por favor, la Rostro hacia la cámara y permanecer quieto durante el registro. La pantalla debería verse así:

Métodos de autenticación y registro facial

Instrucciones 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 cambiar la expresión facial. (sonriendo, enojado, guiñando un ojo, etc.)

• Si no sigue las instrucciones en pantalla, el registro facial puede tardar más o fallar.

• Tenga cuidado de no cubrirse los ojos o las cejas.

• No use sombreros, anteojos de sol o anteojos.

• Tenga cuidado de no mostrar dos Rostros en la pantalla. Registre solo una persona a la vez..

• Se recomienda que un usuario con gafas registre al mismo tiempo su rostro con y sin gafas.

Instrucciones para autenticar un rostro

• Asegúrese de que la Rostro aparezca dentro del área de detección que se muestra en la pantalla del dispositivo.

• Si usted ha cambiado sus anteojos, la autenticación puede fallar. Si ha registrado su Rostro sin gafas, autentique su Rostro sin gafas. Si se ha registrado la Rostro con gafas, autentique nuevamente su Rostro con las gafas usadas con las que se registro.

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

1. Instrucción de Uso

INTERFAZ DE ESPERA

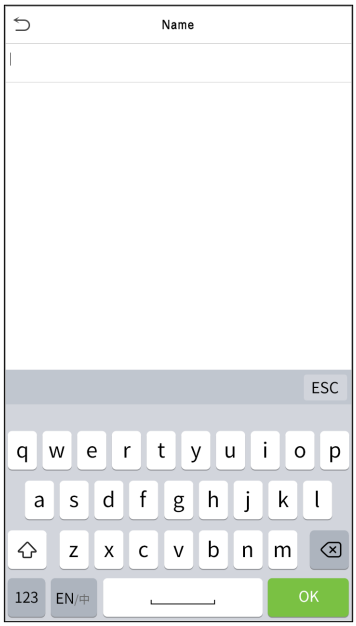
Después de conectar la fuente de alimentación, se muestra la siguiente interfaz de espera:

Nota:

1. Haga clic para ingresar a la interfaz de entrada de ID de usuario.

2. Cuando no haya un superadministrador configurado en el dispositivo, haga clic para ingresar al menú. Después de configurar el superadministrador, se requiere la verificación del superadministrador antes de ingresar a la operación del menú. Para la seguridad del dispositivo, se recomienda registrar el superadministrador la primera vez que utilice el dispositivo.

TECLADO VIRTUAL



Nota:

El dispositivo admite la entrada de chino, inglés, números y símbolos. Haga clic en [En] para cambiar al teclado en inglés. Presione [123] para cambiar al teclado numérico y simbólico, y haga clic en [ABC] para volver al teclado alfabético. Haga clic en el cuadro de entrada, aparece el teclado virtual. Haga clic en [ESC] para salir de la entrada.

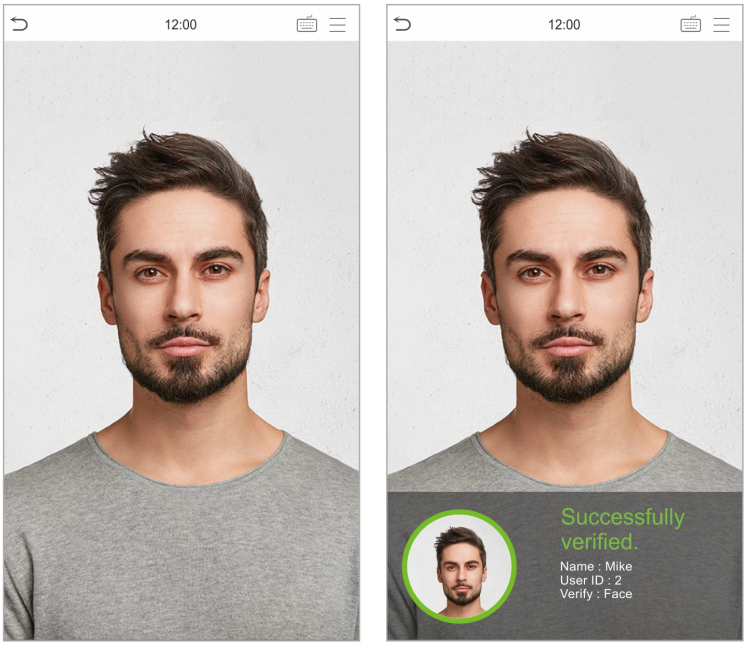
MODO DE VERIFICACIÓN

Verificación Facial

Verificación Facial 1: N (uno a varios)

1.Verificación convencional

Este modo de verificación compara las imágenes faciales adquiridas con todos los datos faciales registrados en el dispositivo. A continuación, se muestra el cuadro de aviso emergente del resultado de la comparación.

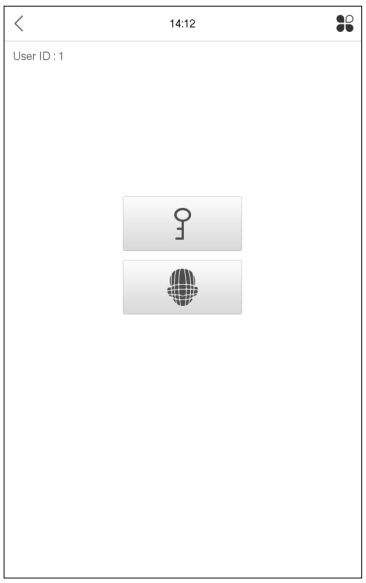


3. Verificación Facial 1: 1 (uno a uno)

Este modo de verificación compara el rostro capturado por la cámara con la plantilla facial relacionada con ID de usuario ingresado.

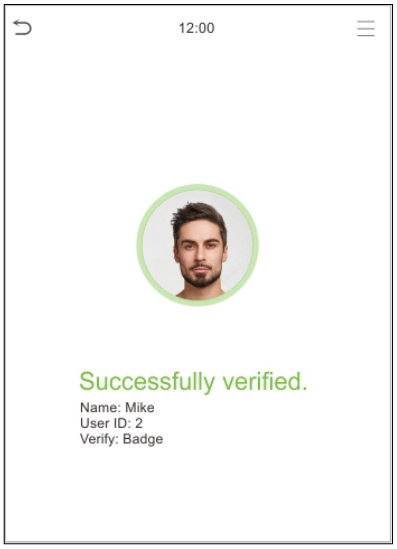
Presione  en la interfaz principal e ingrese al modo de verificación facial 1: 1 (uno a uno). Introduzca el ID de usuario y haga clic en [Aceptar].

Si un empleado registra Contraseña además del rostro, y el método de verificación se establece en Contraseña/Rostro, La siguiente pantalla aparecerá. Seleccione el icono  para ingresar al modo de verificación facial.



1. Instrucción de Uso

Después de una verificación exitosa, aparecerá el cuadro de aviso " verificado exitosamente ".



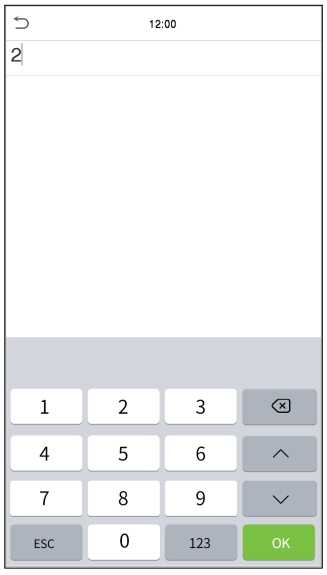
Si la verificación falla, aparecerá el mensaje "¡Por favor, ajuste su posición!".

Verificación de contraseña

El modo de verificación de contraseña compara la contraseña ingresada con el ID de usuario y la contraseña registrados.

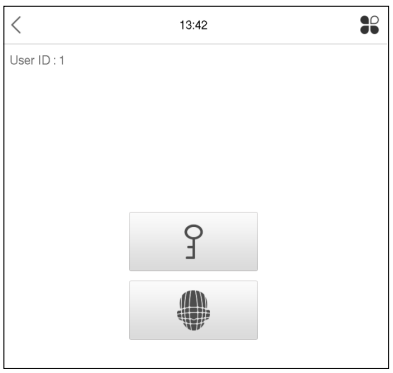
Haga clic en el botón de la pantalla principal para abrir el modo de verificación de contraseña 1: 1 (uno a uno).

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

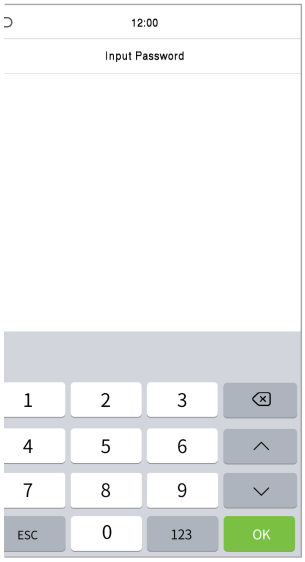


1. Instrucción de Uso

Si un empleado registra Rostro además de Contraseña, y el método de verificación es contraseña / Rostro, aparecerá la siguiente pantalla. Selecciona el ícono  para ingresar al modo de verificación de Contraseña.

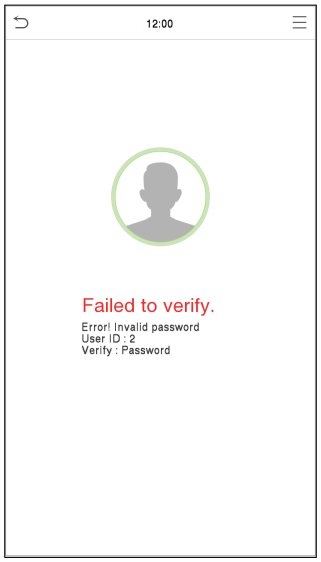


2. Ingrese la Contraseña y presione [OK].



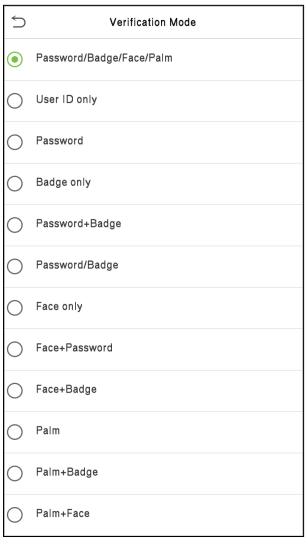
Verificación Exitosa

Verificación Fallida



Verificación combinada

Para aumentar la seguridad, este dispositivo ofrece la opción de utilizar múltiples métodos de verificación. Se pueden utilizar un total de 12 combinaciones de verificaciones diferentes, como se muestra a continuación:



Nota:
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 de Rostro pero el modo de verificación es Rostro + Contraseña, este usuario nunca pasará la verificación.

