

MANUAL DE USUARIO

Soluciones de 2.8" Tiempo y Asistencia

Fecha: Abril 2020

Versión: 1.0

Español

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

Sin el consentimiento previo por escrito de ZKTeco, ninguna parte de este manual puede copiarse o reenviarse de ninguna manera o forma. Todas las partes de este manual pertenecen a ZKTeco y sus subsidiarias (en adelante la "Compañía" o "ZKTeco").

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 Compañía

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 del producto de Tiempo y Asistencia de 2,8 pulgadas.

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

Configuración de la instalación.....	07
1. Procedimiento operacional.....	08
1.1 Registro facial.....	08
1.2 Posiciones correctas e incorrectas.....	09
1.3 Interfaz de espera.....	10
1.4 Teclado virtual.....	11
1.5 Modo de verificación.....	11
2. Menú principal.....	14
3. Gestión de usuarios.....	15
3.1 Agregar usuarios.....	15
3.2 Configuración del rol de usuario.....	15
3.3 Búsqueda de usuarios.....	17
3.4 Editar usuarios.....	17
3.5 Borrar usuarios.....	17
4. Rol de usuario.....	18
5. Ajustes de comunicación.....	19
5.1 Conexión a PC.....	19
5.2 Configuración Ethernet.....	20
5.3 Configuración Wi-Fi.....	21
5.4 Configuración del servidor de nube.....	23
6. Configuración del sistema.....	23
6.1 Fecha y hora.....	24
6.2 Parámetros de asistencia.....	24
6.3 Parámetros faciales.....	25
6.4 Restablecimiento de fábrica.....	23
7. Personalización.....	27
7.1 Configuración de la interfaz.....	27
7.2 Configuración de sonido.....	28
7.3 Horarios de timbre.....	29
7.4 Opciones de estado de verificación.....	30
7.5 Asignaciones de teclas de método abreviado.....	31
8. Gestión de datos.....	32
8.1 Eliminar datos.....	32
9. Búsqueda de asistencia.....	33
10. Control de Acceso.....	35
10.1 Opciones de Control de Acceso.....	35

11. Autotest..... 36

12. Información del sistema..... 37

- 12.1 Agregar biométrico al software..... 37
- 12.2 Información de conexión..... 38
- 12.3 Datos del dispositivo..... 40
- 12.4 Búsqueda..... 40

Apéndice 1..... 41

- Requisitos para la recopilación en vivo y el registro de imágenes visible light..... 41
- Requisitos para datos de imagen facial digital visible Light Digital..... 42

Apéndice 2..... 43

- Declaración sobre el derecho a la privacidad..... 43
- Eco-friendly operación..... 44

Configuración de la Instalación

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.

Lugar 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.

Herramientas de instalación

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

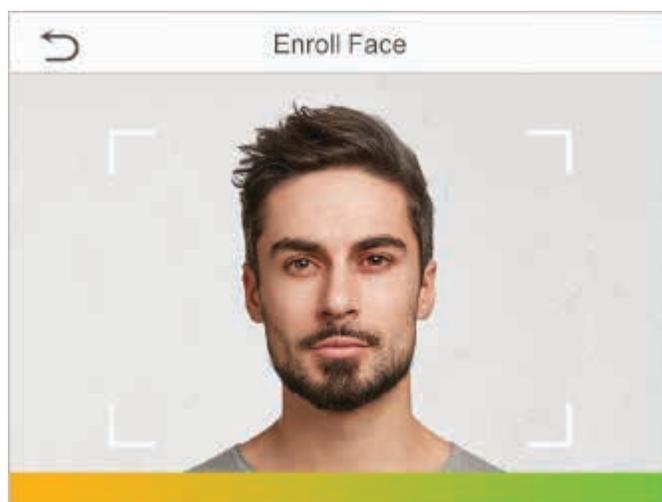
Pasos de instalación

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.

1. Procedimiento Operacional

1.1 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:

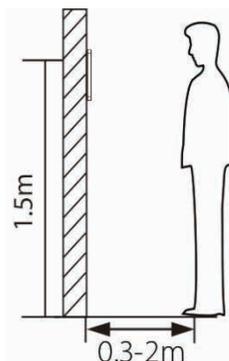
- Al registrar un rostro, mantenga una distancia de 40 cm a 80 cm entre el dispositivo y el rostro.
- Tenga cuidado de no a cambiar el rostro de expresión. (cara sonriente , cara dibujada , guiño, etc.)
- Si usted qué no sigue las instrucciones en la pantalla, el rostro de registro puede tomar más tiempo 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.

1.2 Posiciones correctas e incorrectas

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:



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.

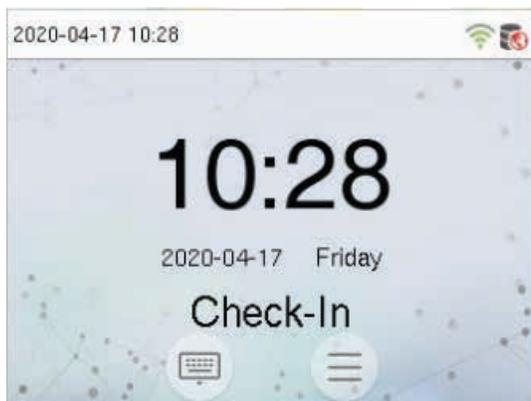
- Expresión facial de postura de pie



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

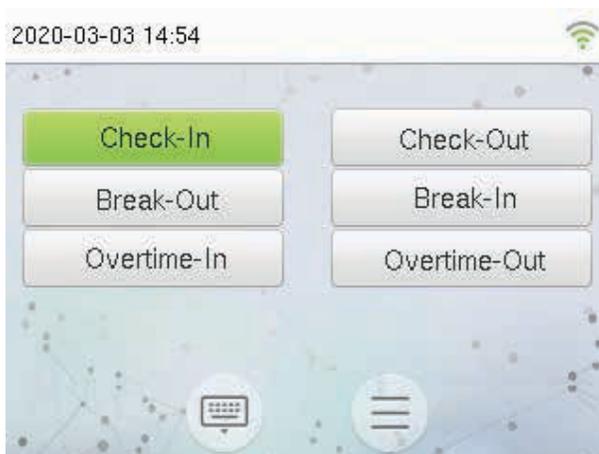
1.3 Interfaz de espera

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.
3. *El cambio de estado de verificación se puede hacer directamente usando las teclas de acceso directo de la pantalla. Haga clic en cualquier lugar de la pantalla sin iconos y aparecerán seis teclas de método abreviado, como se muestra en la siguiente figura:



Presione la tecla de método abreviado correspondiente para seleccionar el estado de perforación actual, que se muestra en verde. Consulte "Asignaciones de teclas de método abreviado" a continuación para conocer el método de operación específico.