2. Menú Principal

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

Menú	Descripción
Usuarios	Para agregar, editar, ver y eliminar información básica sobre un usuario.
Privilegios	Para establecer el alcance del permiso del rol personalizado y el registrador, es decir, los derechos para operar el sistema.
Red	Para configurar los parámetros relevantes de red, comunicación en serie, conexión a PC, WIFI, nube servidor y Wiegand.
Sistema	Para configurar los parámetros relacionados con el sistema, incluida la fecha y la hora, los registros de acceso, las plantillas faciales, restablecimiento de la configuración de fábrica y gestión de la temperatura.
Personalizar	Para personalizar la configuración de la pantalla de la interfaz, el audio y el timbre.
Datos	Para eliminar todos los datos relevantes en el dispositivo.
Acceso	Para configurar los parámetros de la cerradura y el dispositivo de control de acceso correspondiente.
Búsqueda de Eventos	Consulte el registro de acceso especificado, verifique las fotos de asistencia y las fotos de la lista negra.
Pruebas	Para probar automáticamente si cada módulo funciona correctamente, incluida la pantalla, el audio, cámara y reloj en tiempo real.
Información	Para ver la capacidad de datos, el dispositivo y la información de firmware del dispositivo actual.

3. Gestión de Usuarios

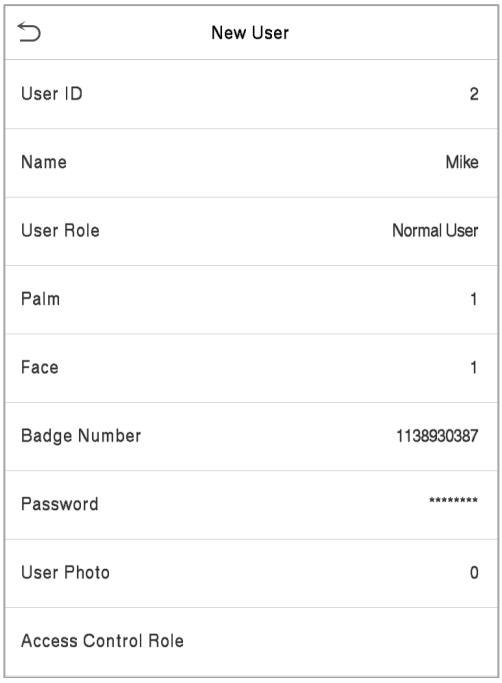
AGREGAR USUARIOS

Haga clic en User Mgt. en el menú principal.

Haga clic en Nuevo usuario.

Registrar un ID de usuario y un nombre

Ingrese el ID de usuario y el nombre



Notas:

1. Un nombre de usuario puede contener 17 caracteres.

2. El ID de usuario puede contener de 1 a 9 dígitos predeterminadamente.

3. Durante el registro inicial, puede modificar su ID, que no se puede modificar después del registro.

4. Si aparece un mensaje "El ID ya existe", debe elegir otro ID.

Configuración de la función del usuario

Hay dos tipos de cuentas de usuario: los usuarios normales 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 personalizados para el usuario.

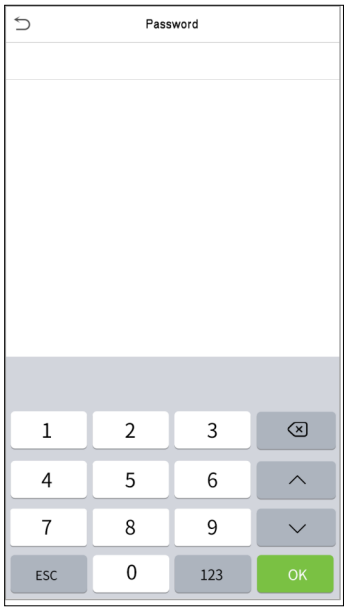
Haga clic en Rol de usuario para seleccionar Usuario normal o Superadministrador.

Nota: Si el rol de usuario seleccionado es el superadministrador, el usuario debe pasar la autenticación de identidad para acceder al menú principal.

3. Gestión de Usuarios

Registrar Rostro

Haga clic en la palma de abrir la palma de la página de registro. Seleccione la palma que desea dar de alta.



Registrar Contraseña

Haga clic en Contraseña para abrir 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 predeterminadamente.

3. Gestión de Usuarios

Registrar foto de usuario

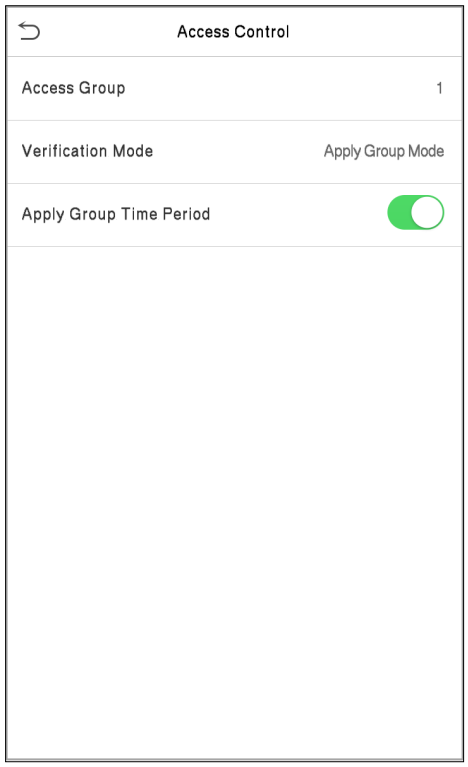
Cuando un usuario registrado con una foto pasa la autenticación, se mostrará la foto registrada. Haga clic en Foto de usuario; haga clic en el icono de la cámara para tomar una foto. El sistema volverá a la interfaz de nuevo usuario después de tomar una foto.

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 de usuarios establece los derechos de desbloqueo de puertas de cada persona, incluido el grupo y el período de tiempo al que pertenece el usuario. 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.

Haga clic en Período de tiempo, seleccione el período de tiempo que desee utilizar.



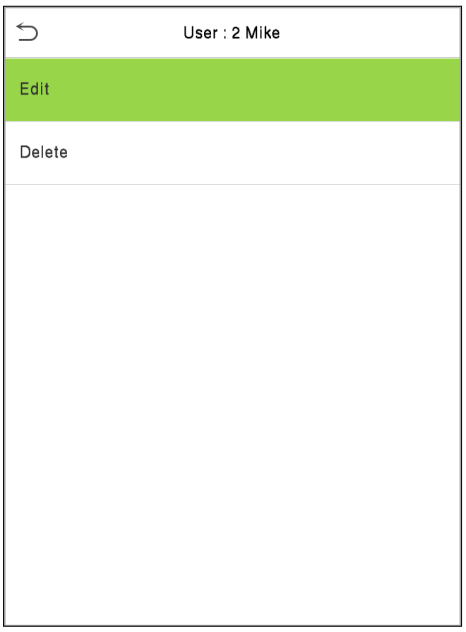
BÚSQUEDA DE USUARIOS

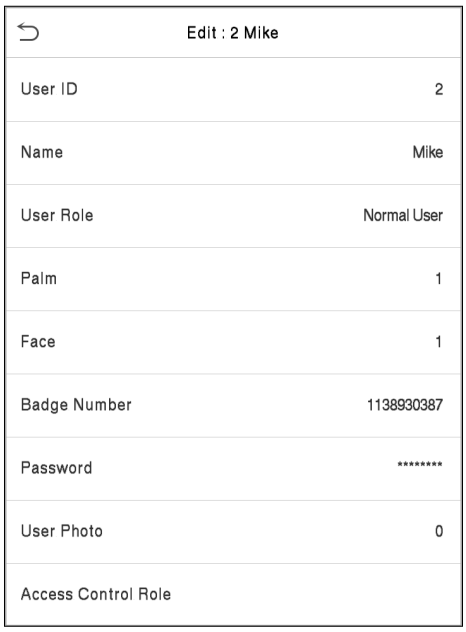
Haga clic en la barra de búsqueda en la lista de usuarios e ingrese la palabra clave (la palabra clave puede ser una ID, apellido o nombre completo) . El sistema buscará los usuarios relacionados con la información.

3. Gestión de Usuarios

EDITAR USUARIOS

Seleccione un usuario de la lista y haga clic en Editar para ingresar a la interfaz de edición de usuario.



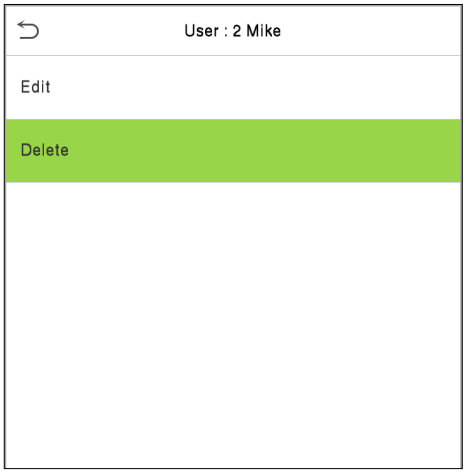


Nota: La operación de editar un usuario es la misma que la de agregar un usuario, excepto que el ID de usuario no se puede modificar al editar un usuario. Para más detalles, consulte "43.1 Agregar usuarios ".

BORRAR USUARIOS

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

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



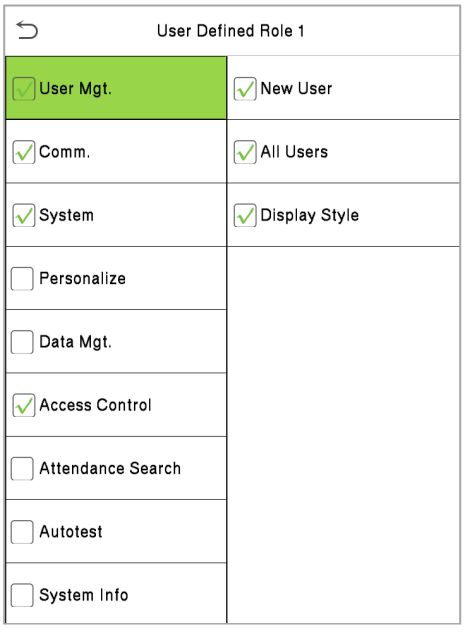
4. Rol de Usuario

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.

Haga clic en cualquier rol de usuario para establecer un rol definido. Alterne el botón Habilitar rol definido para habilitar este rol definido. Haga clic en Nombre e ingrese el nombre del rol.

1. Haga clic en Definir función de usuario para asignar privilegios a la función. Una vez que se complete la asignación de privilegios, haga clic en Volver.

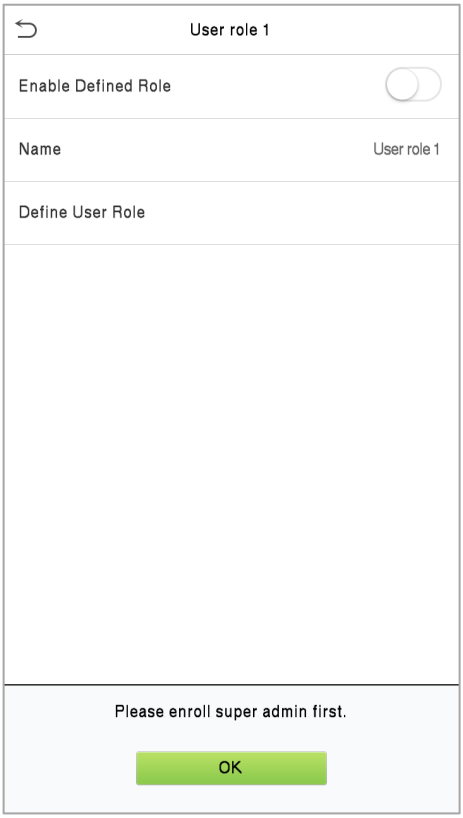


Nota: Durante la asignación de privilegios, el menú principal está a la izquierda y sus submenús están a la derecha. Solo necesita seleccionar las funciones en los submenús.

Si el dispositivo hace una función activada, puede asignar las funciones que establezca para los usuarios haciendo clic con el usuario Mgt. > Nuevo usuario> Rol de usuario.

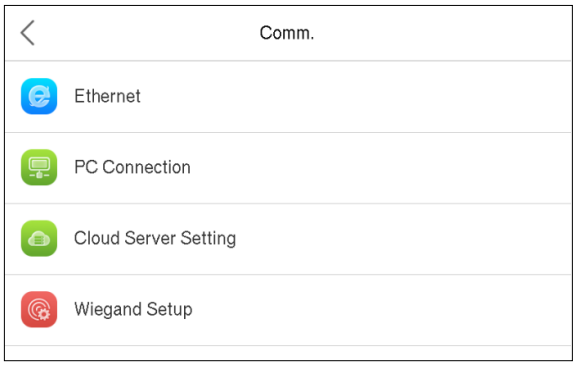
5. Configuración de Comunicación

Si no hay ningún superadministrador registrado, el dispositivo mostrará " P leaseinscribirse super administrador¡primero!" después de hacer clic en la barra de habilitación, Como se muestra abajo.



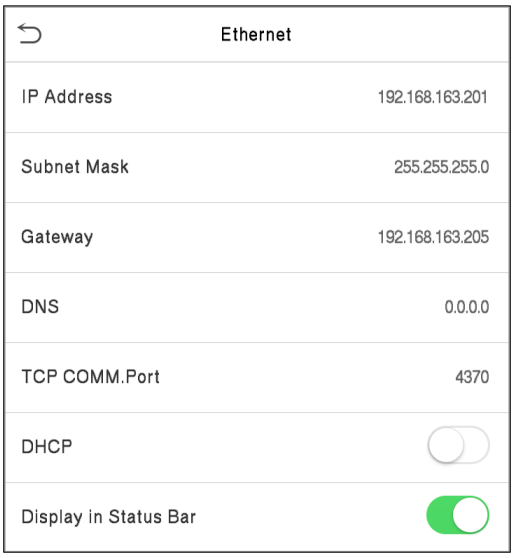
CONFIGURACIÓN DE COMUNICACIÓN

Los ajustes de comunicación se utilizan para configurar los parámetros de la red, la conexión a la PC ,Red inalámbrica, Servidor en la nube y Wiegand.
Toque RED . en el menú principal.



Configuración de red

Cuando el dispositivo necesita comunicarse con una PC a través de Ethernet, debe configurar los ajustes de red y asegurarse de que el dispositivo y la PC se estén conectando al mismo segmento de red.
Haga clic en Ethernet en la interfaz de RED.



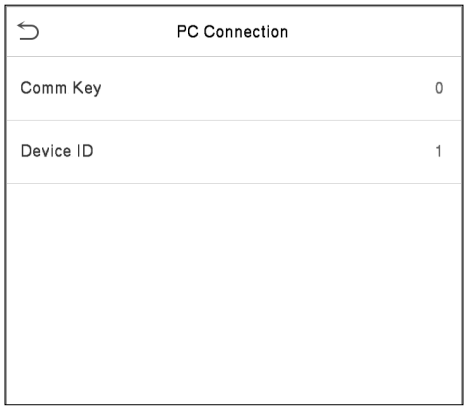
5. Configuración de Comunicación

Menú	Descripción
Dirección IP	El valor predeterminado de fábrica es 192.168.1.201. Configure la dirección IP según los requisitos.
Cubrebocas de subred	El valor predeterminado de fábrica es 255.255.255.0. Establezca el valor según los requisitos.
Puerta de enlace	La dirección predeterminada de fábrica es 0.0.0.0. Establezca el valor según los requisitos.
DNS	La dirección predeterminada de fábrica es 0.0.0.0. Establezca el valor según los requisitos.
Puerto de comunicación	El valor predeterminado de fábrica es 4370. Configure el valor según los requisitos.
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.

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, se debe ingresar esta contraseña de conexión antes de que el dispositivo se pueda conectar al software de la PC.

Haga clic en Conexión a PC en RED. Interfaz de configuración .

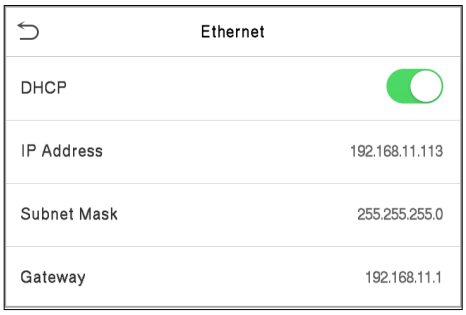


Menú	Descripción
Clave de comunicación	Clave de comunicación: la contraseña predeterminada es 0, que se puede cambiar. La clave de comunicación puede contener de 1 a 6 dígitos.
ID del dispositivo	El número de identidad del dispositivo, que varía entre 1 y 254. Si el método de comunicación es RS232 /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

5. Configuración de Comunicación

Opciones avanzadas

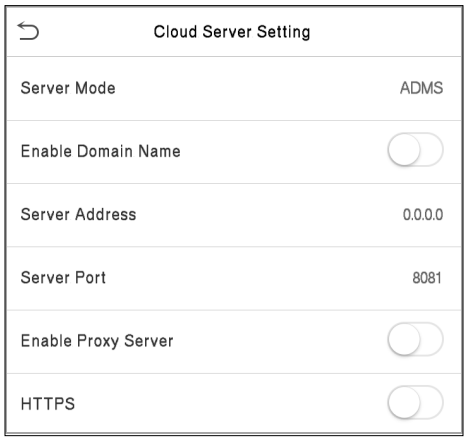
Se utiliza para configurar los parámetros de la red Wi-Fi.



Menú	Descripción
DHCP	Abreviatura de Dynamic Host Configuration Protocol, que implica la asignación de direcciones IP dinámicas a los clientes de la red.
Dirección IP	Dirección IP de la red Wi-Fi.
Cubrebocas de subred	Cubrebocas de subred de la red Wi-Fi.
Puerta	Dirección de puerta de enlace de la red Wi-Fi.

CONFIGURACIÓN DEL SERVIDOR DE NUBE

Esto representa la configuración utilizada para conectar el servidor ADMS. Haga clic en Configuración del servidor de nube en la Interfaz de configuración de RED.



5. Configuración de Comunicación

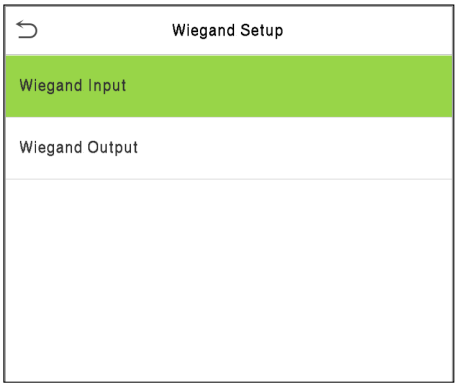
Menú		Descripción
Habilitar nombre de dominio	Dirección del servidor	Cuando esta función está habilitada, se utilizará el modo de nombre de dominio "http: // ...", como http://www.XYZ.com, mientras que "XYZ" indica el nombre de dominio cuando este modo está encendido.
Deshabilitar el nombre de dominio	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.

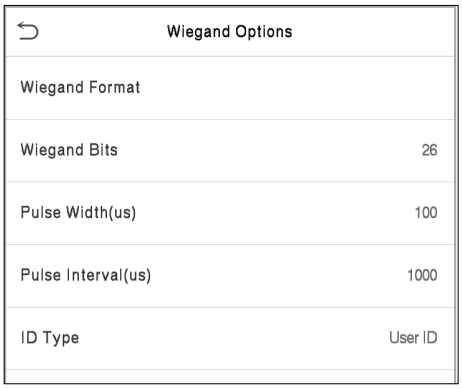
CONFIGURACIÓN DE WIEGAND

El menú se utiliza para configurar los parámetros de entrada y salida de Wiegand.

Haga clic en Ajustes Wiegand en la Interfaz de configuración de RED.

Entrada Wiegand



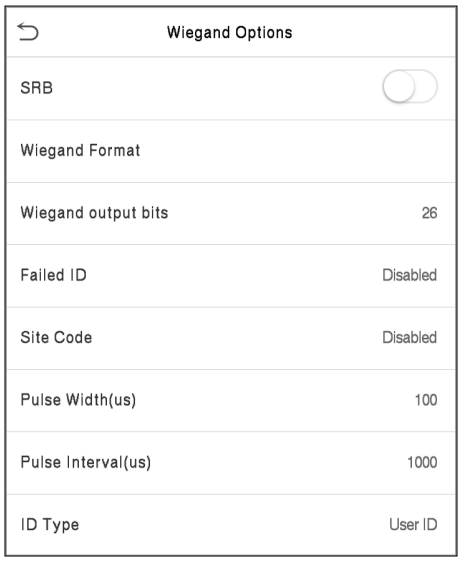


5. Configuración de Comunicación

Menú	Descripción
Formato Wiegand	Los valores oscilan entre 26 bits, 34 bits, 36 bits, 37 bits y 50 bits.
Pedazos de Wiegand	Número de bits de datos Wiegand.
Ancho de pulso (mu.)	El valor del ancho de pulso enviado por Wiegand es de 100 microsegundos por defecto, que se puede ajustar dentro del rango de 20 a 100 microsegundos.
Intervalo de pulso (mu.)	El valor predeterminado es 1000 microsegundos, que se puede ajustar dentro del rango de 200 a 20000 microsegundos.
Tipo de identificación	Seleccione entre el ID de usuario y el número de placa.

Definiciones de varios formatos Wiegand comunes:

Salida Wiegand



5. Configuración de Comunicación

Formato Wiegand	Definiciones
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El primer bit es el bit de paridad par de los bits 2º a 13º, mientras que el bit 26º es el bit de paridad impar de los bits 14º a 25º. Los bits 2 a 25 son los números de tarjeta.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El primer bit es el bit de paridad par de los bits 2º a 13º, mientras que el bit 26º es el bit de paridad impar de los bits 14º a 25º. Los bits 2 a 9 son los códigos de sitio, mientras que los bits 10 a 25 son los números de tarjeta.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El primer bit es el bit de paridad par de los bits segundo a 17, mientras que el bit 34 es el bit de paridad impar de los bits 18 a 33. Los bits 2 a 25 son los números de tarjeta.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El primer bit es el bit de paridad par de los bits segundo a 17, mientras que el bit 34 es el bit de paridad impar de los bits 18 a 33. Los bits 2 a 9 son los códigos de sitio, mientras que los bits 10 a 25 son los números de tarjeta.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El primer bit es el bit de paridad impar del segundo al décimo octavo bit, mientras que el bit 36 es el bit de paridad par del decimonoveno al treinta y cinco bits. Los bits 2 a 17 son los códigos de dispositivo. Los bits 18 a 33 son los números de tarjeta y los bits 34 a 35 son los códigos del fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consta de 36 bits de código binario. El primer bit es el bit de paridad par del segundo al décimo octavo bit, mientras que el bit 36 es el bit de paridad impar del decimonoveno al treinta y cinco bits. Los bits del 2 al 19 son los códigos de dispositivo, y los bits del 20 al 35 son los números de la tarjeta.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCE Consta de 37 bits de código binario. El primer bit es el bit de paridad impar del segundo al décimo octavo bit, mientras que el 37o bit es el bit de paridad par del decimonoveno al 36o bit. Los bits segundo a cuarto son los códigos del fabricante. Los bits 5 a 16 son los códigos de sitio, y los bits 21 a 36 son los números de tarjeta.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCO Consta de 37 bits de código binario. El primer bit es el bit de paridad par del segundo al decimoctavo bits, mientras que el 37.o bit es el bit de paridad impar del decimonoveno al 36o bit. Los bits segundo a cuarto son los códigos del fabricante. Los bits 5 a 14 son los códigos de dispositivo, los bits 15 a 20 son los códigos de sitio, y los bits 21 a 36 son los números de tarjeta.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 50 bits de código binario. El primer bit es el bit de paridad par de los bits 2 a 25, mientras que el bit 50 es el bit de paridad impar de los bits 26 a 49. Los bits 2 a 17 son los códigos de sitio, y los bits 18 a 49 son los números de tarjeta.