1.4 Teclado virtual



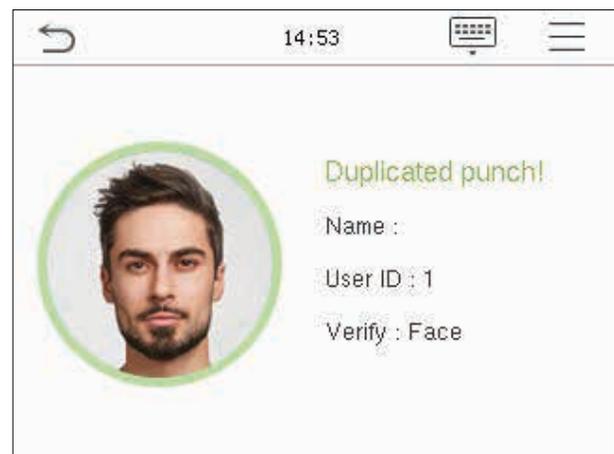
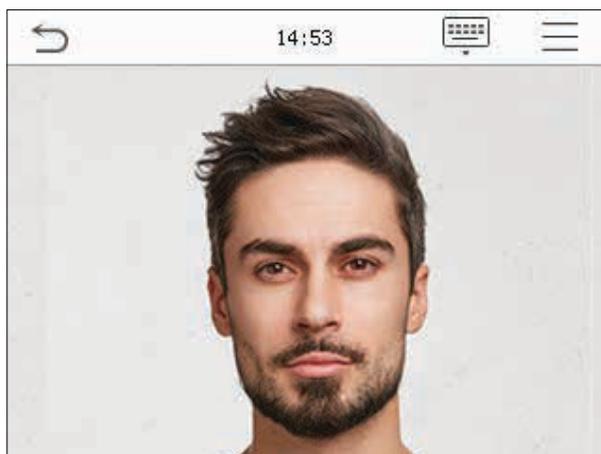
Nota:

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.

1.5 Modo de verificación

Verificación Facial 1: N

Compara las imágenes faciales adquiridas con todos los datos faciales registrados en el dispositivo. El siguiente es 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.



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



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

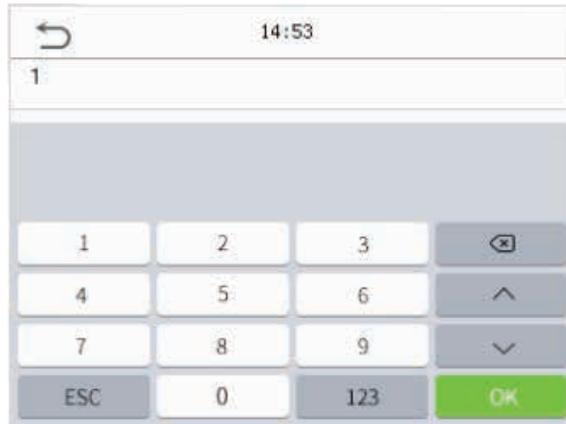


Verificación de contraseña

Compara la contraseña ingresada con el ID de usuario y la contraseña registrada.

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 presione OK.



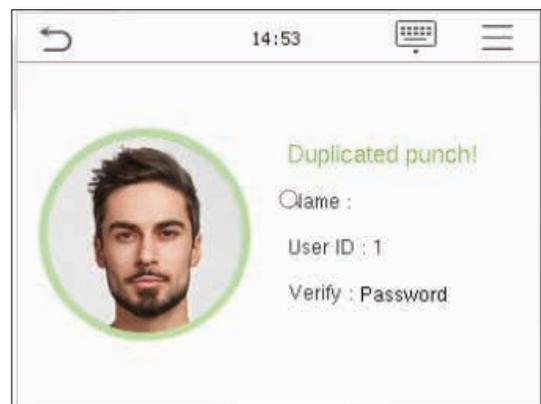
Si un empleado registra su cara además de la contraseña, aparecerá la siguiente pantalla. Seleccione el icono  para ingresar al modo de verificación de contraseña.



2. Ingrese la contraseña y presione OK.



3. Verificación Exitosa.



2. Menú Principal

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



Menú	Descripción
Admin. de usuarios	Para agregar, editar, ver y eliminar información básica sobre un usuario.
Rol de 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, comunicación en serie, conexión a PC, 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.
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 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, el audio, cámara y reloj en tiempo real.
Info. del sistema	Para ver la capacidad de datos, el dispositivo y la información de firmware del dispositivo actual.

3. Gestión de Usuarios

3.1 Agregar usuarios

1. Haga clic en User Mgt. en el menú principal.
2. Haga clic en Nuevo usuario, registrar un ID de usuario y un nombre.
3. Ingrese el ID de usuario y el nombre.

A screenshot of the 'New User' registration form. It includes a back arrow, a refresh icon, and several input fields: 'User ID' (with the value '3'), 'Name', 'User Role' (with the value 'Normal User'), 'Face' (with the value '0'), and 'Password'.

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.

3.2 Configuración del rol de 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.

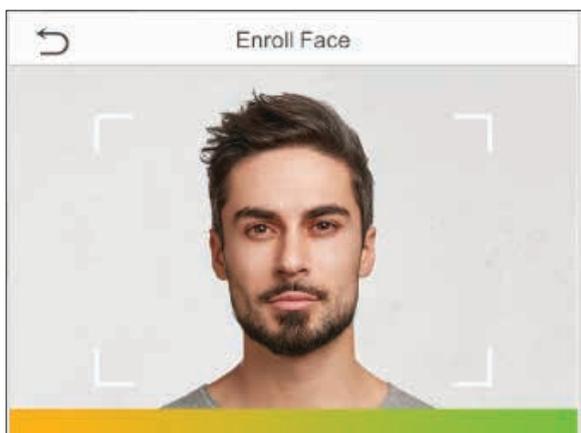
Haga clic en Rol de usuario para seleccionar Usuario normal o Superadministrador.

A screenshot of the 'User Role' selection screen. It features a back arrow and two radio button options: 'Normal User' (which is selected) and 'Super Admin'.

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 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 predeterminadamente.

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.



3.3 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.