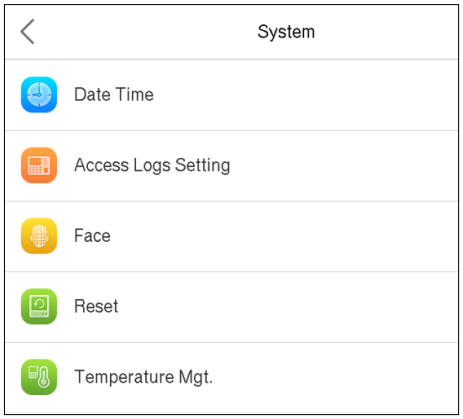
6. Configuración del Sistema

"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" denota el código del fabricante; "P" denota el bit de paridad; y "S" indica el código del sitio.

CONFIGURACIÓN DEL SITEMA

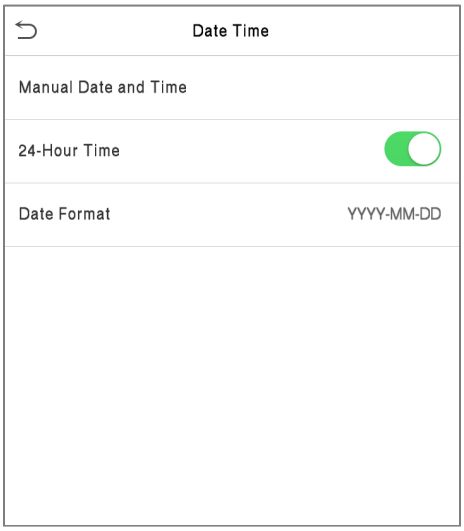
La configuración del sistema se utiliza para establecer los parámetros del sistema relacionados para optimizar el rendimiento del dispositivo.

Haga clic en Sistema en la interfaz del menú principal.



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.Puede configurar manualmente la fecha y la hora y hacer clic en Confirmar para guardar.

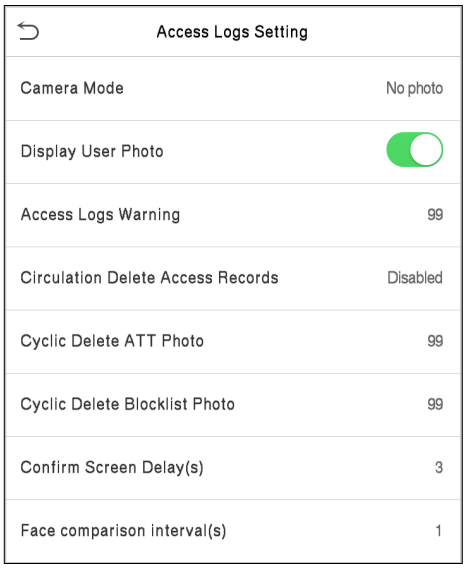
Al restaurar a fábrica los justes, el tiempo (24 -Hora) y formato de fecha (AAAA-MM-DD) pueden ser restauradas, pero la fecha y la hora del dispositivo no se pueden recuperar.

Nota: Por ejemplo, el usuario ajusta el tiempo del dispositivo (18:35 el 15 de marzo, 2019) a las 18:30 horas del 1 de enero de 2020. Después de la restauración de la configuración de fábrica s , el tiempo del dispositivo cambiará a 18: 30, 1 de enero de 2020.

6. Configuración del Sistema

CONFIGURACIÓN DE REGISTROS DE ACCESO

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

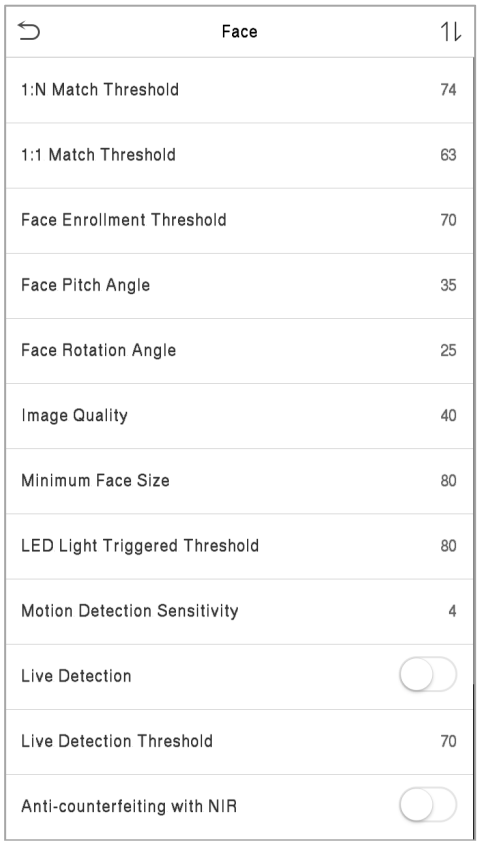


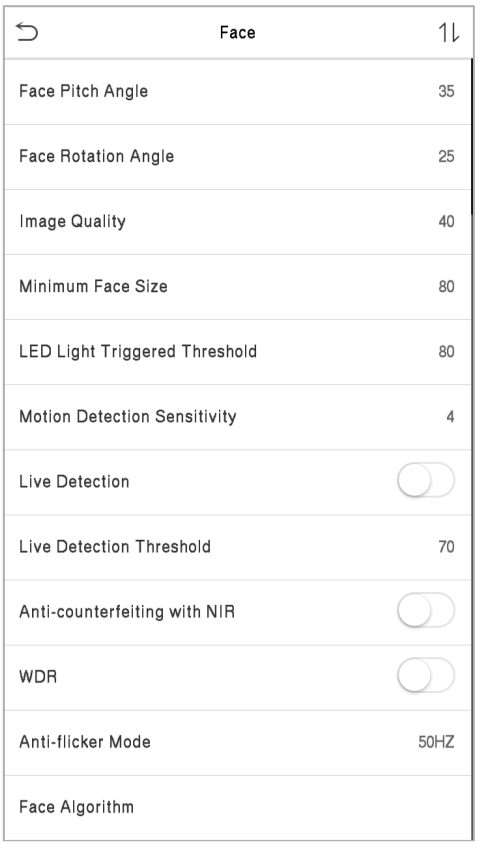
Menú	Descripción
Modo cámara	Ya sea para capturar y guardar la imagen instantánea actual durante la verificación. Hay 5 modos: Sin foto: no se toma ninguna foto durante la verificación del usuario. Tomar foto, no guardar: la foto se toma pero no se guarda durante la verificación. Tomar una foto y guardar: 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.
Eventos de Excepción	Cuando el espacio de registro restante alcanza un valor preestablecido, el dispositivo mostrará automáticamente una advertencia. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999.
Borrar Eventos antiguos	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.
Borrado Cíclico de Fotos de Asistencia	Cuando las fotos de asistencia hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un valor establecido de las fotos de asistencia antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Borrado Cíclico Fotos de Lista Negra	Cuando bl o cklisted fotos han alcanzado la plena capacidad, el dispositivo borrará automáticamente un valor establecido de edad bl o fotos cklisted. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
(s)	El tiempo que el mensaje de éxito se muestra en la pantalla. El rango válido es de 1 a 9 segundos.
Intervalo (s) de comparación de caras	Para configurar el intervalo de tiempo de coincidencia de la plantilla facial según sea necesario. El intervalo de tiempo válido es de 0 a 9 segundos.

6. Configuración del Sistema

PARÁMETROS DE ROSTRO

Haga clic en Rostro en la interfaz del sistema .





Menú	Descripción
Umbral de Verificación 1: N (uno a muchos)	En el modo de verificación 1: N (uno a muchos), 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 Verificación1: 1 (uno a uno)	En el modo de verificación 1: 1 (uno a uno), 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 son los umbrales, menor es la tasa de errores de juicio, mayor es la tasa de rechazo y viceversa. Se recomienda el valor predeterminado de 63.
Umbral de enrolado de rostros	Durante el registro facial, se utiliza la comparación 1: N (uno a muchos) 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 rostro	Es la tolerancia al ángulo de inclinación de un rostro para el registro facial y la verificación. Si el ángulo de inclinación de un rostro excede este valor establecido, será filtrado por el algoritmo, es decir, ignorado por la terminal, por lo que no se activará ninguna interfaz de registro o verificación.

6. Configuración del Sistema

Angulo de rotación de rostro	La tolerancia del ángulo de rotación de una cara para el registro y la comparación de plantillas faciales. Si el ángulo de rotación de una cara excede este valor de ajuste, se filtra por el algoritmo, es decir, ignorada por el terminal por lo tanto no r se activarán EGISTRO y la interfaz de comparación.
Calidad de la imagen	Calidad de imagen para registro facial y comparación. Cuanto mayor sea el valor, más clara será la imagen.
Tamaño mínimo de la cara	Requerido para el registro facial y la comparación. Si el tamaño de un objeto es menor que este valor establecido, el objeto 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 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 de activación de luz LED	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, con mayor frecuencia se encenderá la luz LED.
Sensibilidad de detección de movimiento	Una medida de la cantidad de cambio en el campo de visión de una cámara que califica 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 se activa con frecuencia.
Detección de vida	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 de vida	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.
Detección de rostro falso 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 utiliza cuando WDR está desactivado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea con la misma frecuencia que la luz.
Algoritmo facial	Solía hacerlo actualizar o ver la versión principal y la versión secundaria del algoritmo de la carametro, y pausar la actualización de la plantilla facial.
Notas	Un ajuste inadecuado de los parámetros de exposición y calidad puede afectar gravemente al rendimiento del dispositivo. Ajuste el parámetro de exposición solo bajo la guía del personal de servicio posventa de nuestra empresa.

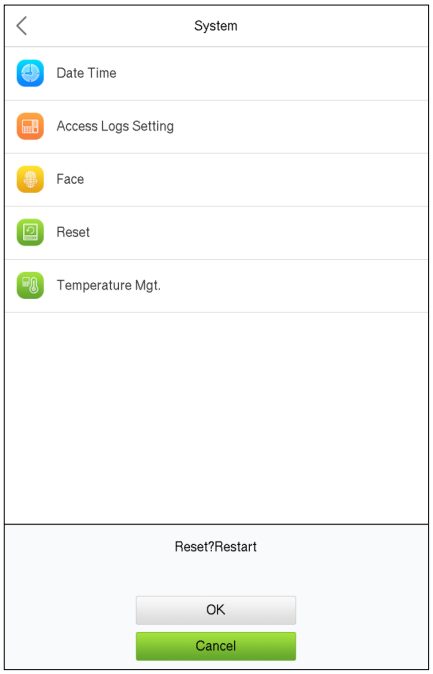
7. Personalización

RESTABLECIMIENTO DE FÁBRICA

Esta opción restaura el dispositivo, como la configuración de comunicación y la configuración del sistema, a la configuración de fábrica (no borra los datos de usuario registrados).