3.4 Editar usuarios

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

 User : 1 Mick	 Edit : 1 Mick 
Edit	User ID 1
Delete	Name Mick
	User Role Normal User
	Face 1
	Password *****

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".

3.5 Borrar 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.

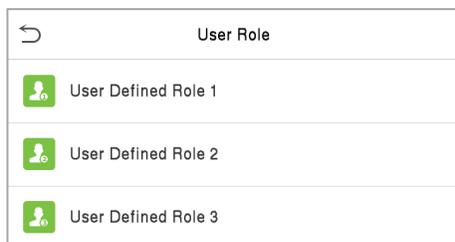
 User : 1 Mick	 Delete : 1 Mick
Edit	Delete User
Delete	Delete Face Only
	Delete Password Only

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.

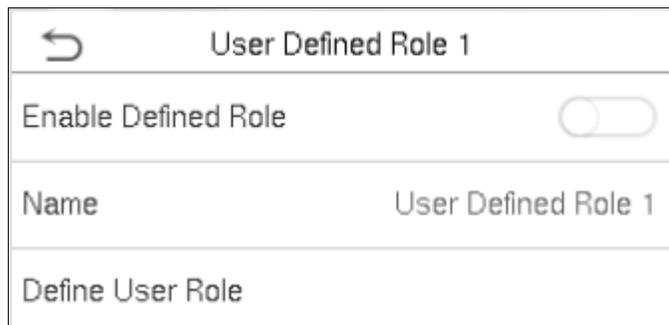
Puede establecer el alcance del permiso del rol personalizado (hasta 3 roles) y el registrador, es decir, el alcance del permiso del menú de operación.

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



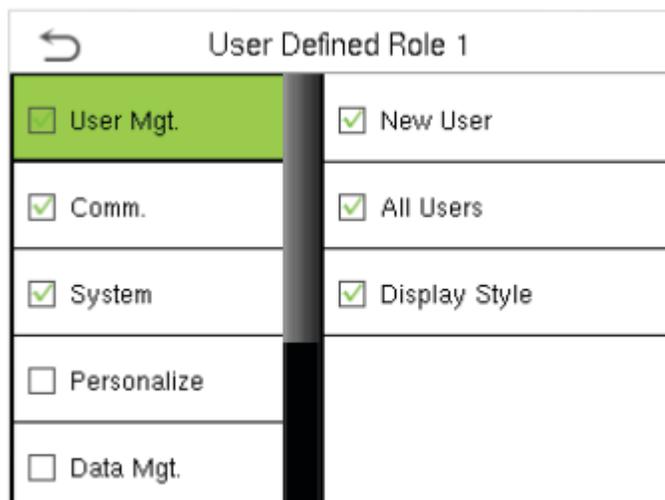
1. Haga clic en cualquier elemento para establecer una función definida. Haga clic en la fila de Habilitar rol definido para habilitar este rol definido. Haga clic en Nombre e ingrese el nombre del rol.

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

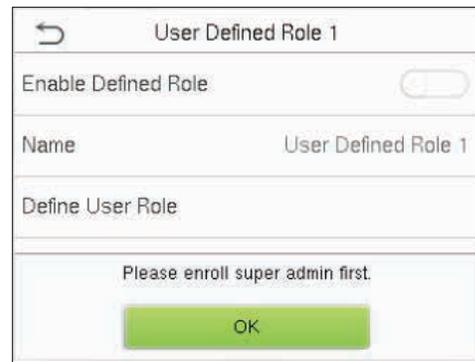
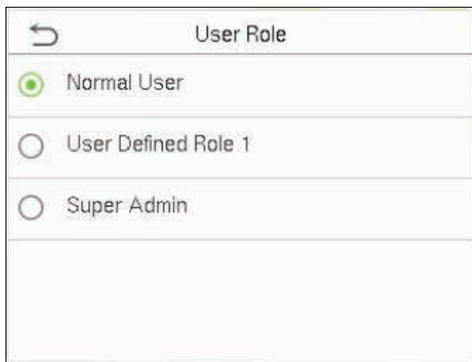


Nota: Durante la asignación de privilegios, el menú principal está a la izquierda y sus submenús están a la derecha. Solo necesita seleccionar las funciones en los submenús.

Si el dispositivo ha s una función activada, puede asignar las funciones que establezca para los usuarios haciendo clic con el usuario Mgt. > 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.



5. Ajustes de comunicación

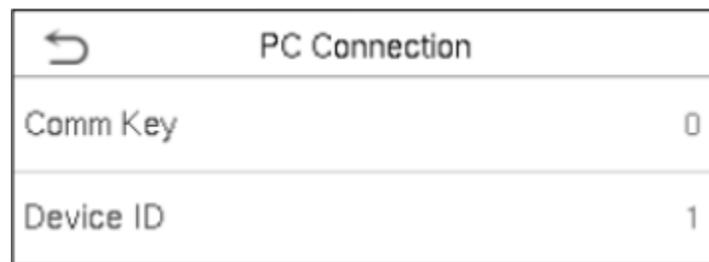
Ingrese a **comunicación** en el **Menú principal** para configurar los parámetros en la comunicación Ethernet, conexión de PC, WI-FI, Comunicación con el servidor de nube y el diagnóstico de la red.



5.1 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 .



5.2 Configuración Ethernet

Cuando el dispositivo necesita comunicarse con un PC a través de Ethernet, debe configurar los ajustes de red y asegurarse de que el dispositivo y el PC están conectados al mismo segmento de red.

Ingrese a **Ethernet** en el menú de **comunicación** y configure los ajustes.

Ethernet	
IP Address	192.168.163.99
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	0.0.0.0
TCP COMM.Port	4370
DHCP	<input type="checkbox"/>

Ethernet	
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	0.0.0.0
TCP COMM.Port	4370
DHCP	<input type="checkbox"/>
Display in Status Bar	<input checked="" type="checkbox"/>

Descripción de funciones

Nombre de funciones	Descripción de funciones
Dirección IP	La IP por default es 192.168.1.201 se puede modificar de acuerdo al segmento de red.
Mascara de subred	La mascara de subred es 255.255.255.0 se puede modificar de acuerdo al segmento de red.
Gateway	La dirección gateway es 0.0.0.0 se puede modificar de acuerdo al segmento de red.
DNS	La dirección del DNS por default es 0.0.0.0 se puede modificar de acuerdo al segmento de red
Puerto de comunicación TCP	El puerto de comunicación por default es 4370 se puede modificar de acuerdo al segmento de red.
DHCP	Son las siglas de Dynamic Host Configuration Protocol. Su función es asignar una IP dinámica.
Mostrar el estado en la barra	Activa el icono de la comunicación Ethernet en la barra de estado que se encuentra en la parte superior del dispositivo.