Haga clic en Restablecer en la interfaz del sistema .

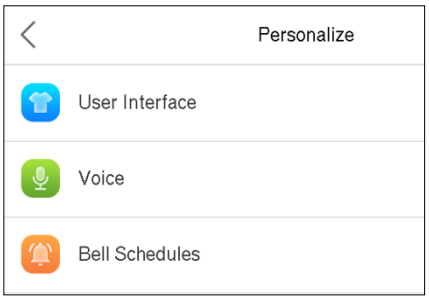
Haga clic en Aceptar para restablecer.



PERSONALIZACIÓN

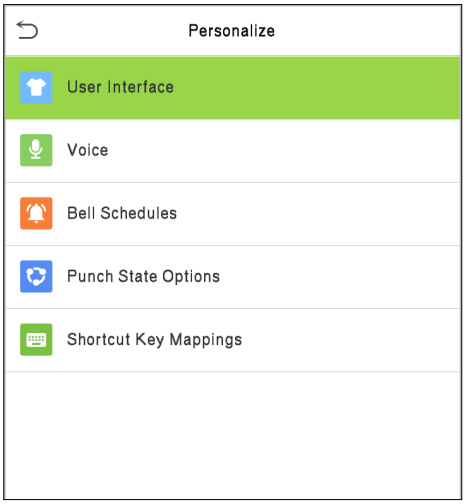
Puede personalizar la configuración de la interfaz , el audio y el timbre.

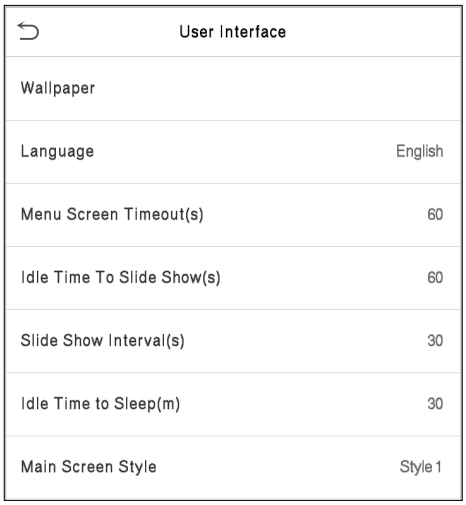
Haga clic en Personalizar en la interfaz del menú principal .



CONFIGURACIÓN DE LA INTERFAZ

Puede personalizar el estilo de visualización de la interfaz principal. Haga clic en Interfaz de usuario en la interfaz Personalizar.



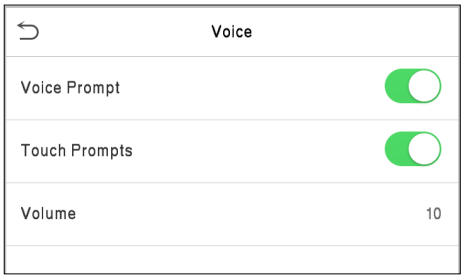


7. Personalización

Menú	Descripción
Fondo de pantalla	Para seleccionar el fondo de pantalla de la pantalla principal según sus preferencias personales.
Idioma	Para seleccionar el idioma del dispositivo.
Tiempo de espera del menú (s)	Cuando no hay operación y el tiempo excede el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. Puede deshabilitar la función o establecer el valor entre 60 y 99999 segundos.
Tiempo para protector de pantalla	Cuando no se realiza 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 de imágenes	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 para reposo (m)	Si ha activado el modo de suspensión, cuando no haya ninguna operación, el dispositivo entrará en el 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.

CONFIGURACIÓN DE VOZ

Haga clic en Voz en la interfaz Personalizar.

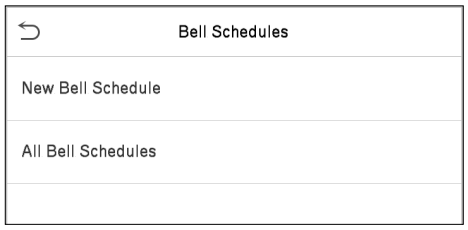


Menú	Descripción
Mensaje de voz	Seleccione si desea habilitar las indicaciones de voz durante la operación.
Sonido de touchscreen	Seleccione si desea habilitar los sonidos del teclado.
Volumen	Ajuste el volumen del dispositivo; valor válido: 0 a 100.

7. Personalización

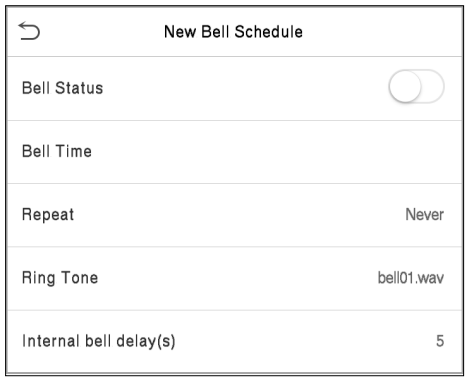
TIMBRE PROGRAMADO

Haga clic en Timbres programados en la interfaz Personalizar.



Agregar un timbre

1. Haga clic en Nuevo horario de timbre para ingresar a la interfaz de adición:



Menú	Descripción
Estado del timbre	Establezca si desea habilitar el timbre.
Tiempo de Timbre	A esta hora del día, el dispositivo hará sonar el timbre automáticamente.
Repetir	Configure el ciclo de repetición de la campana.
Tono	Seleccione un tono de timbre.
Duración del timbre	Configure la duración del timbre interno. Los valores válidos oscilan entre 1 y 999 segundos.

2. Volver a la interfaz de Horarios de Timbre; haga clic en Todos los horarios de campana para ver el timbre recién agregado.

Editar un timbre

En la interfaz Horarios de Timbre, toque el timbre para editarlo.

• Haga clic en Editar, el método de edición es el mismo que las operaciones de agregar un timbre

Eliminar una campana

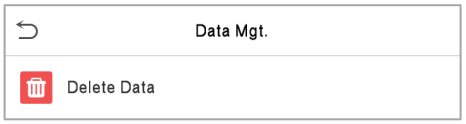
• En la interfaz de Todos los horarios de timbre, toque el timbre para eliminarlo

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

8. Gestión de Datos

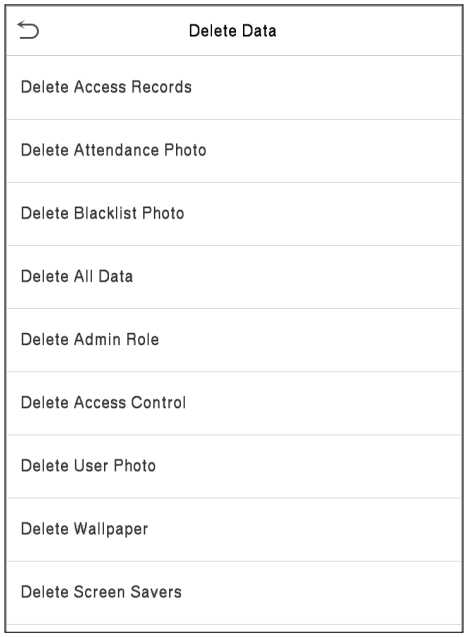
La gestión de datos se utiliza para eliminar los datos relevantes en el dispositivo.

Haga clic Datos. en la interfaz del menú principal.



ELIMINAR DATOS

Haga clic en Borrar Datos en el Administrador de datos.

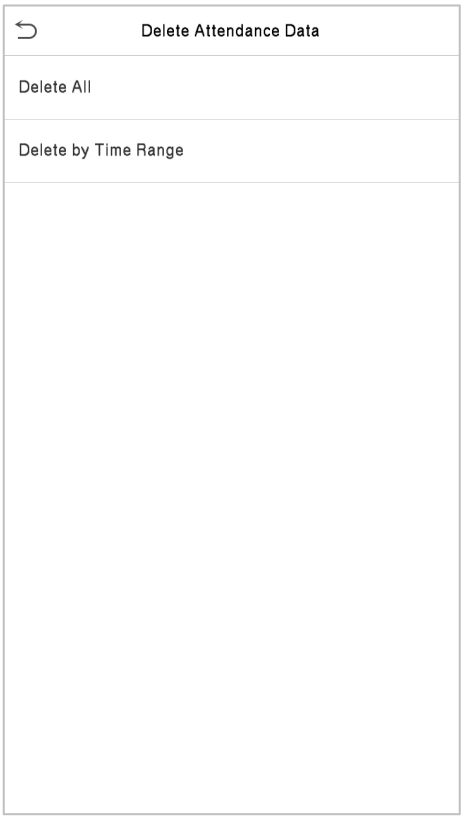


Menú	Descripción
Borrar Eventos de acceso	Eliminar los datos de asistencia / registros de acceso de forma condicional.
Borrar Fotos de Eventos	Eliminar las fotos de asistencia del personal designado.
Borrar Fotos, No aprobados	Para borrar las fotos tomadas durante las verificaciones fallaron.
Borrar Todo	Eliminar información y registros de asistencia / registros de acceso de todos los usuarios registrados.
Borrar Privilegio de Administrador	Para eliminar los privilegios de administrador.
Eliminar control de acceso	Eliminar todos los datos de acceso.
Eliminar foto de usuario	Para eliminar todas las fotos de usuario en el dispositivo.

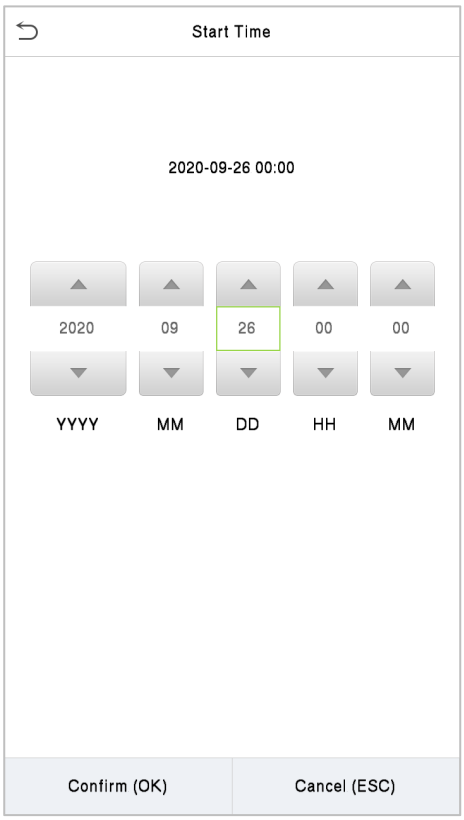
8. Gestión de Datos

Menú	Descripción
Eliminar fondo de pantalla	Para eliminar todos los fondos de pantalla del dispositivo.
Borrar Protectores de pantalla	Para eliminar los protectores de pantalla del dispositivo.

Nota: Al eliminar los acceso registros, la asistencia p oto s, o bl o ck figuran p oto s, puede seleccionar Eliminar todo o Eliminar por periodo de tiempo. Si selecciona Eliminar por rango de tiempo, debe establecer un rango de tiempo específico para eliminar todos los datos con el período.



Seleccione Eliminar por rango de tiempo.

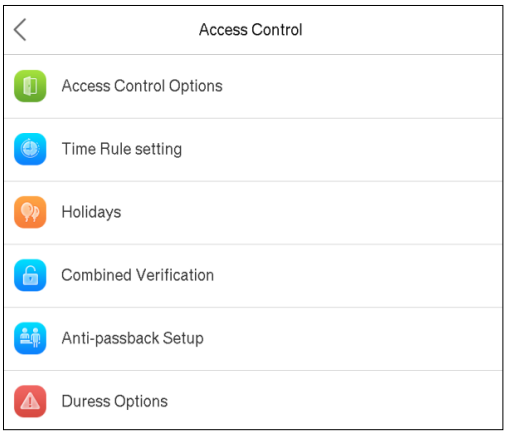


Establezca el rango de tiempo y haga clic en Aceptar.

9. Control de Acceso

El control de acceso se utiliza para establecer el horario de apertura de una puerta, 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:

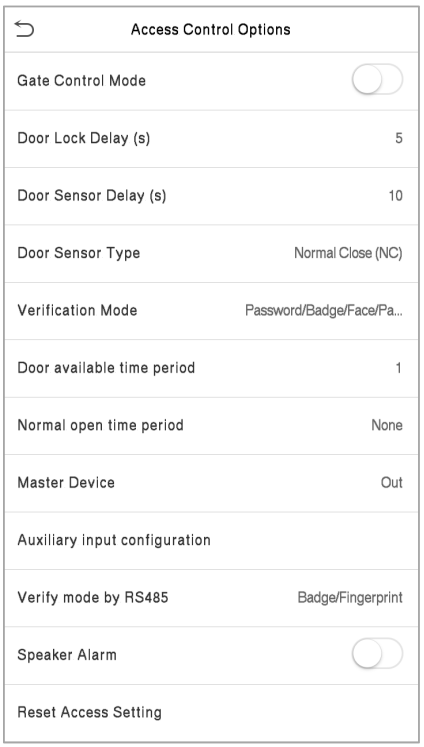
1.El tiempo de desbloqueo de la puerta actual debe estar dentro de cualquier zona horaria válida del período de tiempo del usuario.

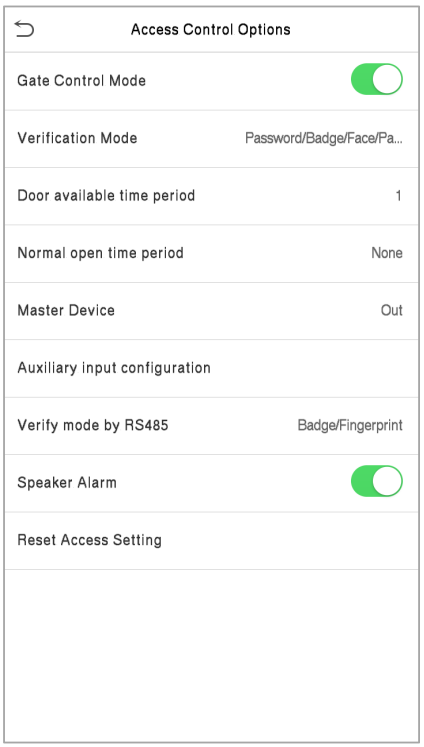
2.El grupo del usuario debe estar en la combinación de desbloqueo de la puerta (cuando hay otros grupos en el mismo combo de acceso, también se requiere la verificación de los miembros de esos grupos para desbloquear la puerta).

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 un estado de desbloqueo.

OPCIONES DE CONTROL DE ACCESO

Esta opción se utiliza para configurar los parámetros del bloqueo de control del dispositivo y los parámetros relacionados. Haga clic en Opciones de control de acceso en la interfaz de Control de acceso.





9. Control de Acceso

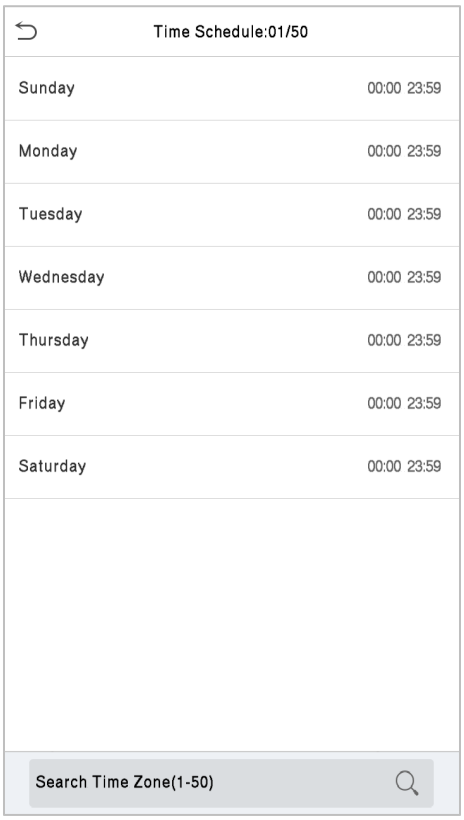
Menú	Descripción
Modo de control de barrera	Ya sea para activar el modo de control de barrera o no. Cuando está en ON, en esta interfaz se quitará el relé de cerrado de puerta, el relé de sensor de puerta y la función de tipo de sensor de puerta.
Retardo de la cerradura	El tiempo que el dispositivo controla la cerradura eléctrica para abrir. Valor válido: 1 a 10 segundos; 0 segundos representa la desactivación de la función.
Retardo 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, Normalmente Abierto y Normalmente 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 encendid
Modo de verificación	El modo de verificación admitido incluye Contraseña /Tarjeta/Rostro/Palma, Solo ID de usuario, Contraseña, Solo Tarjeta, contraseña + tarjeta, Contraseña / tarjeta, Solo Rostro, Rostro + Contraseña, Rostro + Tarjeta, Palma, Palma + Tarjeta, Palma + Rostro.
Horario de puerta habilitada	Para establecer un período de tiempo para la puerta, de modo que la puerta sea accesible solo durante este período de tiempo.
Periodo normalmente abierto	Período de tiempo programado para el modo de "apertura normal", de modo que la puerta siempre esté desbloqueada durante este período.
Dispositivo maestro	Al configurar el maestro y el esclavo, el estado del maestro se puede configurar en fuera o en. Fuera: El registro verificado en el host es el registro de salida. En: El registro verificado en el host es el registro de entrada.
Ajustes 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.
Verificar el modo por RS485	Para configurar el modo de verificación por RS485. Opcional solo para insignia, insignia + contraseña.
Altavoz de alarma	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 del bloqueo 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, un dispositivo maestro y una alarma. Sin embargo, los datos de control de acceso borrados en Data Mgt. está excluido. a; Normalmente cerrado significa que la puerta siempre está cerrada cuando la electricidad está encendida.

9. Control de Acceso

HORARIO

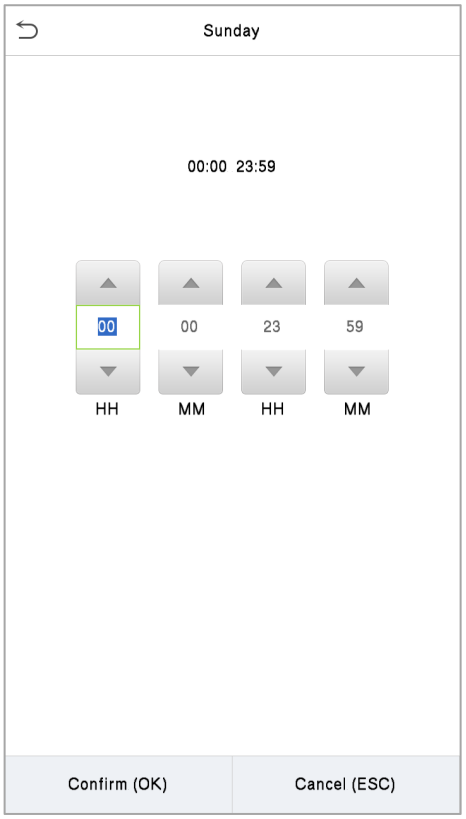
Todo el sistema puede definir hasta 50 reglas de tiempo . Cada regla de tiempo representa diez zonas horarias, es decir, una semana y 3 días festivos , y cada zona horaria es un período de tiempo válido dentro de las 24 horas del día. Puede establecer un máximo de 3 períodos de tiempo para cada zona horaria . La relación entre estos períodos de tiempo es "o". Cuando el tiempo de verificación cae en cualquiera de estos períodos de tiempo , la verificación es válida. Cada formato de período de tiempo de la zona horaria : HH MM-HH MM, que tiene una precisión de minutos según el reloj de 24 horas. Haga clic en Configuración de regla de tiempo 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.

9. Control de Acceso



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 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.

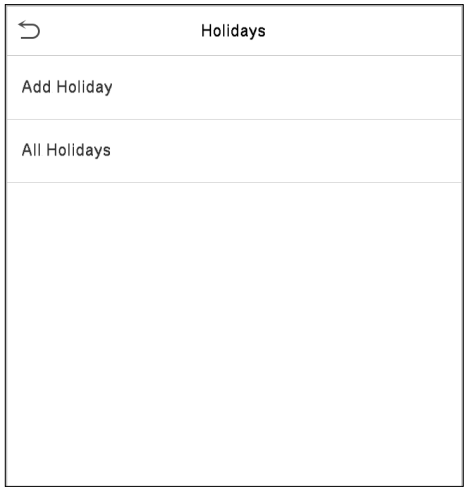
2. El período de tiempo efectivo para desbloquear la puerta: abrir todo el día (00: 00 ~ 23: 59) o cuando la hora de finalización es posterior a la hora de inicio, como 08: 00 ~ 23: 59.

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

CONFIGURACIÓN DE DÍAS FESTIVOS

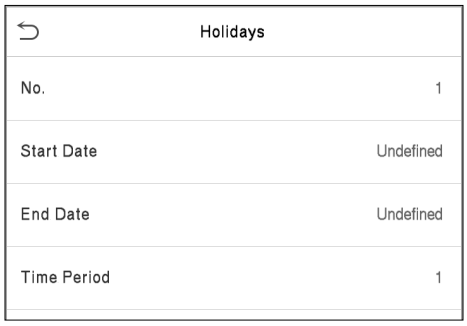
Siempre que haya un día festivo, es posible que necesite un horario de acceso especial; pero cambiar el tiempo de acceso de todos uno por uno es extremadamente engorroso, por lo que puede establecer un tiempo de acceso de vacaciones que se aplique a todos los empleados, y el usuario podrá abrir la puerta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

Haga clic en Días Festivos en la interfaz de Control de acceso .



Agregar un nuevo día festivo

Haga clic en Agregar Día Festivo 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 un Día Festivo

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.