5.3 Configuraciones Wi-Fi

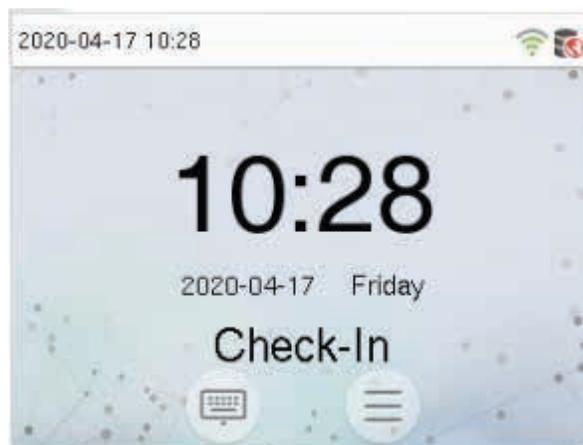
Wi-Fi es la abreviatura de Wireless Fidelity. El dispositivo proporciona un módulo Wi-Fi, que puede integrarse en el molde del dispositivo o conectarse externamente, para permitir la transmisión de datos a través de Wi-Fi y establecer un entorno de red inalámbrica.

El Wi-Fi está habilitado en el sistema de forma predeterminada. Si no es necesario utilizar la red Wi-Fi, puede tocar el botón  para desactivar Wi-Fi



Cuando Wi-Fi esté habilitado, presiona la red buscada. Presiona el cuadro de texto para ingresar la contraseña y presiona Conectarse a Wi-Fi (OK).

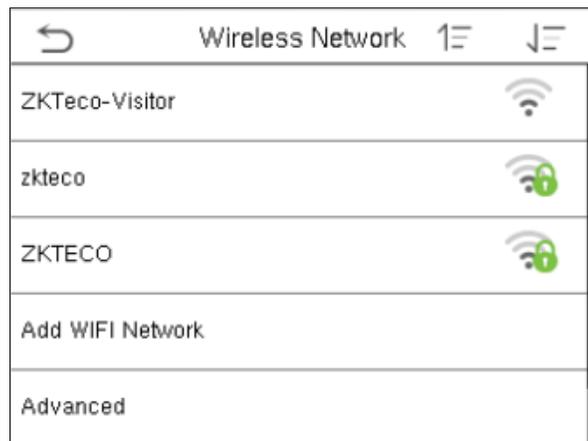
La conexión se realiza correctamente y el estado se muestra en la barra de iconos.



Agregando una nueva red WiFi

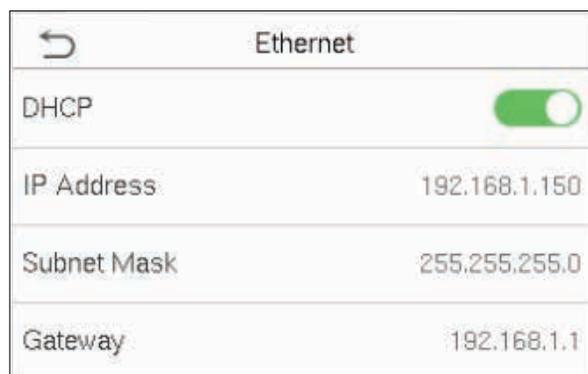
Si la red Wi-Fi deseada no está en la lista, puede agregar la red Wi-Fi manualmente. Toque Page Down y Add Wi-Fi Network.

Ingrese los parámetros de la red Wi-Fi. (La red agregada debe existir).



Opciones avanzadas

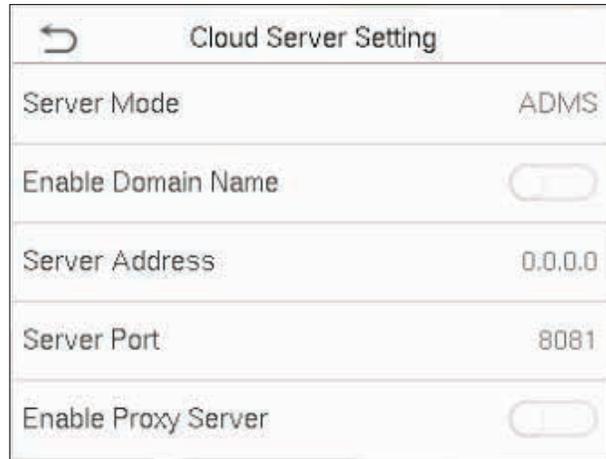
Se utiliza para configurar los parámetros de la red Wi-Fi.



Menú	Descripción
DHCP	Abreviatura de Protocolo de configuración dinámica de host, que implica la asignación de direcciones IP dinámicas a los clientes de la red.
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.

5.4 Configuración del servidor de nube

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



Cloud Server Setting	
Server Mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	0.0.0.0
Server Port	8081
Enable Proxy Server	<input type="checkbox"/>

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.

6. 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.



System	
 Date Time	
 Attendance	
 Face	
 Reset	

6.1 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.

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.

6.2 Parámetros de asistencia

Haga clic en Asistencia en la interfaz del sistema.

Attendance	
Duplicate Punch Period(m)	1
Camera Mode	No photo
Display User Photo	<input checked="" type="checkbox"/>
Attendance Log Alert	99
Cyclic Delete ATT Data	Disabled

Attendance	
Cyclic Delete ATT Data	Disabled
Cyclic Delete ATT Photo	99
Cyclic Delete Blacklist Photo	99
Confirm Screen Delay(s)	3
Face comparison interval(s)	1

Menú	Descripción
Período de verificación duplicado (m)	Dentro de un período de tiempo establecido (unidad: minutos), los registros de asistencia duplicados no se reservarán (el valor varía de 1 a 999999 minutos).
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.
Alerta de registro de asistencia	Cuando el almacenamiento restante es menor que el valor establecido, el dispositivo alertará automáticamente a los usuarios sobre la información de almacenamiento restante. Puede desactivarse o configurarse en un valor comprendido entre 1 y 9999.
Borrar Eventos antiguos	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.
Borrado Cíclico de Fotos de Asistencia	La cantidad de fotos de asistencia que se permite eliminar de una vez cuando se alcanza el almacenamiento máximo. Puede desactivarse o establecerse en un valor comprendido entre 1 y 99.
Borrado Cíclico Fotos de 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.