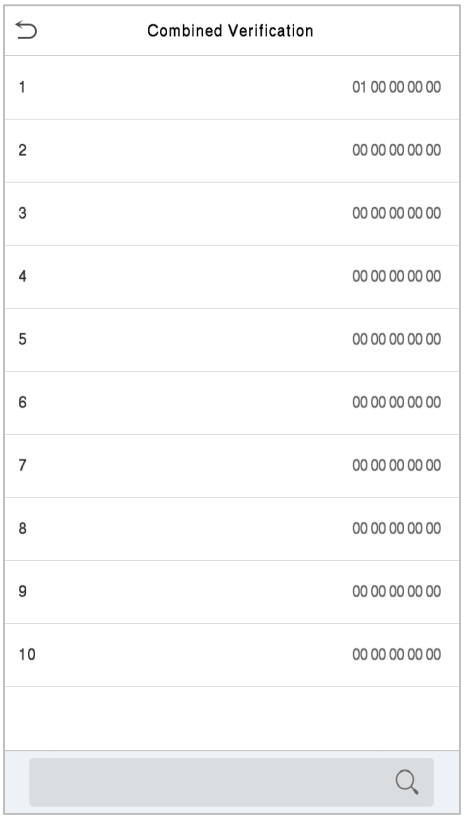
CONFIGURACIÓN DE VERIFICACIÓN COMBINADA

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.

9. 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.

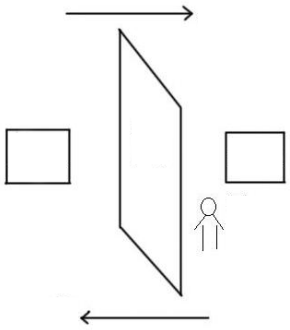
La combinación de desbloqueo de puerta 4 se establece como (03 05 08 00 00), lo que indica que la combinación de desbloqueo 4 consta de tres personas. La primera persona es del grupo AC 3, la segunda persona es del grupo AC 5 y la tercera persona es del grupo AC 8.

Eliminar una combinación de desbloqueo de puertas

.

9. Control de Acceso

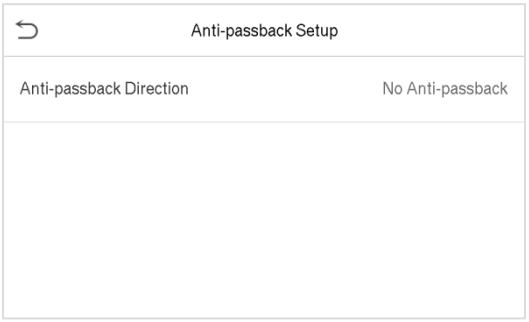
CONFIGURACIÓN ANTI-PASSBACK



Es posible que algunas personas sigan a los usuarios para entrar por la puerta sin verificación, lo que resultará en un problema de seguridad. Entonces, para evitar esta situación, se desarrolla la opción Anti-Passback. Una vez habilitado, 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.

Hacer clic Configuración anti-passback en la interfaz de control de acceso.



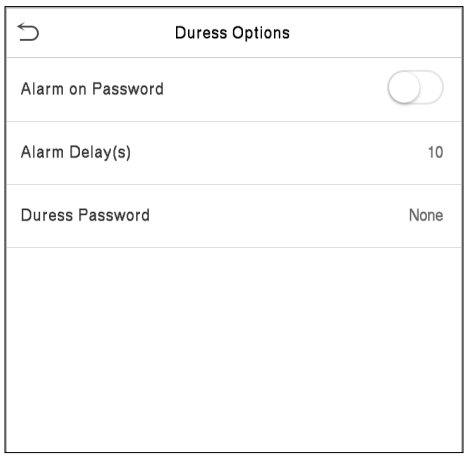
Menú	Descripción
Dirección anti-passback	Sin Anti-passback: la función Anti-passback está deshabilitada, lo que significa que la verificación exitosa a través del dispositivo maestro o esclavo puede desbloquear la puerta. El estado de asistencia no se guarda. Anti-passback de salida: después de que un 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. Anti-passback Entrada: 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. Anti-passback entrada / salida: después de que un usuario entra / sale, solo si el último registro es un registro de salida, el usuario puede volver a registrarse; o un registro de check-in, el usuario puede volver a entrar; de lo contrario, se activará la alarma.

9. Control de Acceso

CONFIGURACIÓN DE LAS OPCIONES DE COACCIÓN

Si un usuario activó la función de verificación de coacción con 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 .



Menú	Descripción
Alarma por contraseña	Cuando un usuario usa 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 coacción	Configure la contraseña de coacción de 6 dígitos. Cuando el usuario ingresa esta contraseña de coacción para verificación, se generará una señal de alarma.

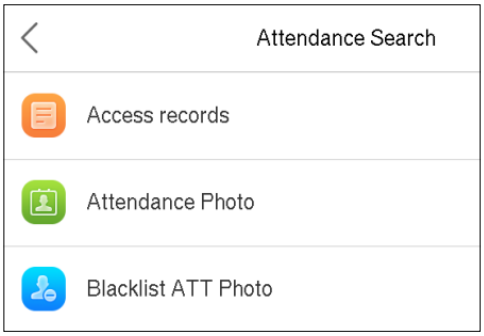
10. Búsqueda de asistencia

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

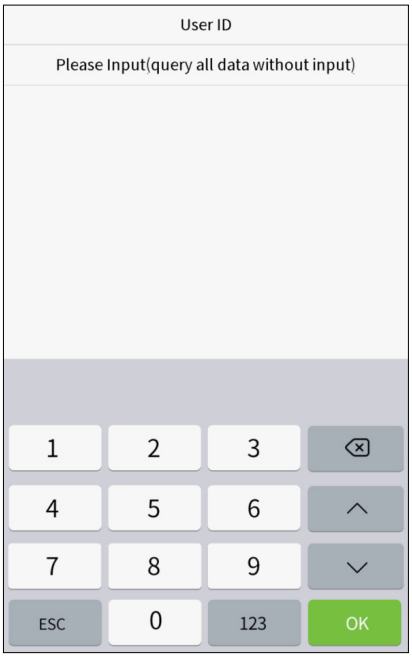
Haga clic en Búsqueda de asistencia en la interfaz del menú principal.

El proceso de búsqueda de asistencia y bl o cklist P hoto s es similar a la de la búsqueda deregistro de eventos. El siguiente es un ejemplo de búsqueda deregistro de eventos.

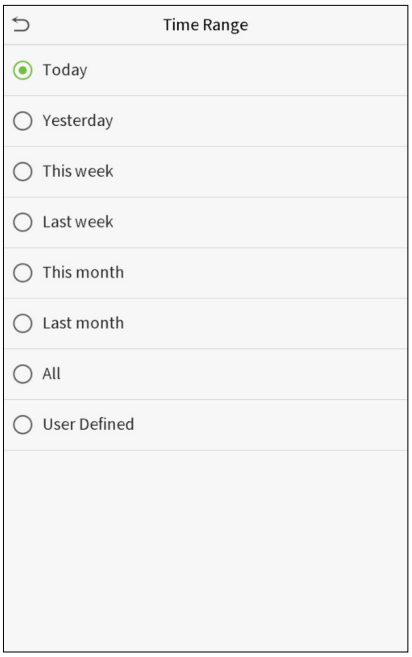
En la interfaz de búsqueda de asistencia, haga clic en Registro de eventos.



1. Ingrese el ID de usuario a buscar y haga clic en Aceptar. Si desea buscar registros de todos los usuarios, haga clic en Aceptar sin ingresar ningún ID de usuario.

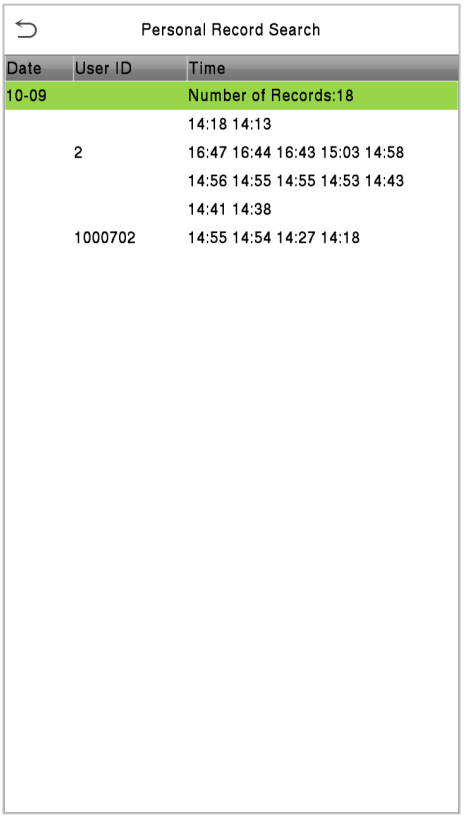


2. Seleccione el rango de tiempo en el que los registros que desea buscar.

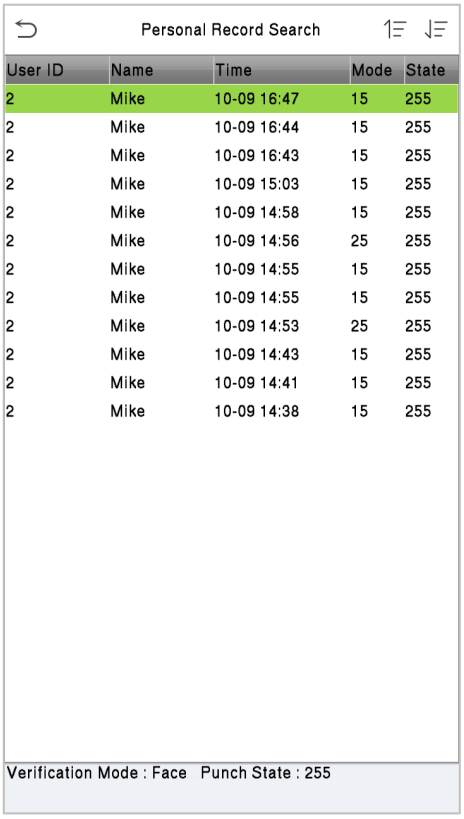


10. Búsqueda de asistencia

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



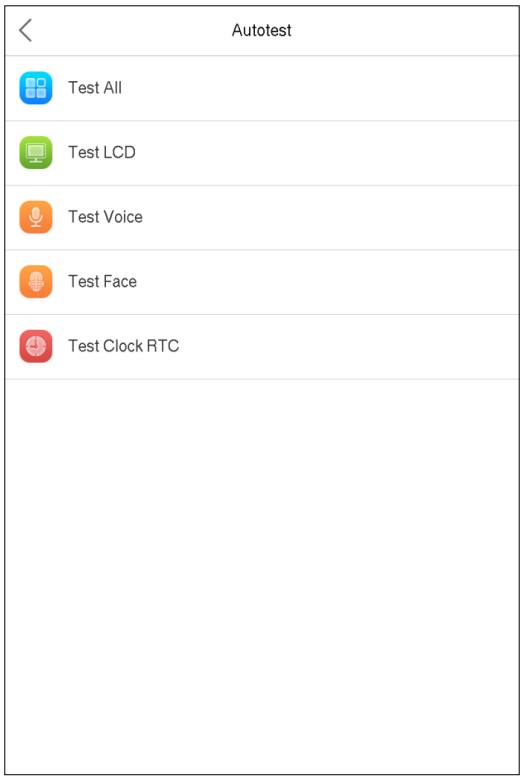
4. La siguiente figura muestra los detalles del registro seleccionado.



11. Pruebas de Sistema

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

Haga clic en Pruebas en la interfaz del menú principal.

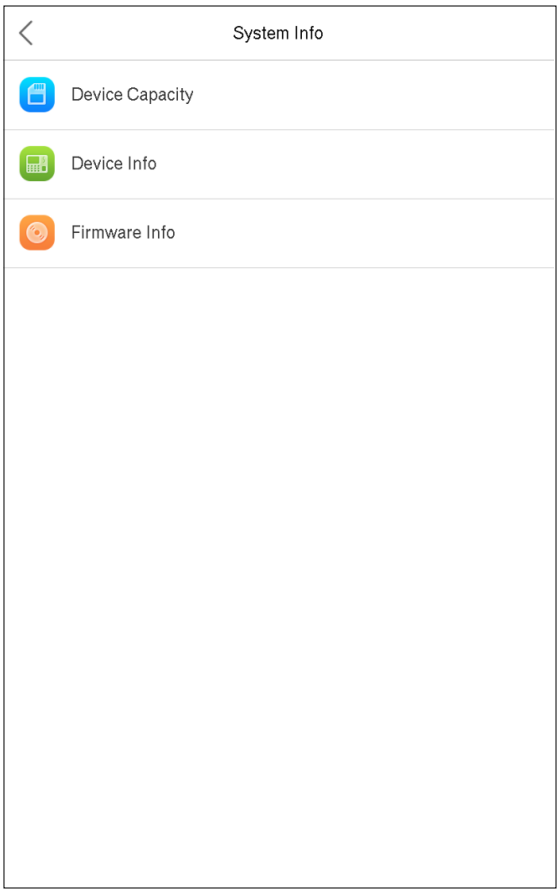


Menú	Descripción
Probar todo	Para probar automáticamente si la pantalla LCD, el audio, la cámara y el RTC son normales.
Probar de LCD	Para probar automáticamente el efecto de visualización de la pantalla LCD mostrando a todo color, blanco puro y negro puro para verificar si la pantalla muestra los colores normalmente.
Probar de voz	Para probar automáticamente si los archivos de audio almacenados en el dispositivo están completos y la calidad de voz es buena.
Probar Rostro	Para probar si la cámara funciona correctamente, verifique las imágenes tomadas para ver si son lo suficientemente claras.
Probar 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 nuevamente para dejar de contar.

12. 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.



Menú	Descripción
Capacidad del dispositivo	Muestra el espacio de almacenamiento del dispositivo actual , palma, contraseña y la Rostro, los administradores, registros de acceso, asistencia fotos de no permitidos, 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 la versión del dispositivo.

13. Conectarse al Software ZKBioAccess

ESTABLECER LA DIRECCIÓN DE COMUNICACIÓN

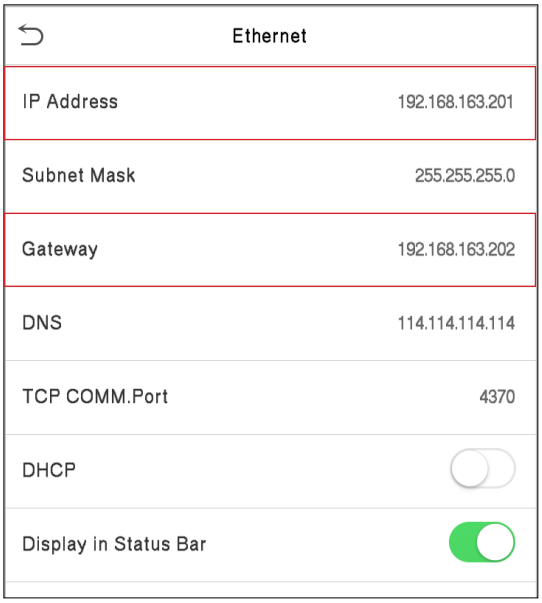
Lado del dispositivo

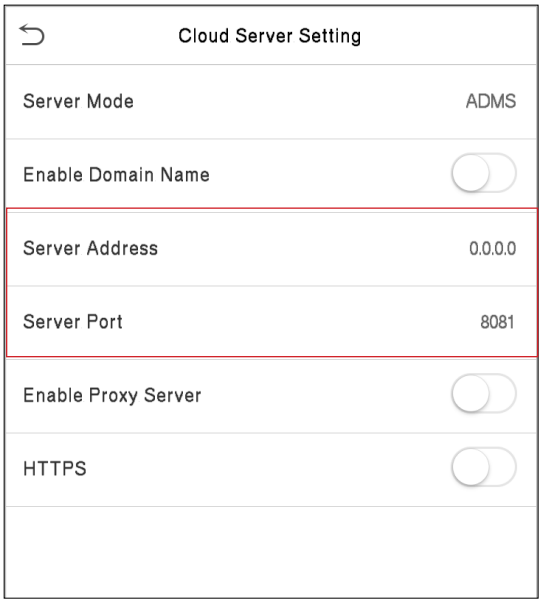
1. Hacer clic RED.> Ethernet en el menú principal para configurar la dirección IP y la puerta de enlace de el dispositivo. (Nota: La dirección IP debe poder comunicarse con el servidor ZKBioAccess, preferiblemente en el mismo segmento de red con la dirección del servidor..)

2. En el menú principal, haga clic en RED. > Configuración del servidor de nube para configurar la dirección del servidor y el puerto del servidor.

Dirección del servidor:Establecer como la dirección IP del servidor ZKBioAcess.

Puerto del servidor: Establecer como puerto de servicio de ZKBioAccess (el valor predeterminado es 8088).





Lado del software

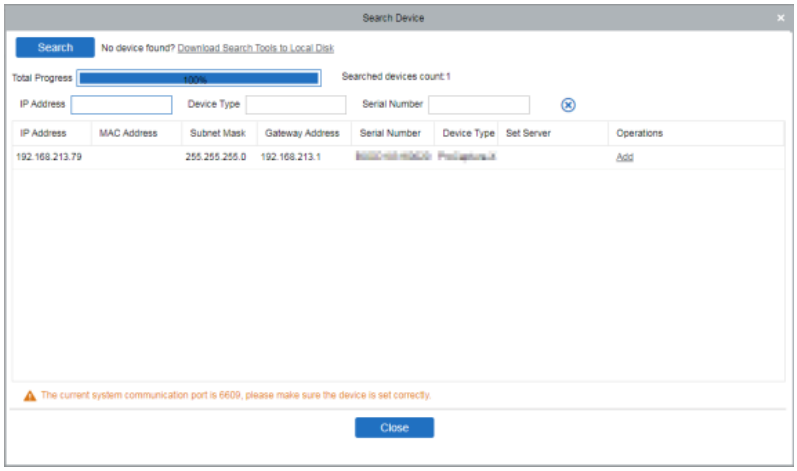
Inicie sesión en el software ZKBioAccess, haga clic en Sistema> Comunicación> Monitor de comunicación para configurar el puerto de servicio ADMS, como se muestra en la siguiente figura:

13. Conectarse al Software ZKBioAccess

AGREGAR DISPOSITIVO AL SOFTWARE

Puede agregar un dispositivo buscandolo. El proceso es el siguiente:

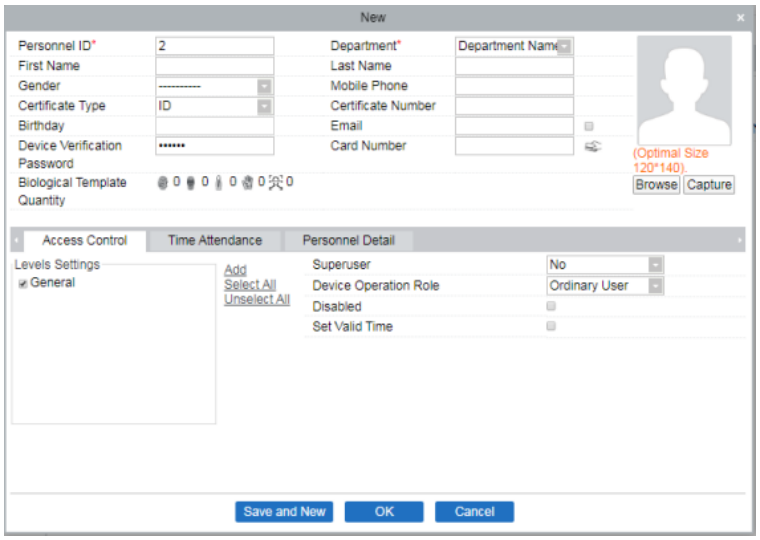
1. Haga clic en Control de acceso> Dispositivo> Buscar dispositivo, para abrir la interfaz de búsqueda.
2. Haga clic en Buscar y aparecerá [Buscando ……].
3. Después de la búsqueda, se mostrará la lista y el número total de controladores de acceso..



4. Haga clic en Agregar para agregar el dispositivo específico al software.

AGREGAR PERSONAL AL SOFTWARE

1. Haga clic en Personal> Persona> Nuevo.



2. Después de configurar todos los parámetros, haga clic en Aceptar.

Apéndice 1

Requisitos para la recopilación en vivo y el registro de imágenes visible light

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

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

3)Se recomienda que en el registro las prendas de color sean diferentes del color de fondo.

4) Muestre su cara y frente, y no cubra su cara y cejas con su cabello, lentes de sol o lentes de aumento.

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 simultaneamente.

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.

9) Se recomienda una distancia de captura de 50 cm a 80 cm , ajustable en función de la altura del cuerpo.

Área de captura de rostro de Imagen 1

Apéndice 1

Requisitos para datos de imagen facial digital visible Light Digital

La foto 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 deberan enrolarelse con los anteojos para la captura de fotografías.

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

Expresión facial
Se recomienda un Rostro sencillo 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 °.

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

Rostro
La imagen debe tener un contorno claro, una escala real, una luz distribuida uniformemente y sin sombras.

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

Requerimientos 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) Se prefiere un Rostro sencillo o una sonrisa, no se prefiere mostrar los dientes.

La persona capturada debe ser vista claramente, de color natural y sin un giro obvio de la imagen, sin sombras, puntos de luz o reflejos en el Rostro o el fondo, y un nivel de contraste y luminosidad apropiado..

Apéndice 2

Declaración sobre el derecho a la privacidad

Estimados 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..

Nosotros declaramos que:

1.Todos nuestros dispositivos de reconocimiento de huellas dactilares civiles 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.

Si desea disputar cuestiones de derechos humanos o privacidad relacionadas 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. No se puede violar la casa de un ciudadano;

El derecho de un ciudadano a la comunicación 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 será utilizada en el comercio electrónico, banca, seguros, judicial y otros sectores en el futuro. Cada año el mundo sufre grandes pérdidas debido a la inseguridad de Contraseñas. Los productos biométricos sirven para proteger su identidad en entornos de alta seguridad.

Apéndice 2

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 operativo 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	×	o	o	o	o	o
Condensador	×	o	o	o	o	o
Inductor	×	o	o	o	o	o
Diodo	×	o	o	o	o	o
Componente ESD	×	o	o	o	o	o
Buzzer/Bocina	×	o	o	o	o	o
Adaptador	×	o	o	o	o	o
Tornillos	o	o	o	×	o	o

o 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 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.

Green Label

www.zkteco.com

www.zktecolatinoamerica.com