6.3 Parámetros faciales

Haga clic en Rostro en la interfaz del sistema.

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

Face		Face	
1:N Match Threshold	74	Minimum Face Size	80
1:1 Match Threshold	63	LED Light Triggered Threshold	80
Face Enrollment Threshold	70	Motion Detection Sensitivity	4
Face Pitch Angle	35	Live Detection	<input checked="" type="checkbox"/>
Face Rotation Angle	25	Live Detection Threshold	70

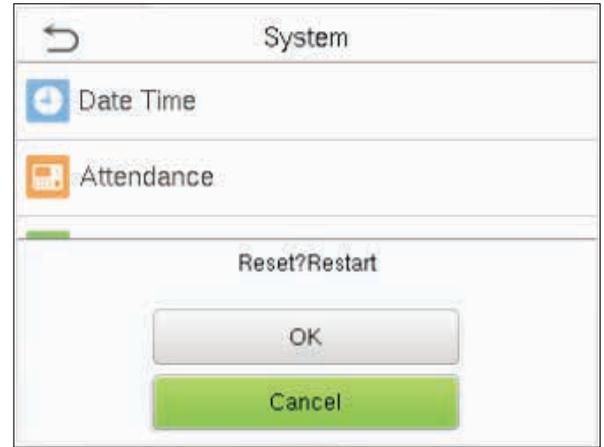
Menú	Descripción
Umbral de verificación 1: N	En el modo de verificación 1: N (uno a muchos), la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas sea mayor que el valor establecido. El valor válido varía de 65 a 120. Cuanto 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 Verificación 1: 1	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	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.
Angulo de rotación de rostro	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.
Tamaño mínimo de rostro	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 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 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 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.
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.

6.4 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.

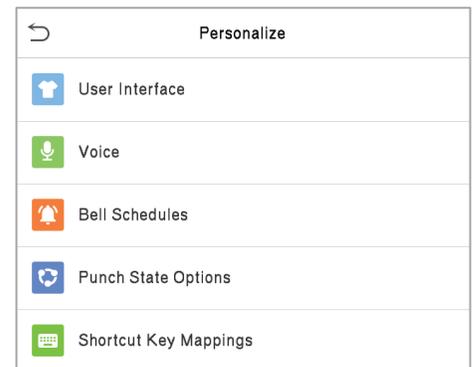
Haga clic en OK para restablecer.



7. Personalización

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

Haga clic en Personalizar en la interfaz del menú principal .



7.1 Configuración de la interfaz

Puede personalizar el estilo de visualización de la interfaz principal.

Haga clic en Interfaz de usuario en la interfaz Personalizar .

↶	User Interface	1↓	↶	User Interface	1↓
	Wallpaper			Menu Screen Timeout(s)	60
	Language	English		Idle Time To Slide Show(s)	60
	Menu Screen Timeout(s)	60		Slide Show Interval(s)	30
	Idle Time To Slide Show(s)	60		Idle Time to Sleep(m)	Disabled
	Slide Show Interval(s)	30		Main Screen Style	Style 1

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.

7.2 Configuración de sonido

Haga clic en **Voz** en la interfaz de Personalizar.



Menú	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.

7.3 Horarios de timbre

Haga clic en Programación de timbre en la interfaz Personalizar.



Agregar un nuevo Timbre

1. Haga clic en New Bell Schedule para ingresar a la interfaz de adición:



Menú	Descripción
Estado del timbre	Establezca si habilitar el estado del timbre.
Tiempo de Timbre	A esta hora del día, el dispositivo hace sonar el timbre automáticamente.
Repetir	Configure el ciclo de repetición del timbre.
Tono	Seleccione un tono.
Duración del timbre	Establezca la duración de la timbre interno. 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 timbre para ver el timbre recién agregado.

Editar una timbre

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 un timbre.

Eliminar una timbre

En la interfaz de Todos los horarios de timbre, toque el timbre para eliminarlo. Toque Eliminar y seleccione [Sí] para eliminar el timbre.

7.4 Opciones de estado de verificación

Haga clic en Opciones de estado de Verificación en la interfaz Personalizar.

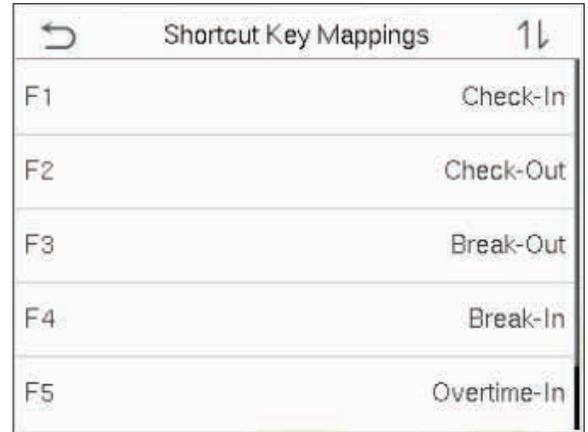
Punch State Options	
Punch State Mode	Manual and Auto Mode
Punch State Timeout(s)	10
Punch State Required	<input type="checkbox"/>

Menú	Descripción
Modo del estado de Asistencia	<p>Seleccione un modo de estado de perforación, que puede ser:</p> <p>Off: Para deshabilitar la función de la tecla de estado de perforación. La clave de estado de perforación establecida en el menú Asignaciones de teclas de acceso directo dejará de ser válida.</p> <p>Modo manual: Para cambiar la tecla de estado de verificación manualmente, y la tecla de estado de verificación desaparecerá después Tiempo de espera del estado de verificación.</p> <p>Modo automático: Después de elegir este modo, configure el tiempo de conmutación de la tecla de estado de perforación en Asignaciones de teclas de acceso directo; cuando se alcanza el tiempo de conmutación, la tecla de estado de perforación establecida se cambiará automáticamente.</p> <p>Modo manual y automático: En este modo, la interfaz principal mostrará la tecla de estado de perforación de conmutación automática, mientras que admite el cambio manual de la tecla de estado de perforación. Después del tiempo de espera, la tecla de estado de perforación de conmutación manual se convertirá en una tecla de estado de perforación de conmutación automática.</p> <p>Modo fijo manual: Después de que la clave de estado de verificación se cambie manualmente, la clave de estado de verificación permanecerá sin cambios hasta que se cambie manualmente la próxima vez</p> <p>Modo fijo: Solo se mostrará la tecla de estado de verificación fija y no se puede cambiar.</p>
Tiempo de espera de estado de verificación	Se muestra el tiempo de un estado de verificación. El estado de verificación desaparecerá o cambiará a otros estados de verificación a medida que se agote el tiempo. El valor es 5 ~ 999 segundos.
Se requiere estado de verificación	Establezca si desea seleccionar el estado de verificación durante la verificación.

7.5 Asignaciones de teclas de método abreviado

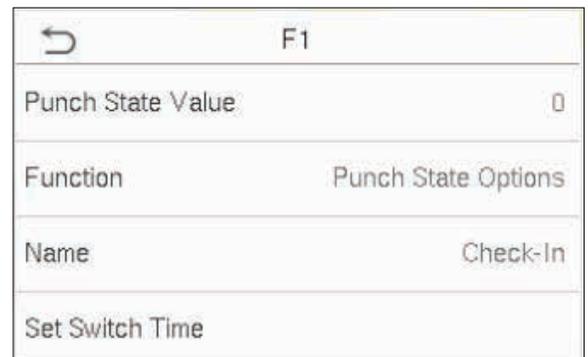
Los usuarios pueden definir accesos directos como estado de asistencia o teclas funcionales. En la interfaz principal, cuando se presionan las teclas de acceso directo, se mostrará rápidamente el estado de asistencia correspondiente o la interfaz de función.

Haga clic en Teclas de función en la interfaz Personalizar.



Shortcut Key Mappings	
F1	Check-In
F2	Check-Out
F3	Break-Out
F4	Break-In
F5	Overtime-In

Toque la tecla de acceso directo para configurar.



F1	
Punch State Value	0
Function	Punch State Options
Name	Check-In
Set Switch Time	

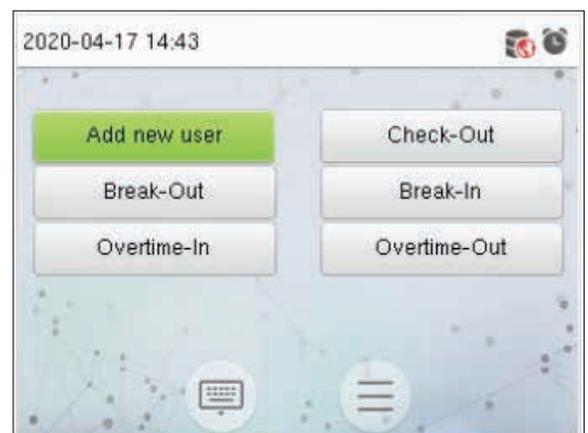
Establezca el valor de estado, la función correspondiente y el nombre de la tecla de estado para esta tecla táctil.



F1	
Punch State Value	6
Function	Punch State Options
Name	Add new user
Set Switch Time	

Toque la interfaz principal para mostrar el menú de acceso directo.

Toque el estado de asistencia para realizar un cambio. Toque la función para acceder rápidamente a la configuración de la función. (Toque F1 Nuevo usuario para acceder rápidamente a este menú).



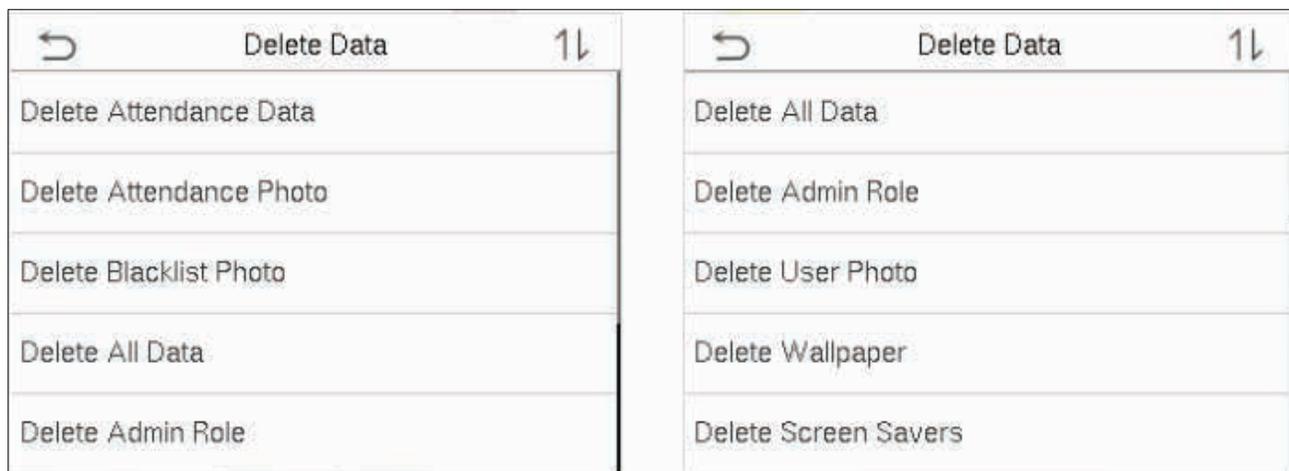
8. Gestión de Datos

Para eliminar los datos relevantes en el dispositivo. Haga clic en Data Mgt. en la interfaz del menú principal.



8.1 Eliminar datos

Haga clic en Borrar Datos en el Administrador de datos.



Menú	Descripción
Eliminar registros de acceso	Eliminar registros de acceso condicionalmente.
Eliminar foto de asistencia	Eliminar las 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 asistencia / registros de acceso de todos los usuarios registrados.
Eliminar función de administrador	Para eliminar los privilegios de administrador.
Eliminar control de acceso	Para borrar todos los datos de acceso.
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.
Borrar Protectores de pantalla	Para eliminar los protectores de pantalla del dispositivo.

Nota: Al eliminar los acceso registros, la asistencia p o t o s, o b l o c k figuran p o t o 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. 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.

Date	User ID	Time
04-17		Number of Records:01
	2	09:47

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

User ID	Name	Time	Mode	State
2	Lily	04-17 09:47	0	0

Verification Mode : Password
Punch State : Add new user

10. Control de Acceso

En el Menú inicial, ingrese al menú de Control de Acceso para configurar los horarios de apertura de puerta.



10.1 Opciones de Control de Acceso

Ingrese a la Opción de Control de Acceso, en la interfaz podrá configurar los parámetros del tiempo del cierre de puertas del dispositivo, el retardo del sensor de puerta, etc.

A screenshot of a mobile application interface for 'Access Control Options'. The header bar has a back arrow icon on the left and the text 'Access Control Options' in the center. Below the header, there are three rows of configuration options. The first row is 'Door Lock Delay (s)' with a value of '10'. The second row is 'Door Sensor Delay (s)' with a value of '10'. The third row is 'Door Sensor Type' with a value of 'Normal Close (NC)'. Below these rows, there is a large empty rectangular area.

Descripción de funciones

Nombre de funciones	Descripción de funciones
Retardo de apertura de puerta	Es el tiempo que el dispositivo puede configurar para controlar el retardo del desbloqueo de una apertura de puerta. Puede configurarse de 1~10 segundos; 0 segundos representa el estado desactivado de esta función. puerta. Puede configurarse de 1~10 segundos; 0 segundos representa el estado desactivado de esta función.
Mascara de subred	Se activa una alarma si la puerta no se cierra en un tiempo definido (Retardo del sensor de puerta). El valor válido de Retardo del sensor de puerta va de 1 a 255 segundos.
Gateway	Hay tres tipos de sensores: Ninguno, Normalmente Abierto y Normalmente Cerrado. Ninguno: Significa que el sensor de la puerta no está en uso. Normalmente Abierto: Significa que la puerta siempre está abierta cuando hay energía eléctrica. Normalmente Cerrado: Significa que la puerta siempre está cerrada cuando la energía eléctrica está encendida.

11. Autotest

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 Autotest en la interfaz del menú principal.

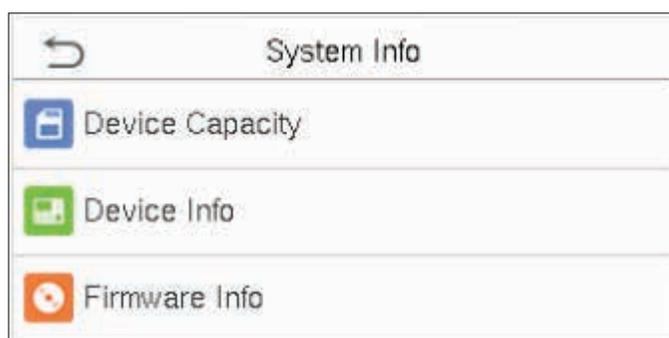


Menú	Descripción
Probar todo	Para probar automáticamente si la pantalla LCD, el audio, la cámara y el RTC son normales.
Probar de LCD	Para probar automáticamente el efecto de visualización de la pantalla LCD mostrando a todo color, blanco puro y negro puro para verificar si la pantalla muestra los colores 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.

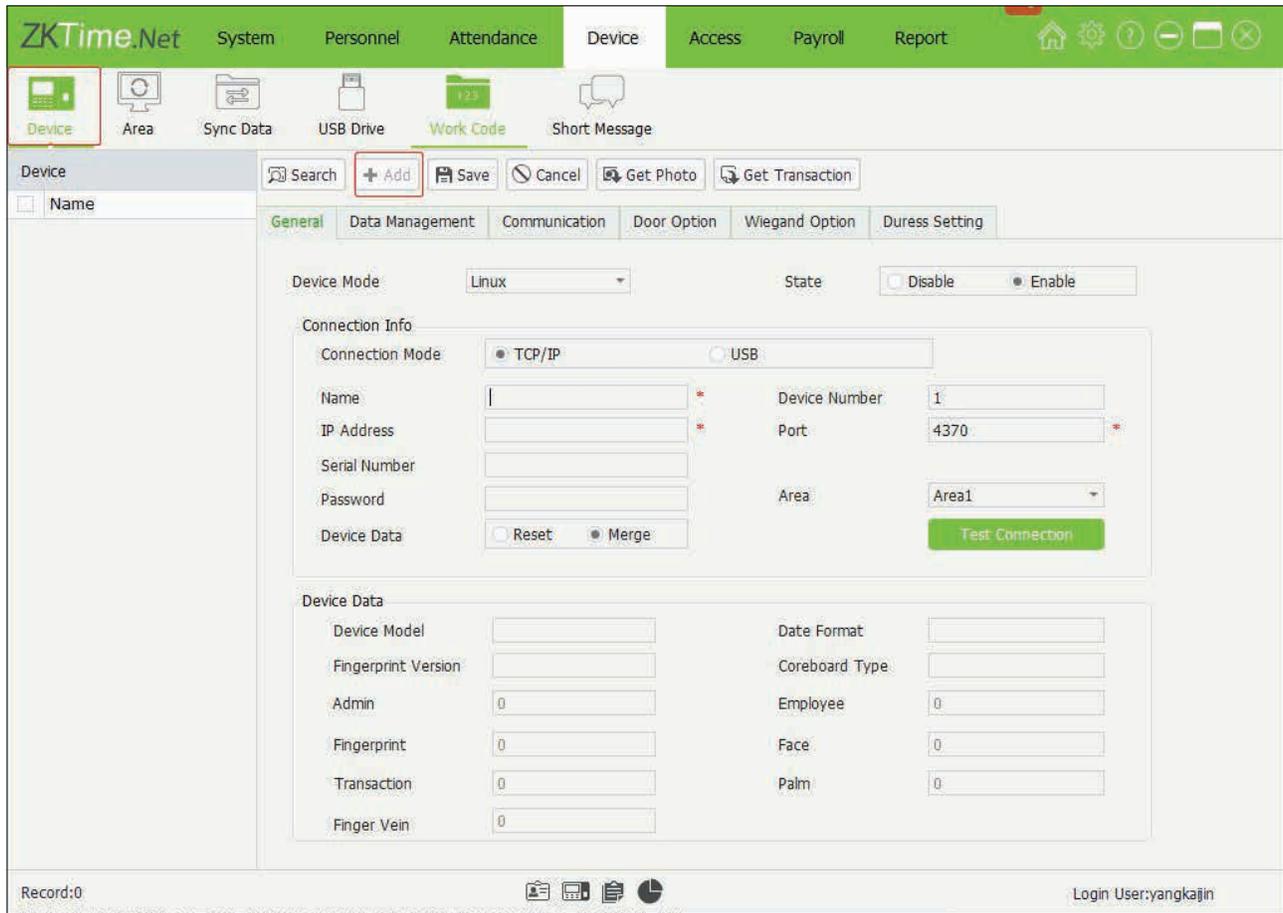


Menú	Descripción
Capacidad del dispositivo	Muestra el espacio de almacenamiento del dispositivo actual , palma, contraseña y la Rostro, los administradores, registros de acceso, asistencia fotos de no permitidos, y fotos de usuario.
Información del dispositivo	Muestra el nombre del dispositivo, el número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

12.1 Agregar biométrico al software

Hay dos métodos para agregar un dispositivo, a saber, Agregar manualmente y Agregar búsqueda LAN.

Agregar biométrico manualmente: Haga clic en el botón Agregar para ingresar a la interfaz Agregar dispositivo, establezca los parámetros según sea necesario. El parámetro con *, significa que no puede estar vacío.



Modo de dispositivo: haga clic en el botón ▼ y luego seleccione el modo de dispositivo (Linux o MT100) en la lista desplegable.

Estado: seleccione Desactivado o Activado según sea necesario.

Cuando el estado es Habilitado, el dispositivo está activo, puede cargar el código de trabajo y de empleado en el dispositivo, o descargar registros de empleados y asistencia desde el dispositivo según sea necesario, etc. realizado

12.2 Información de conexión

Modo de conexión: puede seleccionar TCP / IP o USB según sea necesario.

Nombre: ingrese el nombre para identificar el dispositivo.

Número de serie: se genera automáticamente después de conectar el dispositivo correctamente.

Dirección IP, puerto, contraseña: introduzca la dirección IP, el número de puerto. y Contraseña del dispositivo al que desea conectarse, según corresponda.

Datos del dispositivo: seleccione según sea necesario.

- Restablecer: si se selecciona esta opción (indica seleccionada), los datos del dispositivo prevalecerán y sobrescribirán los datos correspondientes en el software cuando el dispositivo sincronice los datos con el software después de su primera conexión.

- Fusionar: si esta opción está seleccionada (indica seleccionada), los datos se fusionarán de acuerdo con el modo de sincronización de datos seleccionado por el usuario cuando el dispositivo sincronice los datos con el software después de su primera conexión.

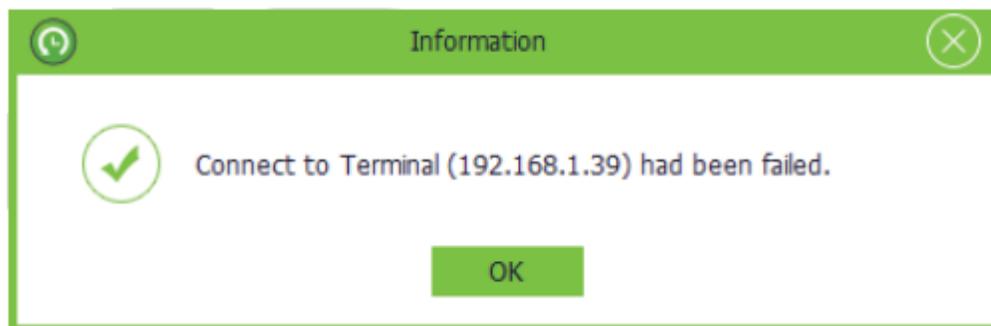
Área: haga clic en el botón ▼ y seleccione el área a la que pertenece el dispositivo. (Nota: un dispositivo solo se puede configurar en un área).

Después de la configuración, haga clic en el botón Probar conexión para verificar si el dispositivo está conectado al sistema. Si la conexión es exitosa, aparecerá el cuadro de Información.



Si falla la conexión, verifique:

- 1) Los parámetros de conexión del dispositivo son consistentes con los parámetros de comunicación en el menú del dispositivo.
- 2) El cable de comunicación está conectado correctamente o existe una red WiFi configurada.



12.3 Datos del dispositivo

Cuando el dispositivo se conecta correctamente al sistema, la información del dispositivo se mostrará automáticamente, incluido el modelo de dispositivo, formato de fecha, modelo de huella digital, tipo de placa base, número de administrador y empleado y recuento de transacciones, huella digital, palma, cara y vena del dedo.

The screenshot shows the 'Device' configuration page in ZKTime.Net. The 'Add' button is highlighted with a red box. The 'Connection Info' section includes fields for Name, IP Address, Serial Number, Password, Device Number, and Port. The 'Device Data' section includes fields for Device Model, Fingerprint Version, Admin, Fingerprint, Transaction, Finger Vein, Date Format, Coreboard Type, Employee, Face, and Palm. A 'Test Connection' button is also highlighted with a red box.

Haga clic en el botón Guardar para guardar la información del dispositivo

12.4 Búsqueda

El software puede detectar el dispositivo fuera de línea en la LAN mediante la búsqueda, lo cual es conveniente para que los usuarios lo agreguen al software.

<input type="checkbox"/>	IP Address	MAC Address
<input type="checkbox"/>	192.168.218.151	00:17:61:10:cc:24
<input type="checkbox"/>	192.168.218.233	00:17:61:10:99:19
<input type="checkbox"/>	192.168.218.241	00:17:61:11:01:80
<input type="checkbox"/>	192.168.218.208	00:17:61:11:6d:bb
<input type="checkbox"/>	0.0.0.0	00:17:61:10:fe:c3
<input type="checkbox"/>	192.168.218.202	00:17:61:12:a8:c4
<input type="checkbox"/>	192.168.218.245	00:17:61:11:CD:41

Buttons: Add, Cancel

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 simultáneamente.
- 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

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 deberán enrollarse 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 $\pm 10^\circ$, la elevación no debe exceder $\pm 10^\circ$ y el ángulo de depresión no debe exceder $\pm 10^\circ$.

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.



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.

Nombre del Componente	Sustancias peligrosas o tóxicas y sus cantidades					
	Sustancia / elemento peligroso / tóxico					
	Plomo (Pb)	Mercurio (Hg)	Cadmio (Cd)	Cromo hexavalente (Cr6 +)	Bifenilos polibromados (PBB)	Éteres de difenilo polibromados (PBDE)
Resistencia	×	○	○	○	○	○
Condensador	×	○	○	○	○	○
Inductor	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
Componente ESD	×	○	○	○	○	○
Buzzer/Bocina	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Tornillos	○	○	○	×	○	○

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

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

Nota: El 80% de los componentes de este producto 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



Derechos de Autor © 2022, ZKTeco CO, LTD. Todos los derechos reservados.
ZKTeco puede, en cualquier momento y sin previo aviso, realizar cambios o mejoras en los productos y servicios o detener su producción o comercialización.
El logo ZKTeco y la marca son propiedad de ZKTeco CO, LTD.